6 Advanced Features and Usage 202

7 Examples 203
   7.1 Hashed ElGamal 203
   7.2 BR93 203

References 204

Index 205
Chapter 1

Getting Started

1.1 Introduction

EASYCRYPT \cite{BDG+:14, BHZ:11} is a framework for interactively finding, constructing, and machine-checking security proofs of cryptographic constructions and protocols using the code-based sequence of games approach \cite{BR:04, BR:06, SH:04}. In EASYCRYPT, cryptographic games and algorithms are modeled as modules, which consist of procedures written in a simple user-extendible imperative language featuring while loops and random sampling operations. Adversaries are modeled by abstract modules—modules whose code is not known and can be quantified over. Modules may be parameterized by abstract modules.

EASYCRYPT has four logics: a probabilistic, relational Hoare logic (pRHL), relating pairs of procedures; a probabilistic Hoare logic (pHL) allowing one to carry out proofs about the probability of a procedure’s execution resulting in a postcondition holding; an ordinary (possibilistic) Hoare logic (HL); and an ambient higher-order logic for proving general mathematical facts and connecting judgments in the other logics. Once lemmas are expressed, proofs are carried out using tactics, logical rules embodying general reasoning principles, and which transform the current lemma (or goal) into zero or more subgoals—sufficient conditions for the original lemma to hold. Simple ambient logic goals may be automatically proved using SMT solvers. Proofs may be structured as sequences of lemmas, and EASYCRYPT’s theories may be used to group together related types, predicates, operators, modules, axioms and lemmas. Theory parameters that may be left abstract when proving its lemmas—types, operators and predicates—may be instantiated via a cloning process, allowing the development of generic proofs that can later be instantiated with concrete parameters.

1.2 Installing EasyCrypt

EASYCRYPT may be found on GitHub.

https://github.com/EasyCrypt/easycrypt

Detailed building instructions for EASYCRYPT and its dependencies and supporting tools can be found in the project’s README file.\footnote{https://github.com/EasyCrypt/easycrypt/blob/1.0/README.md}

1.3 Running EasyCrypt

EASYCRYPT scripts resides in files with the .ec suffix. (As we will see in Chapter 4, EASYCRYPT also has abstract theories, which must be cloned before being used. Such theories reside in files with the .eca suffix.)

To run EASYCRYPT in batch mode, simply invoke it from the shell, giving it an EASYCRYPT script—with suffix .ec—as argument:
CHAPTER 1. GETTING STARTED

easycrypt file.ec

EASYCRYPT will display its progress as it checks the file. Information about EASYCRYPT’s command-line arguments can be found in Chapter 6.

When developing EASYCRYPT scripts, though, EASYCRYPT can be run interactively, as a subprocess of the Emacs text editor. One’s interaction with EASYCRYPT is mediated by Proof General, a generic Emacs front-end for proof assistants. Upon visiting an EASYCRYPT file, the “Proof-General” tab of the Emacs menu may be used execute the file, step-by-step, as well as to undo steps, etc. Information about the “EasyCrypt” menu tab may be found in Chapter 6.

A sample EASYCRYPT script is shown in Listing 1.1.

```plaintext
(* Load (require) the theories Bool and DBool, and import their definitions and lemmas into the environment. Bool defines the exclusive-or operator (^^), and DBool defines the uniform distribution on the booleans \{0,1\}. *)
require import Bool DBool.

(* G1.f() yields a randomly chosen boolean *)
module G1 = {
  proc f() : bool = {
    var x : bool;
    x <$ {0,1}; (* sample x in \{0,1\} *)
    return x;
  }
}.

(* G2.f() yields the exclusive-or of two randomly chosen booleans *)
module G2 = {
  proc f() : bool = {
    var x, y : bool;
    x <$ {0,1}; y <$ {0,1};
    return x ^^ y;
  }
}.

(* PRHL judgement relating G1.f and G2.f. ={res} means res\{1\} = res\{2\}, i.e., the result of G1.f is equal to (has same distribution as) result of G2.f *)
lemma G1_G2_f : equiv[G1.f ~ G2.f : true ==> ={res}].
proof.
  proc.
  (* handle choice of x in G2.f *)
  seq 0 1 : true.
  rnd \{2\}. skip. smt.
  (* handle choice of x in G1.f / y in G2.f *)
  rnd (fun (z : bool) => z ^^ x\{2\}). skip. smt.
qed.

(* G1.f and G2.f are equally likely to return true: *)
lemma G1_G2_true &m :
  Pr[G1.f() @ &m : res] = Pr[G2.f() @ &m : res].
proof.
  byequiv.
  apply G1_G2_f. trivial. trivial.
```
(∗ G1.f and G2.f are equally likely to return false: ∗)

**Lemma** G1_G2_false &m :
Pr[G1.f() @ &m : !res] = Pr[G2.f() @ &m : !res].

**Proof**
byequiv.
apply G1_G2_f. trivial. trivial.
qed.

---

Listing 1.1: Sample EASYCRYPT Script

As can be inferred from the example, comments begin and end with (∗ and ∗), respectively; they may be nested. Each sentence of an EASYCRYPT script is terminated with a dot (period, full stop). Much can be learned by experimenting with this script, and in particular by executing it step-by-step in Emacs.

### 1.4 More Information

More information about EASYCRYPT—and about the EASYCRYPT Team and its work—may be found at

https://www.easycrypt.info

The EASYCRYPT Club mailing list features discussion about EASYCRYPT usage:

https://lists.gforge.inria.fr/mailman/listinfo/easycrypt-club

Support requests should be sent to this list, as answers to questions will be of use to other members of the EASYCRYPT community.

### 1.5 Bug Reporting

EASYCRYPT bugs should be reported using the Tracker:

https://www.easycrypt.info/trac/report

You can log into the Tracker to create tickets or comment on existing ones using any GitHub account.

### 1.6 About this Documentation

The source for this document, along with the macros and language definitions used, are available from its GitHub repository.² Feel free to use the language definitions to typeset your EASYCRYPT-related documents, and to contribute improvements to the macros if you have any.

This document is intended as a reference manual for the EASYCRYPT tool, and not as a tutorial on how to build a cryptographic proof, or how to conduct interactive proofs. We provide some detailed examples in Chapter 7, but they may still seem obscure even with a good understanding of cryptographic theory. We recommend experimenting.

---

²https://github.com/EasyCrypt/easycrypt-doc
Chapter 2

Specifications

In this chapter, we present EASYCRYPT’s language for writing cryptographic specifications. We start by presenting its typed expression language, go on to consider its module language for expressing cryptographic games, and conclude by presenting its ambient logic—which includes judgments of the HL, pHL and pRHL logics.

EASYCRYPT has a typed expression language based on the polymorphic typed lambda calculus. Expressions are guaranteed to terminate, although their values may be under-specified. Its type system has:

- several pre-defined base types;
- product (tuple) and record types;
- user-defined abbreviations for types and parameterized types; and
- user-defined concrete datatypes (like lists and trees).

In its expression language:

- one may use operators imported from the EASYCRYPT library, e.g., for the pre-defined base types;
- user-defined operators may be defined, including by structural recursion on concrete datatypes.

For each type, there is a type of probability distributions over that type.

EASYCRYPT’s modules consist of typed global variables and procedures. The body of a procedure consists of local variable declarations followed by a sequence of statements:

- ordinary assignments;
- random assignments, assigning values chosen from distributions to variables;
- procedure calls, whose results are assigned to variables;
- conditional (if-then-else) statements;
- while loops; and
- return statements (which may only appear at the end of procedures).

A module’s procedures may refer to the global variables of previously declared modules. Modules may be nested. Modules may be parameterized by abstract modules, which may be used to model adversaries; and modules types—or interfaces—may be formalized, describing modules with at least certain specified typed procedures.

EASYCRYPT has four logics: a probabilistic, relational Hoare logic (pRHL), relating pairs of procedures; a probabilistic Hoare logic (pHL) allowing one to carry out proofs about the probability
of a procedure’s execution resulting in a postcondition holding; an ordinary (possibilistic) Hoare logic (HL); and an ambient higher-order logic for proving general mathematical facts, as well as for connecting judgments from the other logics.

Proofs are carried out using tactics, which is the focus of Chapter 3. EasyCrypt also has ways (theories and sections) of structuring specifications and proofs, which will be described in Chapter 4. In Chapter 5, we’ll survey the EasyCrypt Library, which consists of numerous theories, defining mathematical structures (like groups, rings and fields), data structures (like finite sets and maps), and cryptographic constructions (like random oracles and different forms of encryption).

2.1 Lexical Categories

EasyCrypt’s language has a number of lexical categories:

- **Keywords.** EasyCrypt has the following keywords: `abbrev`, `abort`, `abstract`, `admit`, `admitted`, `algebra`, `alias`, `apply`, `as`, `assert`, `assumption`, `async`, `auto`, `axiom`, `axiomatized`, `beta`, `by`, `byequiv`, `byphoare`, `bypr`, `call`, `case`, `cifold`, `change`, `class`, `clear`, `clone`, `congr`, `conseq`, `const`, `cut`, `debug`, `declare`, `delta`, `do`, `done`, `dump`, `eager`, `elif`, `elim`, `else`, `end`, `equiv`, `eta`, `exact`, `exfalso`, `exists`, `expect`, `export`, `fel`, `field`, `fieldeq`, `first`, `fission`, `forall`, `fun`, `fusion`, `glob`, `goal`, `have`, `hint`, `hoare`, `idtac`, `if`, `import`, `in`, `include`, `inductive`, `inline`, `instance`, `iota`, `islossless`, `kill`, `last`, `left`, `lemma`, `let`, `local`, `logic`, `modpath`, `module`, `move`, `nsmmt`, `notation`, `of`, `op`, `phoare`, `pose`, `Pr`, `pr_bounded`, `pragma`, `pred`, `print`, `proc`, `progress`, `proof`, `prover`, `qed`, `roondf`, `roondt`, `realize`, `reflexivity`, `remove`, `rename`, `replace`, `require`, `res`, `return`, `rewrite`, `right`, `ring`, `ringeq`, `rnd`, `rnormal`, `search`, `section`, `Self`, `seq`, `sim`, `simplify`, `skip`, `smt`, `solve`, `sp`, `split`, `splitwhile`, `strict`, `subst`, `suff`, `swap`, `symmetry`, `then`, `theory`, `time`, `timeout`, `Top`, `transitivity`, `trivial`, `try`, `type`, `undo`, `unroll`, `var`, `while`, `why3`, `with`, `wlog`, `wp` and `zeta`.

- **Identifiers.** An identifier is a sequence of letters, digits, underscores (_ ) and apostrophes (’ ) that begins with a letter or underscore, and isn’t equal to an underscore or a keyword other than `abort`, `admitted`, `async`, `dump`, `expect`, `field`, `fieldeq`, `first`, `last`, `left`, `right`, `ring`, `ringeq`, `solve`, `strict` or `wlog`.

- **Operator names.** An operator name is an identifier, a binary operator name, a unary operator name, or a mixfix operator name.

- **Binary operator names.** A binary operator name is:

  - a nonempty sequence of equal signs (=), less than signs (<), greater than signs (>)
  - forward slashes (/), backward slashes (\), plus signs (+), minus signs (-), times signs (*), vertical bars (|), colons (:), ampersands (&), up arrows (^ ) and percent signs (%) or
  - a backtick mark (‘), followed by a nonempty sequence of one of these characters, followed by a backtick mark; or
  - a backward slash followed by a nonempty sequence of letters, digits, underscores and apostrophes.

A binary operator name is an *infix operator name* iff it is surrounded by backticks, or begins with a backslash, or:

- it is neither << nor >>; and
- it doesn’t contain a colon, unless it is a sequence of colons of length at least two; and
- it doesn’t contain =>, except if it is =>; and
- it doesn’t contain !, except if it is !; and
- it doesn’t contain /, except if it is /, /\, or a sequence of slashes of length at least 3.
The precedence hierarchy for infix operators is (from lowest to highest):
- \( \Rightarrow \) (right-associative);
- \( \Leftrightarrow \) (non-associative);
- \( || \) and \( \lor \) (right-associative);
- \( \&\& \) and \( \land \) (right-associative);
- \( = \) and \( <> \) (non-associative);
- \(<\), \(>,<\) and \(>=\) (left-associative);
- \(-\) and \(+\) (left-associative);
- \(*\), and any nonempty combination of \(/\) and \(\%\) (other than \(/\), which is illegal) (left-associative);
- all other infix operators except sequences of colons (left-associative);
- sequences of colons of length at least two (right-associative).

- **Unary operator names.** A unary operator name is a negation sign (\(!\)), a nonempty sequence of plus signs (\(+\)), a nonempty sequence of minus signs (\(-\)), or a backward slash followed by a nonempty sequence of letters, digits, underscores and apostrophes. A prefix operator name is any unary operator name not consisting of either two more plus signs or two or more minus signs.

- **Mixfix operator names.** A mixfix operator name is of the following sequences of characters: \(\_\|\_\), \(\_\[\_\]\), \(\_\_\) or \(\_\_\_\) or \(\_\_\_\). (We’ll see below how they may be used in mixfix form.)

- **Record field projections.** A record field projection is an identifier.

- **Constructor names.** A constructor name is an identifier or a symbolic operator name.

- **Type variables.** A type variable consists of an apostrophe followed by a sequence of letters, digits, underscores and apostrophes that begins with a lowercase letter or underscore, and isn’t equal to an underscore.

- **Type or type operator names.** A type or type operator name is an identifier.

- **Variable names.** A variable name is an identifier that doesn’t begin with an uppercase letter.

- **Procedure names.** A procedure name is an identifier that doesn’t begin with an uppercase letter.

- **Module names.** A module name is an identifier that begins with an uppercase letter.

- **Module type names.** A module type name is an identifier that begins with an uppercase letter.

- **Lemma and axiom names.** A lemma or axiom name is an identifier.

- **Theory names.** A theory name is an identifier that begins with an uppercase letter.

- **Section names.** A section name is an identifier that begins with an uppercase letter.

- **Memory identifiers.** A memory identifier consists an ampersand followed by either a nonempty sequence of digits or an identifier whose initial character isn’t an upper case letter.
2.2 Script Structure, Name spaces, Printing and Searching

An EASYCRYPT script consists of a sequence of steps, terminated by dots (.). Steps may:

- declare types;
- declare operators and predicates;
- declare modules or module types;
- state axioms or lemmas;
- apply tactics;
- require (make available) theories;
- enter or exit theories or sections;
- print types, operators, predicates, modules, module types, axioms and lemmas;
- search for lemmas involving operators.

Operators, predicates, record field projections and type constructors share the same name space. Lemmas and axioms share the same name space.

To print an entity, one may say:

\begin{verbatim}
print type t.
print op f.
print op (+).
print op [-].
print op "_.[.]".
print pred p.
print module Foo.
print module type FOO.
print axiom foo.
print lemma goo.
\end{verbatim}

The entity kind may be omitted, in which case all entities with the given name are printed. `print op` and `print pred` may be used interchangeably, and may be applied to record field projections and datatype constructors, as well as to operators and predicates. `print axiom` and `print lemma` are also interchangeable. Infix operators must be parenthesized; unary operators must be enclosed in square brackets; and mixfix operators must be enclosed in double quotation marks.

To search for axioms and lemmas involving all of a list of operators, one can say

\begin{verbatim}
search f.
search (+).
search [-].
search "_.[.]".
search (+) (-). (* axioms/lemmas involving both operators *)
\end{verbatim}

Declared/stated entities may refer to previously declared/stated entities, but not to themselves or later ones (with the exception of recursively declared operators on datatypes, and to references to a module’s own global variables).

2.3 Expressions Language

2.3.1 Type Expressions

EASYCRYPT’s type expressions are built from type variables, type constructors (or named types) function types and tuple (product) types. Type constructors include built-in types and user-defined types, such as record types and datatypes (or variant types). The syntax of type expressions
\tau, \sigma ::= \text{tyvar} \quad \text{type variable}

\text{-} \quad \text{anonymous type variable}

(\tau) \quad \text{parenthesized type}

\tau \rightarrow \sigma \quad \text{function type}

(\tau_1 * \cdots * \tau_n) \quad \text{tuple type}

tyname \quad \text{named type}

\tau \text{ tyname} \quad \text{applied type constructor}

(\tau_1, \ldots, \tau_n) \text{ tyname} \quad \text{ibid.}

Figure 2.1: EasyCrypt’s type expressions

<table>
<thead>
<tr>
<th>Operator</th>
<th>Associativity</th>
</tr>
</thead>
<tbody>
<tr>
<td>type constructor application</td>
<td>—</td>
</tr>
<tr>
<td>*</td>
<td>tuple constructor</td>
</tr>
<tr>
<td>\rightarrow</td>
<td>function type</td>
</tr>
</tbody>
</table>

constructions with higher precedences come first

Figure 2.2: Type operators precedence and associativity

is given in Figure 2.1, whereas the precedence and associativity of type operators are given in Figure 2.2.

It is worth noting that EasyCrypt’s types must be inhabited — i.e. nonempty.

**Built-in types** EasyCrypt comes with built-in types for booleans (bool), integers (int) and reals (real), along with the singleton type unit that is inhabited by the single element tt (or \( () \)).

In addition, to every type \( t \) is associated the type \( t \text{ distr} \) of (real) discrete sub-distribution. A discrete sub-distribution over a type \( t \) is fully defined by its mass function, i.e. by a non-negative function from \( t \) to \( \mathbb{R} \) s.t. \( \sum_x f(x) \leq 1 \) — implying that \( f \) has a discrete support. When the sum is equal to 1, we say that we have a distribution. Note that distr is not a proper type on its own, but a type constructor, i.e. a function from types to types. A proper type is obtained by applying distr to an actual type, as in int distr or bool distr. See the paragraph on type constructors for more information.

**Function types** The type expression \( \tau \rightarrow \sigma \) denotes the type of total functions mapping elements of type \( \tau \) to elements of type \( \sigma \). Note that \( \rightarrow \) associates to the right, so that int \( \rightarrow \) bool \( \rightarrow \) real and int \( \rightarrow \) (bool \( \rightarrow \) real) denotes the same type.

**Tuple (product) types** The type expression \( \tau_1 * \cdots * \tau_n \) denotes the type of \( n \)-tuples whose elements are resp. of type \( \tau_i \). This includes the type of pairs as well as the type of tuples of 3 elements or more. Note that \( \tau_1 * (\tau_2 * \tau_3) \), \((\tau_1 * \tau_2) * \tau_3 \) and \( \tau_1 * \tau_2 * \tau_3 \) are all distinct types. The first two are pair types, whereas the last one is the type of 3-tuples.

**Type variables** Type variables represent unknown types or type parameters. For example, the type ‘\( a * a \)’ is the type the of pair whose elements are of unknown type ‘\( a \)’. Type variables may be used in type declarations (Section 2.3.2) to define type constructors or in operators/predicates declarations (Section 2.3.3) to define polymorphic operators/predicates. The special type variable _ (underscore) represents a type variable whose name is not specified.

**Type constructors** Type constructors are not type expressions per se, but functions from types to types. As seen in the built-in section, distr is such a type constructor: when applied to the type \( \tau \), it gives the type \( \tau \text{ distr} \) of sub-distributions over \( \tau \). Note that the application is in
**CHAPTER 2. SPECIFICATIONS**

postfix form. One other common type constructors is the one list of polymorphic list, the type expression \( \tau \text{ list} \) denoting the type of lists whose elements are of type \( \tau \).

Type constructors may depend on several type arguments, i.e. may be of arity strictly greater than 1. In that case, the type application is curried. For example, the type of finite map \((\tau, \sigma) \text{ map}\) (whose keys are of type \( \tau \) and values of type \( \sigma \)) is constructed from the type constructor \( \text{map} \) of arity 2.

By abuse of notations, named types (as \( \text{bool} \) or \( \text{int} \)) can be seen as type constructors with no arguments.

**Datatypes and record types** There are no expressions for describing datatypes and record types. Indeed, those are always named and must be defined and named before use. See Section 2.3.2 for how to define variant and record types.

### 2.3.2 Type Declarations

Record types may be declared like this:

```plaintext
type t = { x : int; y : bool; }.
type u = { y : real; yy : int; yyy : real; }.
```

Here \( t \) is the type of records with field projections \( x \) of type \( \text{int} \), and \( y \) of type \( \text{bool} \). The order of projections is irrelevant. Different record types can’t use overlapping projections, and record projections must be disjoint from operators (see below). Records may have any non-zero number of fields; values of type \( u \) are record with three fields. We may also define record type operators, as in:

```plaintext
type 'a t = { x : 'a; f : 'a -> 'a; }.
type ('a, 'b) u = { f : 'a -> 'b; x : 'a; }.
```

Then, a value \( v \) of type \( \text{int t} \) would have fields \( x \) and \( f \) of types \( \text{int} \) and \( \text{int} \rightarrow \text{int} \), respectively; and a value \( v \) of type \( \langle \text{int, bool} \rangle u \) would have fields \( x \) and \( f \) with types \( \text{int} \) and \( \text{int} \rightarrow \text{bool} \), respectively.

Datatypes and datatype operators may be declared like this:

```plaintext
type enum = [ First | Second | Third ].
type either_int_bool = [ First of int | Second of bool ].
type ('a, 'b) either = [ First of 'a | Second of 'b ].
type intlist = [ Nil | Cons of (int * intlist) ].
type 'a list = [ Nil | Cons of 'a & 'a list ].
```

Here, First, Second, Third, Nil and Cons are constructors, and must be distinct from all operators, record projections and other constructors. \( \text{enum} \) is an enumerated type with the three elements \( \text{First, Second and Third} \). The elements of \( \text{either_int_bool} \) consist of \( \text{First} \) applied to an integer, or \( \text{Second} \) applied to a boolean, and the datatype operator \( \text{either} \) is simply its generalization to arbitrary types \( \langle \text{a and b} \rangle \). \( \text{intlist} \) is an inductive datatype: its elements are \( \text{Nil} \) and the results of applying \( \text{Cons} \) to a pairs of the form \( \langle x, ys \rangle \), where \( x \) is an integer and \( ys \) is a previously constructed \( \text{intlist} \). Note that a vertical bar (|) is permitted before the first constructor of a datatype. Finally, \( \text{list} \) is the generalization of \( \text{intlist} \) to lists over an arbitrary type \( \langle \text{a} \rangle \), but with a twist. The use of \& means that \( \text{Cons} \) is “curried”: instead of applying \( \text{Cons} \) to a pair \( \langle x, ys \rangle \), one gives it \( x : \langle \text{a} \rangle \) and \( y s : \langle \text{a list} \rangle \) one at a time, as in \( \text{Cons} x y s \). Unsurprisingly, more than one occurrence of \& is allowed in a constructor’s definition. E.g., here is the datatype for binary trees whose leaves and internal nodes are labeled by integers:

```plaintext
type tree = [ Leaf of int
```
Cons of tree & int & tree

Cons\(tr_1 \times tr_2\) will be the tree constructed from an integer \(x\) and trees \(tr_1\) and \(tr_2\). EasyCrypt must be able to convince itself that a datatype is nonempty, most commonly because it has at least one constructor taking no arguments, or only arguments not involving the datatype.

Types and type operators that are simply abbreviations for pre-existing types may be declared, as in:

\[
\begin{align*}
\text{type } t &= \text{int } \times \text{bool}. \\
\text{type } ('a, b) \text{ arr} &= 'a -> 'b.
\end{align*}
\]

Then, e.g., \((\text{int, bool})\) arr is the same type as \(\text{int} \to \text{bool}\).

Finally, abstract types and type operators may be declared, as in:

\[
\begin{align*}
\text{type } t. \\
\text{type } ('a, b) u. \\
\text{type } t, ('a, b) u.
\end{align*}
\]

We’ll see later how such types and type operators may be used.

2.3.3 Expressions and Operator Declarations

We’ll now survey EasyCrypt’s typed expressions. Anonymous functions are written

\[
\text{fun } (x : t_1) => e,
\]

where \(x\) is an identifier, \(t_1\) is a type, and \(e\) is an expression—probably involving \(x\). If \(e\) has type \(t_2\) under the assumption that \(x\) has type \(t_1\), then the anonymous function will have type \(t_1 \to t_2\). Function application is written using juxtapositioning, so that if \(e_1\) has type \(t_1 \to t_2\), and \(e_2\) has type \(t_1\), then \(e_1 e_2\) has type \(t_2\). Function application associates to the left, and anonymous functions extend as far to the right as possible. EasyCrypt infers the types of the bound variables of anonymous function when it can. Nested anonymous functions may be abbreviated by collecting all their bound variables together. E.g., consider the expression

\[
(\text{fun } (x : \text{int}) => \text{fun } (y : \text{int}) => \text{fun } (z : \text{bool}) => y)\ 0\ 1\ \text{false}
\]

which evaluates to \(1\). It may be abbreviated to

\[
(\text{fun } (x\ y : \text{int, z : bool}) => y)\ 0\ 1\ \text{false}
\]

or

\[
(\text{fun } (x : \text{int}) (y : \text{int}) (z : \text{bool}) => y)\ 0\ 1\ \text{false}
\]

or (letting EasyCrypt carry out type inference)

\[
(\text{fun } x\ y\ z => y)\ 0\ 1\ \text{false}
\]

In the type inference, only the type of \(y\) is determined, but that’s acceptable. EasyCrypt has let expressions

\[
\text{let } x : t = e \text{ in } e
\]

which are equivalent to

\[
(\text{fun } x : t => e)e
\]

As with anonymous expressions, the types of their bound variables may often be omitted, letting EasyCrypt infer them.

An operator may be declared by specifying its type and giving the expression to be evaluated. E.g.,
Here \( f \) is a curried function—it takes its arguments one at a time. Hence \( y \) and \( z \) have the same value: 1. As illustrated by the declaration of \( z \), one may omit the operator’s type when it can be inferred from its expression. The declaration of \( f \) may be abbreviated to

\[
\text{op } f (x : \text{int}) (y : \text{bool}) = x.
\]

or

\[
\text{op } f (x : \text{int}, y : \text{bool}) = x.
\]

Polymorphic operators may be declared, as in

\[
\text{op } g [\text{a, b}] : \text{a} \rightarrow \text{b} \rightarrow \text{a} = \text{fun} (x : \text{a}, y : \text{b}) = x.
\]

or

\[
\text{op } g [\text{a, b}] (x : \text{a}, y : \text{b}) = x.
\]

or

\[
\text{op } g (x : \text{a}, y : \text{b}) = x.
\]

Here \( g \) has all the types formed by substituting types for the types variable \( \text{a} \) and \( \text{b} \) in \( \text{a} \rightarrow \text{b} \rightarrow \text{a} \). This allows us to use \( g \) at different types

\[
\text{op } a = g \text{ true 0}.
\]

\[
\text{op } b = g \text{ 0 false}.
\]

making \( a \) and \( b \) evaluate to \( \text{true} \) and \( 0 \), respectively.

Abstract operators may be declared, i.e., ones whose values are unspecified. E.g., we can declare

\[
\text{op } x : \text{int}.
\]

\[
\text{op } f : \text{int} \rightarrow \text{int}.
\]

\[
\text{op } g [\text{a, b}] : \text{a} \rightarrow \text{b} \rightarrow \text{a}.
\]

Equivalently, \( f \) and \( g \) may be declared like this:

\[
\text{op } f (x : \text{int}) : \text{int}.
\]

\[
\text{op } g [\text{a, b}] (x : \text{a}, y : \text{b}) : \text{a}.
\]

One may declare multiple abstract operators of the same type:

\[
\text{op } f, g : \text{int} \rightarrow \text{int}.
\]

\[
\text{op } g, h [\text{a, b}] : \text{a} \rightarrow \text{b} \rightarrow \text{a}.
\]

We’ll see later how abstract operators may be used.

Binary operators may be declared and used with infix notation (as long as they are infix operators). One parenthesizes a binary operator when declaring it and using it in non-infix form (i.e., as a value). If \( \text{io} \) is an infix operator and \( e_1, e_2 \) are expressions, then \( e_1 \text{ io } e_2 \) is translated to \( (\text{io}) e_1 e_2 \), whenever the latter expression is well-typed. E.g., if we declare

\[
\text{op } (--) [\text{a, b}] (x : \text{a}, y : \text{b}) = x.
\]

\[
\text{op } x : \text{int} = (--) 0 \text{ true}.
\]

\[
\text{op } x' : \text{int} = 0 -- \text{ true}.
\]

\[
\text{op } y : \text{bool} = (--) \text{ true 0}.
\]

\[
\text{op } y' : \text{bool} = \text{true} -- 0.
\]
then \( x \) and \( x' \) evaluate to 0, and \( y \) and \( y' \) evaluate to true.

Unary operators may be declared and used with prefix notation (as long as they are prefix operators). One (square) brackets a unary operator when declaring it and using it in non-prefix form (i.e., as a value). If \( po \) is a prefix operator and \( e \) is an expression, then \( po \, e \) is translated to \( [po \, e] \), whenever the latter expression is well-typed. E.g., if we declare

\[
\begin{align*}
\text{op } x & : \text{int} . \\
\text{op } f & : \text{int} \rightarrow \text{int} . \\
\text{op } [!] & : \text{int} \rightarrow \text{int} . \\
\text{op } y & : \text{int} = ![f \, x] . \\
\end{align*}
\]

then \( y \) and \( y' \) both evaluate to the result of applying the abstract operator \( ![\,] \) of type \( \text{int} \rightarrow \text{int} \) to the result of applying the abstract operator \( f \) of type \( \text{int} \rightarrow \text{int} \) to the abstract value \( x \) of type \( \text{int} \). Function application has higher precedence than prefix operators, which have higher precedence than infix operators, prefix operators group to the right, and infix operators have the associativities and relative precedences that were detailed in Section 2.1.

The four mixfix operators may be declared and used as follows. They are (double) quoted when being declared or used in non-mixfix form (i.e., as values).

- \( ([]) \) is translated to "[". E.g., if we declare

\[
\begin{align*}
\text{op } "[]" & : \text{int} = 3 . \\
\text{op } x & : \text{int} = []. \\
\end{align*}
\]

then \( x \) will evaluate to 3.

- \( (\ |_|) \) If \( e \) is an expression, then \( _| \mid e \) is translated to "\( [_| \mid e \) \), as long as the latter expression is well-typed. E.g., if we declare

\[
\begin{align*}
\text{op } "[|_]" & : \text{int} \rightarrow \text{bool} . \\
\text{op } x & : \text{bool} = "[|_\mid 3]. \\
\text{op } y & : \text{bool} = _{|3]. \\
\end{align*}
\]

then \( y \) will evaluate to the same value as \( x \).

- \( (_\mid [\]) \) If \( e_1, e_2 \) are expressions, then \( _\mid [\, e_2 \) is translated to "\( _\mid [\, e_2 \) \( e_1 \), whenever the latter expression is well-typed. E.g., if we declare

\[
\begin{align*}
\text{op } "[\mid _\]" & : \text{int} \rightarrow \text{int} \rightarrow \text{bool} . \\
\text{op } x & : \text{bool} = "[\mid _\] 3 4 . \\
\text{op } y & : \text{bool} = 3.[4]. \\
\end{align*}
\]

then \( y \) will evaluate to the same value as \( x \).

- \( (_\mid[\mid\leftarrow\mid\]) \) If \( e_1, e_2, e_3 \) are expressions, \( e_1. [e_2 \leftarrow e_3] \) is translated to "\( _\mid[\mid\leftarrow\mid\, e_1 \) \( e_2 \), whenever the latter expression is well-typed. E.g., if we declare

\[
\begin{align*}
\text{op } "[\mid[\mid\leftarrow\mid\]" & : \text{int} \rightarrow \text{int} \rightarrow \text{int} \rightarrow \text{bool} . \\
\text{op } x & : \text{bool} = "[\mid[\mid\leftarrow\mid\] 3 4 5 . \\
\text{op } y & : \text{bool} = 3.[4 \leftarrow 5]. \\
\end{align*}
\]

then \( y \) will evaluate to the same value as \( x \).

In addition, if \( e_1, \ldots , e_n \) are expressions then

\[
[e_1; \ldots ; e_n] \quad \text{is translated to} \quad e_1 : \ldots : e_n : []
\]

whenever the latter expression is well-typed. The initial argument of "\( _\mid[\] \)" and "\( _\mid[\mid\leftarrow\mid\]) \" have higher precedence than even function application. E.g., one can’t omit the parentheses in
Some operators are built-in to EASYCRYPT, automatically understood by its ambient logic:

- \( \text{op } f : \text{int} \rightarrow \text{int} \)
- \( \text{op } y : \text{bool} = (f \ 3) \[4\]. \)
- \( \text{op } z : \text{bool} = (f \ 3) \[4 < -5\]. \)

The operator \( = \) is equality. On the booleans, we have negation \( ! \), two forms of disjunction (\( \lor \) and \( || \)) and conjunction (\( \land \) and \( && \)). The two disjunctions (respectively, conjunctions) are semantically equivalent, but are treated differently by EASYCRYPT proof engine. The associativities and precedences of the infix operators were given in Section 2.1, and (as a prefix operator) \( ! \) has higher precedence than all of them. The expression \( e_1 \leftrightarrow e_2 \) is treated as \( !(e_1 = e_2) \). \( <> \) is not an operator, but it has the precedence and non-associative status of Section 2.1. The intended meaning of \( \text{mu} \ dp \) is the probability that randomly choosing a value of the given type from the sub-distribution \( d \) will satisfy the function \( p \) (in the sense of causing it to return true).

If \( e \) is an expression of type int, then \( e \% r \) is the corresponding real. \( \% r \) has higher precedence than even function application.

If \( e_1 \) is an expression of type bool and \( e_2, e_3 \) are expressions of some type \( t \), then the conditional expression

\[
e_1 \ ? \ e_2 \ : \ e_3
\]

evaluates to \( e_2 \), if \( e_1 \) evaluates to \( \text{true} \), and evaluates to \( e_3 \), if \( e_1 \) evaluates to \( \text{false} \). Conditionals may also be written using if-then-else notation:

\[
\text{if } e_1 \text{ then } e_2 \text{ else } e_3
\]

E.g., if we write

\[
\text{op } x : \text{int} = (3 < 4) \ ? 4 + 7 : (9 - 1).
\]

then \( x \) evaluates to 11. The conditional expression’s precedence at its first argument is lower than function application, but higher than the prefix operators; its second argument needn’t be parenthesized; and the precedence at its third argument is lower than the prefix operators, but higher than the infix operators.

For the built-in types bool, int and real, and the type operator distr, the EASYCRYPT Library (see Chapter 5) provides corresponding theories, Bool, Int, Real and Distr. These theories provide various operations, axioms, etc. To make use of a theory, one must “require” it. E.g.,

\[
\text{require } \text{Bool Int Real Distr.}
\]

will make the theories just mentioned available. This would allow us to write, e.g.,

\[
\text{op } x = \text{Int.}(+) \ 3 \ 4.
\]

making \( x \) evaluate to 7. But to be able to use + and the other operators provided by Int in infix form and without qualification (specifying which theory to find them in), we need to import Int. If we do
import Bool Int Real.

op x : int = 3 + 4 - 7 * 2.
op y : real = 5%r * 3%r / 2%r.
op z : bool = x%r >= y.

we’ll end up with z evaluating to false. One may combine requiring and importing in one step:

require import Bool Int Real Distr.

We’ll cover theories and their usage in detail in Chapter 4.

Requiring the theory Bool makes available the value {0,1} of type bool distr, which is the uniform distribution on the booleans. (No whitespace is allowed in the name for this distribution, and the 0 must come before the 1.) Requiring the theory Distr make available syntax for the uniform distribution of integers from a finite range. If e₁ and e₂ are expressions of type int denoting n₁ and n₂, respectively, then [e₁..e₂] is the value of type int distr that is the uniform distribution on the set of all integers that are greater-than-or-equal to n₁ and less-than-or-equal-to n₂—unless n₁ > n₂, in which case it is the sub-distribution assigning probability 0 to all integers.

Values of product (tuple) and record types are constructed and destructed as follows:

op x : int * int * bool = (3, 4, true).
op b : bool = x.

type t = { u : int; v : bool; }.
op y : t = {| v = false; u = 10; |}.
op a : bool = y.

Then, b evaluates to true, and a evaluates to false. Note the field order in the declaration of y was allowed to be a permutation of that of the record type t.

When we declare a datatype, its constructors are available to us as values. E.g, if we declare

```plaintext
type ('a, 'b) either = [Fst of 'a | Snd of 'b].
op x : (int, bool) either = Fst 10.
op y : int -> (int, bool) either = Fst.
op z : (int, bool) either = y 10.
```

then z evaluates to the same result as x.

We can declare operators using pattern matching on the constructors of datatypes. E.g., continuing the previous example, we can declare and use an operator fst by:

```plaintext
op fst ['a, 'b] (def : 'a) (ei : ('a, 'b) either) : 'a =
    with ei = Fst a => a
    with ei = Snd b => def.

op l1 : (int, bool) either = Fst 10.
op l2 : (int, bool) either = Snd true.
op m1 : int = fst (-1) l1.
op m2 : int = fst (-1) l2.
```

Here, m₁ will evaluate to 10, whereas m₂ will evaluate to -1. Such operator declarations may be recursive, as long as EASYCRYPT can determine that the recursion is well-founded. E.g., here is one way of declaring an operator length that computes the length of a list:

```plaintext
type 'a list = [Nil | Cons of 'a & 'a list].
op len ['a] (acc : int, xs : 'a list) : int =
    with xs = Nil => acc
    with xs = Cons y ys => len (acc + 1) ys.

op length ['a] (xs : 'a list) = len 0 xs.
op xs = Cons 0 (Cons 1 (Cons 2 Nil)).
op n : int = length xs.
```

Then n will evaluate to 3.
2.4 Module System

2.4.1 Modules

EASYCRYPT’s modules consist of typed global variables and procedures, which have different name spaces. Listing 2.1 contains the definition of a simple module, M, which exemplifies much of the module language.

```
require import Int Bool DInterval.

module M = {
  var x : int

  proc init(bnd : int) : unit = {
    x <$ [-bnd .. bnd];
  }

  proc incr(n : int) : unit = {
    x <- x + n;
  }

  proc get() : int = {
    return x;
  }

  proc main() : bool = {
    var n : int;
    init(100);
    incr(10); incr(-50);
    n @$ get();
    return n < 0;
  }
}.
```

Listing 2.1: Simple Module

M has one global variable—x—which is used by the procedures of M—init, incr, get and main. Global variables must be declared before the procedures that use them.

The procedure init (“initialize”) has a parameter (or argument) bnd (“bound”) of type int. init uses a random assignment to assign to x an integer chosen uniformly from the integers whose absolute values are at most bnd. The return type of init is unit, whose only element is tt; this is implicitly returned by init upon exit.

The procedure incr (“increment”), increments the value of x by its parameter n. The procedure get takes no parameters, but simply returns the value of x, using a return statement—which is only allowed as the final statement of a procedure.

And the main procedures takes no parameters, and returns a boolean that’s computed as follows:

- It declares a local variable, n, of type int—local in the sense that other procedures can’t access or affect it.
- It uses a procedure call to call the procedure init with a bound of 100, causing x to be initialized to an integer between -100 and 100.
- It calls incr twice, with 10 and then -50.
- It uses a procedure call assignment to call the procedure get with no arguments, and assign get’s return value to n.
- It evaluates the boolean expression n < 0, and returns the value of this expression as its boolean result.
EASYCRYPT tries to infer the return types of procedures and the types of parameters and local variables. E.g., our example module could be written

```plaintext
module M = {
  var x : int
  proc init(bnd) = {
    x <$ [-bnd .. bnd];
  }
  proc incr(n) = {
    x <- x + n;
  }
  proc get() = {
    return x;
  }
  proc main() = {
    var n;
    init(100);
    incr(10); incr(-50);
    n <$@ get();
    return n < 0;
  }
}.
```

Listing 2.2: Simple Module with Type Inference

As we’ve seen, each declaration or statement of a procedure is terminated with a semicolon. One may combine multiple local variable declarations, as in:

```plaintext
var x, y, z : int;
var u, v;
var x, y, z : int <- 10;
var x, y, z <- 10;
```

Procedure parameters are variables; they may be modified during the execution of their procedures. A procedure’s parameters and local variables must be distinct variable names. The three kinds of assignment statements differ according to their allowed right-hand sides (rhs):

- The rhs of a random assignment must be a single (sub-)distribution. When choosing from a proper sub-distribution, the random assignment may fail, causing the procedure call that invoked it to fail to terminate.
- The rhs of an ordinary assignment may be an arbitrary expression (which doesn’t include use of procedures).
- The rhs of a procedure call assignment must be a single procedure call.

If the rhs of an assignment produces a tuple value, its left-hand side may use pattern matching, as in

```plaintext
(x, y, z) <- ...;
```

in the case where ... produces a triple.

The two remaining kinds of statements are illustrated in Listing 2.3: conditionals and while loops.

```plaintext
require import Bool Int DInterval.

module N = {
```
proc loop() : int = {
  var y, z : int;
  y <- 0;
  while (y < 10) {
    z <$> [1 .. 10];
    if (z <= 5) {
      y <- y - z;
    } else {
      y <- y + (z - 5);
    }
  }
  return y;
}

Listing 2.3: Conditionals and While Loops

N has a single procedure, loop, which begins by initializing a local variable y to 0. It then enters a while loop, which continues executing until (which may never happen) y becomes 10 or more. At each iteration of the while loop, an integer between 1 and 10 is randomly chosen and assigned to the local variable z. The conditional is used to behave differently depending upon whether the value of z is less-than-or-equal-to 5 or not.

- When the answer is “yes”, y is decremented by z.
- When the answer is “no”, y is incremented by z - 5.

Once (if) the while loop is exited—which means y is now 10 or more—the procedure returns y’s value as its return value.

When the body of a while loop, or the then or else part of a conditional, has a single statement, the curly braces may be omitted. E.g., the conditional of the preceding example could be written:

if (z <= 5) y <- y - z;
else y <- y + (z - 5);

As illustrated in Listing 2.4, modules may access the global variables, and call the procedures, of previously declared modules.

require import Bool Int.

module M = {
  var x : int
  proc f() : unit = {
    x <- x + 1;
  }
}.

module N = {
  var x : int
  proc g(n m : int, b : bool) : bool = {
    if (b) M.f();
    M.x <- M.x + x + n - m;
    return 0 < M.x;
  }
}.
CHAPTER 2. SPECIFICATIONS

```
proc h = M.f 
```

Listing 2.4: One Module Using Another Module

Procedure $g$ of $N$ both accesses the global variable $x$ of module $M$ ($M.x$), and calls $M$’s procedure, $f$ ($M.f$). The parameter list of $g$ could equivalently be written:

```
n : int, m : int, b : bool
```

A module may refer to its own global variables using its own module name, allowing us to write

```
proc f() : unit = {
  M.x <- M.x + 1;
}
```

for the definition of procedure $M.f$. The procedure $h$ of $N$ is an alias for procedure $M.f$: calling it is equivalent to directly calling $M.f$. One declare a module name to be an alias for a module, as in

```
module L = N.
```

A procedure call is carried out in the context of a *memory* recording the values of all global variables of all declared modules. So all global variables are—by definition—initialized. On the other hand, the local variables of a procedure start out as arbitrary values of their types. This is modeled in EASycrypt’s program logics by our not knowing anything about them. For example, the probability of $X.f()$

```
module X = {
  proc f() : bool = {
    var b : bool;
    return b;
  }
}. 
```

returning true is undefined—we can’t prove anything about it. On the other hand, just because a local variable isn’t initialized before use doesn’t mean the result of its use will be indeterminate, as illustrated by the procedure $Y.f$, which always returns 0:

```
module Y = {
  proc f() : int = {
    var x : int;
    return x - x;
  }
}. 
```

2.4.2 Module Types

EASYCrypt’s *module types* specify the types of a set of procedures. E.g., consider the module type $\text{OR}$:

```
module type OR = {
  proc init(secret : int, tries : int) : unit 
  proc guess(guess : int) : unit 
  proc guessed() : bool 
}. 
```

$\text{OR}$ describes minimum expectations for a “guessing oracle”—that it provide at least procedures with the specified types. The order of the procedures in a module type is irrelevant. In a procedure’s type, one may combine multiple parameters of the same type, as in:

```
proc init(secret tries : int) : unit 
```
The names of procedure parameters used in module types are purely for documentation purposes; one may elide them instead using underscores, writing, e.g.,

\[
\text{proc init(_ : int, _ : int) : unit}
\]

Note that module types say nothing about the global variables a module should have. Modules types have a different name space than modules.

Listing 2.5 contains an example guessing oracle implementation.

\[
\text{module Or = }
\]

\[
\text{var sec : int}
\]

\[
\text{var tris : int}
\]

\[
\text{var guessed : bool}
\]

\[
\text{proc init(secret, tries : int) : unit = }
\]

\[
\text{sec} \leftarrow \text{secret};
\]

\[
\text{tris} \leftarrow \text{tries};
\]

\[
\text{guessed} \leftarrow \text{false};
\]

\[
\]

\[
\text{proc guess(guess : int) : unit = }
\]

\[
\text{if } (0 < \text{tris}) \{ 
\text{guessed} \leftarrow \text{guessed} \lor (\text{guess} = \text{sec});
\text{tris} \leftarrow \text{tris} - 1;
\}
\]

\[
\}
\]

\[
\text{proc guessed() : bool = }
\]

\[
\text{return} \text{guessed};
\]

\[
\}
\]

Listing 2.5: Guessing Oracle Module

Its \text{init} procedure stores the supplied secret in the global variable \text{sec}, initializes the allowed number of guesses in the global variable \text{tris}, and initializes the \text{guessed} global variable to record that the secret hasn’t yet been guessed. If more allowed tries remain, the \text{guess} procedure updates \text{guessed} to take into account the supplied guess, and decrements the allowed number of tries; otherwise, it does nothing. And its \text{guessed} procedure returns the value of \text{guessed}, indicating whether the secret has been successfully guessed, so far. \text{Or} satisfies the specification of the module type \text{OR}, and we can ask \text{EASYCRYPT} to check this by supplying that module type when declaring \text{Or}, as in Listing 2.6.

\[
\text{module Or : OR = }
\]

\[
\text{var sec : int}
\]

\[
\text{var tris : int}
\]

\[
\text{var guessed : bool}
\]

\[
\text{proc init(secret, tries : int) : unit = }
\]

\[
\text{sec} \leftarrow \text{secret};
\]

\[
\text{tris} \leftarrow \text{tries};
\]

\[
\text{guessed} \leftarrow \text{false};
\]

\[
\]

\[
\text{proc guess(guess : int) : unit = }
\]

\[
\text{if } (0 < \text{tris}) \{ 
\text{guessed} \leftarrow \text{guessed} \lor (\text{guess} = \text{sec});
\text{tris} \leftarrow \text{tris} - 1;
\}
\]

\[
\}
\]

\[
\]}.
\begin{verbatim}
proc guessed() : bool = {
  return guessed;
}
\end{verbatim}

Listing 2.6: Guessing Oracle Module with Module Type Check

Supplying a module type \textit{doesn't} change the result of a module declaration. E.g., if we had omitted \texttt{guessed} from the module type \texttt{OR}, the module \texttt{Or} would still have had the procedure \texttt{guessed}. Furthermore, when declaring a module, we can ask \textsc{EasyCrypt} to check whether it satisfies multiple module types, as in:

\begin{verbatim}
module type A = { proc f() : unit }.
module type B = { proc g() : unit }.
module X : A, B = {
  var x, y : int
  proc f() : unit = { x <- x + 1; }
  proc g() : unit = { y <- y + 1; }
}.
\end{verbatim}

When declaring a module alias, one may ask \textsc{EasyCrypt} to check that the module matches a module type, as in:

\begin{verbatim}
module X' : A, B = X.
\end{verbatim}

Suppose we want to declare a cryptographic game using our guessing oracle, parameterized by an adversary with access to the \texttt{guess} procedure of the oracle, and which provides two procedures—one for choosing the range in which the guessing game will operate, and one for doing the guessing. We’d like to write something like:

\begin{verbatim}
module type GAME = {
  proc main() : bool
}.
module Game(Adv : ADV) : GAME = {
  module A = Adv(Or)
  proc main() : bool = { ... }
}.
\end{verbatim}

Thus, the module type \texttt{ADV} for adversaries must be parameterized by an implementation of \texttt{OR}. Given the adversary procedures we have in mind, the syntax for this is

\begin{verbatim}
module type ADV(O : OR) = {
  proc chooseRange() : int * int
  proc doGuessing() : unit {O.guess}
}.
\end{verbatim}

But this declaration would give the adversary access to all of \texttt{O}'s procedures, which isn't what we want. Instead, we can write

\begin{verbatim}
module type ADV(O : OR) = {
  proc chooseRange() : int * int {}
  proc doGuessing() : unit {O.guess}
}.
\end{verbatim}

meaning that \texttt{chooseRange} has no access to the oracle, and \texttt{doGuessing} may only call its \texttt{guess} procedure. Using this notation, our original attempt would have to be written

\begin{verbatim}
module type ADV(O : OR) = {
  proc chooseRange() : int * int {O.init O.guess O.guessed}
  proc doGuessing() : unit {O.init O.guess O.guessed}
}.
\end{verbatim}
Finally, we can specify that chooseRange must initialize all of the adversary’s global variables (if any) by using a star annotation:

```
module type ADV(O : OR) = {
  proc * chooseRange() : int * int {}
  proc doGuessing() : unit {O.guess}
}.
```

The enforcement of such checks is not carried out by EASYCRYPT’s type checker, but by its logic (see the apply (p. 60) and rewrite (p. 62) tactics).

The full Guessing Game example is contained in Listing 2.7.

```
require import Bool Int IntDiv DInterval.

module type OR = {
  proc init(secret tries : int) : unit
  proc guess(guess : int) : unit
  proc guessed() : bool
}.

module Or : OR = {
  var sec : int
  var tris : int
  var guessed : bool

  proc init(secret tries : int) : unit = {
    sec <- secret;
    tris <- tries;
    guessed <- false;
  }

  proc guess(guess : int) : unit = {
    if (0 < tris) {
      guessed <- guessed \/ (guess = sec);
      tris <- tris - 1;
    }
  }

  proc guessed() : bool = {
    return guessed;
  }
}.

module type ADV(O : OR) = {
  proc * chooseRange() : int * int {}
  proc doGuessing() : unit {O.guess}
}.

module (SimpAdv : ADV) (O : OR) = {
  var range : int * int
  var tries : int

  proc chooseRange() : int * int = {
    range <- (1, 100);
    tries <- 10;
    return range;
  }

  proc doGuessing() : unit = {
    var x : int;
    while (0 < tries) {
```
module type GAME = {
  proc main() : bool
}.

module Game(Adv : ADV) : GAME = {
  module A = Adv(Or)
  proc main() : bool = {
    var low, high, tries, secret : int;
    var advWon : bool;
    (low, high) <$> A.chooseRange();
    if (high - low < 10)
      advWon <$> false;
    else {
      tries <- (high - low + 1) % 10; (* /% is integer division *)
      secret <$> [low .. high];
      Or.init(secret, tries);
      A.doGuessing();
      advWon <$> Or.guessed();
    }
    return advWon;
  }
}.

module SimpGame : GAME = Game(SimpAdv).

Listing 2.7: Full Guessing Game Example

SimpAdv is a simple implementation of an adversary. The inclusion of the constraint SimpAdv : ADV in SimpAdv’s declaration

makes EASYCRYPT check that SimpAdv implements the module type ADV: its implementation of chooseRange doesn’t use O at all; its implementation of doGuessing doesn’t use any of O’s procedures other than guess; and that chooseRange initializes SimpAdv’s global variables. Its chooseRange procedure chooses the range of 1 to 100, and initializes global variables recording this range and the number of guesses it will make (see the code of Game to see why 10 is a sensible choice). The doGuessing procedure makes 10 random guesses. It would be legal for the parameter O in SimpAdv’s definition to be constrained to match a module type T providing a proper subset of Or’s procedures, but that would further limit what procedures of O SimpAdv’s procedures could call. On the other hand, it would be illegal for T to provide procedures not in Or.

Despite SimpAdv being a parameterized module, to refer to one of its global variables from another module one ignores the parameter, saying, e.g.,

module X = {
  proc f() : int = {
    return SimpAdv.tries;
  }
}.

On the other hand, to call one of SimpAdv’s procedures, one needs to specify which oracle parameter it will use, as in:
The module `X` defines a function `f` that calls the `doGuessing` procedure of the `SimpAdv(Or)` module.

The module `Game` gives its adversary parameter, `Adv`, the concrete guessing oracle `Or`, calling the resulting module `A`. Its main function then uses `Or` and `A` to run the game.

- It calls `A`’s `chooseRange` procedure to get the adversary’s choice of guessing range. If the range doesn’t have at least ten elements, it returns `false` without doing anything else—the adversary has supplied a range that’s too small.
- Otherwise, it uses `Or.init` to initialize the guessing oracle with a secret that’s randomly chosen from the range, plus a number of allowed guesses that’s one tenth of the range’s size.
- It then calls `A.doGuessing`, allowing the adversary to attempt the guess the secret.
- Finally, it calls `Or.guessed` to learn whether the adversary has guessed the secret, returning this boolean value as its result.

Finally, the declaration

```
module SimpGame = Game(SimpAdv).
```

declares `SimpGame` to be the specialization of `Game` to our simple adversary, `SimpAdv`. When processing this declaration, EASYCRYPT’s type checker verifies that `SimpAdv` satisfies the specification ADV. The reader might be wondering what—if anything—prevents us writing a version of `SimpAdv` that directly accesses/calls the global variables and procedures of `Or` (or of `Game`, were `SimpAdv` declared after it), violating our understanding of the adversary’s power. The answer is that EASYCRYPT’s type checker isn’t in a position to do this. Instead, we’ll see in the next section how such constraints are modeled using EASYCRYPT’s logic.

### 2.4.3 Global Variables

The set of all global variables of a module `M` is the union of

- the set of global variables that are declared in `M`; and
- the set of all that global variables declared in other modules such that the variables could be read or written by a series of procedure calls beginning with a call of one of `M`’s procedures. By “could” we mean the read/write analysis assumes the execution of both branches of conditionals, the execution of while loop bodies, and the terminal of while loops.

To print the global variables of a module `M`, one runs:

```
print glob M.
```

For example, suppose we make these declarations:

```
module Y1 = {
  var y, z : int
  proc f() : unit = { y <- 0; }
  proc g() : unit = { }
}. module Y2 = {
  var y : int
  proc f() : unit = { Y1.f(); }
}
module Y3 = {
  var y : int
```

```
Then: the set of global variables of \( Y_1 \) consists of \( Y_1.y \) and \( Y_1.z \); the set of global variables of \( Y_2 \) consists of \( Y_1.y \) and \( Y_2.y \); the set of global variables of \( Y_3 \) consists of \( Y_3.y \); the set of global variables of \( Z \) consists of \( Z.y \); and the set of global variables of \( Z(Y_1) \) consists of \( Z.y \) and \( Y_1.y \). In the case of \( Z \), because its parameter \( X \) is abstract, no global variables are obtained from \( X \).

For every module \( M \), there is a corresponding type, \( \text{glob } M \), where a value of type \( \text{glob } M \) is a tuple consisting of a value for each of the global variables of \( M \). Nothing can be done with values of such types other than compare them for equality.

### 2.5 Logics

#### 2.5.1 Formulas

The formulas of EasyCrypt’s ambient logic are formed by adding to EasyCrypt’s expressions

- universal and existential quantification,
- application of built-in and user-defined predicates,
- probability expressions and lossless assertions, and
- \( \text{HL}, \text{pHL} \) and \( \text{pRHL} \) judgments,

and identifying the formulas with the extended expressions of type \( \text{bool} \). This means we automatically have all boolean operators as operators on formulas, with their normal precedences and associativities, including negation

\[
\begin{align*}
\text{op } [!] : \text{bool} &\to \text{bool}. \\
\text{the two semantically equivalent disjunctions} \\
\text{op } (||) : \text{bool} &\to \text{bool} \to \text{bool}. \\
\text{op } (\lor) : \text{bool} &\to \text{bool} \to \text{bool}. \\
\text{the two semantically equivalent conjunctions} \\
\text{op } (\&\&) : \text{bool} &\to \text{bool} \to \text{bool}. \\
\text{op } (\land) : \text{bool} &\to \text{bool} \to \text{bool}. \\
\text{implication} \\
\text{op } (\Rightarrow) : \text{bool} &\to \text{bool} \to \text{bool}. \\
\text{and if-and-only-if} \\
\text{op } (\Leftrightarrow) : \text{bool} &\to \text{bool} \to \text{bool}.
\end{align*}
\]

The quantifiers’ bound identifiers are typed, although EasyCrypt will attempt to infer their types if they are omitted. Universal and existential quantification are written as

\[
\text{forall } (x : t), \phi
\]

and
exists \( (x : t), \phi \)

respectively, where the formula \( \phi \) typically involves the identifier \( x \) of type \( t \). We can abbreviate nested universal or existential quantification in the style of nested anonymous functions, writing, e.g.,

\[
\begin{align*}
&\text{forall } (x : \text{int}, y : \text{int}, z : \text{bool}), \ldots \\
&\text{forall } (x y : \text{int}, z : \text{bool}), \ldots \\
&\text{exists } (x : \text{int}, y : \text{int}, z : \text{bool}), \ldots \\
&\text{exists } (x y : \text{int}, z : \text{bool}), \ldots \\
&\text{exists } (x y : \text{int}) (z : \text{bool}), \ldots
\end{align*}
\]

Quantification extends as far to the right as possible, i.e., has lower precedence than the binary operations on formulas.

Abstract predicates may be defined as in:

\[
\begin{align*}
&\text{pred } P_0. \\
&\text{pred } P_1 : \text{int}. \\
&\text{pred } P_2 : \text{int} \& (\text{int} * \text{bool}). \\
&\text{pred } P_3 : \text{int} \& (\text{int} * \text{bool}) \& (\text{real} \rightarrow \text{int}).
\end{align*}
\]

\( P_0, P_1, P_2 \) and \( P_3 \) are extended expressions of types \( \text{bool}, \text{int} \rightarrow \text{bool}, \text{int} \rightarrow \text{int} \& \text{bool} \rightarrow \text{bool} \) and \( \text{int} \rightarrow \text{int} \& \text{bool} \rightarrow (\text{real} \rightarrow \text{int}) \rightarrow \text{bool} \), respectively. The parentheses are mandatory in \( (\text{int} \& \text{bool}) \) and \( (\text{real} \rightarrow \text{int}) \). Thus, if \( e_1, e_2 \) and \( e_3 \) are extended expressions of types \( \text{int}, \text{int} \& \text{bool} \) and \( \text{real} \rightarrow \text{int} \), respectively, then \( P_0, P_1 e_1, P_2 e_1 e_2 \) and \( P_3 e_1 e_2 e_3 \) are formulas.

Concrete predicates are defined in a way that is similar to how operators are declared. E.g., if we declare

\[
\begin{align*}
&\text{pred } Q (x y : \text{int}, z : \text{bool}) = x = y \& z.
\end{align*}
\]

or

\[
\begin{align*}
&\text{pred } Q (x : \text{int}) (y : \text{int}) (z : \text{bool}) = x = y \& z.
\end{align*}
\]

then \( Q \) is an extended expression of type

\[
\begin{align*}
&\text{int} \rightarrow \text{int} \rightarrow \text{bool} \rightarrow \text{bool}
\end{align*}
\]

meaning that, e.g.,

\[
(\text{fun } (b : \text{bool} \rightarrow \text{bool}) \Rightarrow b \text{ true}) \ (Q \ 3 \ 4)
\]

is a formula. And here is how polymorphic predicates may be defined:

\[
\begin{align*}
&\text{pred } R \ ['a', 'b'] : (\ 'a', \ 'a \ast \ 'b'). \\
&\text{pred } R' \ ['a', 'b'] (x : \ 'a, y : \ 'a \ast \ 'b) = (y \cdot 1 = x).
\end{align*}
\]

Extended expressions also include program memories, although there isn’t a type of memories, and anonymous functions and operators can’t take memories as inputs. If \( \&m \) is a memory and \( x \) is a program variable that’s in \( \&m \)’s domain, then \( x\{m\} \) is the extended expression for the value of \( x \) in \( \&m \). Quantification over memories is allowed:

\[
\begin{align*}
&\text{forall } \&m, \phi
\end{align*}
\]

Here, \( \&m \) ranges over all memories with domains equal to the set of all variables declared as global in currently declared modules. E.g., suppose we have declared:

\[
\begin{align*}
&\text{module } X = \{ \text{var } x : \text{int} \}. \\
&\text{module } Y = \{ \text{var } y : \text{int} \}.
\end{align*}
\]

Then, this is a (true) formula:
forall \&m, X.x{m} < Y.y{m} => X.x{m} + 1 <= Y.y{m}

EASYCRIPT’s logics can introduce memories whose domains include not just the global variables of modules but also:

- the local variables and parameters of procedures; and
- res, whose value in a memory resulting from running a procedure will record the result (return value) of the procedure.

There is no way for the user to introduce such memories directly. We can’t do anything with memories other than look up the values of variables in them. In particular, formulas can’t test or assert the equality of memories.

If \( M \) is a module and \( \&m \) is a memory, then \((\text{glob}\,M)(m)\) is the value of type \( \text{glob}\,M \) consisting of the tuple whose components are the values of all the global variables of \( M \) in \( \&m \).

(See Subsection 2.4.3 for the definition of the set of all global variables of a module.)

For convenience, we have the following derived syntax for formulas: If \( \phi \) is a formula and \( \&m \) is a memory, then \( \phi\{m\} \) means the formula in which every subterm \( u \) of \( \phi \) consisting of a variable or res or glob\,\(M\), for a module \( M \), is replaced by \( u\{m\} \). For example,

\[
(Y1.y = Y1.z \Rightarrow Y1.z = Y1.y)(m)
\]

expands to

\[
Y1.y(m) = Y1.z(m) \Rightarrow Y1.z(m) = Y1.y(m)
\]

The parentheses are necessary, because \( \{m\} \) has higher precedence than even function application. We say that \( \&m \) satisfies \( \phi \) iff \( \phi\{m\} \) holds.

Extended expressions also include modules, although there isn’t a type of modules, and anonymous functions and operators can’t take modules as inputs. Quantification over modules is allowed. If \( T \) is a module type, and \( M \) is a module name, then

\[
\forall (M <: T), \phi
\]

means

for all modules \( M \) satisfying \( T \), \( \phi \) holds.

Formulas can’t talk about module equality.

There is also a variant form of module quantification of the the form

\[
\forall (M <: T(N_1, \ldots, N_l)), \phi
\]

where \( N_1, \ldots, N_l \) are modules, for \( l \geq 1 \). Its meaning is

for all modules \( M \) satisfying \( T \) whose sets of global variables are disjoint from the sets of global variables of the \( N_i \), \( \phi \) holds.

Finally, EASYCRIPT’s ambient logic has probability expressions, HL, pHL and pRHL judgments, and lossless assertions:

- **(Probability Expressions)** A probability expression has the form

  \[
  \Pr[M, p(e_1, \ldots, e_n) \otimes \&m : \phi]
  \]

  where:

  - \( p \) is a procedure of module \( M \) that takes \( n \) arguments, whose types agree with the types of the \( e_i \);
  - \( \&m \) is a memory whose domain is the global variables of all declared modules;
– the formula $\phi$ may involve the term $\text{res}$, whose type is $M.p$’s return type, as well as global variables of modules.

Occurrences in $\phi$ of bound identifiers (bound outside the probability expression) whose names conflict with parameters and local variables of $M.p$ will refer to the bound identifiers, not the parameters/local variables.

The informal meaning of the probability expression is the probability that running $M.p$ with arguments $e_1, \ldots, e_n$, and initial memory $\&m$ will terminate in a final memory satisfying $\phi$. To run $M.p$:

– $\&m$ is extended to map $M.p$’s parameters to the $e_i$, and to map the procedure’s local variables to arbitrary initial values;
– the body of the procedure is run in this extended memory;
– if the procedure returns, its return value will be stored in a component $\text{res}$ of the resulting memory, and the procedure’s parameters and local variables will be removed from that memory.

If the procedure doesn’t initialize its local variables before using them, the probability expression may be undefined.

• (HL Judgments) A HL judgment has the form

\[
\text{hoare}(M.p : \phi \Rightarrow \psi)
\]

where:

– $p$ is a procedure of module $M$;
– the formula $\phi$ may involve the global variables of declared modules, as well as the parameters of $M.p$;
– the formula $\psi$ may involve the term $\text{res}$, whose type is $M.p$’s return type, as well as the global variables of declared modules.

Occurrences in $\phi$ and $\psi$ of bound identifiers (bound outside the judgment) whose names conflict with parameters and local variables of $M.p$ will refer to the bound identifiers, not the parameters/local variables.

The informal meaning of the HL judgment is that, for all initial memories $\&m$ satisfying $\phi$ and whose domains consist of the global variables of declared modules plus the parameters and local variables of $M.p$, if running the body of $M.p$ in $\&m$ results in termination with a memory, the restriction of that memory to $\text{res}$ and the global variables of declared modules satisfies $\psi$.

• (pHL Judgments) A pHL judgment has one of the forms

\[
\text{phoare} [M.p : \phi \Rightarrow \psi] < e \\
\text{phoare} [M.p : \phi \Rightarrow \psi] = e \\
\text{phoare} [M.p : \phi \Rightarrow \psi] > e
\]

where:

– $p$ is a procedure of module $M$;
– the formula $\phi$ may involve the global variables of declared modules, as well as the parameters of $M.p$;
– the formula $\psi$ may involve the term $\text{res}$, whose type is $M.p$’s return type, as well as the global variables of declared modules;
– $e$ is an expression of type real.
Occurrences in \( \phi \) and \( \psi \) and of bound identifiers (bound outside the judgment) whose names conflict with parameters or local variables of \( M.p \) will refer to the bound identifiers, not the parameters/local variables. \( e \) will have to be parenthesized unless it is a constant or nullary operator.

The informal meaning of the \( \text{pHL} \) judgment is that, for all initial memories \( km \) satisfying \( \phi \) and whose domains consist of the global variables of declared modules plus the parameters and local variables of \( M.p \), the probability that

\[
\text{running the body of } M.p \text{ in } km \text{ results in termination with a memory whose restriction to } \text{res} \text{ and the global variables of declared modules satisfies } \psi
\]

has the indicated relation to the value of \( e \).

- (PRHL Judgments) A PRHL judgment has the form

\[
\text{equiv}[M.p - N.q : \phi => \psi]
\]

where:

- \( p \) is a procedure of module \( M \), and \( q \) is a procedure of module \( N \);
- the formula \( \phi \) may involve the global variables of declared modules, the parameters of \( M.p \), which must be interpreted in memory \( \&1 \) (e.g., \( x(1) \)), and the parameters of \( N.q \), which must be interpreted in memory \( \&2 \);
- the formula \( \psi \) may involve the global variables of declared modules, \( \text{res}(1) \), which has the type of \( M.p \)'s return type, and \( \text{res}(2) \), which has the type of \( N.q \)'s return type.

Occurrences in \( \psi \) of bound identifiers (bound outside the judgment) whose names conflict with parameters and local variables of \( M.p \) and \( N.q \) will refer to the bound identifiers, not the parameters and local variables, even if they are enclosed in memory references (e.g., \( x(1) \)). If \( \&1 \) (resp., \( \&2 \)) is a bound memory (outside the judgment), then all references to \( \&1 \) (resp., \( \&2 \)) in \( \phi \) and \( \psi \) are renamed to use a fresh memory.

The informal meaning of the PRHL judgment is that, for all initial memories \( \&1 \) whose domains consist of the global variables of declared modules plus the parameters and local variables of \( M.p \), for all initial memories \( \&2 \) whose domains consist of the global variables of declared modules plus the parameters and local variables of \( N.q \), if \( \phi \) holds, then the sub-distributions on memories \( \Pi_p \) and \( \Pi_q \) obtained by running \( M.p \) on \( \&1 \), storing \( p \)'s result in the component \( \text{res} \) of the resulting memory, from which \( p \)'s parameters and local variables are removed, and running \( N.q \) on \( \&2 \), storing \( q \)'s result in the component \( \text{res} \) of the resulting memory, from which \( q \)'s parameters and local variables are removed, satisfy \( \psi \), in the following sense. (The probability of a memory in \( \Pi_p \) (resp., \( \Pi_q \)) is the probability that \( p \) (resp., \( q \)) will terminate with that memory. \( \Pi_p \) and \( \Pi_q \) are sub-distributions on memories because \( p \) and \( q \) may fail to terminate.)

We say that \((\Pi_p, \Pi_q)\) satisfy \( \psi \) iff there is a function \( f \) dividing the probability assigned to each memory \( km \) by \( \Pi_p \) among the memories \( km \) related to it by \( \psi \) (\( km \) and \( kn \) are related according to \( \psi \) iff \( \psi \) holds when references to \( \&1 \) are replaced by reference to \( km \), and reference to \( \&2 \) are replaced by reference to \( kn \) such that, for all memories \( km \), the value assigned to \( km \) by \( \Pi_q \) is the sum of all the probabilities distributed to \( km \) by \( f \). (When \( \psi \) is an equivalence like \( \equiv \text{res} \) (i.e., \( \text{res}(1) = \text{res}(2) \)), this is particularly easy to interpret.)

- (Lossless Assertions) A lossless assertion has the form

\[
\text{islossless } M.p
\]

and is simply an abbreviation for
For the purpose of giving some examples, consider these declarations:

```plaintext
module G1 = {
  proc f() : bool = {
    var x : bool;
    x <$> {0,1};
    return x;
  }
}.

module G2 = {
  proc f() : bool = {
    var x, y : bool;
    x <$> {0,1}; y <$> {0,1};
    return x ^^ y; (* ^^ is exclusive or *)
  }
}.
```

Then:

- The expression
  \[ \text{Pr}_{G1.f() \& \& m} : \text{res} \]
  is the probability that \( G1.f() \) returns true when run in the memory \( \&m \). (The memory is irrelevant, and the expression’s value is \( 1/2 \).)

- The HL judgement
  \[ \text{hoar}_{G2.f : true \Rightarrow !\text{res}} \]
  says that, if \( G2.f() \) halts (which we know it will), then its return value will be false. (This judgement is false.)

- The pHL judgement
  \[ \text{phoar}_{G2.f : true \Rightarrow \text{res}} = (1/2) \]
  says that the probability of \( G2.f() \) returning true is \( 1/2 \). (This judgement is true.)

- The pRHL judgement
  \[ \text{equiv}_{G1.f - G2.f : true \Rightarrow \text{res}} \]
  says that \( G1.f() \) and \( G2.f() \) are equally likely to return true as well as equally likely to return false. (This judgement is true.)

- The lossless assertion
  \[ \text{lossless G2.f} \]
  says that \( G2.f() \) always terminates, no matter what memory it’s run in. (This judgement is true.)
2.5.2 Axioms and Lemmas

One states an **axiom** or **lemma** by giving a well-typed formula with no free identifiers, as in:

```
axiom Sym : forall (x y : int), x = y => y = x.
lemma Sym : forall (x y : int), x = y => y = x.
```

The difference between axioms and lemmas is that axioms are trusted by EASYCRYPT, whereas lemmas must be proved, in the steps that follow. The **proof** of a lemma has the form

```
proof.
tactic1. ... tacticn.
qed.
```

Actually the proof step is optional, but it’s good style to include it. The steps of the proof consist of tactic applications; but print and search commands are also legal steps. The qed step saves the lemma, making it available for reuse; it’s only allowed when the proof is complete. If the name chosen for a lemma conflicts with an already stated axiom or lemma, one only finds this out upon running qed, which will fail. When the proof for a lemma has a very simple form, the proof may be included as part of the lemma’s statement:

```
lemma name : phi by [tactic].
```

or

```
lemma name : phi by [].
```

In the first case, the proof consists of a single tactic; the meaning of by [] will be described in Chapter 3.

One may also parameterize an axiom of lemma by the free identifiers of its formula, as in:

```
lemma Sym (x : int) (y : int) : x = y => y = x.
```

This version of Sym has the same logical meaning as the previous one. But we’ll see in Chapter 3 why the parameterized form makes an axiom or lemma easier to apply.

Polymorphic axioms and lemmas may be stated using a syntax reminiscent of the one for polymorphic operators:

```
lemma Sym ['a] (x y : 'a) : x = y => y = x.
lemma PairEq ['a, 'b] (x x' : 'a) (y y' : 'b) : x = x' => y = y' => (x, y) = (x', y').
```

or

```
lemma Sym (x y : 'a) : x = y => y = x.
lemma PairEq (x x' : 'a) (y y' : 'b) : x = x' => y = y' => (x, y) = (x', y').
```

We can axiomatize the meaning of abstract types, operators and relations. E.g., an abstract type of monoids may be axiomatized by:

```
type monoid.
op id : monoid.
op (+) : monoid -> monoid -> monoid.
axiom LeftIdentity (x : monoid) : id + x = x.
axiom RightIdentity (x : monoid) : x + id = x.
axiom Associative (x y z : monoid) : x + (y + z) = (x + y) + z.
```
Any proofs we do involving monoids will then apply to any valid instantiation of monoid, 1d and (+). In Chapter 4, we’ll see how to carry out such instantiations using theory cloning.

One must be careful with axioms, however, because it’s easy to introduce inconsistencies, allowing one to prove false formulas. E.g., because all types must be nonempty in EASYCRYPT, writing

```plaintext
type t.
axiom Empty : !(exists (x : t), true).
```

will allow us to prove false.

Axioms and lemmas may be parameterized by memories and modules. Consider the declarations:

```plaintext
module type T = {
  proc f() : unit
}.
module G(X : T) = {
  var x : int
  proc g() : unit = {
    X.f();
  }
}.
```

Then lemma Lossless

```plaintext
lemma Lossless (X <: T) : islossless X.f => islossless G(X).g.
```

which is parameterized by an abstract module X of module type T, says that G(X).g always terminates, no matter the memory it’s run in, as long as this is true of X.f. Lemma Invar

```plaintext
lemma Invar (X <: T{G}) (n : int) :
  islossless X.f =>
  phoare [G(X).g : G.x = n ==> G.x = n] = 1%r.
```

which is parameterized by an abstract module X of module type T that is guaranteed not to access or modify G.x, and an integer n, says that, assuming X.f is lossless, if G(X).g() is run in a memory giving G.x the value n, then G(X).g() is guaranteed to terminate in a memory in which G.x’s value is still n. Finally lemma Invar’

```plaintext
lemma Invar’ (X <: T{G}) (n : int) &m :
  islossless X.f =>
  Pr[G(X).g() @ &m : G.x = n] = 1%r.
```

which has the parameters of Invar plus a memory &m, says the same thing as Invar, but using a probability expression rather than a PHL judgement.
Chapter 3

Tactics

Proofs in EasyCrypt are carried out using tactics, logical rules embodying general reasoning principles, which transform the current lemma (or goal) into zero or more subgoals—sufficient conditions for the lemma/goal to hold. Simple ambient logic goals may be automatically proved using SMT solvers.

In this chapter, we introduce EasyCrypt’s proof engine, before describing the tactics for EasyCrypt’s four logics: ambient, pRHL, pHL and HL.

3.1 Proof Engine

EasyCrypt’s proof engine works with goal lists, where a goal has two parts:

- A context consisting of
  - a set of type variables, and
  - an ordered set of assumptions, consisting of identifiers with their types, memories, module names with their module types and restrictions, local definitions, and hypotheses, i.e., formulas. An identifier’s type may involve the type variables, the local definitions and formulas may involve the type variables, identifiers, memories and module names.

- A conclusion, consisting of a single formula, with the same constraints as the assumption formulas.

Informally, to prove a goal, one must show the conclusion to be true, given the truth of the hypotheses, for all valid instantiations of the assumption identifiers, memories and module names.

For example,

```
Type variables: 'a, 'b

x : 'a
x' : 'a
y : 'b
y' : 'b
eq_xx': x = x'
eq_yy': y = y'

(x, y) = (x', y')
```

is a goal. And, in the context of the declarations

```
module type T = {
  proc f() : unit
}.;
module G(X : T) = {
```

35
CHAPTER 3. TACTICS

var x : int
proc g() : unit = {
    X.f();
}
).

this is a goal:

Type variables: <none>
X : T{G}
n : int
LL: islossless X.f

pre = G.x = n
G(X).g
[=] 1%r
post = G.x = n

The conclusion of this goal is just a nonlinear rendering of the formula

phoare [G(X).g : G.x = n => G.x = n] = 1%r.

EASYCRYPT’s pretty printer renders pRHL, pHL and HL judgements in such a nonlinear style when the judgements appear as (as opposed to in) the conclusions of goals.

Internally, EASYCRYPT’s proof engine also works with pRHL, pHL and HL judgments involving lists of statements rather than procedure names, which we’ll call statement judgements, below. For example, given this declaration

module M = {
    proc f(y : int) = {
        if (y %% 3 = 1) y <- y + 4;
        else y <- y + 2;
        return y;
    }
}.

this is an pHL statement judgement:

Type variables: <none>
x : int
zor1_x: x = 1 \lor x = 2

Context : M.f
pre = y %% 3 = x

(1--) if (y %% 3 = 1) {
(1.1) y <- y + 4
(1--) } else {
(1?) y <- y + 2
(1--) }

post = y %% 3 = x %% 2 + 1

The pre- and post-conditions of a statement judgement may refer to the parameters and local variables of the procedure context of the conclusion—\% x in the preceding example. They may also refer to the memories \&1 and \&2 in the case of pRHL statement judgements. When a statement
judgement appears anywhere other than as the conclusion of a goal, the pretty printer renders it in abbreviated linear syntax. E.g., the preceding goal is rendered as

```
hoare [if (x %% 3 = 1) { · · · } : x %% 3 = n ==> x %% 3 = n %% 2 + 1]
```

Statement judgements can’t be directly input by the user.

We use the term *program* to refer to either a procedure appearing in a PRHL, PHL or HL judgement, or a statement list appearing in a PRHL, PHL or HL statement judgement. In the case of PRHL (statement) judgements, we speak of the left and right programs, also using *program 1* for the left program, and *program 2* for the right one. We will only speak of a program’s *length* when it’s a statement list we are referring to. By the *empty* program, we mean the statement list with no statements.

When the proof of a lemma is begun, the proof engine starts out with a single goal, consisting of the lemma’s statement. E.g., the lemma

```
lemma PairEq ['a, 'b] :
  forall (x x' : 'a) (y y' : 'b),
  x = x' => y = y' => (x, y) = (x', y').
```

gives rise to the goal

```
Type variables: 'a, 'b

forall (x x' : 'a) (y y' : 'b), x = x' => y = y' => (x, y) = (x', y')
```

For parameterized lemmas, the goal includes the lemma’s parameters as assumptions. E.g.,

```
lemma PairEq (x x' : 'a) (y y' : 'b) :
  x = x' => y = y' => (x, y) = (x', y').
```

gives rise to

```
Type variables: 'a, 'b

x : 'a
x' : 'a
y : 'b
y' : 'b

x = x' => y = y' => (x, y) = (x', y')
```

EasyCrypt’s tactics, when applicable, reduce the first goal to zero or more subgoals. E.g., if the first goal is

```
Type variables: <none>

x : int
zor1_x: x = 1 \/ x = 2

Context : M.f

pre = y %% 3 = x

(1--) if (y %% 3 = 1) {
  (1.1) y <- y + 4
  (1--) }
else {
  (1?) y <- y + 2
  (1--) }

post = y %% 3 = x %% 2 + 1
```
then applying the if tactic (handle a conditional) reduces (replaces) this goal with the two goals

\[
\begin{align*}
\text{Type variables: } & <\text{none}> \\
x & : \text{int} \\
zor1_x & : x = 1 \lor x = 2 \\
\text{Context: } & M.f \\
\text{pre} & = y \mod 3 = x \land y \mod 3 = 1 \\
(1) & y < - y + 4 \\
\text{post} & = y \mod 3 = x \mod 2 + 1
\end{align*}
\]

and

\[
\begin{align*}
\text{Type variables: } & <\text{none}> \\
x & : \text{int} \\
zor1_x & : x = 1 \lor x = 2 \\
\text{Context: } & M.f \\
\text{pre} & = y = 3 = x \lor y = 3 \not= 1 \\
(1) & y <= y + 2 \\
\text{post} & = y \mod 3 = x \mod 2 + 1
\end{align*}
\]

(Leaving the remaining goals, if any, unchanged). If the first goal is

\[
\begin{align*}
\text{Type variables: } & <\text{none}> \\
x & : \text{int} \\
zor1_x & : x = 1 \lor x = 2 \\
\text{forall } & \forall \text{hr}, \\
y(\text{hr}) \mod 3 = x \lor y(\text{hr}) \mod 3 = 1 => (y(\text{hr}) + 4) \mod 3 = x \mod 2 + 1
\end{align*}
\]

then applying the smt tactic (try to solve the goal using SMT provers) solves the goal, i.e., replaces it with no subgoals. Applying a tactic may fail; in this case an error message is issued and the list of goals is left unchanged.

A lemma’s proof may be saved, using the step qed, when the list of goals becomes empty. And this must be done before anything else may be done.

**Remark.** In the descriptions of EASYCRYPT’s tactics given in the following two sections, unless otherwise specified, you should assume that the subgoals to which a tactic reduces a goal have the same contexts as that original goal.

### 3.2 Matching

Statement patterns are an extension of statements. Fixme Note: Add explanation of new replace tactic, which uses statement patterns.
Blocks

| {} | empty statement |
| {}s | start and end anchors around s |
| [ ]s | start anchor at the beginning of s |
| [ ]s | end anchor at the end of s |
| [ ]s | find s at any position in the statements, without looking into possible branches |
| <s> | find s at any position in the statements, and looking into possible branches |

Statements

| _ | any sequence of statements |
| n_ | a sequence of n statements |
| s as X | s that is associated with the name X |
| X | interpreted as _ as X |
| !s | repeat s, can be zero time |
| ?s | s is to appear once, or zero time |
| n!s | repeat s n times |
| [n..m]!s | repeat s at least n times, up to m times |
| [..m]!s | repeat s up to m times |
| ~s | apply not greedy characteristics to s if that makes sense |
| s1 ; s2 | s1 followed directly by s2 |
| s1 s2 | s1 followed directly by s2 |
| s1 | s1 or s2 |
| _ <- _ ; | any affectation |
| _ <$ _ ; | any sample |
| _ <@ _ ; | any procedure call |
| if ; | any if statement |
| while ; | any while statement |
| if _ bt else bf | a if statement where bt is the block matched in the branch true’s corpse, and bf the block in the branch false’s body |
| while _ b | a while branch where the block b is matched in the corpse of the loop |

3.3 Ambient logic

In this section, we describe the proof terms, tactics and tacticals of EASYCRYPT’s ambient logic.

3.3.1 Proof Terms

Formulas introduce identifier and formula assumptions using universal quantifiers and implications. For example, the formula

```
forall (x y : bool), x = y => forall (z : bool), y = z => x = z.
```

introduces the assumptions

```
x : bool
y : bool
eq_xy : x = y
z : bool
eq_yz : y = z
```

(where the names of the two formulas were chosen to be meaningful), and has x = z as its conclusion. We refer to the first assumption of a formula as the formula’s top assumption. E.g., the top assumption of the preceding formula is x : bool.

EASYCRYPT has proof terms, which partially describe how to prove a formula. Their syntax is described in Figure 3.1, where X ranges over lemma (or formula assumption) names. A proof term for a lemma (or formula assumption) X has components corresponding to the assumptions introduced by X. A component corresponding to a variable consists of an expression of the
variable’s type. The proof term is explaining how the instantiation of the lemma’s conclusion with these expressions may be proved. A formula component consists of a proof term explaining how the instantiation of the formula may be proved. Proof holes will get turned into subgoals when a proof term is used in backward reasoning, e.g., by the apply (p. 60) tactic. \textbf{Fixme Note:} Need explanation of how a proof term may be used in forward reasoning.

Consider, e.g., the following declarations and axioms

\begin{verbatim}
pred P : int.
pred Q : int.
pred R : int.
axiom P (x : int) : P x.
axiom Q (x : int) : P x => Q x.
axiom R (x : int) : P(x + 1) => Q x => R x.
\end{verbatim}

Then, given that \(x : \text{int}\) is an assumption,

\[
(R \times (P(x + 1)) \times (Q \times (P x)))
\]

is a proof term proving the conclusion \(R x\). And

\[
(R \times _\times (Q \times _\times))
\]

is a proof term that turns proofs of \(P(x + 1)\) and \(P x\) into proofs of \(R x\). When used in backward reasoning, it will reduce a goal with conclusion \(R x\) to subgoals with conclusions \(P(x + 1)\) and \(P x\). \textbf{Fixme Note:} Can it be used in forward reasoning?

Some of a proof term’s expressions may be replaced by \(\_\), asking EASYCRYPT to infer them from the context. Going even further, one may abbreviate a one-level proof term all of whose components are \(\_\) to just its lemma name. For example, we can write \(R\) for \(R _\times _\times _\times\). When used in backward reasoning, it will reduce a goal with conclusion \(R x\) to subgoals with conclusions \(P(x + 1)\) and \(Q x\). \textbf{Fixme Note:} In forward reasoning they aren’t equivalent—why?

\section{3.3.2 Occurrence Selectors and Rewriting Directions}

Some ambient logic tactics use occurrence selectors to restrict their operation to certain occurrences of a term or formula in a goal’s conclusion or formula assumption. The syntax is \(\{i_1, \ldots, i_n\}\), specifying that only occurrences \(i_1\) through \(i_n\) of the term/formula in a depth-first, left-to-right traversal of the goal’s conclusion or formula assumption should be operated on. Specifying \(\{-i_1, \ldots, i_n\}\) restricts attention to all occurrences not in the following list. They may also be empty, meaning that all applicable occurrences should be operated on.

Some ambient logic tactics use rewriting directions, \(\text{dir}\), which may either be empty (meaning rewriting from left to right), or \(\_\), meaning rewriting from right to left.

\section{3.3.3 Introduction and Generalization}

\textbf{Introduction.} One moves the assumptions of a goal’s conclusion into the goal’s context using the introduction tactical. This tactical uses introduction patterns, which are defined in Figure 3.2. In this definition, \(\text{occ}\) ranges over occurrence selectors, and \(\text{dir}\) ranges over directions—see Subsection 3.3.2).

If a list \(i_1, \ldots, i_n\) of introduction patterns consists entirely of // (apply the trivial (p. 55) tactic), /= (apply the simplify (p. 56) tactic) and //= (apply the simplify and then trivial),
\(t ::= b\)  
\[\text{name}\]
\[-\]  
\[\text{no name}\]
\[+\]  
\[\text{auto revert}\]
\[?\]  
\[\text{find name}\]
\[%]  
\[\text{rewrite using assumption}\]
\[occ ->\]  
\[\text{rewrite in reverse using assumption}\]
\[occ <-\]  
\[\text{substitute using assumption}\]
\[\text{->}\]  
\[\text{replace assumption by applying proof term}\]
\[\ll\]  
\[\text{clear introduced assumptions}\]
\[\text{/}\]  
\[\text{replace assumption by applying proof term}\]
\[\{a_1 \cdots a_n\}\]  
\[\text{simplify}\]
\[\text{//}\]  
\[\text{trivial}\]
\[\text{//=}\]  
\[\text{simplify then trivial}\]
\[\text{dir occ @/ op}\]  
\[\text{unfold definition of operator}\]
\[\text{[}\]\]  
\[\text{case pattern}\]
\[b ::= x\]  
\[\text{identifier}\]
\[M\]  
\[\text{module name}\]
\[km\]  
\[\text{memory name}\]

Figure 3.2: Introduction Patterns

then applying \(t_1, \ldots, t_n\) to a list of goals \(G_1, \ldots, G_m\) is done by applying the tactics corresponding to the \(t_i\) in order to each \(G_j\), causing some of the goals to be solved and thus disappear and some of the goals to be simplified.

\(\tau \Rightarrow t_1 \cdots t_n\)

Runs the tactic \(\tau\), matching the resulting goals, \(G_1, \ldots, G_l\), with the introduction patterns \(t_1, \ldots, t_n\):

- Suppose \(k\) is such that all of \(t_1, \ldots, t_{k-1}\) are //, /= and /=, and either \(k > n\) or \(t_k\) is not //, /= or /=.
- Let \(G'_1, \ldots, G'_l\) be the goals resulting from applying \(t_1, \ldots, t_{k-1}\) to \(G_1, \ldots, G_l\).
- If \(l' = 0\), the tactical produces no subgoals.
- Otherwise, if \(k > n\), the tactical’s result is \(G'_1, \ldots, G'_l\).
- Otherwise, if \(t_k\) is not a case pattern, each subgoal \(G'_i\) is matched against \(t_k, \ldots, t_n\) by the procedure described below, with the resulting subgoals being collected into a list of goals (maintaining order viz a viz the indices \(i\)) as the tactical’s result.
- Otherwise, \(t_k\) is a case pattern \([t_{i_1} \cdots t_{i_{m_1}} | \cdots | t_{r_1} \cdots t_{r_{m_r}}]\).
- If \(\tau\) is not equivalent to idtac (p. 47), the tactic fails unless \(r = l'\), in which case each \(G'_i\) is matched against
\[t_{i_1} \cdots t_{i_{m_1}} t_{k+1} \cdots t_n\]
by the procedure described below, with the resulting subgoals being collected into the tactical’s result.
- Otherwise, \(\tau\) is equivalent to idtac (p. 47) (and so \(l' = 1\)). In this case \(G'_1\) is matched against \(t_k, \ldots, t_n\) by the procedure described below, with the resulting subgoals being collected into a list of goals as the tactical’s result.
CHAPTER 3. TACTICS

Matching a single goal against a list of patterns: To match a goal $G$ against a list of introduction patterns $\iota_1, \ldots, \iota_n$, the introduction patterns are processed from left-to-right, as follows:

- $(b)$ The top assumption (universally quantified identifier, module name or memory; or left side of implication) is consumed, and introduced with this name. Fails if the top assumption has neither of these forms.

- $(b \uparrow)$ Same as the preceding case, except that $b$ is used as the base of the introduced name, extending the base to avoid naming conflicts.

- $(\_)$ Same as the preceding case, except the assumption is introduced with an anonymous name (which can’t be uttered by the user).

- $(\pm)$ Same as the preceding case, except that after a branch of the procedure completes, yielding a goal, the assumption will be reverted, i.e., un-introduced (using a universal quantifier or implication as appropriate).

- $(\pm)$ Same as the preceding case, except EasyCrypt chooses the name by which the assumption is introduced (using universally quantified names as assumption bases).

- $(\text{occ} \rightarrow)$ Consume the top assumption, which must be an equality, and use it as a left-to-right rewriting rule in the remainder of the goal’s conclusion, restricting rewriting to the specified occurrences of the equality’s left side.

- $(\text{occ} \leftarrow)$ The same as the preceding case, except the rewriting is from right-to-left.

- $(\rightarrow)$ The same as $\rightarrow$, except the consumed equality assumption is used to perform a left-to-right substitution in the entire goal, i.e., in its assumptions, as well as its conclusion.

- $(\leftarrow)$ The same as the preceding case, except the substitution is from right-to-left.

- $(/p)$ Replace the top assumption by the result of applying the proof term $p$ to it using forward reasoning.

- $(\{a_1 \cdots a_n\})$ Doesn’t affect the goal’s conclusion, but clears the specified assumptions, i.e., removes them. Fails if one or more of the assumptions can’t be cleared, because a remaining assumption depends upon it.

- $(/\_)$ Apply simplify (p. 56) to goal’s conclusion.

- $(//)$ Apply trivial (p. 55) to goal’s conclusion; this may solve the goal, i.e., so that the procedure’s current branch yields no goals.

- $(/=)$ Apply simplify (p. 56) and then trivial (p. 55) to goal’s conclusion; this may solve the goal, so that the procedure’s current branch yields no goals.

- $(\text{dir occ} \# /op)$ Unfold (fold, if the direction is -) the definition of operator $op$ at the specified occurrences of the goal’s conclusion. See the rewrite (p. 62) tactic for the details.

- $(\{\iota_{i1} \cdots \iota_{im1} \mid \cdots \mid \iota_{i1} \cdots \iota_{imr}\})$
  - If $r = 0$, then the top assumption of the goal is destructed using the case (p. 64) tactic, the resulting goals are matched against $\iota_{2}, \ldots, \iota_{n}$, and their subgoals are assembled into a list of goals.
  - Otherwise $r > 0$. The goal’s top assumption is destructed using the case (p. 64) tactic, yielding subgoals $H_1, \ldots, H_p$. If $p \neq r$, the procedure fails. Otherwise each subgoal $H_i$ is matched against $\iota_{i1} \cdots \iota_{im}, \iota_{2} \cdots \iota_{n}$ with the resulting goals being collected into a list as the procedure’s result.
The following examples use the tactic \texttt{move} (p. 47), which is equivalent to \texttt{idtac} (p. 47). In its simplest form, the introduction tactical simply gives names to assumptions. For example, if the current goal is

\[
\text{forall } (x \ y : \text{int}), \ x = y \Rightarrow \text{forall} \ (z : \text{int}), \ y = z \Rightarrow x = z
\]

then running

\[
\text{move=} x \ y \ \text{eq}_{xy} \ z \ \text{eq}_{yz}.
\]

produces

\[
\text{Type variables: } <\text{none}>
\]
\[
x : \text{int} \\
y : \text{int} \\
\text{eq}_{xy} : x = y \\
z : \text{int} \\
\text{eq}_{yz} : y = z \\
x = z
\]

Alternatively, we can use the introduction pattern \texttt{?} to let \textsc{EasyCrypt} choose the assumption names, using \texttt{H} as a base for formula assumptions and starting from the identifier names given in universal quantifiers:

\[
\text{move=} ? \ ? \ ? \ ? \ ?.
\]

produces

\[
\text{Type variables: } <\text{none}>
\]
\[
x : \text{int} \\
y : \text{int} \\
\text{H} : x = y \\
z : \text{int} \\
\text{H0} : y = z \\
x = z
\]

To see how the \texttt{->} rewriting pattern works, suppose the current goal is

\[
\text{Type variables: } <\text{none}>
\]
\[
x : \text{int} \\
y : \text{int} \\
x = y \Rightarrow \text{forall} \ (z : \text{int}), \ y = z \Rightarrow x = z
\]

Then running

\[
\text{move=} \Rightarrow .
\]

produces

\[
\text{Type variables: } <\text{none}>
\]
\[
x : \text{int} \\
y : \text{int} \\
\text{forall} \ (z : \text{int}), \ y = z \Rightarrow y = z
\]
Alternatively, one can introduce the assumption \( x = y \), and then use the \( \rightarrow \rightarrow \) substitution pattern: if the current goal is

```
Type variables: <none>

x : int
y : int
H1: x = y
z : int

y = z \rightarrow x = z
```

then running

```
move=\rightarrow\rightarrow.
```

produces

```
Type variables: <none>

x : int
y : int
z : int
H1: x = z

x = z
```

To see how a view may be applied to a not-yet-introduced formula assumption, suppose the current goal is

```
Type variables: <none>

Sym: \forall (u \ v : int), u = v \rightarrow v = u
x : int
y : int

x = y \rightarrow \forall (z : int), y = z \rightarrow x = z
```

Then running

```
move=\rightarrow /Sym.
```

produces

```
Type variables: <none>

Sym: \forall (u \ v : int), u = v \rightarrow v = u
x : int
y : int

y = x \rightarrow \forall (z : int), y = z \rightarrow x = z
```

And then running

```
move=\rightarrow .
```

on this goal produces

```
Type variables: <none>

Sym: \forall (u \ v : int), u = v \rightarrow v = u
x : int
y : int

\forall (z : int), x = z \rightarrow x = z
```
Finally, let’s see examples of how a disjunction assumption may be destructed, either using the \texttt{case} tactic followed by a case introduction pattern, or by making the case introduction pattern do the destruction. For the first case, if the current goal is

\begin{verbatim}
Type variables: <none>

x : bool
y : bool

x \lor y =>
(x => \forall (z : bool), P x z) =>
(y => \forall (z : bool), Q y z) =>
(\forall (z : bool), P x z) \lor \forall (z : bool), Q y z
\end{verbatim}

then running

\begin{verbatim}
move=> [Hx HP _ | Hy _ HQ].
\end{verbatim}

produces the two goals

\begin{verbatim}
Type variables: <none>

x : bool
y : bool
Hx: x
HP: x => \forall (z : bool), P x z
_ : y => \forall (z : bool), Q y z

(\forall (z : bool), P x z) \lor \forall (z : bool), Q y z
\end{verbatim}

and

\begin{verbatim}
Hx: y
_ : x => \forall (z : bool), P x z
HQ: y => \forall (z : bool), Q y z

(\forall (z : bool), P x z) \lor \forall (z : bool), Q y z
\end{verbatim}

And for the second case, if the current goal is

\begin{verbatim}
Type variables: <none>

x : bool
y : bool

x \lor y =>
(x => \forall (z : bool), P x z) =>
(y => \forall (z : bool), Q y z) =>
(\forall (z : bool), P x z) \lor \forall (z : bool), Q y z
\end{verbatim}

then running

\begin{verbatim}
case=> [Hx HP X | Hy X HQ] {X}.
\end{verbatim}

produces the two goals

\begin{verbatim}
Type variables: <none>

x : bool
\end{verbatim}
CHAPTER 3. TACTICS

y : bool
Hx: x
HP: x => forall (z : bool), P x z

(forall (z : bool), P x z) \ / forall (z w : bool), Q y z w

and

Type variables: <none>

x : bool
y : bool
Hy: y
HQ: y => forall (z w : bool), Q y z w

(forall (z : bool), P x z) \ / forall (z w : bool), Q y z w

Note how we used the clear pattern to discard the assumption x.

Generalization. The generalization tactical moves assumptions from the context into the conclusion and generalizes subterms or formulas of the conclusion.

\( \tau: \pi_1 \cdots \pi_n \)

Generalize the patterns \( \pi_1, \ldots, \pi_n \), starting from \( \pi_n \) and going back, and then run tactic \( \tau \). This tactical is only applicable to certain tactics: move (p. 47), case (p. 64) (just the version that destructs the top assumption of a goal’s conclusion) and elim (p. 67).

- \( \pi \) may be an assumption from the context, it’s moved back into the conclusion, using universal quantification or an implication, as appropriate. If one assumption depends on another, one can’t generalize the later without also generalizing the former.

For example, if the current goal is

Type variables: <none>

x : int
y : int
eq_xy: x = y

y = x

then running

move: x eq_xy.

produces

Type variables: <none>

y : int

forall (x : int), x = y => y = x

In this example, one can’t generalize x without also generalizing eq_xy.

- \( \pi \) may also be a subformula or subterm of the goal, or \( _\_ \), which stands for the whole goal, possibly prefixed by an occurrence selector. This replaces the formula or subterm with a universally quantified identifier of the appropriate type.

For example, if the current goal is
3.3.4 Tactics

idtac

Does nothing, i.e., leaves the goal unchanged.

move

Does nothing, equivalent to idtac (p. 47). It is mainly used in conjunction with the introduction tactical and the generalization mechanism. See Section 3.3.3.

clear a₁⋅⋅⋅aₙ

Clear assumptions a₁⋅⋅⋅aₙ from the goal’s context. Fail if any remaining hypotheses depend on any of the aᵢ.

For example, if the current goal is

then running
CHAPTER 3. TACTICS

clear z eq_yz.

produces

Type variables: <none>
x : int
y : int
eq_xy: x = y

x - 1 = y - 1

assumption

Search in the context for a hypothesis that is convertible to the goal’s conclusion, solving the
goal if one is found. Fail if none can be found.
For example, if the current goal is

Type variables: <none>
x : int
y : int
eq_xy: x = y

x = y

then running

assumption.

solves the goal.

reflexivity

Solve goals with conclusions of the form \( b = b \) (up to computation).
For example, if the current goal is

Type variables: <none>
y : bool

(fun (x : bool) => !x) y = !y

then running

reflexivity.

solves the goal.

left

Reduce a goal whose conclusion is a disjunction to one whose conclusion is its left member.
For example, if the current goal is

Type variables: <none>
x : int
y : int
eq_xy: x - 1 = y

x = y + 1 \lor y = x + 1

then running
produces the goal

```
Type variables: <none>

x : int
y : int
eq_xy: x - 1 = y

x = y + 1
```

\( \textit{left.} \)

Reduce a goal whose conclusion is a disjunction to one whose conclusion is its right member. For example, if the current goal is

```
Type variables: <none>

x : int
y : int
eq_yz: y - 1 = x

x = y + 1 \lor y = x + 1
```

then running

```
\textit{right.}
```

produces the goal

```
Type variables: <none>

x : int
y : int
eq_yz: y - 1 = x

y = x + 1
```

If we replace \( \lor \) by \( \mid\mid \) in this example, we can see the difference between the two versions of disjunction: if the current goal is

```
Type variables: <none>

x : int
y : int
eq_yz: y - 1 = x

x = y + 1 \mid\mid y = x + 1
```

then running

```
\textit{right.}
```

produces the goal

```
Type variables: <none>

x : int
y : int
eq_yz: y - 1 = x

x \neq y + 1 \Rightarrow y = x + 1
```
CHAPTER 3. TACTICS

50

6 \texttt{exists e}

Reduces proving an existential to proving the witness \(e\) satisfies the existential’s body. For example, if the current goal is

\begin{verbatim}
Type variables: <none>

x : int
rng_x: 0 < x < 5

exists (x0 : int), 5 < x0 < 10
\end{verbatim}

then running

\texttt{exists (x + 5)}.

produces the goal

\begin{verbatim}
Type variables: <none>

x : int
rng_x: 0 < x < 5

5 < x + 5 < 10
\end{verbatim}

6 \texttt{split}

Break a goal whose conclusion is intrinsically conjunctive into goals whose conclusions are its conjuncts. For instance, it can:

- close any goal that is convertible to true or provable by \texttt{reflexivity},
- replace a logical equivalence by the direct and indirect implications,
- replace a goal of the form \(\phi_1 \land \phi_2\) by the two subgoals for \(\phi_1\) and \(\phi_2\). The same applies for a goal of the form \(\phi_1 \lor \phi_2\),
- replace an equality between \(n\)-tuples by \(n\) equalities on their components.

For example, if the current goal is

\begin{verbatim}
Type variables: <none>

x : int
y : int

x = y \leftrightarrow x - 1 = y - 1
\end{verbatim}

then running

\texttt{split}.

produces the goals

\begin{verbatim}
Type variables: <none>

x : int
y : int

x = y \Rightarrow x - 1 = y - 1
\end{verbatim}

and
CHAPTER 3. TACTICS

Type variables: <none>

\( x : \text{int} \)
\( y : \text{int} \)

\[ x - 1 = y - 1 \Rightarrow x = y \]

And if the current goal is

Type variables: <none>

\( x : \text{int} \)
\( y : \text{int} \)
\( z : \text{int} \)
\( w : \text{int} \)
\( \text{eq}_{xy}: x = y \)
\( \text{eq}_{zw}: z = w \)

\[ x - 1 = y - 1 \text{ \(/\)} z + 1 = w + 1 \]

then running

\texttt{split}.

produces the goals

Type variables: <none>

\( x : \text{int} \)
\( y : \text{int} \)
\( z : \text{int} \)
\( w : \text{int} \)
\( \text{eq}_{xy}: x = y \)
\( \text{eq}_{zw}: z = w \)

\[ x - 1 = y - 1 \]

and

Type variables: <none>

\( x : \text{int} \)
\( y : \text{int} \)
\( z : \text{int} \)
\( w : \text{int} \)
\( \text{eq}_{xy}: x = y \)
\( \text{eq}_{zw}: z = w \)

\[ z + 1 = w + 1 \]

Repeating the last example with \texttt{&&} rather than \texttt{/\}, if the current goal is

Type variables: <none>

\( x : \text{int} \)
\( y : \text{int} \)
\( z : \text{int} \)
\( w : \text{int} \)
\( \text{eq}_{xy}: x = y \)
\( \text{eq}_{zw}: z = w \)

\[ x - 1 = y - 1 \text{ \&\&} z + 1 = w + 1 \]
then running

\texttt{split}.

produces the goals

\begin{verbatim}
Type variables: <none>

  x : int
  y : int
  z : int
  w : int
  eq_xy: x = y
  eq_zw: z = w

  x - 1 = y - 1
\end{verbatim}

and

\begin{verbatim}
Type variables: <none>

  x : int
  y : int
  z : int
  w : int
  eq_xy: x = y
  eq_zw: z = w

  x - 1 = y - 1 => z + 1 = w + 1
\end{verbatim}

This illustrates the difference between \(\mathbin{\backslash/}\) and \(\mathbin{\&\&}\). And if the current goal is

\begin{verbatim}
Type variables: <none>

  x : int
  y : int
  z : int
  w : int
  eq_xz: x = z + 9
  eq_yw: y = w - 12

  (x - 7, 2 + y) = (z + 2, w - 10)
\end{verbatim}

then running

\texttt{split}.

produces the goals

\begin{verbatim}
Type variables: <none>

  x : int
  y : int
  z : int
  w : int
  eq_xz: x = z + 9
  eq_yw: y = w - 12

  x - 7 = z + 2
\end{verbatim}

and
Type variables: <none>

x : int
y : int
z : int
w : int
eq_xz: x = z + 9
eq_yw: y = w - 12

2 + y = w - 10

\texttt{\textcopyright cong}\texttt{r}

Replace a goal whose conclusion has the form \( f t_1 \cdots t_n = f u_1 \cdots u_n \), where \( f \) is an assumption identifier or operator, with subgoals having conclusions \( t_i = u_i \) for all \( i \). Subgoals solvable by \texttt{reflexivity} are automatically closed. Also works when the operator is used in infix form.

For example, if the current goal is

\[
\begin{align*}
\text{Type variables: } &\text{<none>} \\
x : \text{int} \\
y : \text{int} \\
x' : \text{int} \\
y' : \text{int} \\
f : \text{int} \rightarrow \text{int} \rightarrow \text{int} \\
eq_{xx'}: x = x' - 2 \\
eq_{yy'}: y = y' + 2 \\
f (x + 1) (y - 1) = f (x' - 1) (y' + 1)
\end{align*}
\]

then running

\texttt{congr}.

produces the goals

\[
\begin{align*}
\text{Type variables: } &\text{<none>} \\
x : \text{int} \\
y : \text{int} \\
x' : \text{int} \\
y' : \text{int} \\
f : \text{int} \rightarrow \text{int} \rightarrow \text{int} \\
eq_{xx'}: x = x' - 2 \\
eq_{yy'}: y = y' + 2 \\
x + 1 = x' - 1
\end{align*}
\]

and

\[
\begin{align*}
\text{Type variables: } &\text{<none>} \\
x : \text{int} \\
y : \text{int} \\
x' : \text{int} \\
y' : \text{int} \\
f : \text{int} \rightarrow \text{int} \rightarrow \text{int} \\
eq_{xx'}: x = x' - 2 \\
eq_{yy'}: y = y' + 2 \\
y - 1 = y' + 1
\end{align*}
\]
And if the current goal is

```
Type variables: <none>

x : int
y : int
x' : int
y' : int
eq_xx': x = x' - 2
eq_yy': y = y' + 2

x + 1 + (y - 1) = x' - 1 + (y' + 1)
```

then running

```
congr.
```

produces this same pair of subgoals.

```

\textbf{\texttt{\textcircled{5}} subst_x | subst}

\textbf{Syntax: subst } x. \text{ Search for the first equation of the form } x = t \text{ or } t = x \text{ in the context and replace all the occurrences of } x \text{ by } t \text{ everywhere in the context and the conclusion before clearing it.}

For example, if the current goal is

```
Type variables: <none>

x : bool
y : bool
z : bool
w : bool
eq_yx: y = x
eq_yz: y = z
eq_zw: z = w

x = w
```

then running

```
subst x.
```

takes us to

```
Type variables: <none>

y : bool
z : bool
w : bool
eq_zw: z = w
eq_yz: y = z

y = w
```

from which running

```
subst y.
```

takes us to

```
Type variables: <none>

z : bool
w : bool
```
CHAPTER 3. TACTICS

eq_zw: z = w

\[
\begin{align*}
\text{z} & = \text{w} \\
\end{align*}
\]

from which running

\texttt{subst} \texttt{z}.

takes us to

Type variables: <none>

w : bool

\[
\begin{align*}
\text{w} & = \text{w} \\
\end{align*}
\]

\textbf{Syntax:} \texttt{subst}. Repeatedly apply \texttt{subst} \texttt{x} to all identifiers in the context.

For example, if the current goal is

Type variables: <none>

x : bool
y : bool
z : bool
w : bool
eq_yx: y = x
eq_yz: y = z
eq_zw: z = w

\[
\begin{align*}
x & = \text{w} \\
\end{align*}
\]

then running

\texttt{subst}.

takes us to

Type variables: <none>

x : bool

\[
\begin{align*}
x & = x \\
\end{align*}
\]

\texttt{trivial}

Try to solve the goal by using a mixture of low-level tactics. This tactic is called by the introduction pattern //.

For example, if the current goal is

Type variables: <none>

\[
\begin{align*}
\texttt{forall} & (x \ y : \texttt{int}), x = y \Rightarrow y - 1 = x - 1 \\
\end{align*}
\]

then running

\texttt{trivial}.

solves the goal. On the other hand, if the current goal is

Type variables: <none>

\[
\begin{align*}
\texttt{forall} & (x \ y \ z : \texttt{bool}), (x \land y \Rightarrow z) \Leftrightarrow (x \Rightarrow y \Rightarrow z) \\
\end{align*}
\]
then running

\texttt{trivial.}

leaves the goal unchanged.

\textbf{Fixme} Note: Be a bit more detailed about what this tactic does?

\textcircled{5} \texttt{done}

Apply \texttt{trivial} (p. 55) and fail if the goal is not closed.

\textcircled{6} \texttt{simplify $|$ simplify $\delta_1 \cdots \delta_n$ $|$ simplify $\delta$

Reduce the goal's conclusion to its $\beta\iota\xi\Lambda$-head normal form, followed by one step of parallel, strong $\delta$-reduction if \texttt{delta} is given. The $\delta$-reduction can be restricted to a set of defined symbols by replacing \texttt{delta} by a non-empty sequence of targeted symbols. You can reduce the conclusion to its $\beta$-head normal form (resp. $\iota$, $\xi$, $\Lambda$-head normal form) by using the tactic \texttt{beta} (resp. \texttt{iota}, \texttt{zeta}, \texttt{logic}). These tactics can be combined together, separated by spaces, to perform head reduction by any combination of the rule sets.

For example, if the current goal is

\begin{verbatim}
Type variables: <none>

y : bool
z : bool
imp_yz: y => z

true => true <=> (y => true /\ z)
\end{verbatim}

then running

\texttt{simplify.}

produces the goal

\begin{verbatim}
Type variables: <none>

y : bool
z : bool
imp_yz: y => z

y => z
\end{verbatim}

And if the current goal is

\begin{verbatim}
Type variables: <none>

y : bool
z : bool
imp_yz: y => z

false => false <=> (y => false /\ z)
\end{verbatim}

then running

\texttt{simplify.}

produces the goal

\begin{verbatim}
Type variables: <none>

y : bool
z : bool
imp_yz: y => z

false => false <=> (y => false /\ z)
\end{verbatim}
CHAPTER 3. TACTICS

\[ \text{imp}_yz : y \Rightarrow z \]

\[ \text{true} \]

FiXme Note: Is this the right place to define “convertible”?

\( \text{progress} \mid \text{progress} \tau \)

Break the goal into multiple simpler ones by repeatedly applying split, subst and move\( \Rightarrow \). The tactic \( \tau \) given to progress is tentatively applied after each step. For example, if the current goal is

\[
\text{forall } (x \ y \ z : \text{bool}), (x \ \forall \ y \Rightarrow z) \iff (x \Rightarrow y \Rightarrow z)
\]

then running

\[ \text{progress}. \]

solves the goal.

FiXme Note: Describe progress options.

\( \text{smt} \text{smt}-\text{options} \)

Try to solve the goal using SMT solvers. The goal is sent along with the local hypotheses plus selected axioms and lemmas. The SMT solvers used, their options, and the axiom selection algorithm are specified by smt-option.

For example, if the current goal is

\[
\text{forall } (x \ y \ z : \text{bool}), (x \ \forall \ y \Rightarrow z) \iff (x \Rightarrow y \Rightarrow z)
\]

then running

\[ \text{smt}. \]

solves the goal.

Options

- \textbf{timeout} \( n \): set the timeout for provers to \( n \) (in seconds).
- \textbf{maxprovers} \( n \): set the maximum number of provers running in parallel to \( n \)
- \textbf{prover} \{\text{prover-selector}\}: select the provers, where \text{prover-selector} is a list of modified prover names:
  - \textbf{`prover-name'':} use the listed prover;
  - \textbf{`+prover-name'':} add \text{prover-name} to the current list of provers;
  - \textbf{-`prover-name'':} remove \text{prover-name} from the current list of provers;

Examples:

- \{`Z3' `Alt-Ergo'\}: use only Z3 and Alt-Ergo;
- \{`Z3' `Alt-Ergo' -`Z3'\}: use only Alt-Ergo;
- \{`CVC4'\}: remove CVC4 from the current list of provers;
- \{`CVC4'\}: add CVC4 to the current list of provers;

FiXme Note: Describe failure states of prover selection.

- Axiom selection: axioms and lemmas are not all send to smt provers, EASYCRYPT use a strategy to automatically select them. Lemmas and axioms marked with “nosmt” are not selected by default. This strategy can be parametrized using different options:
  - unwantedlemmas=\text{dbhint}: do not send axiom/lemma selected by \text{dbhint}
  - wantedlemmas=\text{dbhint}: send axiom/lemma selected by \text{dbhint}
all: select all available axioms/lemmas except those specified by unwantedlemmas (if any).
- maxlemmas=n: set the maximum number of selected axioms/lemmas to n. Keep this number small is generally more efficient. Variant: n
- iterate: try to incrementally augment the number of selected axioms/lemmas. Last call will be equivalent to all.

**Fixme Note:** Describe dbhint options.

**Variant:** Short options.
Options can also be specified by short name, for example:

```smt 100 [+''Z3] tmo=4 mp=2```

is equivalent to

```smt maxlemmas=100 prover=[+''Z3] timeout=4 maxprovers=2```

Short options can be any substring of the full option names that uniquely identifies the desired option: when several options match, their full names are given.
Smt option can be set globally using the following syntax: `prover smt-options` **Fixme Note:** Make this a pragma?

**Remark:** By default, smt failures cannot be caught by the try (p. 69) tactical.

---

**admit**

Close the current goal by admitting it.
For example, if the current goal is

```Type variables: <none>

x : int
y : int

x = y + 1 /
  x = y - 1```

then running

```
admit.
```

solves the goal.

---

**change φ**

Replace the current goal’s conclusion by φ—φ must be convertible to the current goal’s conclusion.
For example, if the current goal is

```Type variables: <none>

y : bool
z : bool

imp_yz: y => z

true => true <=> (y => true /
  z)```

then running

```
change (y => z).
```

produces the goal

```Type variables: <none>

y : bool
z : bool```
CHAPTER 3. TACTICS

imp_yz: y => z

y => z

\[ \text{pose } x := \pi \]

Search for the first subterm \( t \) of the goal’s conclusion matching \( \pi \) and leading to the full instantiation of the pattern. Then introduce to the goal’s context, after instantiation, the local definition \( x := t \), and abstract all occurrences of \( t \) in the goal’s conclusion as \( x \). An occurrence selector can be used (see Subsection 3.3.2).

For example, if the current goal is

Type variables: <none>

\( x : \text{int} \)
\( y : \text{int} \)

\( 2 \times ((x + 1 + y) \times x) = (x + 1 + y) \times x + (x + 1 + y) \times x \)

then running

\[ \text{pose } z := (_ + y) \times _. \]

produces the goal

Type variables: <none>

\( x : \text{int} \)
\( y : \text{int} \)
\( z : \text{int} := (x + 1 + y) \times x \)

\( 2 \times z = z + z \)

\[ \text{have } \iota : \phi \]

Logical cut. Generate two subgoals: one whose conclusion is the cut formula \( \phi \), and one with conclusion \( \phi \Rightarrow \psi \) where \( \psi \) is the current goal’s conclusion. Moreover, the introduction pattern \( \iota \) is applied to the second subgoal.

For example, if the current goal is

Type variables: <none>

\( x : \text{bool} \)
\( \text{notnot}_x : (x \Rightarrow \text{false}) \Rightarrow \text{false} \)

then running

\[ \text{cut } \text{excl_or} : x \lor (x \Rightarrow \text{false}). \]

produces the goals

Type variables: <none>

\( x : \text{bool} \)
\( \text{notnot}_x : (x \Rightarrow \text{false}) \Rightarrow \text{false} \)

\( x \lor (x \Rightarrow \text{false}) \)

and
Type variables: <none>

\[
\begin{align*}
x & : \text{bool} \\
\text{notnot}_x & : (x => \text{false}) => \text{false} \\
\text{excl_or} & : x \lor (x => \text{false})
\end{align*}
\]

Syntax: \textit{have }τ: φ \textit{ by } τ. Attempts to use tactic τ to close the first subgoal (corresponding to the cut formula φ), and fails if impossible.

- \textbf{cut }τ: φ
  
  Same as \textit{have} (p. 59).

- \textbf{apply }\ p | \textit{apply }/\ p_1 \cdots /\ p_n \ | \textit{apply }\ p \text{ in } H
  
  Syntax: \textit{apply } p. Tries to match the conclusion of the proof term p with the goal’s conclusion. If the match succeeds and leads to the full instantiation of the pattern, then the goal is replaced, after instantiation, with the subgoals of the proof term.

Consider the declarations

\[
\begin{align*}
pred & P : \text{int}. \\
pred & Q : \text{int}. \\
pred & R : \text{int}. \\
axiom & P (x : \text{int}) : P x. \\
axiom & Q (x : \text{int}) : P x => Q x. \\
axiom & R (x : \text{int}) : P(x + 1) => Q x => R x.
\end{align*}
\]

If the current goal is

\[
\begin{align*}
\text{Type variables: } <\text{none}> \\
x & : \text{int} \\
R & x
\end{align*}
\]

then running

\[
\textit{apply } R.
\]

produces the goals

\[
\begin{align*}
\text{Type variables: } <\text{none}> \\
x & : \text{int} \\
P & (x + 1)
\end{align*}
\]

and

\[
\begin{align*}
\text{Type variables: } <\text{none}> \\
x & : \text{int} \\
Q & x
\end{align*}
\]

And running

\[
\textit{apply } (R x _ (Q x _)).
\]

from that initial goal produces the goals
Syntax: \texttt{apply }/ p_1 \cdots / p_n. \text{ Apply the proof terms } p_1, \ldots , p_n \text{ in sequence. At each stage of this process, we have some number of goals. Initially, we have just the current goal. After applying } p_1 \text{, we have whatever goals } p_1 \text{ has produced from the current goal. } p_2 \text{ is applied to the last of these goals, and that last goal is replaced by the goals produced by running } p_2, \text{ etc. Fails without changing the goal if any of these applications fails. For example, if the current goal is}

\begin{align*}
\text{Type variables: <none>} \\
x : \text{int} \\
P (x + 1)
\end{align*}

and

\begin{align*}
\text{Type variables: <none>} \\
x : \text{int} \\
P x
\end{align*}

then running

\begin{align*}
\text{apply } / R / Q / P / P.
\end{align*}

solves the goal.

Syntax: \texttt{apply } p \text{ in } H. \text{ Apply } p \text{ in forward reasoning to } H, \text{ replacing } H \text{ by the result. For example, if the current goal is}

\begin{align*}
\text{Type variables: <none>} \\
x : \text{int} \\
\text{HP: } P (x + 1) \\
Q x \Rightarrow R x
\end{align*}

then running

\begin{align*}
\text{apply } R \text{ in } HP.
\end{align*}

produces the goal

\begin{align*}
\text{Type variables: <none>} \\
x : \text{int} \\
\text{HP: } Q x \Rightarrow R x \\
Q x \Rightarrow R x
\end{align*}

© \texttt{exact } p \mid \texttt{exact } / p_1 \cdots / p_n.

Syntax: \texttt{exact } p. \text{ Equivalent to } \texttt{by } apply \ p, \text{ i.e., apply the given proof-term and then try to close the goals with trivial—failing if not all goals can be closed.}

Syntax: \texttt{exact } / p_1 \cdots / p_n. \text{ Equivalent to } \texttt{by } apply / p_1 \cdots / p_n.
CHAPTER 3. TACTICS

rewite $\pi_1 \cdots \pi_n$ | rewrite $\pi_1 \cdots \pi_n$ in $H$

Syntax: rewrite $\pi_1 \cdots \pi_n$. Rewrite the rewrite-pattern $\pi_1 \cdots \pi_n$ from left to right, where the $\pi_i$ can be of the following form:

- one of $\text{//}$, $\text{/=}$, $\text{//=}$,
- a proof-term $p$, or
- a pattern prefixed by $\text{/}$ (slash).

The two last forms can be prefixed by a direction indicator (the sign $-$, see Subsection 3.3.2), followed by an occurrence selector (see Subsection 3.3.2), followed (for proof-terms only) by a repetition marker ($!$, $?$, $n!$ or $n?$). All these prefixes are optional.

Depending on the form of $\pi$, rewrite $\pi$ does the following:

- For $\text{//}$, $\text{/=}$, and $\text{//=}$. see Subsection 3.3.3.

- If $\pi$ is a proof-term with conclusion $f_1 = f_2$, then rewrite searches for the first subterm of the goal’s conclusion matching $f_1$ and resulting in the full instantiation of the pattern. It then replaces, after instantiation of the pattern, all the occurrences of $f_1$ by $f_2$ in the goal’s conclusion, and creates new subgoals for the instantiations of the assumptions of $p$. If no subterms of the goal’s conclusion match $f_1$ or if the pattern cannot be fully instantiated by matching, the tactic fails. The tactic works the same if the pattern ends by $f_1 <=>$ $f_2$. If the direction indicator $-$ is given, rewrite works in the reverse direction, searching for a match of $f_2$ and then replacing all occurrences of $f_2$ by $f_1$.

- If $\pi$ is a $\text{/}$-prefixed pattern of the form $o p_1 \cdots p_n$, with $o$ a defined symbol, then rewrite searches for the first subterm of the goal’s conclusion matching $o p_1 \cdots p_n$ and resulting in the full instantiation of the pattern. It then replaces, after instantiation of the pattern, all the occurrences of $o p_1 \cdots p_n$ by the $\beta\delta$ head-normal form of $o p_1 \cdots p_n$, where the $\delta$-reduction is restricted to subterms headed by the symbol $o$. If no subterms of the goal’s conclusion match $o p_1 \cdots p_n$ or if the pattern cannot be fully instantiated by matching, the tactic fails. If the direction indicator $-$ is given, rewrite works in the reverse direction, searching for a match of the $\beta\delta_o$ head-normal of $o p_1 \cdots p_n$ and then replacing all occurrences of this head-normal form with $o p_1 \cdots p_n$.

The occurrence selector restricts which occurrences of the matching pattern are replaced in the goal’s conclusion—see Subsection 3.3.3.

Repetition markers allow the repetition of the same rewriting. For instance, rewrite $\pi$ leads to do! rewrite $\pi$. See the tactical do for more information.

Lastly, rewrite $\pi_1 \cdots \pi_n$ is equivalent to rewrite $\pi_1$; ...; rewrite $\pi_n$.

For example, if the current goal is

```
Type variables: <none>

x : int
y : int
eq_xy : x = y
```

```
forall (z : int), y = z => x = z
```

then running

```
rewrite eq_xy.
```

produces
CHAPTER 3. TACTICS

Type variables: <none>

\[ \begin{align*}
    x &: \text{int} \\
    y &: \text{int} \\
    \text{eq}_{xy}: x = y \\
    \forall (z : \text{int}), y = z \Rightarrow y = z
\end{align*} \]

from which running

\[ \text{rewrite} - \{1\} \text{eq}_{xy}. \]

produces

Type variables: <none>

\[ \begin{align*}
    x &: \text{int} \\
    y &: \text{int} \\
    \text{eq}_{xy}: x = y \\
    \forall (z : \text{int}), x = z \Rightarrow y = z
\end{align*} \]

from which running

\[ \text{rewrite} - \text{eq}_{xy}. \]

produces

Type variables: <none>

\[ \begin{align*}
    x &: \text{int} \\
    y &: \text{int} \\
    \text{eq}_{xy}: x = y \\
    \forall (z : \text{int}), x = z \Rightarrow x = z
\end{align*} \]

Syntax: \( \text{rewrite} \ \pi_1 \cdots \pi_n \ \text{in} \ \text{H} \). Like the preceding case, except rewriting is done in the hypothesis \( H \) instead of in the goal’s conclusion. Rewriting using a proof term is only allowed when the proof term was defined globally or before the assumption \( H \).

For example, if the current goal is

Type variables: <none>

\[ \begin{align*}
    x &: \text{int} \\
    y &: \text{int} \\
    \text{eq}_{xy}: x = y \\
    z &: \text{int} \\
    \text{eq}_{xz}: y = z \\
    x = z
\end{align*} \]

then running

\[ \text{rewrite} - \text{eq}_{xy} \ \text{in} \ \text{eq}_{xz}. \]

produces

Type variables: <none>

\[ \begin{align*}
    x &: \text{int} \\
    y &: \text{int} \\
    \text{eq}_{xy}: x = y
\end{align*} \]
CHAPTER 3. TACTICS

64

\[ z : \text{int} \]
\[ \text{eq}_xz: x = z \]

\[ x = z \]

\[ \text{case} \phi \mid \text{case} \]

**Syntax:** case \( \phi \). Assuming the goal’s conclusion is *not* a statement judgement, do an excluded-middle case analysis on \( \phi \), substituting \( \phi \) in the goal’s conclusion.

For example, if the current goal is

```
Type variables: <none>

x : int
y : int
abs_bnd: \texttt{abs} bnd: \texttt{|x - y| <= 10}
```

\[ x - y <= 10 \lor y - x <= 10 \]

then running

```
case (x <= y).
```

produces the goals

```
Type variables: <none>

x : int
y : int
abs_bnd: \texttt{abs} bnd: \texttt{|x - y| <= 10}
```

\[ x <= y => x - y <= 10 \lor y - x <= 10 \]

and

```
Type variables: <none>

x : int
y : int
abs_bnd: \texttt{abs} bnd: \texttt{|x - y| <= 10}
```

\[ ! x <= y => x - y <= 10 \lor y - x <= 10 \]

**Syntax:** case. Destruct the top assumption of the goal’s conclusion, generating subgoals that are dependent upon the kind of assumption destructed. *This form of the tactic can be followed by the generalization tactical—see Subsection 3.3.3.*

- **(conjunction)** For example, if the current goal is

```
Type variables: <none>

x : int
y : int
z : int
```

\[ x = y \lor y = z => x = z \]

then running

```
case.
```
produces the goal

Type variables: <none>

\[
\begin{align*}
x & : \text{int} \\
y & : \text{int} \\
z & : \text{int}
\end{align*}
\]

\[x = y \Rightarrow y = z \Rightarrow x = z\]

\&\& works identically.

- (disjunction) For example, if the current goal is

Type variables: <none>

\[
\begin{align*}
x & : \text{int} \\
y & : \text{int}
\end{align*}
\]

\[x < y \lor y < x \Rightarrow x - y \neq 0\]

then running

\[
\text{case.}
\]

produces the goals

Type variables: <none>

\[
\begin{align*}
x & : \text{int} \\
y & : \text{int}
\end{align*}
\]

\[x < y \Rightarrow x - y \neq 0\]

and

Type variables: <none>

\[
\begin{align*}
x & : \text{int} \\
y & : \text{int}
\end{align*}
\]

\[y < x \Rightarrow x - y \neq 0\]

\|\| works identically.

- (existential) For example, if the current goal is

Type variables: <none>

\[
\begin{align*}
(\exists x : \text{int}, 0 < x < 5) & \Rightarrow (\exists x : \text{int}, 5 < x < 10)
\end{align*}
\]

then running

\[
\text{case.}
\]

produces the goal

Type variables: <none>

\[
\begin{align*}
\forall x : \text{int}, 0 < x < 5 & \Rightarrow (\exists x_0 : \text{int}, 5 < x_0 < 10)
\end{align*}
\]
• (unit) Substitutes \( \text{tt} \) for the assumption in the remainder of the conclusion.

• (bool) For example, if the current goal is

\[
\text{Type variables: <none>}
\]

\[
\text{forall (x y : bool), x <-> y => x = y}
\]

then running

```plaintext
\text{case.}
```

produces the goals

\[
\text{Type variables: <none>}
\]

\[
\text{forall (y : bool), true <-> y => true = y}
\]

and

\[
\text{Type variables: <none>}
\]

\[
\text{forall (y : bool), false <-> y => false = y}
\]

• (product type) For example, if the current goal is

\[
\text{Type variables: <none>}
\]

\[
\text{forall (x y : bool * bool),}
\]

\[
\text{x <> y => x.1 <> y.1 \lor x.2 <> y.2}
\]

then running

```plaintext
\text{case.}
```

produces the goal

\[
\text{Type variables: <none>}
\]

\[
\text{forall (x1 x2 : bool) (y : bool * bool),}
\]

\[
(x1, x2) <> y =>
\]

\[
(x1, x2).1 <> y.1 \lor (x1, x2).2 <> y.2
\]

• (inductive datatype) Consider the inductive datatype declaration:

\[
\text{type tree = [Leaf | Node of bool & tree & tree].}
\]

Then, if the current goal is

\[
\text{Type variables: <none>}
\]

\[
\text{forall (tr : tree),}
\]

\[
\text{tr = Leaf \lor}
\]

\[
\text{exists (b : bool) (tr1 tr2 : tree), tr = Node b tr1 tr2}
\]
then running

\texttt{case.}

produces the goals

Type variables: <none>

\begin{align*}
\text{Leaf} &= \text{Leaf} \\
\text{exists } (b : \text{bool}) \ (\text{tr1 tr2 : tree}), \ \text{Leaf} = \text{Node } b \ \text{tr1 tr2}
\end{align*}

and

Type variables: <none>

\begin{align*}
\text{forall } (b : \text{bool}) \ (t \ t0 : \text{tree}), \\
\text{Node } b \ t \ t0 &= \text{Leaf} \\
\text{exists } (b0 : \text{bool}) \ (\text{tr1 tr2 : tree}), \\
\text{Node } b \ t \ t0 &= \text{Node } b0 \ \text{tr1 tr2}
\end{align*}

\subsection*{\texttt{elim} | \texttt{elim /L}}

\large\textbf{Syntax: elim.} Eliminates the top assumption of the goal’s conclusion, generating subgoals that are dependent upon the kind of assumption eliminated. \textit{This tactic can be followed by the generalization tactical—see Subsection 3.3.3.}

\texttt{elim} mostly works identically to \texttt{case} (p. 64), the exception being inductive datatype and the integers (for which a built-in induction principle is applied—see the other form).

Consider the inductive datatype declaration:

\begin{align*}
type \ tree &= \text{[Leaf | Node of bool & tree & tree]}. \\
\text{Then, if the current goal is}
\end{align*}

Type variables: <none>

\begin{align*}
p : \text{tree} \rightarrow \text{bool} \\
p \text{basis: } p \ \text{Leaf} \\
p \text{indstep: } \text{forall } (b : \text{bool}) \ (\text{tr1 tr2 : tree}), \\
\ & \ p \ \text{tr1} \Rightarrow p \ \text{tr2} \Rightarrow p \ (\text{Node } b \ \text{tr1 tr2}) \\
\text{forall } (\text{tr : tree}), \ p \ \text{tr}
\end{align*}

running

\texttt{elim.}

produces the goals

Type variables: <none>

\begin{align*}
p : \text{tree} \rightarrow \text{bool} \\
p \text{basis: } p \ \text{Leaf} \\
p \text{indstep: } \text{forall } (b : \text{bool}) \ (\text{tr1 tr2 : tree}), \\
\ & \ p \ \text{tr1} \Rightarrow p \ \text{tr2} \Rightarrow p \ (\text{Node } b \ \text{tr1 tr2}) \\
p \ \text{Leaf}
\end{align*}

and
CHAPTER 3. TACTICS

Type variables: <none>

\[ p : \text{tree} \to \text{bool} \]

basis: \( p \text{ Leaf} \)

indstep: \( \forall (b : \text{bool}) (\text{tr1 tr2 : tree}), \]
\[ p \text{ tr1} \Rightarrow p \text{ tr2} \Rightarrow p (\text{Node } b \text{ tr1 tr2}) \]

\[ \forall (b : \text{bool}) (t t0 : \text{tree}), p t \Rightarrow p t0 \Rightarrow p (\text{Node } b t t0) \]

Syntax: \texttt{elim /L}. Eliminates the top assumption of the goal’s conclusion using the supplied induction principle lemma. \textit{This tactic can be followed by the generalization tactical—see Subsection 3.3.3.} For example, consider the declarations

\texttt{type tree = [Leaf \mid \text{Node } of \; \text{bool} \& \text{tree} \& \text{tree}].}

\texttt{op \text{rev} (t : \text{tree}) : \text{tree} =}
\[ \text{with } t = \text{Leaf} \Rightarrow \text{Leaf} \]
\[ \text{with } t = \text{Node } b \; \text{tr1 tr2} \Rightarrow \text{Node } b \; (\text{rev } \text{tr1}) \; (\text{rev } \text{tr2}). \]

and suppose we’ve already proved

\texttt{lemma \text{IndPrin} :}
\[ \forall (p : \text{tree} \to \text{bool}) (\text{tr : tree}), \]
\[ p \text{ Leaf} \Rightarrow \]
\[ (\forall (b : \text{bool}) (\text{tr1 tr2 : tree}), \]
\[ p \text{ tr1} \Rightarrow p \text{ tr2} \Rightarrow p (\text{Node } b \text{ tr1 tr2})) \Rightarrow \]
\[ p \text{ tr}. \]

Then, if the current goal is

Type variables: <none>

\[ \forall (t : \text{tree}), \text{rev } (\text{rev } t) = t \]

running

\texttt{elim /IndPrin.}

produces the goals

Type variables: <none>

\[ \text{rev } (\text{rev } \text{Leaf}) = \text{Leaf} \]

and

Type variables: <none>

\[ \forall (b : \text{bool}) (\text{tr1 tr2 : tree}), \]
\[ \text{rev } (\text{rev } \text{tr1}) = \text{tr1} \Rightarrow \]
\[ \text{rev } (\text{rev } \text{tr2}) = \text{tr2} \Rightarrow \text{rev } (\text{rev } (\text{Node } b \text{ tr1 tr2})) = \text{Node } b \text{ tr1 tr2} \]

When we consider the \texttt{Int} theory in Chapter 5, we’ll discuss the induction principle on the integers.

\texttt{\copyright \; algebra}

\texttt{Fixme Note: Missing description of algebra.}
3.3.5 Tacticals

Tactics can be combined together, composed and modified by tacticals. We’ve already seen the introduction and generalization tacticals, which turn a tactic $\tau$ and a list of patterns into a composite tactic, which may then combined with other tactics.

3.3.5.1 $\tau_1; \tau_2$

Apply $\tau_2$ to all the subgoals generated by $\tau_1$. Sequencing groups to the left, so that $\tau_1; \tau_2; \tau_3$ means $(\tau_1; \tau_2); \tau_3$.

For example, if the current goal is

```
Type variables: <none>

x : bool
y : bool
z : bool

(x \& y) \& z => x \& y \& z
```

then running

```
case; case.
```

produces the goals

```
Type variables: <none>

x : bool
y : bool
z : bool

x => y => z => x \& y \& z
```

3.3.5.2 $\tau_1 \{ \tau_1 | \cdots | \tau_n \}$

Run $\tau_1$, which must generate exactly $n$ subgoals, $G_1, \ldots, G_n$. Then apply $\tau'_i$ to $G_i$, for all $i$.

For example, if the current goal is

```
Type variables: <none>

x : bool
y : bool
z : bool
tr_x: x
tr_y: y
tr_z: z

x \& y \& z
```

then running

```
split; [assumption | split; assumption].
```

solves the goal.

3.3.5.3 try $\tau$

Execute the tactic $\tau$ if it succeeds; do nothing (leave the goal unchanged) if it fails.
Remark. By default, EASYCRYPT proofs are run in strict mode. In this mode, smt failures cannot be caught using try. This allows EASYCRYPT to always build the proof tree correctly, even in weak check mode, where smt calls are assumed to succeed. Inside a strict proof, weak check mode can be turned on and off at will, allowing for the fast replay of proof sections during development. In any event, we recommend never using try smt: a little thought is much more cost-effective than failing smt calls.

\[ \text{do} \; \tau \]

Apply \( \tau \) to the current goal, then repeatedly apply it to all subgoals, stopping on a branch only when it fails. An error is produced if \( \tau \) does not apply to the current goal.

For example, if the current goal is

<table>
<thead>
<tr>
<th>Type variables: &lt;none&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>x : bool</td>
</tr>
<tr>
<td>y : bool</td>
</tr>
<tr>
<td>z : bool</td>
</tr>
<tr>
<td>w : bool</td>
</tr>
<tr>
<td>((x &amp;&amp; y) &amp;&amp; z) &amp;&amp; w &amp;&amp; (x &amp;&amp; y &amp;&amp; z) &amp;&amp; w \Rightarrow w</td>
</tr>
</tbody>
</table>

then running

\[ \text{do}! \; \text{case.} \]

produces the goals

<table>
<thead>
<tr>
<th>Type variables: &lt;none&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>x : bool</td>
</tr>
<tr>
<td>y : bool</td>
</tr>
<tr>
<td>z : bool</td>
</tr>
<tr>
<td>w : bool</td>
</tr>
<tr>
<td>x =&gt; y =&gt; z =&gt; w =&gt; w</td>
</tr>
</tbody>
</table>

and

<table>
<thead>
<tr>
<th>Type variables: &lt;none&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>x : bool</td>
</tr>
<tr>
<td>y : bool</td>
</tr>
<tr>
<td>z : bool</td>
</tr>
<tr>
<td>w : bool</td>
</tr>
<tr>
<td>x =&gt; y &amp;&amp; z =&gt; w =&gt; w</td>
</tr>
</tbody>
</table>

Variants.

- **do? \( \tau \)** apply \( \tau \) 0 or more times, until it fails
- **do n! \( \tau \)** apply \( \tau \) with depth exactly \( n \)
- **do n? \( \tau \)** apply \( \tau \) with depth at most \( n \)

\[ \tau; \; \text{first} \; \tau_2 \]

Apply the tactic \( \tau_1 \), then apply \( \tau_2 \) on the first subgoal generated by \( \tau_1 \), leaving the other goals unchanged. An error is produced if no subgoals are generated by \( \tau_1 \).
CHAPTER 3. TACTICS

Variants.

$\tau_1$: \texttt{first }$n$ $\tau_2$ apply $\tau_2$ on the first $n$ subgoals generated by $\tau_1$

$\tau_1$: \texttt{last }$\tau_2$ apply $\tau_2$ on the last subgoal generated by $\tau_1$

$\tau_1$: \texttt{last }$n$ $\tau_2$ apply $\tau_2$ on the last $n$ subgoals generated by $\tau_1$

$\tau$: \texttt{first }$n$ \texttt{last }$\tau_2$ reorder the subgoals generated by $\tau$, moving the first $n$ to the end of the list

$\tau$: \texttt{last }$n$ \texttt{first }$\tau_2$ reorder the subgoals generated by $\tau$, moving the last $n$ to the beginning of the list

$\tau$: \texttt{last }$\tau_2$ \texttt{first } reorder the subgoals generated by $\tau$, moving the last one to the beginning of the list

$\tau$: \texttt{first }$\tau_2$ \texttt{last } reorder the subgoals generated by $\tau$, moving the first one to the end of the list

For example, if the current goal is

\[
\text{Type variables: <none>}
\]

\[
x : \text{bool}
\]

\[
y : \text{bool}
\]

\[
z : \text{bool}
\]

\[
(x \land y \Rightarrow z) \iff (x \Rightarrow y \Rightarrow z)
\]

then running

\[
\text{split; last first}.
\]

produces the goals

\[
\text{Type variables: <none>}
\]

\[
x : \text{bool}
\]

\[
y : \text{bool}
\]

\[
z : \text{bool}
\]

\[
(x \Rightarrow y \Rightarrow z) \Rightarrow x \land y \Rightarrow z
\]

and

\[
\text{Type variables: <none>}
\]

\[
x : \text{bool}
\]

\[
y : \text{bool}
\]

\[
z : \text{bool}
\]

\[
(x \land y \Rightarrow z) \Rightarrow x \Rightarrow y \Rightarrow z
\]

Apply the tactic $\tau$ and try to close all the generated subgoals using \texttt{trivial} (p. 55). Fail if not all subgoals can be closed.

Remark. Inside the a lemma’s proof, \texttt{by []} is equivalent to \texttt{by trivial}. But the form

\[
\text{lemma } \cdots \text{ by []}.
\]

means

\[
\text{lemma } \cdots \text{ by (trivial; smt)}.
\]
3.4 Program Logics

In this section, we describe the tactics of EASYCRYPT’s three program logics: pRHL, pHL and HL. There are five rough classes of program logic tactics:

1. those that actually reason about the program in Hoare logic style;
2. those that correspond to semantics-preserving program transformations or compiler optimizations;
3. those that operate at the level of specifications, strengthening, combining or splitting goals without modifying the program;
4. tactics that automate the application of other tactics;
5. advanced tactics for handling eager/lazy sampling and bounding the probability of failure.

We discuss these five classes in turn.

Some of the program reasoning tactics have two modes when used on goals whose conclusions are pRHL statement judgements. Their default mode is to operate on both programs at once. When a side is specified (using τ{1} or τ{2}), a one-sided variant is used, with 1 referring to the left program, and 2 to the right one.

3.4.1 Tactics for Reasoning about Programs

proc

Syntax: proc. Turn a goal whose conclusion is a pRHL, pHL or HL judgement involving concrete procedure(s) into one whose conclusion is a statement judgement by replacing the concrete procedure(s) by their body/ies. Assertions about res/res{i} are turned into ones about the value(s) returned by the procedure(s).

For example, if the current goal is

<table>
<thead>
<tr>
<th>Type variables: &lt;none&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>pre = ={x, y}</td>
</tr>
<tr>
<td>G1.f ~ G2.f</td>
</tr>
<tr>
<td>post = ={res}</td>
</tr>
</tbody>
</table>

then running

proc.

produces the goal

<table>
<thead>
<tr>
<th>Type variables: &lt;none&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;1 (left ) : G1.f</td>
</tr>
<tr>
<td>&amp;2 (right) : G2.f</td>
</tr>
<tr>
<td>pre =</td>
</tr>
<tr>
<td>(x{1}, y{1}).'1 = (x{2}, y{2}).'1 /\</td>
</tr>
<tr>
<td>(x{1}, y{1}).'2 = (x{2}, y{2}).'2</td>
</tr>
<tr>
<td>x &lt;- x + 1</td>
</tr>
<tr>
<td>y &lt;- y + 1</td>
</tr>
<tr>
<td>post = x{1} + y{1} = x{2} + y{2}</td>
</tr>
</tbody>
</table>

(1) y <- y + 1
(2) x <- x + 1
**Syntax:** proc \( I \). Reduce a goal whose conclusion is a pRHL judgement involving the same abstract procedure (but perhaps using different implementations of its oracles) (resp., an HL judgement involving an abstract procedure) to goals whose conclusions are pRHL (resp., HL) judgements on those oracles, plus goals with ambient logic conclusions checking the original judgement’s pre- and postconditions allow such a reduction (the preconditions must assume \( I \) and, in the pRHL case, the equality of the abstract procedure’s parameter(s) and the global variables of the module in which the procedure is contained (except in the case when the module’s type specifies that the abstract procedure initializes its global variables; the postconditions may assume \( I \) and, in the pRHL case, the equality of the results of the procedure call(s) and the values of the global variables). The generated pRHL/HL subgoals have pre- and postconditions assuming/asserting \( I \); in the pRHL case, the preconditions also assume the equality of the oracles’ parameters, and their postconditions also assert the equality of the oracles’ results).

For example, given the declarations

```plaintext
module type OR = {
  proc f1() : unit
  proc f2() : unit
  proc f3() : unit
}.

module Or : OR = {
  var x : int
  proc f1() : unit = {
    x <- x + 2;
  }
  proc f2() : unit = {
    x <- x - 2;
  }
  proc f3() : unit = {
    x <- x + 1;
  }
}.

module type T(O : OR) = {
  proc g() : unit {O.f1 O.f2}
}.
```

if the current goal is

```
M : T{Or}
pre = \{glob M\} \land Or.x{1} \mod 2 = 0 \land Or.x{2} \mod 2 = 0
M(Or).g ~ M(Or).g
post = Or.x{1} \mod 2 = 0 \land Or.x{2} \mod 2 = 0
```

then running

```
proc (Or.x{1} \mod 2 = 0 \land Or.x{2} \mod 2 = 0).
```

produces the goals

```
M : T{Or}
forall \&1 \&2,
```
CHAPTER 3. TACTICS

The tactic would fail without the module restriction $\mathcal{T}(\text{Or})$ on $M$, as then $M$ could directly manipulate $\text{Or}.x$. It would also fail if, in the declaration of the module type $\mathcal{T}$, $g$ were given access to $\text{Or}.f$. Syntax: proc $B$ $I$. Like proc $I$, but just for $\text{pRHL}$ judgements and uses “upto-bad” (upto-failure) reasoning, where the bad (failure) event, $B$, is evaluated in the second program’s memory, and the invariant $I$ only holds up to the point when failure occurs. In addition to subgoals whose conclusions are $\text{pRHL}$ judgments involving the oracles the abstract procedure may query (their preconditions assume $I$ and the equality of oracles’ parameters, as well as that $B$ is false; their postconditions assert $I$ and the equality of the oracles’ results—but only when $B$ does not hold), subgoals are generated that check that: the original judgement’s pre- and postconditions support the reduction; the abstract procedure is lossless, assuming the losslessness of the oracles it may query; the oracles used by the abstract procedure in the first program are lossless once the bad event occurs; and the oracles used by the abstract procedure in the second program guarantee the stability of the failure event with probability 1.

For example, suppose we have the following declarations

```plaintext
module type OR = {
    proc qry(x : int) : int
}.

op low : int = -100.
op upp : int = 100.
```
module Or1 : OR = {
    var qry, rsp : int
    var queried : bool

    proc qry(x : int) : int = {
        var y : int;
        if (x = qry) {
            y <- rsp;
            queried <- true;
        } else {
            y <$ [low .. upp];
        }
        return y;
    }
}.}

module Or2 : OR = {
    var qry : int
    var queried : bool

    proc qry(x : int) : int = {
        var y : int;
        y <$ [low .. upp];
        queried <- queried / x = qry;
        return y;
    }
}.}

module type ADV(O : OR) = {
    proc * f() : bool
}.}

Then, if the current goal is

running
proc Or2.queried (Or1.qry{1} = Or2.qry{2}).

produces the goals

forall &1 &2,
    Or1.qry{1} = Or2.qry{2} =>
    !Or2.queried{2} => true \ Or1.qry{1} = Or2.qry{2}
CHAPTER 3. TACTICS

and

Type variables: <none>

Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
            islossless O.qry => islossless Adv(O).f

forall &1 &2,
  (!Or2.quered{2} =>
  ={res} / \ ={glob Adv} / \ Or1.qry{1} = Or2.qry{2}) =>
  !Or2.quered{2} => ={res}

and

Type variables: <none>

Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
            islossless O.qry => islossless Adv(O).f

forall (O <: OR{Adv}), islossless O.qry => islossless Adv(O).f

and

Type variables: <none>

Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
            islossless O.qry => islossless Adv(O).f

pre = !Or2.quered{2} / \ ={x} / \ Or1.qry{1} = Or2.qry{2}
    Or1.qry = Or2.qry

post = !Or2.quered{2} => ={res} / \ Or1.qry{1} = Or2.qry{2}

and

Type variables: <none>

Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
            islossless O.qry => islossless Adv(O).f

forall &2, Or2.quered{2} => islossless Or1.qry

and

Type variables: <none>

Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
            islossless O.qry => islossless Adv(O).f

forall _,
  phoare[ Or2.qry : Or2.quered / \ true => Or2.quered / \ true ] = 1%r

Syntax: proc B I J. Like proc B I, but where the extra invariant, J, holds after failure has occurred. In the pRHL subgoals involving oracles called by the abstract procedure: the preconditions assume I and the equality of the oracles’ parameters, as well as that B is false; and the postconditions assert
• $I$ and the equality of the oracles’ results—when $B$ does not hold; and
• $J$—when $B$ does hold.

For example, given the declarations of the `proc B I` example, if the current goal is

```
Type variables: <none>

Adv: ADV(Or1, Or2)
ll_Adv_f: forall (O <: OR{Adv}),
    islossless O.qry => islossless Adv(O).f
```

pre = Or1.qry{1} = Or2.qry{2} \ Or1.queried{1} = Or2.queried{2}

```
Adv(Or1).f - Adv(Or2).f
```

post = Or1.queried{1} = Or2.queried{2} \ (!Or2.queried{2} => ={res})

then running

```
proc Or2.queried
    (Or1.qry{1} = Or2.qry{2} \ Or1.queried{1} = Or2.queried{2})
    (Or1.queried{1} = Or2.queried{2})
```

produces the goals

```
Type variables: <none>

Adv: ADV(Or1, Or2)
ll_Adv_f: forall (O <: OR{Adv}),
    islossless O.qry => islossless Adv(O).f
```

```
forall &1 &2,
    Or1.qry{1} = Or2.qry{2} \ Or1.queried{1} = Or2.queried{2} =>
    if Or2.queried{2} then Or1.queried{1} = Or2.queried{2}
    else
        true \ /
        Or1.qry{1} = Or2.qry{2} \ Or1.queried{1} = Or2.queried{2}
```

and

```
Type variables: <none>

Adv: ADV(Or1, Or2)
ll_Adv_f: forall (O <: OR{Adv}),
    islossless O.qry => islossless Adv(O).f
```

```
forall &1 &2,
    if Or2.queried{2} then Or1.queried{1} = Or2.queried{2}
    else
        ={res} \ /
        ={glob Adv} \ /
        Or1.qry{1} = Or2.qry{2} \ Or1.queried{1} = Or2.queried{2} =>
        Or1.queried{1} = Or2.queried{2} \ (!Or2.queried{2} => ={res})
```

and

```
Type variables: <none>

Adv: ADV(Or1, Or2)
ll_Adv_f: forall (O <: OR{Adv}),
    islossless O.qry => islossless Adv(O).f
```
forall (O <: OR{Adv}), islossless O.qry => islossless Adv(O).f

Type variables: <none>

Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
    islossless O.qry => islossless Adv(O).f

pre =
  !Or2.queried{2} /
  ={x} /
  Or1.qry{1} = Or2.qry{2} /
  Or1.queried{1} = Or2.queried{2}

Or1.qry - Or2.qry

post =
  if Or2.queried{2} then Or1.queried{1} = Or2.queried{2}
  else
      ={res} /
      Or1.qry{1} = Or2.qry{2} /
      Or1.queried{1} = Or2.queried{2}

Syntax: proc*. Reduce a PRHL (resp., HL) judgement to a PRHL (resp., HL) statement judgement involving calls (resp., a call) to the procedures (resp., procedure).

For example, if the current goal is

pre = ={x, y}

G1.f ~ G2.f
post = \{\text{res}\}

then running

\text{proc}\ast.

produces the goal

Type variables: <none>

$k1$ (left) : \text{G1.f}
$k2$ (right) : \text{G2.f}

pre = \{(x, y)\}

$r <\exists \text{G1.f}(x, y)$ \quad (1) \quad r <\exists \text{G2.f}(x, y)$

post = \{(r)\}

\textbf{Remark.} This tactic is particularly useful in combination with \textit{inline} (p. 106) when faced with a \textit{pRHL} judgment where one of the procedures is concrete and the other is abstract.

\textcircled{5} \textbf{skip}

If the goal’s conclusion is a statement judgement whose program(s) are empty, reduce it to the goal whose conclusion is the ambient logic formula $P \Rightarrow Q$, where $P$ is the original conclusion’s precondition, and $Q$ is its postcondition.

For example, if the current goal is

Type variables: <none>

$k1$ (left) : \text{M.f}
$k2$ (right) : \text{N.f}

pre = $x\{1\} = -x\{2\} \land =y$

post = $x\{1\} + y\{1\} = -(x\{2\} - y\{2\})$

then running

\textbf{skip}.

produces the goal

Type variables: <none>

\texttt{forall} $k1, k2, x\{1\} = -x\{2\} \land =y \Rightarrow x\{1\} + y\{1\} = -(x\{2\} - y\{2\})$

\textcircled{5} \textbf{seq}

\textbf{Syntax:} seq $n_1 n_2 : R$. \textbf{pRHL sequence rule.} If $n_1$ and $n_2$ are natural numbers and the goal’s conclusion is a \textit{pRHL} statement judgement with precondition $P$, postcondition $Q$ and such that the lengths of the first and second programs are at least $n_1$ and $n_2$, respectively, then reduce the goal to two subgoals:
• A first goal whose conclusion has precondition $P$, postcondition $R$, first program consisting of the first $n_1$ statements of the original goal’s first program, and second program consisting of the first $n_2$ statements of the original goal’s second program.

• A second goal whose conclusion has precondition $R$, postcondition $Q$, first program consisting of all but the first $n_1$ statements of the original goal’s first program, and second program consisting of all but the first $n_2$ statements of the original goal’s second program.

For example, if the current goal is

$$\text{Type variables: <none>}
\begin{align*}
&\&1 \text{ (left ) : G1.f} \\
&\&2 \text{ (right) : G2.f} \\
&\text{pre = } \{x, y\} \\
&x \leftarrow x + 1 \quad (1) \quad y \leftarrow y + 1 \\
&y \leftarrow y + 1 \quad (2) \quad x \leftarrow x + 1 \\
&\text{post = } x\{1\} + y\{1\} = x\{2\} + y\{2\}
\end{align*}$$

then running

$$\text{seq 1 1 : (x\{1\} = x\{2\} + 1 \& y\{2\} = y\{1\} + 1).}$$

produces the goals

$\text{Type variables: <none>}
\begin{align*}
&\&1 \text{ (left ) : G1.f} \\
&\&2 \text{ (right) : G2.f} \\
&\text{pre = } \{x, y\} \\
&x \leftarrow x + 1 \quad (1) \quad y \leftarrow y + 1 \\
&\text{post = } x\{1\} = x\{2\} + 1 \& y\{2\} = y\{1\} + 1
\end{align*}$

and

$\text{Type variables: <none>}
\begin{align*}
&\&1 \text{ (left ) : G1.f} \\
&\&2 \text{ (right) : G2.f} \\
&\text{pre = } x\{1\} = x\{2\} + 1 \& y\{2\} = y\{1\} + 1 \\
&y \leftarrow y + 1 \quad (1) \quad x \leftarrow x + 1 \\
&\text{post = } x\{1\} + y\{1\} = x\{2\} + y\{2\}
\end{align*}$

**Syntax:** $\text{seq n : R. HL sequence rule.}$ If $n$ is a natural number and the goal’s conclusion is an HL statement judgement with precondition $P$, postcondition $Q$ and such that the length of the program is at least $n$, then reduce the goal to two subgoals:

• A first goal whose conclusion has precondition $P$, postcondition $R$, and program consisting of the first $n$ statements of the original goal’s program.
• A second goal whose conclusion has precondition $R$, postcondition $Q$, and program consisting of all but the first $n$ statements of the original goal’s program.

For example, if the current goal is

\[
\begin{array}{l}
\text{Type variables: <none>} \\
\hline
\text{Context : } M.f \\
\text{pre} = x \% 2 = 0 \\
(1) \ x \leftarrow x + 1 \\
(2) \ x \leftarrow x + 1 \\
\text{post} = x \% 2 = 0
\end{array}
\]

then running

\[
\text{seq 1 : (} x \% 2 = 1). \\
\]

produces the goals

\[
\begin{array}{l}
\text{Type variables: <none>} \\
\hline
\text{Context : } M.f \\
\text{pre} = x \% 2 = 0 \\
(1) \ x \leftarrow x + 1 \\
\text{post} = x \% 2 = 1
\end{array}
\]

and

\[
\begin{array}{l}
\text{Type variables: <none>} \\
\hline
\text{Context : } M.f \\
\text{pre} = x \% 2 = 1 \\
(1) \ x \leftarrow x + 1 \\
\text{post} = x \% 2 = 0
\end{array}
\]

\[
\text{sp}
\]

**Syntax:** sp. If the goal’s conclusion is a PRHL, PHL or HL statement judgement, consume the longest prefix(es) of the conclusion’s program(s) consisting entirely of statements built-up from ordinary assignments (not random assignments or procedure call assignments) and if statements, replacing the conclusion’s precondition by the strongest postcondition $R$ such that the statement judgement consisting of the conclusion’s original precondition, the consumed prefix(es) and $R$ holds.

For example, if the current goal is

\[
\begin{array}{l}
\text{Type variables: <none>} \\
\hline
\text{Context : } M.f \\
\text{pre} = x \% 2 = 0 \\
(1) \ x \leftarrow x + 1 \\
\text{post} = x \% 2 = 0
\end{array}
\]
\(\&1\) (left) : M.f
\(\&2\) (right) : N.f

\text{pre} = \{ y \}

\text{if} (y = 0) \{ \text{(1--) if} (y = 0) \{ y \ll 2 \text{(1.1)} y \ll 3 \}
\}
\text{else} \{ \text{(1--) else} \{ y \ll y - 2 \text{(1?1)} y \ll y - 1 \}
\}
\text{x }<@ \text{M.g()} \text{(2--) x }\leq [1..10]

\text{post} = x(1) + y(1) = x(2) + y(2) - 1

then running

sp.

produces the goal

Type variables: <none>

\(\&1\) (left) : M.f
\(\&2\) (right) : N.f

\text{pre} =
\exists (y_R : \text{int}),
  y(2) = 3 \lor
  y_R = 0 \lor
  (\exists (y_L : \text{int}), y(1) = 2 \lor y_L = 0 \lor y_L = y_R) \lor
  \exists (y_L : \text{int}), y(1) = y_L - 2 \lor y_L <> 0 \lor y_L = y_R)
\lor
\exists (y_R : \text{int}),
  y(2) = y_R - 1 \lor
  y_R <> 0 \lor
  (\exists (y_L : \text{int}), y(1) = 2 \lor y_L = 0 \lor y_L = y_R) \lor
  \exists (y_L : \text{int}), y(1) = y_L - 2 \lor y_L <> 0 \lor y_L = y_R)
\text{x }<@ \text{M.g()} \text{(1) x }\leq [1..10]

\text{post} = x(1) + y(1) = x(2) + y(2) - 1

\textbf{Syntax:} \texttt{sp} \(n_1\) \(n_2\). In \texttt{pRHL}, let \texttt{sp} consume \textit{exactly} \(n_1\) statements of the first program and \(n_2\) statements of the second program. Fails if this isn’t possible.

\textbf{Syntax:} \texttt{sp} \(n\). In \texttt{pHL} and \texttt{HL}, let \texttt{sp} consume \textit{exactly} \(n\) statements of the program. Fails if this isn’t possible.

\(\uparrow\) \texttt{wp}

\textbf{Syntax:} \texttt{wp}. If the goal’s conclusion is a \texttt{pRHL}, \texttt{pHL} or \texttt{HL} statement judgement, consume the longest suffix(es) of the conclusion’s program(s) consisting entirely of statements built-up from ordinary assignments (not random assignments or procedure call assignments) and \texttt{if} statements, replacing the conclusion’s postcondition by the weakest precondition \(R\) such that the statement judgement consisting of \(R\), the consumed suffix(es) and the conclusion’s original postcondition holds.

For example, if the current goal is

Type variables: <none>
then running  

\[ \text{wp}. \]

produces the goal  

Type variables: <none>

\[ \text{wp } n_1 \text{ } n_2. \text{ In } \text{pRHL}, \text{ let } \text{wp } \text{consume } \text{exactly } n_1 \text{ statements of the first program and } n_2 \text{ statements of the second program. Fails if this isn’t possible.} \]

Syntax: \text{wp } n. \text{ In } \text{pHL and HL}, \text{ let } \text{wp } \text{consume } \text{exactly } n \text{ statements of the program. Fails if this isn’t possible.} \]

\text{rnd} 

When describing the variants of this tactic, we only consider random assignments whose left-hand sides consist of single identifiers. The generalization to multiple assignment, when distributions over tuple types are sampled, is straightforward.

Syntax: \text{rnd } f | \text{rnd } f g. \text{ If the conclusion is a } \text{pRHL statement judgement whose programs end with random assignments } x_1 <\$ d_1 \text{ and } x_2 <\$ d_2, \text{ and } f \text{ and } g \text{ are functions between the types of } x_1 \text{ and } x_2, \text{ then consume those random assignments, replacing the conclusion’s postcondition by the probabilistic weakest precondition of the random assignments wrt. } f \text{ and } g. \text{ The new postcondition checks that:}  

\begin{itemize}  
\item \( f \) \text{ and } g \text{ are an isomorphism between the distributions } d_1 \text{ and } d_2;\end{itemize}
• for all elements \( u \) in the support of \( d_1 \), the result of substituting \( u \) and \( f \ u \) for \( x_1 \{1\} \) and \( x_2 \{2\} \) in the conclusion’s original postcondition holds.

When \( g \) is \( f \), it can be omitted. When \( f \) is the identity, it can be omitted.

For example, if the current goal is

\[
\text{Type variables: } <\text{none}>
\]

\[
n : \text{int}
\]

\[
&1 \text{ (left)} : \text{M.h}
\]

\[
&2 \text{ (right)} : \text{N.h}
\]

\[
\text{pre} = y\{2\} = n
\]

\[
x <\$ \{0,1\} \quad (1) \quad y \leftarrow y - 1
\]

\[
x <\$ [2..3] \quad (2) \quad x <\$ [2..3]
\]

\[
\text{post} = x\{1\} \leftrightarrow x\{2\} + y\{2\} = n + 2
\]

then running

\[
\text{rnd (fun } b \Rightarrow b ? 3 : 2) \text{ (fun } m \Rightarrow m = 3).\]

produces the goal

\[
\text{Type variables: } <\text{none}>
\]

\[
n : \text{int}
\]

\[
&1 \text{ (left)} : \text{M.h}
\]

\[
&2 \text{ (right)} : \text{N.h}
\]

\[
\text{pre} = y\{2\} = n
\]

\[
\text{post} = \begin{cases} y \leftarrow y - 1 \\ \forall xR : \text{int}, xR \in [2..3] \Rightarrow xR = 3 \\ \forall xL : \text{bool}, xL \in \{0,1\} \Rightarrow ((\text{if } xL \text{ then } 3 \text{ else } 2) \in [2..3]) \\ (xL \leftrightarrow (\text{if } xL \text{ then } 3 \text{ else } 2) + y\{2\} = n + 2) \end{cases}
\]

Note that if one uses the other isomorphism between \( \{0,1\} \) and \( [2..3] \) the generated subgoal will be false.

**Syntax:** `rnd(1)` | `rnd(2)`. If the conclusion is a PRHL statement judgement whose designated program (1 or 2) ends with a random assignment \( x <\$ d \), then consume that random assignment, replacing the conclusion’s postcondition with a check that:

- the weight of \( d \) is 1 (so the random assignment can’t fail);
- for all elements \( u \) in the support of \( d \), the result of substituting \( u \) for \( x(i) \)—where \( i \) is the selected side—in the conclusion’s original postcondition holds.

For example, if the current goal is
&1 (left) : M.f [programs are in sync]
&2 (right) : M.f

pre = true

(1) $x \in \{0,1\}$

post = $\{x\}$

then running

\texttt{rnd(1)}.

produces the (false!) goal

&1 (left) : M.f
&2 (right) : M.f

pre = true

(1) $x \in \{0,1\}$

post = is_lossless \{0,1\} \& forall ($x_0 : \text{bool}$), $x_0 \in \{0,1\} \Rightarrow x_0 = x$

**Syntax:** \texttt{rnd}. If the conclusion is an HL statement judgement whose program ends with a random assignment, then consume that random assignment, replacing the conclusion’s postcondition by the possibilistic weakest precondition of the random assignment.

For example, if the current goal is

Type variables: <none>

Context : M.f

pre = true

(1) $y \gets 2$
(2) $x \in [1..10]$

post = 3 \leq x + y \leq 12

then running

\texttt{rnd}.

produces the goal

Type variables: <none>

Context : M.f

pre = true
CHAPTER 3. TACTICS

(1)  \( y \leftarrow 2 \)

\[ \text{post} = \forall (x_0 : \text{int}), x_0 \in [1..10] \implies 3 \leq x_0 + y \leq 12 \]

**Syntax:** \( \text{rnd} \mid \text{rnd} \ E \). In PHL, compute the probabilistic weakest precondition of a random sampling with respect to event \( E \). When \( E \) is not specified, it is inferred from the current postcondition.

\[ \text{(if)} \]

**Syntax:** \( \text{if} \). If the goal’s conclusion is a PRHL statement judgement whose programs both begin with \( \text{if} \) statements, reduce the goal to three subgoals:

- One whose conclusion is the ambient logic formula asserting that the equivalence of the boolean expressions of the \( \text{if} \) statements in their respective memories holds given that the statement judgement’s precondition holds in those memories.
- One in which the \( \text{if} \) statements have been replaced by their “then” parts, and where the assertion of the truth of the first \( \text{if} \) statement’s boolean expression in the first program’s memory has been added to the conclusion’s precondition.
- One in which the \( \text{if} \) statements have been replaced by their “else” parts, and where the assertion of the falsity of the first \( \text{if} \) statement’s boolean expression in the first program’s memory has been added to the conclusion’s precondition.

For example, if the current goal is

\[
\begin{align*}
\text{Type variables: } & \langle \text{none} \rangle \\
\&1 & (\text{left }) : M.f \\
\&2 & (\text{right }) : N.f \\
\text{pre} & = \langle x, y \rangle \\
\text{if} \ & (y < x) \{ \ & \text{(1--) if} \ (y < x) \{ \ & z \leftarrow x - y \ (1.1) \ & \text{if} \ (y < x) \{ \ & z \leftarrow x - y + 1 \ (1--) \ & \text{else} \{ \ & z \leftarrow y - x \ (1?1) \ & \text{else} \{ \ & z \leftarrow y - x + 1 \ (1--) \ & \text{else} \{ \ & z \leftarrow z \times 2 \ (2--) \ & z & \leftarrow z \times 2 \ (2--) \\
\text{post} & = 0 \leq z\{1\} \land z\{1\} = 2 \times (z\{2\} - 1)
\end{align*}
\]

then running

\[ \text{if} \]

produces the goals

\[ \begin{align*}
\text{Type variables: } & \langle \text{none} \rangle \\
\forall \&1 \ & \&2, \langle x, y \rangle \implies y\{1\} < x\{1\} \iff y\{2\} < x\{2\}
\end{align*} \]

and

\[ \begin{align*}
\text{Type variables: } & \langle \text{none} \rangle \\
\&1 & (\text{left }) : M.f
\end{align*} \]
CHAPTER 3. TACTICS

\( k2 \) (right) : N.f

pre = \( \{ x, y \} \land y(1) < x(1) \)

\( z \leftarrow x - y \) \hspace{1cm} (1) \hspace{1cm} z \leftarrow x - y + 1

\( z \leftarrow z \ast 2 \) \hspace{1cm} (2)

post = 0 <= z(1) \land z(1) = 2 * (z(2) - 1)

and

Type variables: <none>

\( k1 \) (left) : M.f

\( k2 \) (right) : N.f

pre = \( \{ x, y \} \land \lnot y(1) < x(1) \)

\( z \leftarrow y - x \) \hspace{1cm} (1) \hspace{1cm} z \leftarrow y - x + 1

\( z \leftarrow z \ast 2 \) \hspace{1cm} (2)

post = 0 <= z(1) \land z(1) = 2 * (z(2) - 1)

Syntax: \texttt{if\{1\} | if\{2\}}. If the goal’s conclusion is a PRL judgement in which the first statement of the specified program is an \texttt{if} statement, then reduce the goal to two subgoals:

- One where the \texttt{if} statement has been replaced by its “then” part, and the precondition has been augmented by the assertion that the \texttt{if} statement’s boolean expression is true in the specified program’s memory.
- One where the \texttt{if} statement has been replaced by its “else” part, and the precondition has been augmented by the assertion that the \texttt{if} statement’s boolean expression is false in the specified program’s memory.

For example, if the current goal is

\( k1 \) (left) : M.f

\( k2 \) (right) : N.f

pre = \( \{ x, y \} \)

\( \text{if } (y < x) \{ \hspace{1cm} (1--) \hspace{1cm} \text{if } (y < x) \{ \)

\hspace{1cm} \hspace{1cm} z \leftarrow x - y \hspace{1cm} (1.1) \hspace{1cm} z \leftarrow x - y + 1

\hspace{1cm} \hspace{1cm} \} \hspace{1cm} \} \)

\hspace{1cm} \hspace{1cm} \} \hspace{1cm} \}

\hspace{1cm} \} \hspace{1cm} \}

\hspace{1cm} z \leftarrow y - x \hspace{1cm} (1?1) \hspace{1cm} z \leftarrow y - x + 1

\hspace{1cm} \} \hspace{1cm} \}

\hspace{1cm} \} \hspace{1cm} \}

\hspace{1cm} z \leftarrow z \ast 2 \hspace{1cm} (2--)\)

post = 0 <= z(1) \land z(1) = 2 * (z(2) - 1)

then running

\texttt{if\{1\}.

produces the goals

Type variables: <none>
\&1 (left) : M.f
\&2 (right) : N.f

pre = =\{x, y\} \land \ y(1) < x(1)

z \leftarrow x - y
\quad (1--) \textbf{if} (y < x) *\{
\quad (1.1) \quad z \leftarrow x - y + 1
\quad \quad (1--) \textbf{else} *\{
\quad (1?1) \quad z \leftarrow y - x + 1
\quad \quad (1--) \}
\quad z \leftarrow z \ast 2
\quad (2--)

post = 0 <= z(1) \land z(1) = 2 \ast (z(2) - 1)

and

Type variables: <none>

\&1 (left) : M.f
\&2 (right) : N.f

pre = =\{x, y\} \land \neg \ y(1) < x(1)

z \leftarrow y - x
\quad (1--) \textbf{if} (y < x) *\{
\quad (1.1) \quad z \leftarrow x - y + 1
\quad \quad (1--) \textbf{else} *\{
\quad (1?1) \quad z \leftarrow y - x + 1
\quad \quad (1--) \}
\quad z \leftarrow z \ast 2
\quad (2--)

post = 0 <= z(1) \land z(1) = 2 \ast (z(2) - 1)

Syntax: \textbf{if}. If the goal’s conclusion is an HL judgement whose first statement is an \textbf{if} statement, then reduce the goal to two subgoals:

- One where the \textbf{if} statement has been replaced by its “then” part, and the precondition has been augmented by the assertion that the \textbf{if} statement’s boolean expression is true.

- One where the \textbf{if} statement has been replaced by its “else” part, and the precondition has been augmented by the assertion that the \textbf{if} statement’s boolean expression is false.

For example, if the current goal is

Type variables: <none>

Context : M.f

pre = true

(1--) \textbf{if} (y < x) *\{
(1.1) \quad z \leftarrow x - y
(1--) \textbf{else} *\{
(1?1) \quad z \leftarrow y - x
(1--) \}
(2--) \quad z \leftarrow z \ast 2

post = 0 <= z
then running

```plaintext
if.
```

produces the goals

Type variables: <none>

Context : M.f
pre = y < x

(1) z <- x - y  
(2) z <- z * 2

post = 0 <= z

and

Type variables: <none>

Context : M.f
pre = ! y < x

(1) z <- y - x  
(2) z <- z * 2

post = 0 <= z

\(\text{\textcopyright while}\)

**Syntax:** `while I`. Here \(I\) is an invariant (formula), which may reference variables of the two programs, interpreted in their memories. If the goal's conclusion is a pRHL statement judgement whose programs both end with `while` statements, reduce the goal to two subgoals whose conclusions are pRHL statement judgements:

- One whose first and second programs are the bodies of the first and second while statements, whose precondition is the conjunction of \(I\) and the while statements’ boolean expressions (the first of which is interpreted in memory \&1, and the second of which is interpreted in \&2) and whose postcondition is the conjunction of \(I\) and the assertion that the while statements’ boolean expressions (interpreted in the appropriate memories) are equivalent.

- One whose precondition is the original goal’s precondition, whose first and second programs are all the results of removing the while statements from the two programs, and whose postcondition is the conjunction of:
  
  - the conjunction of \(I\) and the assertion that the while statements’ boolean expressions are equivalent; and
  
  - the assertion that, for all values of the variables modified by the while statements, if the while statements’ boolean expressions don’t hold, but \(I\) holds, then the original goal’s postcondition holds (in \(I\), the while statements’ boolean expressions, and the postcondition, variables modified by the while statements are replaced by universally quantified identifiers; otherwise, the boolean expressions are interpreted in the program’s respective memories, and the memory references of \(I\) and the postcondition are maintained).

For example, if the current goal is
CHAPTER 3. TACTICS

Type variables: <none>

\[ n : \text{int} \]

\&1 (left) : M.f  
\&2 (right) : N.f  

pre = \((x, y) \land y(1) = n\)

\[ z \gets 0 \quad (1--) \quad z \gets 1 \]
while \((0 < x)\) {
  \[ z \gets z + 1 \quad (2--) \quad i \gets 1 \]
  \[ x \gets x - 1 \quad (2.1) \]
}

\[ z \gets z - 1 \quad (2.2) \]
while \((i <= x)\) {
  \[ z \gets z + 1 \quad (3--)
    (3.1) \quad z \gets z + 2
    (3.2) \quad i \gets i + 1
  \]
}

post = \((z(1) + y(1) - n) \ast 2 + 1 = z(2) + y(2) - n\)

then running

while \((x(1) - 1 = x(2) - i(2) \land z(1) \ast 2 + 1 = z(2))\).

produces the goals

Type variables: <none>

\[ n : \text{int} \]

\&1 (left) : M.f  
\&2 (right) : N.f  

pre = \((x(1) - 1 = x(2) - i(2) \land z(1) \ast 2 + 1 = z(2)) \land
0 < x(1) \land i(2) <= x(2)\)

\[ z \gets z + 1 \quad (1) \quad z \gets z + 2 \]
\[ x \gets x - 1 \quad (2) \quad i \gets i + 1 \]

post = \((x(1) - 1 = x(2) - i(2) \land z(1) \ast 2 + 1 = z(2)) \land
(0 < x(1) \iff i(2) <= x(2))\)

and

Type variables: <none>

\[ n : \text{int} \]

\&1 (left) : M.f  
\&2 (right) : N.f  

pre = \((x, y) \land y(1) = n\)

\[ z \gets 0 \quad (1) \quad z \gets 1 \]
\[ i \gets 1 \quad (2) \]

post = \[((x(1) - 1 = x(2) - i(2) \land z(1) \ast 2 + 1 = z(2)) \land
(0 < x(1) \iff i(2) <= x(2))\)
(0 < x{1} <=> i(2) <= x(2)) /\ 
forall (x_L z_L i_R z_R : int),
  ! 0 < x_L =>
  ! i_R <= x{2} =>
  x_L - 1 = x{2} - i_R /\ z_L * 2 + 1 = z_R =>
  (z_L + y{1} - n) * 2 + 1 = z_R + y{2} - n

Syntax: \texttt{while}\{1\} I v \mid \texttt{while}\{2\} I v. Here \(I\) is an invariant (formula) and \(v\) is a termination variant integer expression, both of which may reference variables of the two programs, interpreted in their memories. If the goal’s conclusion is a \texttt{pRHL} statement judgement whose designated program (1 or 2) ends with a \texttt{while} statement, reduce the goal to two subgoals;

- One whose conclusion is a \texttt{pHL} statement judgement, saying that running the body of the while statement in a memory in which \(I\) holds and the while statement’s boolean expression is true is guaranteed to result in termination in a memory in which \(I\) holds and in which the value of the variant expression \(v\) has decreased by at least 1. (More precisely, the \texttt{pHL} statement judgment is universally quantified by the memory of the non-designated program and the initial value of \(v\). References to the variables of the non-designated program in \(I\) and \(v\) are interpreted in this memory; reference to the variables of the designated program have their memory references removed.)

- One whose conclusion is a \texttt{pRHL} statement judgement whose precondition is the original goal’s precondition, whose designated program is the result of removing the while statement from the original designated program, whose other program is unchanged, and whose postcondition is the conjunction of \(I\) and the assertion that, for all values of the variables modified by the while statement, that the conjunction of the following formulas holds:
  - the assertion that, if \(I\) holds, but the variant expression \(v\) is not positive, then the while statement’s boolean expression is false;
  - the assertion that, if the while statement’s boolean expression doesn’t hold, but \(I\) holds, then the original goal’s postcondition holds.

For example, if the current goal is

\begin{align*}
\text{Type variables: } & \langle \text{none} \rangle \\
& \&1 \text{ (left ) : M.f} \\
& \&2 \text{ (right ) : N.f} \\
\text{pre} & = \{n\} \setminus 0 <= n{1} \\
\text{x} & \gets 0 \quad \langle 1-- \rangle \\\text{i} & \gets 0 \quad \langle 2-- \rangle \\
\text{while } (i < n) \{ \quad \langle 3-- \rangle \\
& \text{x} \gets x + (i + 1) \quad \langle 3.1 \rangle \\
& \text{i} \gets i + 1 \quad \langle 3.2 \rangle \\
\} \\
\text{post} & = x{1} <= n{2} \bullet n{2}
\end{align*}

then running

\begin{align*}
\text{while}\{1\} \langle 0 <= i{1} <= n{1} \setminus x{1} <= i(1) \bullet i(1) \rangle \langle n(1) - i(1) \rangle.
\end{align*}

produces the goals

\begin{align*}
\text{Type variables: } & \langle \text{none} \rangle
\end{align*}
forall \_ (z : int),
\phoare\!
x \leftarrow x + (i + 1); i \leftarrow i + 1 : 
\,(0 \leq i \leq n \land x \leq i \land i < n) \land n - i = z \implies 
\,(0 \leq i \leq n \land x \leq i \land i < n) \land n - i < z = 1%r

and

Type variables: <none>

&1 \text{(left)} : M.f
&2 \text{(right)} : N.f

\pre = \{n\} \land 0 \leq n{1}

x \leftarrow 0  \quad (1)
i \leftarrow 0  \quad (2)

\post =
\quad \{0 \leq i{1} \leq n{1} \land x{1} \leq i{1} \land i{1} \implies \}
\quad \forall (i_L x_L : \text{int}),
\quad \{0 \leq i_L \leq n{1} \land x_L \leq i_L \land i_L \implies \}
\quad n{1} - i_L \leq 0 \implies ! i_L < n{1} \land 
\quad ! i_L < n{1} \implies 0 \leq i_L \leq n{1} \land x_L \leq i_L \land i_L \implies x_L \leq n{2} \times n{2})

\textbf{Syntax: while } I. \text{ Here } I \text{ is an invariant \textit{formula}, which may reference variables of the program. If the goal’s conclusion is an HL statement judgement ending with a } \textbf{while } \text{ statement, reduce the goal to two subgoals whose conclusions are HL statement judgements:}

\begin{itemize}
  \item One whose program is the body of the while statement, whose precondition is the conjunction of } I \text{ and the while statement’s boolean expression, and whose postcondition is } I. \text{ }
  \item One whose precondition is the original goal’s precondition, whose program is the result of removing the while statement from the original program, and whose postcondition is the conjunction of:
    \begin{itemize}
      \item } I; \text{ and}
      \item the assertion that, for all values of the variables } \textit{modified} \text{ by the while statement, if the while statement’s boolean expression doesn’t hold, but } I \text{ holds, then the original goal’s postcondition holds (in } I, \text{ the while statement’s boolean expression, and the postcondition, variables modified by the while statement are replaced by universally quantified identifiers).}
    \end{itemize}
\end{itemize}

For example, if the current goal is

Type variables: <none>

\m : \text{int}

\textbf{Context} : M.f

\pre = m = n \land 0 \leq n

\quad {1-} x \leftarrow 0
\quad {2-} i \leftarrow 0
\quad {3-} \textbf{while } (i < n) \{ 
\quad {3.1} \quad x \leftarrow x + (i + 1)
(3.2) \( i \leftarrow i + 1 \)
(3--) \}

post = \( x \leftarrow m \times m \)

then running

\[
\text{while } (0 \leq i \leq n \land x \leq i \times i).
\]

produces the goals

Type variables: <none>

\( m : \text{int} \)

Context: \( \text{M.f} \)

pre = \((0 \leq i \leq n \land x \leq i \times i) \land i < n\)

(1) \( x \leftarrow x + (i + 1) \)
(2) \( i \leftarrow i + 1 \)

post = \(0 \leq i \leq n \land x \leq i \times i \)

and

Type variables: <none>

\( m : \text{int} \)

Context: \( \text{M.f} \)

pre = \(m = n \land 0 \leq n\)

(1) \( x \leftarrow 0 \)
(2) \( i \leftarrow 0 \)

post = \((0 \leq i \leq n \land x \leq i \times i) \land \forall (i_0 x_0 : \text{int}),\)

\[ ! i_0 < n \Rightarrow 0 \leq i_0 \leq n \land x_0 \leq i_0 \times i_0 \Rightarrow x_0 \leq m \times m \]

Syntax: while/\( \_ \) \( v \). pHL version...

\( \odot \) call

When describing the variants of this tactic, we only consider procedure call assignments whose left-hand sides consist of single identifiers. The generalization to multiple assignment, when values of tuple types are returned, is straightforward.

Syntax: call \( (\_ : P \Rightarrow Q) \). If the goal’s conclusion is a pRHL statement judgement whose programs end with procedure calls or procedure call assignments (resp., an HL statement judgement whose program ends with a procedure call or procedure call assignment), then generate two subgoals:

- One whose conclusion is a pRHL judgement (resp., HL judgement) whose precondition is \( P \), whose procedures are the procedures being called (resp., procedure is the procedure being called), and whose postcondition is \( Q \).
- One whose conclusion is a pRHL statement judgement (resp., HL statement judgement) whose precondition is the original goal’s precondition, whose programs are (resp., program is) the result of removing the procedure calls (resp., call) from the programs (resp., program), and whose postcondition is the conjunction of
the result of replacing the procedures’ (resp., procedure’s) parameter(s) by their actual argument(s) in $P$; and

– the assertion that, for all values of the global variable(s) modified by the procedures (resp., procedure) and the results (resp., result) of the procedure calls (resp., procedure call), if $Q$ holds (where these quantified identifiers have been substituted for the modified variables and procedure results), then the original goal’s postcondition holds (where the modified global variables and occurrences of the variables (resp., variable) (if any) to which the results of the procedure calls are (resp., result of the procedure call is) assigned have been replaced by the appropriate quantified identifiers).

For example, if the current goal is

Type variables: <none>

$\&1$ (left) : M.g
$\&2$ (right) : N.g

pre = ={u}

M.x ← 5  \quad (1) \quad N.x ← -5
z ≤ M.f(u)  \quad (2) \quad z ≤ N.f(u)

post = z{1} + M.x{1} = z{2} - N.x{2}

and the procedures $M.f$ and $N.f$ have a single parameter, $y$, then running

\text{call } (_) : ={y} /\ M.x{1} = -N.x{2} => ={res} /\ M.x{1} = -N.x{2}).

produces the goals

Type variables: <none>

pre = ={y} /\ M.x{1} = -N.x{2}

M.f - N.f

post = ={res} /\ M.x{1} = -N.x{2}

and

Type variables: <none>

$\&1$ (left) : M.g
$\&2$ (right) : N.g

pre = ={u}

M.x ← 5  \quad (1) \quad N.x ← -5

post =

(={u} /\ M.x{1} = -N.x{2}) \&
\text{forall } (result_L result_R x_L x_R : int),
result_L = result_R /\ x_L = -x_R =>
result_L + x_L = result_R - x_R

Alternatively, a proof term whose conclusion is a $\text{prHL}$ or $\text{HL}$ judgement involving the procedure(s) called at the end(s) of the program(s) may be supplied as the argument to \text{call}, in which case only the second subgoal need be generated.
For example, in the start-goal of the preceding example, if the lemma \( M.N.f \) is

\[
\text{lemma } M.N.f : \\
\text{equiv}[M.f - N.f : \\
\{y\} \text{ } \land \text{ } M.x\{1\} = -N.x\{2\} \implies \{\text{res}\} \text{ } \land \text{ } M.x\{1\} = -N.x\{2\}] .
\]

then running

\[
\text{call } M.N.f.
\]

produces the goal

\[
\text{Type variables: } <\text{none}>
\]

\[
&1 \text{ (left)} : M.g \\
&2 \text{ (right)} : N.g \\
\text{pre } = \{u\} \\
M.x \leftarrow 5 \quad \text{(1)} \quad N.x \leftarrow -5 \\
\text{post } = \\
\{\{u\} \text{ } \land \text{ } M.x\{1\} = -N.x\{2\}\} \text{ } \land \text{ } \\
\text{forall } \{\text{result}_L \text{ result}_R \text{ x}_L \text{ x}_R : \text{int}, \text{ } \} \\
\text{result}_L = \text{result}_R \text{ } \land \text{ } x_L = -x_R \implies \\
\text{result}_L + x_L = \text{result}_R - x_R
\]

**Syntax:** \texttt{call}(1) (_ : P \Rightarrow Q ) \mid \texttt{call}(2) (_ : P \Rightarrow Q ). If the goal’s conclusion is a \texttt{pRHL} statement judgement whose designated program ends with a procedure call, then generate two subgoals:

- One whose conclusion is a \texttt{pHL} judgement whose precondition is \( P \), whose procedure is the procedure being called, whose postcondition is \( Q \), and whose bound part specifies equality with probability 1. (Consequently, \( P \) and \( Q \) may not mention \&1 and \&2.)

- One whose conclusion is a \texttt{pRHL} statement judgement whose precondition is the original goal’s precondition, whose programs are the result of removing the procedure call from the designated program, and leaving the other program unchanged, and whose postcondition is the conjunction of
  - the result of replacing the procedure’s parameter(s) by their actual argument(s) in \( P \); and
  - the assertion that, for all values of the global variable(s) modified by the procedure and the result of the procedure call, if \( Q \) holds (where these quantified identifiers have been substituted for the modified variables and procedure result), then the original goal’s postcondition holds (where the modified global variables and occurrences the variable (if any) to which the result of the procedure call is assigned have been replaced by the appropriate quantified identifiers).

For example, if the current goal is

\[
\text{Type variables: } <\text{none}>
\]

\[
x2: \text{int} \\
&1 \text{ (left)} : M.g \\
&2 \text{ (right)} : N.g \\
\text{pre } = x2 = N.x\{2\} \text{ } \land \text{ } N.x\{2\} = u\{2\} \text{ } \land \text{ } u\{1\} \text{ } \%\% \text{ } 2 = u\{2\} \text{ } \%\% \text{ } 2
\]
\[ M.x \leftarrow u \] (1)
\[ M.f(7) \] (2)

\[ \text{post} = (M.x{1} \equiv 2 = 0) = (N.x{2} \equiv 2 = 0) \]

then running
\[ \text{call}(1) \ (L : M.x \equiv 2 = x2 \equiv 2 \Rightarrow M.x \equiv 2 = x2 \equiv 2). \]

produces the goals

Type variables: <none>

\[ x2: \text{int} \]

\[ \text{pre} = M.x \equiv 2 = x2 \equiv 2 \]
\[ M.f \]
\[ [=} 1\%r \]

\[ \text{post} = M.x \equiv 2 = x2 \equiv 2 \]

and

Type variables: <none>

\[ x2: \text{int} \]

\[ &1 \left( \text{left} \right) : M.g \]
\[ &2 \right( \text{right} \) : N.g \]

\[ \text{pre} = x2 = N.x{2} \searrow N.x{2} = u{2} \searrow u{1} \equiv 2 = u{2} \equiv 2 \]
\[ M.x \leftarrow u \] (1)

\[ \text{post} = M.x{1} \equiv 2 = x2 \equiv 2 \& \& \]
\[ \text{forall} (x_L : \text{int}), \]
\[ x_L \equiv 2 = x2 \equiv 2 \Rightarrow (x_L \equiv 2 = 0) = (N.x{2} \equiv 2 = 0) \]

Alternatively, a proof term whose conclusion is a \texttt{pHL} judgement specifying equality with probability 1 and involving the procedure called at the end of the designated program may be supplied as the argument to \texttt{call}, in which case only the second subgoal need be generated.

For example, in the start-goal of the preceding example, if the lemma \texttt{M_f} is

\[ \text{lemma} \ M_f (z : \text{int}) : \]
\[ \text{phoare} [ M.f : M.x \equiv 2 = z \equiv 2 = z \equiv 2 \Rightarrow M.x \equiv 2 = z \equiv 2 ] = 1\%r. \]

then running
\[ \text{call}(1) \ (M_f x2). \]

produces the goal

Type variables: <none>

\[ x2: \text{int} \]

\[ &1 \left( \text{left} \right) : M.g \]
\[ &2 \right( \text{right} \) : N.g \]
pre = x2 = N.x(2) \ / N.x(2) = u(2) \ / u(1) \ %\% 2 = u(2) \ %\% 2

M.x <- u

post =
M.x{1} \ %\% 2 = x2 \ %\% 2 &&
forall (x_L : int),
x_L \ %\% 2 = x2 \ %\% 2 => (x_L \ %\% 2 = 0) = (N.x(2) \ %\% 2 = 0)

Syntax: call (_ : I). If the conclusion is a pRHL statement judgement whose programs end with calls to concrete procedures (resp., an HL statement judgement whose program ends with a call to a concrete procedure), then use the specification argument to call generated from the invariant I, and automatically apply proc to its first subgoal. In the pRHL case, its precondition will assume equality of the procedures’ parameters, and its postcondition will assert equality of the results of the procedure calls.

For example, if the current goal is

Type variables: <none>

&1 (left) : M.g
&2 (right) : N.g

pre = ={u}
M.x <- 5                    (1) N.x <- -5
z <@ M.f(u)                (2) z <@ N.f(u)

post = z{1} + M.x{1} = z{2} - N.x{2}

and modules M and N contain

var x : int
proc f(y : int) : int = {
x <- x + y;
return x;
}

and

var x : int
proc f(y : int) : int = {
x <- x - y;
return -x;
}

respectively, then running

call (_ : M.x(1) = -N.x(2)).

produces the goals

Type variables: <none>

&1 (left) : M.f
&2 (right) : N.f

pre = ={y} \ / M.x{1} = -N.x(2)
M.x <- M.x + y              (1) N.x <- N.x - y
post = M.x{1} = -N.x{2} \land M.x{1} = -N.x{2}

and

Type variables: <none>

&1 (left) : M.g
&2 (right) : N.g

pre = ={u}

M.x <- 5

(1) N.x <- -5

post =

({u} \land M.x{1} = -N.x{2}) \land
forall (result_L result_R x_L x_R : int),
result_L = result_R \land x_L = -x_R \Rightarrow
result_L + x_L = result_R - x_R

Syntax: call (_ : I). If the conclusion is a pRHL statement judgement whose programs end with calls of the same abstract procedure (resp., an HL statement judgement whose program ends with a call to an abstract procedure), then use the specification argument to call generated from the invariant I, and automatically apply proc I to its first subgoal, pruning the first two subgoals the application generates, because their conclusions consist of ambient logic formulas that are true by construction. In the pRHL case, its precondition will assume equality of the procedure's parameters and of the global variables of the module containing the procedure, and its postcondition will assume equality of the results of the procedure calls and of the global variables of the containing module.

For example, given the declarations

module type OR = {
  proc init(i : int) : unit
  proc f1() : unit
  proc f2() : unit
}.;

module Or : OR = {
  var x : int
  proc init(i : int) : unit = {
    x <- i;
  }
  proc f1() : unit = {
    x <- x + 2;
  }
  proc f2() : unit = {
    x <- x - 2;
  }
}.;

module type T(O : OR) = {
  proc g() : unit {O.f1 O.f2}
}.;

if the current goal is

Type variables: <none>

Adv: T{Or}
&1 (left) : N(Adv).h
&2 (right) : N(Adv).h
pre = ={y, glob Adv} \ Or.x{1} \mod 2 = 0 \ Or.x{2} \mod 2 = 0
Adv(Or).g() (1) Adv(Or).g()
post = Or.x{1} \mod 2 = 0 \ Or.x{2} \mod 2 = 0

then running
\texttt{call} (_ : Or.x{1} \mod 2 = 0 \ Or.x{2} \mod 2 = 0).

produces the goals

Type variables: <none>

Adv: T{Or}
pre = true \ Or.x{1} \mod 2 = 0 \ Or.x{2} \mod 2 = 0
Or.f1 = Or.f1
post = ={res} \ Or.x{1} \mod 2 = 0 \ Or.x{2} \mod 2 = 0

and

Type variables: <none>

Adv: T{Or}
pre = true \ Or.x{1} \mod 2 = 0 \ Or.x{2} \mod 2 = 0
Or.f2 = Or.f2
post = ={res} \ Or.x{1} \mod 2 = 0 \ Or.x{2} \mod 2 = 0

\textbf{Syntax:} \texttt{call} (_ : B, I). If the conclusion is a pRHL statement judgement whose programs end with calls of the same abstract procedure, then use the specification argument to \texttt{call} generated from the bad event \(B\) and invariant \(I\), and automatically apply \texttt{proc} \(B\ I\) to its first subgoal, pruning the first two subgoals the application generates, because their conclusions consist of ambient logic formulas that are true by construction, and pruning the next goal (showing the losslessness of the abstract procedure given the losslessness of the abstract oracles it uses), if trivial suffices to solve it. The specification’s precondition will assume equality of the procedure’s parameters and of the global variables of the module containing the procedure as well as \(I\), and its postcondition will assert \(I\) and the equality of the results of the procedure calls and of the global variables of the containing module—but only when \(B\) does not hold.

For example, given the declarations

\begin{verbatim}
module type OR = {
  proc init() : unit
  proc qry(x : int) : int
}.

op low : int = -100.
op upp : int = 100.

module Or1 : OR = {
  var qry, rsp : int
}
\end{verbatim}
CHAPTER 3. TACTICS

```plaintext
var queried : bool

proc init() = {
    qry <$ [low .. upp]; rsp <$ [low .. upp];
    queried <- false;
}

proc qry(x : int) : int = {
    var y : int;
    if (x = qry) {
        y <- rsp;
        queried <- true;
    } else {
        y <$ [low .. upp];
    }
    return y;
}
}

module Or2 : OR = {
    var qry : int
    var queried : bool
    proc init() = {
        qry <$ [low .. upp];
        queried <- false;
    }
    proc qry(x : int) : int = {
        var y : int;
        y <$ [low .. upp];
        queried <- queried / x = qry;
        return y;
    }
}

module type ADV(O : OR) = {
    proc * f() : bool {O.qry}
}

if the current goal is

Type variables: <none>
Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
    islossless O.qry => islossless Adv(O).f
&1 (left) : M(Adv).h
&2 (right) : N(Adv).h
pre = Or1.qry{1} = Or2.qry{2}

b <=@ Adv(Or1).f() (1) b <=@ Adv(Or2).f()

post = !Or2.queried{2} => ={b}

then running

call (_ : Or2.queried, (Or1.qry{1} = Or2.qry{2})).

produces the goals
```
Type variables: <none>

Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
   islossless O.qry => islossless Adv(O).f

pre = !Or2.queried(2) \( \land \) \( \{x\} \land \) Or1.qry{1} = Or2.qry{2}
   Or1.qry = Or2.qry

post = !Or2.queried(2) => \{res\} \land Or1.qry{1} = Or2.qry{2}

and

Type variables: <none>

Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
   islossless O.qry => islossless Adv(O).f

\textit{forall} \textit{\&2}, Or2.queried(2) => \textit{islossless} Or1.qry

and

Type variables: <none>

Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
   islossless O.qry => islossless Adv(O).f

\textit{forall} \textit{-},
   \textit{phoare}[ Or2.qry : Or2.queried \land \text{true} \Rightarrow Or2.queried \land \text{true} ] = 1\%

and

Type variables: <none>

Adv: ADV{Or1, Or2}
ll_Adv_f: forall (O <: OR{Adv}),
   islossless O.qry => islossless Adv(O).f

\&1 (left) : \textit{M(Adv)}.h
\&2 (right) : \textit{N(Adv)}.h

pre = Or1.qry{1} = Or2.qry{2}

post =
\langle !Or2.queried(2) => \text{true} \land Or1.qry{1} = Or2.qry{2} \rangle \&
\textit{forall} \textit{\langle result_L result_R : bool \rangle \langle Adv_L Adv_R : (glob \text{ Adv}) \rangle \langle \text{queried_R : bool} \rangle,
   \langle !\text{queried_R} \Rightarrow
   \text{result_L} = \text{result_R} \land
   \text{Adv_L} = \text{Adv_R} \land \text{Or1.qry}{1} = \text{Or2.qry}{2} \rangle \Rightarrow
   \text{!\text{queried_R} \Rightarrow \text{result_L} = \text{result_R}}

\textbf{Syntax: \textit{call \langle \_ : B, I, J \rangle}.} If the conclusion is a pRHL statement judgement whose programs end with calls of the same \textit{abstract} procedure, then use the specification argument to \textit{call} generated from the \textit{bad event} \textit{B} and \textit{invariants} \textit{I} and \textit{J}, and automatically apply \textit{proc B I J} to its first subgoal, pruning the first two subgoals the application generates, because their conclusions
consist of ambient logic formulas that are true by construction, and pruning the next goal (showing the losslessness of the abstract procedure given the losslessness of the abstract oracles it uses), if trivial suffices to solve it. The specification’s precondition will assume equality of the procedure’s parameters and of the global variables of the module containing the procedure as well as $I$, and its postcondition will assert

- $I$ and the equality of the results of the procedure calls and of the global variables of the containing module—if $B$ does not hold; and
- $J$—if $B$ does hold.

For example, given the declarations of the preceding example if the current goal is

```
Type variables: <none>

Adv: ADV{Or1, Or2}
l1_Adv_f: forall (O <: OR{Adv}),
  islossless O.qry => islossless Adv(O).f
```

```
&1 (left ) : M(Adv).h
&2 (right) : N(Adv).h

pre = Or1.qry{1} = Or2.qry{2} \ Or1.queried{1} = Or2.queried{2}

b <> Adv(Or1).f() (1) b <> Adv(Or2).f()

post =
  Or1.queried{1} = Or2.queried{2} \ (!Or2.queried{2} => ={b})
```

then running

```
call (_ : Or2.queried,
  (Or1.qry{1} = Or2.qry{2} \ Or1.queried{1} = Or2.queried{2}),
  (Or1.queried{1} = Or2.queried{2})).
```

produces the goals

```
Type variables: <none>

Adv: ADV{Or1, Or2}
l1_Adv_f: forall (O <: OR{Adv}),
  islossless O.qry => islossless Adv(O).f
```

```
pre =
  !Or2.queried{2} \ (x)
  Or1.qry{1} = Or2.qry{2} \ Or1.queried{1} = Or2.queried{2}
  Or1.qry - Or2.qry

post =
  if Or2.queried{2} then Or1.queried{1} = Or2.queried{2}
  else
    ={res} \ (x)
    Or1.qry{1} = Or2.qry{2} \ Or1.queried{1} = Or2.queried{2}
```

and

```
Type variables: <none>

Adv: ADV{Or1, Or2}
```
CHAPTER 3. TACTICS

3.4.2 Tactics for Transforming Programs

Unless otherwise specified, the tactics of this subsection only apply to goals whose conclusions are PRHL, PHL or HL statement judgements, reducing such a goal to a single subgoal in which only the program(s) of those statement judgements have changed.

Many of these tactics take code positions consisting of a sequence of positive numerals separated by dots. E.g., 2.1.3 says to go to the statement 2 of the program, then to substatement 1 of it, then to sub-substatement 3 of it. We use the variable \( c \) to range over code positions.
All versions of the tactic work for PRHL (an optional side can be given), PHL and HL statement judgements. We’ll describe their operation in terms of a single program (list of statements).

**Syntax:** `swap n m l`. Fails unless $1 \leq n < m \leq l$ and the program has at least $l$ statements. Swaps the statement block from positions $n$ through $m - 1$ with the statement block from $m$ through $l$, failing if these blocks of statements aren’t independent.

**Syntax:** `swap [n..m] k`. Fails unless $1 \leq n \leq m$ and the program has at least $m$ statements.

- If $k$ is non-negative, move the statement block from $n$ through $m$ forward $k$ positions, failing if the program doesn’t have at least $m + k$ statements or if the swapped statements blocks aren’t independent.

- If $k$ is negative, move the statement block from $n$ through $m$ backward $-k$ positions, failing if $n + k < 1$ or if the swapped statement blocks aren’t independent.

**Syntax:** `swap n k`. Equivalent to `swap [n..n] k`.

**Syntax:** `swap k`. If $k$ is non-negative, equivalent to `swap 1 k`. If $k$ is negative, equivalent to `swap n k`, where $n$ is the length of the program.

For example, suppose the current goal is

```plaintext
Type variables: <none>

&1 (left) : M.f [programs are in sync]
&2 (right) : M.f

pre = =\{M.x, M.y, M.z, M.w\}
(1) M.x ← true
(2) M.y ← false
(3) M.z ← true
(4) M.w ← false

post = =\{M.x, M.y, M.z, M.w\}
```

Then running

```
swap 1 3 4.
```

produces goal

```plaintext
Type variables: <none>

&1 (left) : M.f [programs are in sync]
&2 (right) : M.f

pre = =\{M.x, M.y, M.z, M.w\}
(1) M.z ← true
(2) M.w ← false
(3) M.x ← true
(4) M.y ← false

post = =\{M.x, M.y, M.z, M.w\}
```

From which running

```
swap 2 2.
```
produces goal

Type variables: <none>

&1 (left) : M.f [programs are in sync]
&2 (right) : M.f

pre = ={M.x, M.y, M.z, M.w}
(1) M.z ← true
(2) M.x ← true
(3) M.y ← false
(4) M.w ← false

post = ={M.x, M.y, M.z, M.w}

From which running

swap(1) [3 .. 4] -1.

produces goal

Type variables: <none>

&1 (left) : M.f
&2 (right) : M.f

pre = ={M.x, M.y, M.z, M.w}
M.z ← true (1) M.z ← true
M.y ← false (2) M.x ← true
M.w ← false (3) M.y ← false
M.x ← true (4) M.w ← false

post = ={M.x, M.y, M.z, M.w}

From which running

swap 2.

produces goal

Type variables: <none>

&1 (left) : M.f
&2 (right) : M.f

pre = ={M.x, M.y, M.z, M.w}
M.y ← false (1) M.x ← true
M.w ← false (2) M.y ← false
M.z ← true (3) M.z ← true
M.x ← true (4) M.w ← false

post = ={M.x, M.y, M.z, M.w}

From which running

swap(2) -1.
produces goal

```
Type variables: <none>
```

```
&1 (left ) : M.f
&2 (right ) : M.f

pre = ={M.x, M.y, M.z, M.w}
M.y <- false (1) M.x <- true
M.w <- false (2) M.y <- false
M.z <- true (3) M.w <- false
M.x <- true (4) M.z <- true

post = ={M.x, M.y, M.z, M.w}
```
\&1 (left) : M.h \ [programs are in sync] \\
\&2 (right) : M.h \\
pre = ={x} \\
(1) \ b \ <\ M.g(x + 1) \\
post = (\neg b^1) = \neg b^2 \\
then running \\
\texttt{inline} M.g. \\
produces the goal \\
Type variables: <none> \\
\&1 (left) : M.h \ [programs are in sync] \\
\&2 (right) : M.h \\
pre = ={x} \\
(1) \ x_0 \leftarrow x + 1 \\
(2) \ M.y <\ M.f(x_0 - 1) \\
(3) \ b \leftarrow x_0 + M.y + 1 = 3 \\
post = (\neg b^1) = \neg b^2 \\
From which running \\
\texttt{inline} M.f. \\
produces the goal \\
Type variables: <none> \\
\&1 (left) : M.h \\
\&2 (right) : M.h \\
pre = ={x} \\
x_0 \leftarrow x + 1 \\
M.y <\ M.f(x_0 - 1) \\
b \leftarrow x_0 + M.y + 1 = 3 \\
(1) \ x_0 \leftarrow x + 1 \\
(2) \ x_1 \leftarrow x_0 - 1 \\
(3) \ x_1 \leftarrow x_1 + 1 \\
(4) \ M.y \leftarrow x_1 \ast 2 \\
(5) \ b \leftarrow x_0 + M.y + 1 = 3 \\
post = (\neg b^1) = \neg b^2 \\
From which running \\
\texttt{inline} M.f. \\
produces the goal \\
Type variables: <none> \\
\&1 (left) : M.h \ [programs are in sync]
CHAPTER 3. TACTICS

And, if the current goal is

Type variables: <none>

then running

produces the goal

Type variables: <none>

© rcondt

Syntax: rcondt n. If the goal’s conclusion is an HL statement judgement whose nth statement is an if statement, reduce the goal to two subgoals.

- One whose conclusion is an HL statement judgement whose precondition is the original goal’s precondition, program is the first \( n - 1 \) statements of the original goal’s program, and postcondition is the boolean expression of the if statement.

- One whose conclusion is an HL statement judgement that’s the same as that of the original goal except that the if statement has been replaced by its then part.

For example, if the current goal is
Type variables: <none>

Context : M.f

\[ \text{pre} = \text{true} \]

\[ \begin{align*}
(1--) & \quad x <\{0,1\} \\
(2--) & \quad y <- x \, ^{\wedge} \, x \\
(3--) & \quad \text{if} \, \{(y)\} \{ \\
(3.1) & \quad z <- \text{true} \\
(3--) & \quad \text{else} \{ \\
(3?1) & \quad z <- \text{false} \\
(3--) & \}
\end{align*} \]

\[ \text{post} = z \]

then running

\[ \text{rcondt} \, 3. \]

produces the goals

Type variables: <none>

Context : M.f

\[ \text{pre} = \text{true} \]

\[ \begin{align*}
(1) & \quad x <\{0,1\} \\
(2) & \quad y <- x \, ^{\wedge} \, x \\
\end{align*} \]

\[ \text{post} = \, !y \]

and

Type variables: <none>

Context : M.f

\[ \begin{align*}
(1) & \quad x <\{0,1\} \\
(2) & \quad y <- x \, ^{\wedge} \, x \\
(3) & \quad z <- \text{true} \\
\end{align*} \]

\[ \text{post} = z \]

Syntax: \texttt{rcondt} \{1\} \, n \mid \texttt{rcondt} \{2\} \, n. \] If the goal’s conclusion is a \texttt{pRHL} statement judgement where the \(n\)th statement of the designated program is an \texttt{if} statement, reduce the goal to two subgoals.

- One whose conclusion is an \texttt{HL} statement judgement whose precondition is the original goal’s precondition, program is the first \(n - 1\) statements of the original goal’s designated program, and postcondition is the boolean expression of the \texttt{if} statement. Actually, the \texttt{HL} statement judgement is universally quantified by a memory of the non-designated program, and references in the precondition to variables of the non-designated program are interpreted in that memory.
• One whose conclusion is a \texttt{PRHL} statement judgement that’s the same as that of the original goal except that the \texttt{if} statement has been replaced by its \texttt{then} part.

For example, if the current goal is

\begin{verbatim}
Type variables: <none>

\&1 (left ) : N.f
\&2 (right ) : M.f
pre = N.x{1}
(1--) x <$ \{0,1\}
(2--) y <- x ^^ x
(3--) if (!y) {
  (3.1) z <- true
  (3--) }
else {
  (3?1) z <- false
  (3--) }
post = N.x{1} = z{2}
\end{verbatim}

then running
\begin{verbatim}
rcondt{2} 3.
\end{verbatim}

produces the goals

\begin{verbatim}
Type variables: <none>

forall &n, hoare[ x <$ \{0,1\}; y <- x ^^ x : N.x{n} => !y]
\end{verbatim}

and

\begin{verbatim}
Type variables: <none>

\&1 (left ) : N.f
\&2 (right ) : M.f
pre = N.x{1}
(1) x <$ \{0,1\}
(2) y <- x ^^ x
(3) z <- true
post = N.x{1} = z{2}
\end{verbatim}

\textbf{Syntax:} \texttt{rcond} \texttt{n}. If the goal’s conclusion is an HL statement judgement whose \texttt{n}th statement is a \texttt{while} statement, reduce the goal to two subgoals.

• One whose conclusion is an HL statement judgement whose precondition is the original goal’s precondition, program is the first \texttt{n} − 1 statements of the original goal’s program, and postcondition is the boolean expression of the \texttt{while} statement.

• One whose conclusion is an HL statement judgement that’s the same as that of the original goal except that the \texttt{while} statement has been replaced by its body.

For example, if the current goal is
Type variables: <none>

Context : M.f

pre = true

(1--) i <- 0
(2--) while (i < 10) {
(2.1) i <- i + 1
(2--) }
(3--) while (i < 20) {
(3.1) i <- i + 2
(3--) }

post = i = 20

then running

rcondt 3.

produces the goals

Type variables: <none>

Context : M.f

pre = true

(1--) i <- 0
(2--) while (i < 10) {
(2.1) i <- i + 1
(2--) }

post = i < 20

and

Type variables: <none>

Context : M.f

pre = true

(1--) i <- 0
(2--) while (i < 10) {
(2.1) i <- i + 1
(2--) }
(3--) i <- i + 2
(4--) while (i < 20) {
(4.1) i <- i + 2
(4--) }

post = i = 20

Syntax: rcondt{1} n | rcondt{2} n. If the goal’s conclusion is a PRHL statement judgement where the nth statement of the designated program is a while statement, reduce the goal to two subgoals.
• One whose conclusion is an HL statement judgement whose precondition is the original goal’s precondition, program is the first \( n - 1 \) statements of the original goal’s designated program, and postcondition is the boolean expression of the while statement. Actually, the HL statement judgement is universally quantified by a memory of the non-designated program, and references in the precondition to variables of the non-designated program are interpreted in that memory.

• One whose conclusion is a pRHL statement judgement that’s the same as that of the original goal except that the while statement has been replaced by its body.

For example, if the current goal is

\[
\begin{align*}
\text{Type variables: } & \langle \text{none} \rangle \\
& \&1 \text{ (left) : } M.f \\
& \&2 \text{ (right) : } N.f \\
\text{pre} = \text{true} \\
i \leftarrow 0 \\
\text{while } (i < 10) \{ \\
i \leftarrow i + 1 \\
\} \\
\text{while } (i < 20) \{ \\
i \leftarrow i + 2 \\
\} \\
\text{post} = \{ i \}
\end{align*}
\]

then running

\[
\text{rcondt}(i) \ 3.
\]

produces the goals

\[
\begin{align*}
\text{forall } _-, \text{ hoare}[ \ i \leftarrow 0; \ \text{while } (i < 10) \{ \cdots \} : \text{true} \implies i < 20]
\end{align*}
\]
CHAPTER 3. TACTICS

113

Syntax: \texttt{rcondf} \texttt{n}. If the goal’s conclusion is an HL statement judgement whose \texttt{n}th statement is an \texttt{if} statement, reduce the goal to two subgoals.

- One whose conclusion is an HL statement judgement whose precondition is the original goal’s precondition, program is the first \texttt{n} – 1 statements of the original goal’s program, and postcondition is the negation of the boolean expression of the \texttt{if} statement.
- One whose conclusion is an HL statement judgement that’s the same as that of the original goal except that the \texttt{if} statement has been replaced by its \texttt{else} part.

For example, if the current goal is

\begin{center}
\begin{verbatim}
Type variables: <none>

Context : M.f

pre = true

(1--)  x <$> \{0,1\}
(2--)  y <- x ^^ x
(3--)  \texttt{if} (y) {
(3.1)  z <- true
(3--)  \texttt{else} {
(3?1)  z <- false
(3--)  }

post = !z
\end{verbatim}
\end{center}

then running

\begin{center}
\texttt{rcondf} 3.
\end{center}

produces the goals

\begin{center}
\begin{verbatim}
Type variables: <none>

Context : M.f

pre = true

(1)  x <$> \{0,1\}
(2)  y <- x ^^ x

post = !y
\end{verbatim}
\end{center}

and

\begin{center}
\begin{verbatim}
Type variables: <none>

Context : M.f

pre = true

\end{verbatim}
\end{center}
CHAPTER 3. TACTICS

(1) \( x \ll\{0,1\} \)
(2) \( y \leftarrow x \,^\wedge\, x \)
(3) \( z \leftarrow \text{false} \)

\[ \text{post} = \neg z \]

**Syntax:** \( \text{rcondf}^{(1)} n \mid \text{rcondf}^{(2)} n \). If the goal’s conclusion is a pRHL statement judgement where the \( n \)th statement of the designated program is an \textit{if} statement, reduce the goal to two subgoals.

- One whose conclusion is an HL statement judgement whose precondition is the original goal’s precondition, program is the first \( n - 1 \) statements of the original goal’s designated program, and postcondition is the negation of the boolean expression of the \textit{if} statement. Actually, the HL statement judgement is universally quantified by a memory of the non-designated program, and references in the precondition to variables of the non-designated program are interpreted in that memory.

- One whose conclusion is a pRHL statement judgement that’s the same as that of the original goal except that the \textit{if} statement has been replaced by its \textit{else} part.

For example, if the current goal is

\[
\text{Type variables: <none>}
\]

\[
\&1 \text{ (left )} : N.f
\&2 \text{ (right )} : M.f
\]

\[
\text{pre} = \neg N.x^{(1)}
\]

\[
\begin{align*}
\text{(1--) } & \quad x \ll\{0,1\} \\
\text{(2--) } & \quad y \leftarrow x \,^\wedge\, x \\
\text{(3--) } & \quad \text{if} \ (y) \ \{ \\
\ & \quad (3.1) \quad z \leftarrow \text{true} \\
\ & \quad (3.2) \quad \text{else} \ \{ \\
\ & \quad (3?1) \quad z \leftarrow \text{false} \\
\ & \quad (3--) \quad \}
\end{align*}
\]

\[
\text{post} = N.x^{(1)} = z^{(2)}
\]

then running

\[
\text{rcondf}^{(2)} 3.
\]

produces the goals

\[
\text{Type variables: <none>}
\]

\[
\forall \&m, \text{hoare} [ x \ll\{0,1\}; y \leftarrow x \,^\wedge\, x : \neg N.x^{(m)} \Rightarrow \neg y]
\]

and

\[
\text{Type variables: <none>}
\]

\[
\&1 \text{ (left )} : N.f
\&2 \text{ (right )} : M.f
\]

\[
\text{pre} = \neg N.x^{(1)}
\]
Syntax: \texttt{rcondf} \textit{n}. If the goal’s conclusion is an HL statement judgement whose \textit{n}th statement is a \texttt{while} statement, reduce the goal to two subgoals.

- One whose conclusion is an HL statement judgement whose precondition is the original goal’s precondition, program is the first \(n - 1\) statements of the original goal’s program, and postcondition is the negation of the boolean expression of the \texttt{while} statement.

- One whose conclusion is an HL statement judgement that’s the same as that of the original goal except that the \texttt{while} statement has been removed.

For example, if the current goal is

\begin{verbatim}
Type variables: <none>
Context : M.f
pre = true
(1--) i <- 0
(2--) while (i < 10) {
(2.1) i <- i + 1
(2--) }
(3--) while (i < 10) {
(3.1) i <- i + 2
(3--) }
post = i = 10
\end{verbatim}

then running

\begin{verbatim}
rcondf 3.
\end{verbatim}

produces the goals

\begin{verbatim}
Type variables: <none>
Context : M.f
pre = true
(1--) i <- 0
(2--) while (i < 10) {
(2.1) i <- i + 1
(2--) }
post = ! i < 10
\end{verbatim}

and

\begin{verbatim}
Type variables: <none>
\end{verbatim}
Context : M.f
pre = true

(1--) i <- 0
(2--) while (i < 10) {
(2.1) i <- i + 1
(2--) }

post = i = 10

Syntax: $rcondf\{i\} n | rcondf\{2\} n$. If the goal’s conclusion is a pRHL statement judgement where the nth statement of the designated program is a while statement, reduce the goal to two subgoals.

- One whose conclusion is an HL statement judgement whose precondition is the original goal’s precondition, program is the first $n − 1$ statements of the original goal’s designated program, and postcondition is the negation of the boolean expression of the while statement. Actually, the HL statement judgement is universally quantified by a memory of the non-designated program, and references in the precondition to variables of the non-designated program are interpreted in that memory.

- One whose conclusion is a pRHL statement judgement that’s the same as that of the original goal except that the while statement has been removed.

For example, if the current goal is

Type variables: <none>

$\forall \ _, \ hoare[ i \leftarrow 0 ; \ while (i < 10) \{ \_ \} : true \implies ! i < 10]$

and

Type variables: <none>
&1 (left) : M.f
&2 (right) : N.f

pre = true

\[
\begin{align*}
    & i \leftarrow 0 \\
    & \textbf{while} (i < 10) \\
    & \quad i \leftarrow i + 1
\end{align*}
\]

post = \{i\}

\section*{unroll}

\textbf{Syntax:} \texttt{unroll c}. If the goal’s conclusion is an HL statement judgement whose \(c\)th statement is a \texttt{while} statement, then insert before that statement an \texttt{if} statement whose boolean expression is the \texttt{while} statement’s boolean expression, whose \texttt{then} part is the \texttt{while} statement’s body, and whose \texttt{else} part is empty.

For example, if the current goal is

\begin{verbatim}
Type variables: <none>

Context : M.f

pre = true

(1--) x \leftarrow 0
(2--) z \leftarrow 0
(3--) \textbf{while} (x < y) \\
(3.1) z \leftarrow z + x
(3.2) x \leftarrow x + 1
(3--) }

post = 0 \leq z
\end{verbatim}

then running

\begin{verbatim}
unroll 3.
\end{verbatim}

produces the goal

\begin{verbatim}
Type variables: <none>

Context : M.f

pre = true

(1--) x \leftarrow 0
(2--) z \leftarrow 0
(3--) \texttt{if} (x < y) \\
(3.1) z \leftarrow z + x
(3.2) x \leftarrow x + 1
(3--) }
(4--) \textbf{while} (x < y) \\
(4.1) z \leftarrow z + x
(4.2) x \leftarrow x + 1
(4--) }

post = 0 \leq z
\end{verbatim}
And, if the current goal is

\begin{align*}
\text{Type variables: } & \text{<none>} \\
\text{Context : } & M.f \\
\text{pre = true} \\
(1----) & \textbf{if } (0 <= y) \{ \\
(1.1--) & x < - 0 \\
(1.2--) & \textbf{while } (x <> y) \{ \\
(1.2.1) & x < - x + 1 \\
(1.2--) & \} \\
(1----) & \} \\
\text{post = 0 <= y}
\end{align*}

then running

unroll 1.2.

produces the goal

\begin{align*}
\text{Type variables: } & \text{<none>} \\
\text{Context : } & M.f \\
\text{pre = true} \\
(1----) & \textbf{if } (0 <= y) \{ \\
(1.1--) & x < - 0 \\
(1.2--) & \textbf{if } (x <> y) \{ \\
(1.2.1) & x < - x + 1 \\
(1.2--) & \} \\
(1.3--) & \textbf{while } (x <> y) \{ \\
(1.3.1) & x < - x + 1 \\
(1.3--) & \} \\
(1----) & \} \\
\text{post = 0 <= y}
\end{align*}

**Syntax:** unroll\{1\} c | unroll\{2\} c. If the goal’s conclusion is an pRHL statement judgement where the cth statement of the designated program is a \texttt{while} statement, then insert before that statement an \texttt{if} statement whose boolean expression is the \texttt{while} statement’s boolean expression, whose \texttt{then} part is the \texttt{while} statements’s body, and whose \texttt{else} part is empty.

For example, if the current goal is

\begin{align*}
\&1 \ ( \texttt{left} \ ) : M.f \ [\text{programs are in sync}] \\
\&2 \ ( \texttt{right} \ ) : M.f \\
\text{pre = =\{}y\}\}
(1--) & x < - 0 \\
(2--) & z < - 0 \\
(3--) & \textbf{while } (x < y) \{ \\
(3.1) & z < - z + x
\end{align*}
\((3.2)\) \(x \leftarrow x + 1\)
\((3--)\) }

\[\text{post} = \{z\}\]

then running
\[
\text{unroll}\{1\} 3.
\]

produces the goal

Type variables: <none>

\&1 (\textbf{left }) : M.f
\&2 (\textbf{right} ) : M.f

\[\text{pre} = \{y\}\]

\[
\begin{align*}
x & \leftarrow 0 & (1--) \ x & \leftarrow 0 \\
z & \leftarrow 0 & (2--) \ z & \leftarrow 0 \\
\textbf{if} (x < y) \{ & \textbf{while} (x < y) \{ & \\
\ & \ z & \leftarrow z + x & (3.1) \ z & \leftarrow z + x \\
\ & \ x & \leftarrow x + 1 & (3.2) \ x & \leftarrow x + 1 \\
\} & \} \}
\end{align*}
\]

\[
\textbf{while} (x < y) \{ & (4--) \\
\ & \ z & \leftarrow z + x & (4.1) \\
\ & \ x & \leftarrow x + 1 & (4.2) \\
\} \}
\]

\[\text{post} = \{z\}\]

from which running
\[
\text{unroll}\{2\} 3.
\]

produces the goal

Type variables: <none>

\&1 (\textbf{left }) : M.f \ [\text{programs are in sync}]
\&2 (\textbf{right} ) : M.f

\[\text{pre} = \{y\}\]

\[
\begin{align*}
(1--) \ x & \leftarrow 0 \\
(2--) \ z & \leftarrow 0 \\
(3--) \textbf{ if} (x < y) \{ & \\
(3.1) \ z & \leftarrow z + x \\
(3.2) \ x & \leftarrow x + 1 \\
(3--) \} & \}
(4--) \textbf{ while} (x < y) \{ & \\
(4.1) \ z & \leftarrow z + x \\
(4.2) \ x & \leftarrow x + 1 \\
(4--) \} \}
\end{align*}
\]

\[\text{post} = \{z\}\]

\copyright \ splitwhile
Syntax: \texttt{splitwhile} \(c : e\). If the goal’s conclusion is an \(HL\) statement judgement whose \(c\)th statement is a \texttt{while} statement and \(e\) is a well-typed boolean expression in the \texttt{while} statement’s context, then insert before the \texttt{while} statement a copy of the \texttt{while} statement in which \(e\) is added as a conjunct of the statement’s boolean expression.

For example, if the current goal is:

\begin{verbatim}
Type variables: <none>

Context : M.f

\quad pre = true

\quad (1--) x <- 0
\quad (2--) z <- 0
\quad (3--) \texttt{while} (x < y) {
\quad \quad (3.1) z <- z + x
\quad \quad (3.2) x <- x + 1
\quad (3--) }
\quad post = 0 <= z
\end{verbatim}

then running

\begin{verbatim}
\texttt{splitwhile} 3 : z <= 20.
\end{verbatim}

produces the goal:

\begin{verbatim}
Type variables: <none>

Context : M.f

\quad pre = true

\quad (1--) x <- 0
\quad (2--) z <- 0
\quad (3--) \texttt{while} (x < y /\ z <= 20) {
\quad \quad (3.1) z <- z + x
\quad \quad (3.2) x <- x + 1
\quad (3--) }
\quad (4--) \texttt{while} (x < y) {
\quad \quad (4.1) z <- z + x
\quad \quad (4.2) x <- x + 1
\quad (4--) }
\quad post = 0 <= z
\end{verbatim}

Syntax: \texttt{splitwhile}\{c \mid e\} \texttt{splitwhile}\{c \mid e\}. If the goal’s conclusion is a \(pRHL\) statement judgement where the \(c\)th statement of the designated program is a \texttt{while} statement and \(e\) is a well-typed boolean expression in the \texttt{while} statement’s context, then insert before the \texttt{while} statement a copy of the \texttt{while} statement in which \(e\) is added as a conjunct of the statement’s boolean expression.

For example, if the current goal is:

\begin{verbatim}
Type variables: <none>

&1 (left) : M.f [programs are in sync]
&2 (right) : M.f
\end{verbatim}
pre = \{y\}

(1--) x ← 0
(2--) z ← 0
(3--) while (x < y) {
    (3.1) z ← z + x
    (3.2) x ← x + 1
    (3--) }

post = \{z\}

then running

\texttt{splitwhile(2) 3 : z <= 20.}

produces the goal

Type variables: <none>

\$1 \text{ (left) } : M.f$
\$2 \text{ (right) } : M.f$

pre = \{y\}

x ← 0  \hspace{1cm} (1--) x ← 0
z ← 0  \hspace{1cm} (2--) z ← 0
while (x < y) {
    \hspace{1cm} (3--) \texttt{while} (x < y / \ z <= 20) {
        \hspace{1cm} z ← z + x
        \hspace{1cm} (3.1) \hspace{1cm} z ← z + x
        \hspace{1cm} (3.2) \hspace{1cm} x ← x + 1
        \hspace{1cm} (3--) }
    \hspace{1cm} (4--) \texttt{while} (x < y) {
        \hspace{1cm} (4.1) \hspace{1cm} z ← z + x
        \hspace{1cm} (4.2) \hspace{1cm} x ← x + 1
        \hspace{1cm} (4--) }
}

post = \{z\}

from which running

\texttt{splitwhile(1) 3 : z <= 20.}

produces the goal

Type variables: <none>

\$1 \text{ (left) } : M.f [\text{ programs are in sync}]$
\$2 \text{ (right) } : M.f$

pre = \{y\}

(1--) x ← 0
(2--) z ← 0
(3--) while (x < y / \ z <= 20) {
    (3.1) z ← z + x
    (3.2) x ← x + 1
    (3--) }
    (4--) \texttt{while} (x < y) {
        (4.1) \hspace{1cm} z ← z + x
        (4.2) \hspace{1cm} x ← x + 1
Syntax: \texttt{fission} c l \& m, n. HL statement judgement version. Fails unless 0 \leq l \text{ and } 0 \leq m \leq n and the cth statement of the program is a \texttt{while} statement, and there are at least \( l \) statements right before the \texttt{while} statement, at its level, and the body of the \texttt{while} statement has at least \( n \) statements.

Let

- \( s_1 \) be the \( l \) statements before the \texttt{while} statement at position \( c \);
- \( e \) be the boolean expression of the \texttt{while} statement;
- \( s_2 \) be the first \( m \) statements of the body of the \texttt{while} statement;
- \( s_3 \) be the next \( n - m \) statements of the body of the \texttt{while} statement;
- \( s_4 \) be the rest of the body of the \texttt{while} statement.

Fails unless:

- \( e \) doesn’t reference the variables written by \( s_2 \) and \( s_3 \);
- \( s_1 \) and \( s_4 \) don’t read or write the variables written by \( s_2 \) and \( s_3 \);
- \( s_2 \) and \( s_3 \) don’t write the variables written by \( s_1 \) and \( s_4 \);
- \( s_2 \) and \( s_3 \) don’t read or write the variables written by the other.

The tactic replaces

\[
\begin{align*}
\begin{array}{l}
s_1 \texttt{ while } (e) \{ s_2 \ s_3 \ s_4 \}
\end{array}
\end{align*}
\]

by

\[
\begin{align*}
\begin{array}{l}
s_1 \texttt{ while } (e) \{ s_2 \ s_4 \}
\end{array}
\end{align*}
\begin{align*}
\begin{array}{l}
s_1 \texttt{ while } (e) \{ s_3 \ s_4 \}
\end{array}
\end{align*}
\]

For example, if the current goal is

\[
\begin{align*}
\text{Type variables: <none>}
\end{align*}
\]

\[
\begin{align*}
\text{Context : M.f}
\end{align*}
\]

\[
\begin{align*}
\text{pre = 0 < n}
\end{align*}
\]

\[
\begin{align*}
(1--) & \quad x \gets 0 \\
(2--) & \quad y \gets 0 \\
(3--) & \quad i \gets 0 \\
(4--) & \quad j \gets 0 \\
(5--) & \quad \texttt{while } (i + j < n) \{ \\
(5.1) & \quad x \gets x \times i \\
(5.2) & \quad x \gets x + (j + 1) \\
(5.3) & \quad y \gets y \times j \\
(5.4) & \quad y \gets y + (i + 2) \\
(5.5) & \quad i \gets i + 1 \\
(5.6) & \quad j \gets j + 2 \\
(5--) & \}
\end{align*}
\]

\[
\begin{align*}
\text{post = 0 < x + y}
\end{align*}
\]
then running

\[
\textit{fission } 5!2 \oplus 2, 4.
\]

produces the goal

Type variables: <none>

Context : M.f

pre = 0 < n

(1--) x \leftarrow 0
(2--) y \leftarrow 0
(3--) i \leftarrow 0
(4--) j \leftarrow 0
(5--) while (i + j < n) {
  (5.1) x \leftarrow x \cdot i
  (5.2) x \leftarrow x + (j + 1)
  (5.3) i \leftarrow i + 1
  (5.4) j \leftarrow j + 2
(6--) }
(6--) i \leftarrow 0
(7--) j \leftarrow 0
(8--) while (i + j < n) {
  (8.1) y \leftarrow y \cdot j
  (8.2) y \leftarrow y + (i + 2)
  (8.3) i \leftarrow i + 1
  (8.4) j \leftarrow j + 2
(8--) }

post = 0 < x + y

Syntax: \textit{fission } c \oplus m, n. \textit{ Equivalent to fission } c!l \oplus m, n.

Syntax: \textit{fission}(1) \cdots | \textit{fission}(2) \cdots. \textit{The PRHL versions of the above variants, working on the designated program.}

© \textit{fusion}

Syntax: \textit{fusion } c!l \oplus m, n. \textit{HL statement judgement version. Fails unless } 0 \leq l \text{ and } 0 \leq m\text{ and } 0 \leq n\text{ and the } c\text{th statement of the program is a } while \text{ statement, and there are at least } l\text{ statements right before the } while \text{ statement, at its level, and the part of the program beginning from the } l\text{ statements before the while loop may be uniquely matched against}

\[
s_1 \text{ while } (e) \{ s_2 \ s_4 \}
\]

where:

- \( s_1 \) has length \( l \);
- \( s_2 \) has length \( m \);
- \( s_3 \) has length \( n \);
- \( e \) doesn’t reference the variables written by \( s_2 \) and \( s_3 \);
- \( s_1 \) and \( s_4 \) don’t read or write the variables written by \( s_2 \) and \( s_3 \);
- \( s_2 \) and \( s_3 \) don’t write the variables written by \( s_1 \) and \( s_4 \);
• \( s_2 \) and \( s_3 \) don’t read or write the variables written by the other.

The tactic replaces

\[
\begin{align*}
s_1 \text{ while } (e) \{ s_2 \ s_4 \} \\
s_1 \text{ while } (e) \{ s_3 \ s_4 \}
\end{align*}
\]

by

\[
\begin{align*}
s_1 \text{ while } (e) \{ s_2 \ s_3 \ s_4 \}
\end{align*}
\]

For example, if the current goal is

Type variables: <none>

Context : \( M.f \)

\[
\begin{align*}
\text{pre} &= 0 < n \\
(1--) \ x &< 0 \\
(2--) \ y &< 0 \\
(3--) \ i &< 0 \\
(4--) \ j &< 0 \\
(5--) \text{ while } (i + j < n) \{ \\
(5.1) \ x &< x * i \\
(5.2) \ x &< x + (j + 1) \\
(5.3) \ i &< i + 1 \\
(5.4) \ j &< j + 2 \\
(5--) \} \\
(6--) \ i &< 0 \\
(7--) \ j &< 0 \\
(8--) \text{ while } (i + j < n) \{ \\
(8.1) \ y &< y * j \\
(8.2) \ y &< y + (i + 2) \\
(8.3) \ i &< i + 1 \\
(8.4) \ j &< j + 2 \\
(8--) \}
\end{align*}
\]

\[
\begin{align*}
\text{post} &= 0 < x + y
\end{align*}
\]

then running

\texttt{fusion 5!2 @ 2, 2.}

produces the goal

Type variables: <none>

Context : \( M.f \)

\[
\begin{align*}
\text{pre} &= 0 < n \\
(1--) \ x &< 0 \\
(2--) \ y &< 0 \\
(3--) \ i &< 0 \\
(4--) \ j &< 0 \\
(5--) \text{ while } (i + j < n) \{ \\
(5.1) \ x &< x * i \\
(5.2) \ x &< x + (j + 1) \\
(5.3) \ y &< y * j
\end{align*}
\]
\[(5.4) \quad y \leftarrow y + (i + 2)\]
\[(5.5) \quad i \leftarrow i + 1\]
\[(5.6) \quad j \leftarrow j + 2\]
\[(\text{5--) \}}\]
\[\text{post} = 0 < x + y\]

**Syntax:** `fusion c @ m, n`. Equivalent to `fusion c!1 @ m, n`.

**Syntax:** `fusion\{1\} \cdots | fusion\{2\} \cdots`. The pRHL versions of the above variants, working on the designated program.

**alias**

**Syntax:** `alias c with x`. If the goal’s conclusion is an HL statement judgement whose program’s cth statement is an assignment statement, and x is an identifier, then replace the assignment statement by the following two statements:

- an assignment statement of the same kind as the original assignment statement (ordinary, random, procedure call) whose left-hand side is \(x\), and whose right-hand side is the right-hand side of the original assignment statement;

- an ordinary assignment statement whose left-hand side is the left-hand side of the original assignment statement, and whose right-hand side is \(x\).

If \(x\) is a local variable of the program, a fresh name is generated by adding digits to the end of \(x\).

**Syntax:** `alias c`. Equivalent to `alias c with x`.

**Syntax:** `alias c x = e`. If the program has an cth statement, and the expression \(e\) is well-typed in the context of the program, insert before the cth statement an ordinary assignment statement whose left-hand side is \(x\) and whose right-hand side is \(e\). If \(x\) is a local variable of the program, a fresh name is generated by adding digits to the end of \(x\).

**Syntax:** `alias\{1\} \cdots | alias\{2\} \cdots`. The pRHL versions of the preceding forms, where the aliasing is done in the designated program.

For example, if the current goal is

```
Type variables: <none>

Context : M.f

pre = true

(1) \(x \leftarrow 10\)
(2) \((y, z) \leftarrow (x + 1, 6)\)

post = \(y + z = 17\)
```

then running

```
alias 2 with w.
```

produces the goal

```
Type variables: <none>

Context : M.f
```
pre = true

(1) \( x \leftarrow 10 \)
(2) \( w \leftarrow (x + 1, 6) \)
(3) \( \langle y, z \rangle \leftarrow w \)

post = \( y + z = 17 \)

from which running

\texttt{alias 3 u = w.}\texttt{}`\texttt{1 + 7}.

produces the goal

Type variables: <none>

Context : \( M.f \)

pre = true

(1) \( x \leftarrow 10 \)
(2) \( w \leftarrow (x + 1, 6) \)
(3) \( u \leftarrow w.1 + 7 \)
(4) \( \langle y, z \rangle \leftarrow w \)

post = \( y + z = 17 \)

from which running

\texttt{alias 3}.

produces the goal

Type variables: <none>

Context : \( M.f \)

pre = true

(1) \( x \leftarrow 10 \)
(2) \( w \leftarrow (x + 1, 6) \)
(3) \( x0 \leftarrow w.1 + 7 \)
(4) \( u \leftarrow x0 \)
(5) \( \langle y, z \rangle \leftarrow w \)

post = \( y + z = 17 \)

\texttt{cfold}

Syntax: \texttt{cfold} \( c \mid m \). Fails unless \( m \geq 0 \). If the goal’s conclusion is an HL statement judgement in which statement \( c \) of the judgement’s program is an ordinary assignment statement in which constant values are assigned to local identifiers, and the following statement block of length \( m \) does not write any of those identifiers, then replace all occurrences of the assigned identifiers in that statement block by the constants assigned to them, and move the assignment statement to after the modified statement block.

For example, if the current goal is

Type variables: <none>
Context : M.f

pre = true

(1) \text{x} <- 1
(2) \text{y} <- \text{x} + 1
(3) \text{z} <- \text{y} + \text{x} + 2
(4) \text{w} <- \text{x} - \text{z}

post = \text{w} = -4

then running

\text{cfold 1 ! 1.}

produces the goal

Type variables: <none>

Context : M.f

pre = true

(1) \text{y} <- 1 + 1
(2) \text{x} <- 1
(3) \text{z} <- \text{y} + \text{x} + 2
(4) \text{w} <- \text{x} - \text{z}

post = \text{w} = -4

from which running

\text{cfold 2.}

produces the goal

Type variables: <none>

Context : M.f

pre = true

(1) \text{y} <- 1 + 1
(2) \text{z} <- \text{y} + 1 + 2
(3) \text{w} <- 1 - \text{z}
(4) \text{x} <- 1

post = \text{w} = -4

from which running

\text{cfold 1.}

produces the goal

Type variables: <none>

Context : M.f
pre = true

(1) \( z <- 1 + 1 + 1 + 2 \)
(2) \( w <- 1 - z \)
(3) \( x <- 1 \)
(4) \( y <- 1 + 1 \)

post = \( w = -4 \)

from which running

\texttt{cfold 1.}

produces the goal

\texttt{Type variables: <none>}

\texttt{Context : M.f}

pre = true

(1) \( w <- 1 - (1 + 1 + 1 + 2) \)
(2) \( x <- 1 \)
(3) \( y <- 1 + 1 \)
(4) \( z <- 1 + 1 + 1 + 2 \)

post = \( w = -4 \)

\textbf{Syntax:} \texttt{cfold\{1\} c \mid \texttt{cfold\{2\} c \mid m.}} Like the HL version, but operating on the designed program of a PRHL judgement’s conclusion.

\textbf{Syntax:} \texttt{cfold\{1\} c \mid \texttt{cfold\{2\} c.}} Like the general cases, but where \( m \) is set so as to be the number of statements after the assignment statement.

\texttt{\textbf{\textcopyright} kill}

\textbf{Syntax:} \texttt{kill c \mid m.} Fails unless \( m \geq 0 \). If the goal’s conclusion is an HL statement judgement whose program has a statement block starting at position \( c \) and having length \( m \) (when \( m = 0 \), this block is empty), and the variables written by this statement block aren’t used in the judgement’s postcondition or read by the rest of the program, then reduce the goal to two subgoals.

- One whose conclusion is a PHIL statement judgement whose pre- and postconditions are true, whose program is the statement block, and whose bound part is \( = 1\%x \).
- One that’s identical to the original goal except that the statement block has been removed.

For example, if the current goal is

\texttt{Type variables: <none>}

\texttt{Context : M.f}

pre = \( M.y = 3 \)

(1) \( M.y <- M.y + 1 \)
(2) \( M.x <- 0 \)
(3) \( M.x <- M.x + 1 \)
(4) \( M.y <- M.y + 1 \)

post = \( M.y = 5 \)
then running

\[ \text{kill 2 ! 2.} \]

produces the goals

Type variables: <none>

Context : M.f
Bound : \([=] 1\%r\)

pre = true

(1) M.x \leftarrow 0
(2) M.x \leftarrow M.x + 1

post = true

and

Type variables: <none>

Context : M.f

pre = M.y = 3

(1) M.y \leftarrow M.y + 1
(2) M.y \leftarrow M.y + 1

post = M.y = 5

Syntax: kill\{1\} c ! m | kill\{2\} c ! m. Like the HL case but for pRHL judgements, where the statement block to be killed is in the designated program.

For example, if the current goal is

Type variables: <none>

\&1 (left) : M.f [programs are in sync]
\&2 (right) : M.f

pre = ={M.y} \land M.y\{1\} = 3

(1) M.y \leftarrow M.y + 1
(2) M.x \leftarrow 0
(3) M.x \leftarrow M.x + 1
(4) M.y \leftarrow M.y + 1

post = ={M.y} \land M.y\{1\} = 5

then running

\[ \text{kill}(2) 2 ! 2. \]

produces the goals

Type variables: <none>

Context : M.f
CHAPTER 3. TACTICS

Bound : [=} 1\%r

pre = true

(1) M.x <- 0
(2) M.x <- M.x + 1

post = true

and

Type variables: <none>

&1 (left) : M.f
&2 (right) : M.f

pre = ={M.y} \& M.y{1} = 3

M.y <- M.y + 1 (1) M.y <- M.y + 1
M.x <- 0 (2) M.y <- M.y + 1
M.x <- M.x + 1 (3)
M.y <- M.y + 1 (4)

post = ={M.y} \& M.y{1} = 5

Syntax: \texttt{kill} c | \texttt{kill}\{1\} c | \texttt{kill}\{2\} c. Like the general cases, but with $m = 1$.

Syntax: \texttt{kill} c ! * | \texttt{kill}\{1\} c ! * | \texttt{kill}\{2\} c ! *. Like the general cases, but with $m$ set so that the statement block to be killed is the rest of the current level of the (designated) program.

3.4.3 Tactics for Reasoning about Specifications

\textbf{\underline{symmetry}}

Syntax: \texttt{symmetry}. If the goal’s conclusion is a PRHL (statement) judgement, swap the two programs, transforming the pre- and postconditions by swapping the memories they refer to.

For example, if the current goal is

Type variables: <none>

pre = x\{1\} = y\{2\} \& x\{2\} = - y\{1\}

M.f ~ N.g

post = 1 - \texttt{res}\{1\} = \texttt{res}\{2\}

then running

\texttt{symmetry.}

produces the goal

Type variables: <none>

pre = x\{2\} = y\{1\} \& x\{1\} = - y\{2\}

N.g ~ M.f

post = 1 - \texttt{res}\{2\} = \texttt{res}\{1\}
And, if the current goal is

\[
\begin{align*}
\&1 \text{(left ) : } M.f \\
\&2 \text{(right ) : } N.g \\
\text{pre} = \\
&(x\{1\}, y\{1\}).'1 = (x\{2\}, y\{2\}).'2 \\
&(x\{2\}, y\{2\}).'1 = -(x\{1\}, y\{1\}).'2 \\
z &= x - y \\
\text{(1) } z &= x + y \\
\text{post} = 1 - (z\{1\} + 1) = -z\{2\}
\end{align*}
\]

then running

\[\text{symmetry.}\]

produces the goal

\[
\begin{align*}
\&1 \text{(left ) : } N.g \\
\&2 \text{(right ) : } M.f \\
\text{pre} = \\
&(x\{2\}, y\{2\}).'1 = (x\{1\}, y\{1\}).'2 \\
&(x\{1\}, y\{1\}).'1 = -(x\{2\}, y\{2\}).'2 \\
z &= x + y \\
\text{(1) } z &= x - y \\
\text{post} = 1 - (z\{2\} + 1) = -z\{1\}
\end{align*}
\]

\[\text{transitivity}\]

\textbf{Syntax:} transitivity \(N.r\) \((P_1 \implies Q_1)\) \((P_2 \implies Q_2)\). Reduces a goal whose conclusion is a rRHL judgement \((\text{not statement judgement})\)

\[\text{equiv}[M_1.p_1 - M_2.p_2 : P \implies Q]\]

to goals whose conclusions are

- \[\text{equiv}[M_1.p_1 - N.r : P_3 \implies Q_1]\] and
- \[\text{equiv}[N.r - M_2.p_2 : P_5 \implies Q_2],\]

preceded by two auxiliary goals. The tactic fails if the \(P_i\) and \(Q_i\) aren’t compatible with these left and right programs. The conclusion of the first auxiliary goal checks that \(P\) implies the conjunction of \(P_1\) and \(P_2\), where each corresponding pair of \&2 memory references in \(P_1\) and \&1 reference in \(P_2\) is existentially quantified. And the conclusion of the second auxiliary goal checks that the conjunction of \(Q_1\) and \(Q_2\) implies \(Q\), where each corresponding pair of \&2 references in \(Q_1\) and \&1 references in \(Q_2\) are universally quantified.

For example, consider the modules

\[
\begin{align*}
\text{module } M &= \\
\text{proc } f(n : \text{int}, m : \text{int}) : \text{int} &= \\
\text{var } i, x : \text{int}; \\
i &= 0; x &= 0;
\end{align*}
\]
\begin{verbatim}
while (i < n) {
    x =- x + m; i =- i + 1;
}
return x;
}

module N = {
    proc g(n : int, m : int) : int = {
        var j, y : int;
        j =- 0; y =- 0;
        while (j < n) {
            y =- y + m; j =- j + 1;
        }
        return y;
    }
}

module R = {
    proc h(n : int, m : int) : int = {
        return n * m;
    }
}

If the current goal is

Type variables: <none>

\textit{pre} = 0 <= n{1} /\ 0 <= n{2} /\ n{1} * m{1} = n{2} * m{2}
\hspace{1cm} M.f ~ N.g
\hspace{1cm} \textit{post} = \{\textit{res}\}

then running

\textit{transitivity}
\hspace{1cm} R.h
\hspace{1cm} (0 <= n{1} /\ (n * m){1} = (n * m){2} ==> \{\textit{res}\})
\hspace{1cm} (0 <= n{2} /\ (n * m){1} = (n * m){2} ==> \{\textit{res}\}).

produces the four goals

Type variables: <none>

\textit{forall} &1 &2,
\hspace{1cm} 0 <= n{1} /\ 0 <= n{2} /\ n{1} * m{1} = n{2} * m{2} =>
\hspace{1cm} \exists (arg : int * int),
\hspace{1cm} (0 <= n{1} /\ n{1} * m{1} = \text{arg}.'1 * \text{arg}.'2) /\ 
\hspace{1cm} 0 <= n{2} /\ \text{arg}.'1 * \text{arg}.'2 = n{2} * m{2}

and

Type variables: <none>

\textit{forall} &1 &m &2, \text{res}{1} = \text{res}{m} => \text{res}{m} = \text{res}{2} => \{\textit{res}\}

and

Type variables: <none>
\end{verbatim}
pre = 0 <= n1 /\ n1 * m1 = n2 * m2

M.f ~ R.h

post = \{res\}

and

pre = 0 <= n2 /\ n1 * m1 = n2 * m2

R.h ~ N.g

post = \{res\}

Syntax: transitivity(i) \{ s1 \} (P1 ==> Q1) (P2 ==> Q2).

Reduces a goal whose conclusion is a PRHL statement judgement with precondition \( P \), postcondition \( Q \), left program (statement sequence) \( s1 \) and right program \( s2 \) to goals whose conclusions are PRHL statement judgements:

- \( \text{equiv}[s1 - s : P1 ==> Q1] \) and
- \( \text{equiv}[s - s2 : P2 ==> Q2] \),

preceded by two auxiliary goals. If the side \( i = 1 \), then the statement sequence \( s \) may only use variables and unqualified procedures of the left program; when \( i = 2 \), it may only use variables and unqualified procedures of the right program. The tactic fails if the \( P_i \) and \( Q_i \) aren’t compatible with these left and right programs. The conclusion of the first auxiliary goal checks that \( P \) implies the conjunction of \( P_1 \) and \( P_2 \), where each corresponding pair of \&1 memory references in \( P_1 \) and \&1 reference in \( P_2 \) is existentially quantified. And the conclusion of the second auxiliary goal checks that the conjuction of \( Q_1 \) and \( Q_2 \) implies \( Q \), where each corresponding pair of \&2 references in \( Q_1 \) and \&1 references in \( Q_2 \) are universally quantified.

Consider the modules \( M \), \( N \) and \( R \) of the preceding case. If the current goal is

Type variables: <none>

\&1 (left) : M.f
\&2 (right) : N.g

pre =
  j\{2\} = 0 /\ y\{2\} = 0 /\ i\{1\} = 0 /\ x\{1\} = 0 /\ 0 <= n\{1\} /\ 0 <= n\{2\} /\ n\{1\} * m\{1\} = n\{2\} * m\{2\}

\text{while } (i < n) \{ (1--) \text{ while } (j < n) \{ (1.1) y <<- y + m (1.2) j <<- j + 1 \}
\}

post = x\{1\} = y\{2\}

then running

\text{transitivity(1)}

\( \{ x <<- n * m; \} \)

\( 0 <= n\{1\} /\ i\{1\} = 0 /\ x\{1\} = 0 /\ (n * m)\{1\} = (n * m)\{2\} ==> \)
produces the four goals

\[
\begin{align*}
\text{forall } & \forall 1, 2, \\
& j(2) = 0 \land \\
& y(2) = 0 \land \\
& i(1) = 0 \land \\
& x(1) = 0 \land \\
& 0 \leq n(1) \land \\
& 0 \leq n(2) \land \\
& n(1) \times m(1) = n(2) \times m(2) \Rightarrow \\
& \exists (m, n : \text{int}), \\
& (0 \leq n(1) \land \\
& i(1) = 0 \land \\
& x(1) = 0 \land \\
& n(1) \times m(1) = n \times m) \land \\
& 0 \leq n(2) \land \\
& j(2) = 0 \land \\
& y(2) = 0 \land \\
& n \times m = n(2) \times m(2)
\end{align*}
\]

and

\[
\begin{align*}
\text{forall } & \forall 1, m, 2, \\
& x(1) = x(m) \Rightarrow \\
& x(m) = y(2) \Rightarrow \\
& x(1) = y(2)
\end{align*}
\]

and

\[
\begin{align*}
& \forall 1, 2 : M.f \\
& \forall 2, (\text{right}) : M.f
\end{align*}
\]

\[
\begin{align*}
\text{pre } &= 0 \leq n(1) \land \\
& i(1) = 0 \land \\
& x(1) = 0 \land \\
& n(1) \times m(1) = n(2) \times m(2) \\
\text{while } (i < n) \{ \\
& x \leftarrow n \times m \\
& i \leftarrow i + 1
\}
\end{align*}
\]

\[
\begin{align*}
\text{post } &= \{x\}
\end{align*}
\]

and

\[
\begin{align*}
& \forall 1, (\text{left }) : M.f \\
& \forall 2, (\text{right}) : M.f
\end{align*}
\]

\[
\begin{align*}
\text{pre } &= 0 \leq n(2) \land \\
& j(2) = 0 \land \\
& y(2) = 0 \land \\
& n(1) \times m(1) = n(2) \times m(2) \\
& x \leftarrow n \times m \\
\text{while } (j < n) \{ \\
& y \leftarrow y + m \\
& j \leftarrow j + 1
\}
\end{align*}
\]

\[
\begin{align*}
\text{post } &= x(1) = y(2)
\end{align*}
\]

And, if the current goal is
CHAPTER 3. TACTICS

Type variables: <none>

\&1 (left) : M.f
\&2 (right) : N.g

pre =
  j(2) = 0 /
  y(2) = 0 /
  i(1) = 0 /
  x(1) = 0 /
  0 <= n(1) /
  0 <= n(2) /
  n(1) * m(1) = n(2) * m(2)

while (i < n) { (1--) while (j < n) {
  x <- x + m
  y <- y + m
  i <- i + 1
}

post = x(1) = y(2)

then running

transitivity'2
  \{ y <- n * m; \}
  \{ 0 <= n(1) /\ i(1) = 0 /\ x(1) = 0 /\ (n * m){1} = (n * m){2} \Rightarrow x(1) = y(2); \}
  \{ 0 <= n(2) /\ j(2) = 0 /\ y(2) = 0 /\ (n * m){1} = (n * m){2} \Rightarrow y(y); \}

produces the four goals

Type variables: <none>

\forall \&1 \&2, j(2) = 0 /
  y(2) = 0 /
  i(1) = 0 /
  x(1) = 0 /
  0 <= n(1) /
  0 <= n(2) /
  n(1) * m(1) = n(2) * m(2) \Rightarrow
exists (m n : int),
  \{ 0 <= n(1) /\ i(1) = 0 /\ x(1) = 0 /\ n(1) * m(1) = n * m; \}
  \{ 0 <= n(2) /\ j(2) = 0 /\ y(2) = 0 /\ n * m = n(2) * m(2); \}

and

Type variables: <none>

\forall \&1 \&m \&2, x(1) = y(m) \Rightarrow y(m) = y(2) \Rightarrow x(1) = y(2)

and

Type variables: <none>

\&1 (left) : M.f
\&2 (right) : N.g

pre =
  0 <= n(1) /
  i(1) = 0 /
  x(1) = 0 /
  n(1) * m(1) = n(2) * m(2)

while (i < n) { (1--) y <- n * m
\[
\begin{align*}
\text{x} & \leftarrow \text{x} + \text{m} \quad (1.1) \\
\text{i} & \leftarrow \text{i} + 1 \quad (1.2) \\
\end{align*}
\]

\[
\text{post} = \text{x}\{1\} = \text{y}\{2\}
\]

and

Type variables: <none>

\[
\begin{align*}
&\&1 \text{ (left) } : \text{N.g} \\
&\&2 \text{ (right) } : \text{N.g} \\
\text{pre} = \\
0 & \leq \text{n}\{2\} \land \text{j}\{2\} = 0 \land \text{y}\{2\} = 0 \land \text{n}\{1\} \times \text{m}\{1\} = \text{n}\{2\} \times \text{m}\{2\} \\
\text{y} & \leftarrow \text{n} \times \text{m} \quad (1--) \text{ while } \text{j} < \text{n} \{ \\
&\quad (1.1) \text{ y} \leftarrow \text{y} + \text{m} \\
&\quad (1.2) \text{j} \leftarrow \text{j} + 1 \\
&\quad (1--) \} \\
\text{post} = =\{\text{y}\}
\end{align*}
\]

© 2023

**Syntax:** `conseq` \(_P \Longrightarrow Q\).

If the goal’s conclusion is a **pRHL** or **HL** judgement or statement judgement, weaken the conclusion’s precondition to \(P\), and strengthen its postcondition to \(Q\), generating initial auxiliary subgoals checking that this reduction is sound. Fails if \(P\) and \(Q\) aren’t compatible with the judgement type. The conclusion of the first auxiliary subgoal checks that the precondition \(P'\) of the original goal’s conclusion implies \(P\). The conclusion of the second auxiliary subgoal checks that \(Q\) implies the postcondition \(Q'\) of the original goal’s conclusion, except that any memory references to variables that may be modified by the conclusion’s program(s) are universally quantified in \(Q\) and \(Q'\), and \(P\) is also included as an assumption.

\(P\) or \(Q\) may be replaced by \(_\_\) in which case the pre- or postcondition is left unchanged. When a pre- or postcondition is unchanged, the corresponding auxiliary subgoal isn’t generated (as its proof would be trivial). When the goal’s conclusion is a judgement (not a statement judgement), a proof term whose conclusion is a judgement on the procedure(s) of the original goal’s conclusion may be supplied as the argument to `conseq`, in which case \(P\) and \(Q\) are taken to be the pre- and postconditions of this judgement, and only the auxiliary subgoals are generated.

For example, if the current goal is

Type variables: <none>

\[
\begin{align*}
&\&1 \text{ (left) } : \text{M.f} \\
&\&2 \text{ (right) } : \text{N.f} \\
\text{pre} = \\
=\{\text{z}\} \land \text{M.x}\{1\} = \text{N.x}\{2\} \land \text{M.y}\{1\} = \text{N.y}\{2\} \land \text{z}\{1\} < \text{M.x}\{1\} \land \text{z}\{1\} < \text{M.y}\{1\} \\
\text{if} \ (\text{z} \leq \text{M.x} \land \text{z} \leq \text{M.y}) \{ \\
&\quad (1--) \text{ if} \ (\text{z} \leq \text{N.x}) \{ \\
&\quad \text{M.x} \leftarrow \text{M.x} + 1 \quad (1.1) \text{N.x} \leftarrow \text{N.x} - 1 \\
&\quad (1--) \} \\
\text{post} = \text{M.y}\{1\} = \text{N.y}\{2\} \land \text{M.x}\{1\} - \text{N.x}\{2\} \leq 2
\end{align*}
\]
CHAPTER 3. TACTICS

then running

```
conseq (_ : _ ==>
  ={z} /\ M.x{1} = N.x{2} /\ M.y{1} = N.y{2} /\ z{1} <= M.x{1} /\ z{1} <= M.y{1} ==>

produces the goals

```

```
forall &1 &2,
  ={z} /\ 
  M.x{1} = N.x{2} /\  
  M.y{1} = N.y{2} /\ z{1} < M.x{1} /\ z{1} < M.y{1} =>  
  ={z} /\ 
  M.x{1} = N.x{2} /\  
  M.y{1} = N.y{2} /\ z{1} <= M.x{1} /\ z{1} <= M.y{1}
```

and

```
forall &1 &2,
pre =
  ={z} /\ 
  M.x{1} = N.x{2} /\  
  M.y{1} = N.y{2} /\ z{1} <= M.x{1} /\ z{1} <= M.y{1} =>  
  forall (x_L x_R : int),  
  `|x_L - x_R| <= 2 => M.y{1} = N.y{2} /\ `|x_L - x_R| <= 2
```

Continuing from the last of these goals, running

```
conseq (_ : _ ==>

produces the goals

```

```
forall &1 &2,
  ={z} /\ 
  M.x{1} = N.x{2} /\  
  M.y{1} = N.y{2} /\ z{1} <= M.x{1} /\ z{1} <= M.y{1} =>  
  forall (x_L x_R : int),  
  `|x_L - x_R| <= 2 => M.y{1} = N.y{2} /\ `|x_L - x_R| <= 2
```

and

```
forall &1 &2,
pre =
  ={z} /\ 
```

Type variables: <none>
\[
M.x\{1\} = N.x(2) \land M.y\{1\} = N.y(2) \land z(1) \leq M.x\{1\} \land z(1) \leq M.y\{1\}
\]

\[
\text{if } (z \leq M.x \lor z \leq M.y) \{ (1--) \text{ if } (z \leq N.x) \{
M.x \leftarrow M.x + 1 \\
(1.1) \quad N.x \leftarrow N.x - 1 \\
(1--) \}
\}
\]

post = \`|M.x\{1\} - N.x(2)| \leq 2

Continuing from the last of these goals, running

\[
\text{conseq } (_ : \{z\} \land M.x\{1\} = N.x(2) \land z(1) \leq N.x(2) \implies M.x\{1\} = N.x(2) \lor M.x\{1\} = N.x(2) + 2).
\]

produces the goals

Type variables: <none>

\[
\forall \&1 \&2, \{z\} \land M.x\{1\} = N.x(2) \land M.y\{1\} = N.y(2) \land z(1) \leq M.x\{1\} \land z(1) \leq M.y\{1\} \implies \{z\} \land M.x\{1\} = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall \&1 \&2, \{z\} \land M.x\{1\} = N.x(2) \land M.y\{1\} = N.y(2) \land z(1) \leq M.x\{1\} \land z(1) \leq M.y\{1\} \implies \forall (x_L x_R : \text{int}),
\]

\[
x_L = x_R \lor x_L = x_R + 2 \implies \`x_L - x_R| \leq 2
\]

and

Type variables: <none>

\[
\&1 (\text{left}) : M.f \\
\&2 (\text{right}) : N.f
\]

pre = \{z\} \land M.x\{1\} = N.x(2) \land z(1) \leq N.x(2)

\[
\text{if } (z \leq M.x \lor z \leq M.y) \{ (1--) \text{ if } (z \leq N.x) \{
M.x \leftarrow M.x + 1 \\
(1.1) \quad N.x \leftarrow N.x - 1 \\
(1--) \}
\}
\]

post = M.x\{1\} = N.x(2) \lor M.x\{1\} = N.x(2) + 2

If the current goal is

Type variables: <none>

\[
\text{pre } = \{z\} \land M.x\{1\} = N.x(2) \land M.y\{1\} = N.y(2) \land z(1) < M.x\{1\} \land z(1) < M.y\{1\}
\]
CHAPTER 3. TACTICS

\[ M.f \sim N.f \]

\[
\text{post} = M.y(1) = N.y(2) \land |M.x(1) - N.x(2)| \leq 2
\]

then running

\[
\text{conseq} \quad (_ : \forall \mathbf{x}_1, \mathbf{x}_2, z \rightarrow M.x(1) = N.x(2) \land M.y(1) = N.y(2) \land z(1) \leq M.x(1) \land z(1) \leq M.y(1) \implies _).
\]

produces the goals

Type variables: <none>

\[
\begin{align*}
\forall \mathbf{x}_1, \mathbf{x}_2, z \rightarrow M.x(1) = N.x(2) \land M.y(1) = N.y(2) \land z(1) \leq M.x(1) \land z(1) \leq M.y(1) \\
M.f \sim N.f
\end{align*}
\]

\[
\text{post} = M.y(1) = N.y(2) \land |M.x(1) - N.x(2)| \leq 2
\]

Continuing from the last of these goals, running

\[
\text{conseq} \quad (_ : _ \implies |M.x(1) - N.x(2)| \leq 2).
\]

produces the goals

Type variables: <none>

\[
\begin{align*}
\forall \mathbf{x}_1, \mathbf{x}_2, z \rightarrow M.x(1) = N.x(2) \land M.y(1) = N.y(2) \land z(1) \leq M.x(1) \land z(1) \leq M.y(1) \\
\forall (x_L, x_R : \text{int}), |x_L - x_R| \leq 2 \implies M.y(1) = N.y(2) \land |x_L - x_R| \leq 2
\end{align*}
\]

and

Type variables: <none>

\[
\begin{align*}
\forall \mathbf{x}_1, \mathbf{x}_2, z \rightarrow M.x(1) = N.x(2) \land M.y(1) = N.y(2) \land z(1) \leq M.x(1) \land z(1) \leq M.y(1) \\
M.f \sim N.f
\end{align*}
\]
CHAPTER 3. TACTICS

post = \( |M.x(1) - N.x(2)| \leq 2 \)

Continuing from the last of these goals, running

\[
\text{conseq} \quad \forall \text{z} : \\
M.x(1) = N.x(2) \land z(1) \leq N.x(2) \\ M.x(1) = N.x(2) \lor M.x(1) = N.x(2) + 2
\]

produces the goals

Type variables: <none>

\[
\forall \&1 \&2, \\
\{z\} \land M.x(1) = N.x(2) \land M.y(1) = N.y(2) \land z(1) \leq M.x(1) \land z(1) \leq M.y(1) \\ \forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall \&1 \&2, \\
\{z\} \land M.x(1) = N.x(2) \land M.y(1) = N.y(2) \land z(1) \leq M.x(1) \land z(1) \leq M.y(1) \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \. |x_L - x_R| \leq 2
\]

and

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

Given lemma

\[
\text{lemma M_N_3 :} \\
\text{equiv}[M.f \sim N.f : ] \\
\{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2) \\ M.x(1) = N.x(2) \lor M.x(1) = N.x(2) + 2
\]

if the current goal is

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]

and

Type variables: <none>

\[
\forall (x_L x_R : \text{int}), \\
x_L = x_R \lor x_L = x_R + 2 \\ \forall \{z\} \land M.x(1) = N.x(2) \land z(1) \leq N.x(2)
\]
then running

```conseq```
M_N_3.
```
produces the goals

Type variables: <none>

```forall &1 &2,
={z} /
M.x{1} = N.x{2} /
M.y{1} = N.y{2} /\ z{1} < M.x{1} /\ z{1} < M.y{1} =>
={z} /\ M.x{1} = N.x{2} /\ z{1} <= N.x{2}
```

and

Type variables: <none>

```forall &1 &2,
={z} /
M.x{1} = N.x{2} /
M.y{1} = N.y{2} /\ z{1} < M.x{1} /\ z{1} < M.y{1} =>
forall (x_L x_R : int),
x_L = x_R /\ x_L = x_R + 2 =>
M.y{1} = N.y{2} /\ |x_L - x_R| <= 2```

If the current goal is

Type variables: <none>

```x' : int```

Context: M.f

pre = x' = M.x /\ z < M.x /\ z < M.y

(1--) if (z <= M.x /\ z <= M.y) {
(1.1) M.x <= M.x + 1
(1--) }

post = x' < M.x

then running

```conseq```
(_: x' = M.x /\ z <= M.y ==> x' = M.x - 1).
```
produces the goals

Type variables: <none>

```forall &hr,
x' = M.x(hr) /\ z{hr} < M.x(hr) /\ z{hr} < M.y{hr} =>
x' = M.x(hr) /\ z{hr} <= M.y{hr}```

and

Type variables: <none>

```x' : int```
for all $\forall hr$, $x' = M.x(hr) \land z(hr) < M.x(hr) \land z(hr) < M.y(hr) \Rightarrow$

\[ \text{forall} \ (x : \text{int}), \ x' = x - 1 \Rightarrow x' < x \]

and

Type variables: <none>

\[ x' : \text{int} \]

Context : $M.f$

\[ \text{pre} = x' = M.x \land z <= M.y \]

(1--) if $(z <= M.x \lor z <= M.y)$ {

(1.1) $M.x <- M.x + 1$

(1--) }

\[ \text{post} = x' = M.x - 1 \]

If the current goal is

Type variables: <none>

\[ x' : \text{int} \]

\[ \text{pre} = x' = M.x \land z < M.x \land z < M.y \]

\[ M.f \]

\[ \text{post} = x' < M.x \]

then running

\[ \text{conseq} \quad _{._} : x' = M.x \land z <= M.y \Rightarrow x' = M.x - 1 \].

produces the goals

Type variables: <none>

\[ x' : \text{int} \]

\[ \text{forall} \ & hr, \ x' = M.x(hr) \land z(hr) < M.x(hr) \land z(hr) < M.y(hr) \Rightarrow \]

\[ x' = M.x(hr) \land z(hr) <= M.y(hr) \]

and

Type variables: <none>

\[ x' : \text{int} \]

\[ \text{forall} \ & hr, \ x' = M.x(hr) \land z(hr) < M.x(hr) \land z(hr) < M.y(hr) \Rightarrow \]

\[ \text{forall} \ (x : \text{int}), \ x' = x - 1 \Rightarrow x' < x \]

and

Type variables: <none>

\[ x' : \text{int} \]
Given lemma

\[
\text{lemma } M_3 \ (x' : \text{int}) : \\
\text{hoare}\ [M.f : x' = M.x \land z <= M.y \Rightarrow x' = M.x - 1].
\]

if the current goal is

Type variables: <none>

- \(x' : \text{int}\)
- \(\text{pre} = x' = M.x \land z < M.x \land z < M.y\)
- \(\text{post} = x' < M.x\)

then running

\[
\text{conseq}\ (M_3\ x').
\]

produces the goals

Type variables: <none>

- \(x' : \text{int}\)
- \(\forall hr, \ x' = M.x(hr) \land z(hr) < M.x(hr) \land z(hr) < M.y(hr) \Rightarrow x' = M.x(hr) \land z(hr) <= M.y(hr)\)

and

Type variables: <none>

- \(x' : \text{int}\)
- \(\forall hr, \ x' = M.x(hr) \land z(hr) < M.x(hr) \land z(hr) < M.y(hr) \Rightarrow \forall (x : \text{int}), \ x' = x - 1 \Rightarrow x' < x\)

**Syntax:** \(\text{conseq} \ (\_ : P \Rightarrow Q) \ (\_ : P_1 \Rightarrow Q_1) \ (\_ : P_2 \Rightarrow Q_2).\)

This form only applies to pRHL judgements and statement judgements, reducing the goal’s conclusion to

- an HL (statement) judgement for the left program with precondition \(P_1\) and postcondition \(Q_1\);
- an HL (statement) judgement for the right program with precondition \(P_2\) and postcondition \(Q_2\); and
- a pRHL (statement) judgement whose precondition is \(P\), postcondition is \(Q\), and programs are as in the original judgement;

As before, auxiliary goals are generated whose conclusions check the validity of the reduction: that the original conclusion’s precondition \(P'\) implies the conjunction of \(P, P_1\) and \(P_2\); and that
the conjunction of $Q$, $Q_1$ and $Q_2$ implies the original conclusion’s postcondition $Q'$. One of the HL specifications may be replaced by _, which is equivalent to $\text{conseq} \ ((\_ : \text{true} \Rightarrow \text{true})$. And in the case of a pRHL judgement (not a statement judgement), proof terms may be used as the arguments to $\text{conseq}$.

For example, if the current goal is

```
Type variables: <none>

\&1 \ (<\text{left}>) : M.f
\&2 \ (<\text{right}>) : N.f

pre = \{b\} \land M.x\{1\} \mod 2 + N.y\{2\} \mod 2 = 0

M.x <- M.x + 2 \quad (1) \quad N.y <- N.y - 2
b' <$ \{0,1\} \quad (2) \quad b' <$ \{0,1\}
b <- b \land b' \quad (3) \quad b <- b \land b'

post = \{b\} \land M.x\{1\} \mod 2 + N.y\{2\} \mod 2 = 0
```

then running

```
\text{conseq} \ ((\_ : \{b\} \Rightarrow \{b\})
(\_ : M.x \mod 2 = 0 \Rightarrow M.x \mod 2 = 0)
(\_ : N.y \mod 2 = 0 \Rightarrow N.y \mod 2 = 0).
```

produces the goals

```
Type variables: <none>

\forall \&1 \&2,
\{b\} \land M.x\{1\} \mod 2 + N.y\{2\} \mod 2 = 0 \Rightarrow
\{b\} \land M.x\{1\} \mod 2 = 0 \land N.y\{2\} \mod 2 = 0
```

and

```
Type variables: <none>

\forall \&1 \&2,
\{b\} \land M.x\{1\} \mod 2 + N.y\{2\} \mod 2 = 0 \Rightarrow
\forall \ x_L : \text{int} \ (b_L : \text{bool}) \ (y_R : \text{int} \ (b_R : \text{bool}),
b_L = b_R \land x_L \mod 2 = 0 \land y_R \mod 2 = 0 \Rightarrow
b_L = b_R \land x_L \mod 2 + y_R \mod 2 = 0
```

and

```
Type variables: <none>

Context : M.f

pre = M.x \mod 2 = 0

(1) \quad M.x <- M.x + 2
(2) \quad b' <$ \{0,1\}
(3) \quad b <- b \land b'

post = M.x \mod 2 = 0
```
CHAPTER 3. TACTICS

---

Type variables: <none>

Context: \( N.f \)

\( \text{pre} = N.y \mod 2 = 0 \)

1. \( N.y \leftarrow N.y - 2 \)
2. \( b' <\{0,1\} \)
3. \( b \leftarrow b \land b' \)

\( \text{post} = N.y \mod 2 = 0 \)

and

Type variables: <none>

\&1 \( \text{left} \) : \( M.f \)
\&2 \( \text{right} \) : \( N.f \)

\( \text{pre} = \{b\} \)

\( M.x \leftarrow M.x + 2 \) \quad \text{(1)} \quad \( N.y \leftarrow N.y - 2 \)
\( b' <\{0,1\} \) \quad \text{(2)} \quad b' <\{0,1\}
\( b \leftarrow b \land b' \) \quad \text{(3)} \quad b \leftarrow b \land b'

\( \text{post} = \{b\} \)

If the current goal is

Type variables: <none>

\( \text{pre} = \{b\} \land M.x\{1\} \mod 2 + N.y\{2\} \mod 2 = 0 \)
\( M.f \sim N.f \)

\( \text{post} = \{\text{res}\} \land M.x\{1\} \mod 2 + N.y\{2\} \mod 2 = 0 \)

then running

\( \text{conseq} \(_: =\{b\} \implies =\{\text{res}\}\)\)
\( \(_: M.x \mod 2 = 0 \implies M.x \mod 2 = 0\)\)
\( \(_: N.y \mod 2 = 0 \implies N.y \mod 2 = 0\)\).

produces the goals

Type variables: <none>

\( \forall \&1, \&2, \)
\( =\{b\} \land M.x\{1\} \mod 2 + N.y\{2\} \mod 2 = 0 \implies =\{b\} \land M.x\{1\} \mod 2 = 0 \land N.y\{2\} \mod 2 = 0 \)

and

Type variables: <none>

\( \forall \&1, \&2, \)
\( =\{b\} \land M.x\{1\} \mod 2 + N.y\{2\} \mod 2 = 0 \implies \)
forall \( (\text{result}_L \ \text{result}_R : \text{bool}) \ (x_L \ y_R : \text{int}), \)
\[
\text{result}_L = \text{result}_R /\ x_L \%\% 2 = 0 /\ y_R \%\% 2 = 0 => \]
\[
\text{result}_L = \text{result}_R /\ x_L \%\% 2 + y_R \%\% 2 = 0
\]

and

Type variables: <none>

\[
\text{pre} = M.x \%\% 2 = 0
\]
\[
M.f
\]
\[
\text{post} = M.x \%\% 2 = 0
\]

and

Type variables: <none>

\[
\text{pre} = N.y \%\% 2 = 0
\]
\[
N.f
\]
\[
\text{post} = N.y \%\% 2 = 0
\]

and

Type variables: <none>

\[
\text{pre} = \{b\}
\]
\[
M.f - N.f
\]
\[
\text{post} = \{\text{res}\}
\]

And given lemmas

lemma M_N : equiv[M.f - N.f : \{b\} \Rightarrow \{\text{res}\}].

and

lemma M : hoare[M.f : M.x \%\% 2 = 0 \Rightarrow M.x \%\% 2 = 0].

and

lemma N : hoare[N.f : N.y \%\% 2 = 0 \Rightarrow N.y \%\% 2 = 0].

if the current goal is

Type variables: <none>

\[
\text{pre} = \{b\} /\ M.x\{1\} \%\% 2 + N.y\{2\} \%\% 2 = 0
\]
\[
M.f - N.f
\]
\[
\text{post} = \{\text{res}\} /\ M.x\{1\} \%\% 2 + N.y\{2\} \%\% 2 = 0
\]

then running

conseq M_N M N.
produces the goals

\[
\text{forall } \&1 \&2, \\
=\{b\} \wedge M.x{1} \mod 2 + N.y{2} \mod 2 = 0 \Rightarrow \\
=\{b\} \wedge M.x{1} \mod 2 = 0 \wedge N.y{2} \mod 2 = 0
\]

and

\[
\text{forall } \&1 \&2, \\
=\{b\} \wedge M.x{1} \mod 2 + N.y{2} \mod 2 = 0 \Rightarrow \\
\text{forall } (\text{result}_L \text{ result}_R : \text{bool}) (x_L y_R : \text{int}), \\
\text{result}_L = \text{result}_R \wedge x_L \mod 2 = 0 \wedge y_R \mod 2 = 0 \Rightarrow \\
\text{result}_L = \text{result}_R \wedge x_L \mod 2 + y_R \mod 2 = 0
\]

\[\text{case} \]

**Syntax:** \(\text{case } e\). If the goal’s conclusion is a \(pRHL\), \(HL\) or \(pHL\) statement judgement and \(e\) is well-typed in the goal’s context, split the goal into two goals:

- a first goal in which \(e\) is added as a conjunct to the conclusion’s precondition; and
- a second goal in which \(!e\) is added as a conjunct to the conclusion’s precondition.

For example, if the current goal is

\[
\&1 (\text{left }) : M.f \\
\&2 (\text{right }) : N.f \\
\text{pre } = =\{x, y\}
\]

\[
\text{if } (x < y) \{ \\
\quad z \leftarrow y - x \\
\text{else } \{ \\
\quad z \leftarrow x - y \\
\}\}
\]

\[
\text{else } \{ \\
\quad z \leftarrow x - y \\
\}\}
\]

\[
\text{post } = =\{z\}
\]

then running

\[
\text{case } (x{1} < y{1}) .
\]

produces the goals

\[
\&1 (\text{left }) : M.f \\
\&2 (\text{right }) : N.f \\
\text{pre } = =\{x, y\} \wedge x{1} < y{1}
\]

\[
\text{if } (x < y) \{ \\
\quad (1--) \text{ if } (y <= x) \{ \\
\\}
\text{else } \{ \\
\quad (1--) \text{ else } \\
\\}
\]

\[
\quad (1--) \text{ if } (y <= x) \{ \\
\\}
\]

\[
\quad (1--) \\
\end{array}
\]

\[
\]
\[ z \leftarrow y - x \quad (1.1) \quad z \leftarrow x - y \]

\{ else \{ \}

\quad z \leftarrow x - y \quad (1?.1) \quad z \leftarrow y - x 
\}

post = \{z\}

and

Type variables: <none>

\&1 (left) : M.f
\&2 (right) : N.f

pre = \{x, y\} \& ! x{1} < y{1}

\{ if (x < y) { \}
\quad z \leftarrow y - x \quad (1.1) \quad z \leftarrow x - y 
\}

\{ else \{ \}

\quad z \leftarrow x - y \quad (1?.1) \quad z \leftarrow y - x 
\}

post = \{z\}

And if the current goal is

Type variables: <none>

Context : M.f

pre = true

\{1--\} y \leftarrow -1
\{2--\} while (0 < x) {
\quad y \leftarrow y + 2
\quad x \leftarrow x - 1
\}

post = y <> 0

then running

\texttt{case (0 < x)}.

produces the goals

Type variables: <none>

Context : M.f

pre = 0 < x

\{1--\} y \leftarrow -1
\{2--\} while (0 < x) {
\quad y \leftarrow y + 2
\quad x \leftarrow x - 1
\}

post = y <> 0
CHAPTER 3. TACTICS

and

Type variables: <none>

Context : $M.f$

\[ \text{pre} = \neg \ 0 \ < \ x \]

\[
\begin{align*}
(1--) & \ y \ <= \ -1 \\
(2--) & \ \textbf{while} \ (0 \ < \ x) \ \{ \\
(2.1) & \ y \ <= \ y + 2 \\
(2.2) & \ x \ <= \ x - 1 \\
(2--) & \}
\end{align*}
\]

\[ \text{post} = y \leftrightarrow 0 \]

\[ \textit{byequiv} \]

Syntax: $\textit{byequiv} \ (\_ : P \Rightarrow Q)$. If the goal’s conclusion has the form

\[ \Pr[M_1.p_1(a_{1,1}, \ldots, a_{1,n_1}) \ @ \ &m_1 : E_1] = \Pr[M_2.p_2(a_{2,1}, \ldots, a_{2,n_2}) \ @ \ &m_2 : E_2], \]

reduce the goal to three subgoals:

- One with conclusion $\text{equiv}[M_1.p_1 - M_2.p_2 : P \Rightarrow Q]$;
- One whose conclusion says that $P$ holds, where references to memories $\&1$ and $\&2$ have been replaced by $\&m_1$ and $\&m_2$, respectively, and references to the formal parameters of $M_1.p_1$ and $M_2.p_2$ have been replaced by their arguments;
- One whose conclusion says that $Q$ implies that $E_1(1) \ L\Rightarrow E_2(2)$.

The argument to \textit{byequiv} may be replaced by a proof term for $\text{equiv}[M_1.p_1 - M_2.p_2 : P \Rightarrow Q]$, in which case the first subgoal isn’t generated. Furthermore, either or both of $P$ and $Q$ may be replaced by $\_$, asking that the pre- or postcondition be inferred. Supplying no argument to \textit{byequiv} is the same as replacing both $P$ and $Q$ by $\_$. By default, inference of $Q$ attempts to infer a conjunction of equalities implying $E_1(1) \ L\Rightarrow E_2(2)$. Passing the [-eq] option to \textit{byequiv} takes $Q$ to be $E_1(1) \ L\Rightarrow E_2(2)$.

The other variants of the tactic behave similarly with regards to the use of proof terms and specification inference.

For example, consider the module

\[
\begin{align*}
\text{module} \ M & = \{} \\
\text{var} \ x & : \text{int} \\
\text{proc} \ f(y : \text{int}) & : \text{int} = \{} \\
\text{var} \ z & : \text{int}; \\
z & <\$ [x..y]; \\
\text{return} \ z; \\
\text{\}}.
\end{align*}
\]

If the current goal is

Type variables: <none>

\[ y_1: \text{int} \]
\[ y_2: \text{int} \]
\[ \&m_1: \text{memory} \]
\[ \&m_2: \text{memory} \]
CHAPTER 3. TACTICS

\[ x_{eq}: M.x^{m1} = M.x^{m2} \]
\[ y_{eq}: y_1 = y_2 \]

\[
\Pr[M.f(y_1) @ &m1 : res = 0] = \Pr[M.f(y_2) @ &m2 : res = 0]
\]

then running

\texttt{byequiv \{\_ : =\{M.x, y\} \Rightarrow \{res\}\}.}

produces the goals

\[ \text{Type variables: } <\text{none}> \]
\[ y_1: \text{int} \]
\[ y_2: \text{int} \]
\[ &m1: \text{memory} \]
\[ &m2: \text{memory} \]
\[ x_{eq}: M.x^{m1} = M.x^{m2} \]
\[ y_{eq}: y_1 = y_2 \]

\[ \text{pre} = \{M.x, y\} \]
\[ M.f - M.f \]
\[ \text{post} = \{\text{res}\} \]

and

\[ \text{Type variables: } <\text{none}> \]
\[ y_1: \text{int} \]
\[ y_2: \text{int} \]
\[ &m1: \text{memory} \]
\[ &m2: \text{memory} \]
\[ x_{eq}: M.x^{m1} = M.x^{m2} \]
\[ y_{eq}: y_1 = y_2 \]

\[ M.x^{m1} = M.x^{m2} \wedge y_1 = y_2 \]

and

\[ \text{Type variables: } <\text{none}> \]
\[ y_1: \text{int} \]
\[ y_2: \text{int} \]
\[ &m1: \text{memory} \]
\[ &m2: \text{memory} \]
\[ x_{eq}: M.x^{m1} = M.x^{m2} \]
\[ y_{eq}: y_1 = y_2 \]

\[ \forall &1 &2, \{\text{res}\} \Rightarrow \text{res}\{1\} = 0 \iff \text{res}\{2\} = 0 \]

Given the lemma

\[ \text{lemma M\_M\_f : equiv}\{M.f - M.f : =\{M.x, y\} \Rightarrow \{\text{res}\}\}. \]

if the current goal is

\[ \text{Type variables: } <\text{none}> \]
\[ y_1: \text{int} \]
\[ y_2: \text{int} \]
\[ &m1: \text{memory} \]
CHAPTER 3. TACTICS

\[ \begin{aligned}
&m2: \text{memory} \\
x_{eq}: & M.x\{m1\} = M.x\{m2\} \\
y_{eq}: & y1 = y2
\end{aligned} \]

\[ \Pr[M.f(y1) @ &m1 : \text{res} = 0] = \Pr[M.f(y2) @ &m2 : \text{res} = 0] \]

then running

\texttt{byequiv M_M_f.}

produces the goals

Type variables: <none>

\[
\begin{aligned}
y1: & \text{int} \\
y2: & \text{int} \\
&m1: \text{memory} \\
&m2: \text{memory} \\
x_{eq}: & M.x\{m1\} = M.x\{m2\} \\
y_{eq}: & y1 = y2
\end{aligned} \]

\[ M.x\{m1\} = M.x\{m2\} \land y1 = y2 \]

and

Type variables: <none>

\[
\begin{aligned}
y1: & \text{int} \\
y2: & \text{int} \\
&m1: \text{memory} \\
&m2: \text{memory} \\
x_{eq}: & M.x\{m1\} = M.x\{m2\} \\
y_{eq}: & y1 = y2
\end{aligned} \]

\[ \forall &1 &2, =\{\text{res}\} => \text{res}\{1\} = 0 <=\Rightarrow \text{res}\{2\} = 0 \]

And, if the current goal is

Type variables: <none>

\[
\begin{aligned}
y1: & \text{int} \\
y2: & \text{int} \\
&m1: \text{memory} \\
&m2: \text{memory} \\
x_{eq}: & M.x\{m1\} = M.x\{m2\} \\
y_{eq}: & y1 = y2
\end{aligned} \]

\[ \Pr[M.f(y1) @ &m1 : \text{res} = 0] = \Pr[M.f(y2) @ &m2 : \text{res} = 0] \]

then running

\texttt{byequiv.}

produces the goals

Type variables: <none>

\[
\begin{aligned}
y1: & \text{int} \\
y2: & \text{int} \\
&m1: \text{memory} \\
&m2: \text{memory} \\
x_{eq}: & M.x\{m1\} = M.x\{m2\} \\
y_{eq}: & y1 = y2
\end{aligned} \]
CHAPTER 3. TACTICS

pre = y(2) = y2 \M.x(2) = \M.x(\m2) \y(1) = y1 \M.x(1) = \M.x(\m1)  
\M.f - \M.f

post = ={res}

and

Type variables: <none>

y1: int
y2: int
\m1: memory
\m2: memory
\x_eq: \M.x(\m1) = \M.x(\m2)
\y_eq: y1 = y2

\y2 = y2 \M.x(\m2) = \M.x(\m2) \y1 = y1 \M.x(\m1) = \M.x(\m1)

and

Type variables: <none>

y1: int
y2: int
\m1: memory
\m2: memory
\x_eq: \M.x(\m1) = \M.x(\m2)
\y_eq: y1 = y2

forall \&1 &2, ={res} \=> res{1} = 0 <=\=> res{2} = 0

Syntax: byequiv (_ : P \=> Q). If the goal’s conclusion has the form

Pr[M_1.p1(a_1,1,\ldots,a_1,n_1) @ \&m_1 : \res] <= Pr[M_2.p2(a_2,1,\ldots,a_2,n_2) @ \&m_2 : E_2],

then byequiv behaves the same as in the first variant except that the conclusion of the third subgoal says that Q implies \E_1\{1\} => \E_2\{2\}.

For example, if the current goal is

Type variables: <none>

\&m: memory

Pr[M.f() @ \&m : \res] <= Pr[N.f() @ \&m : \res]

then running

byequiv (_ : true \=> \res\{1\} \=> \res\{2\}).

produces the goals

Type variables: <none>

\&m: memory

pre = true

\M.f - \N.f

post = \res\{1\} \=> \res\{2\}
Type variables: <none>
&\text{m}: \text{memory}
true

and

Type variables: <none>
&\text{m}: \text{memory}

\forall \&1 \&2, (\text{res}(1) \Rightarrow \text{res}(2)) \Rightarrow \text{res}(1) \Rightarrow \text{res}(2)

And, if the current goal is

Type variables: <none>
&\text{m}: \text{memory}

\text{Pr}[M.f() @ &\text{m} : \text{res}] \leq \text{Pr}[N.f() @ &\text{m} : \text{res}]

then running

\text{byequiv}.

produces the goals

Type variables: <none>
&\text{m}: \text{memory}

pre = true

M.f \sim N.f

post = \text{res}(1) \Rightarrow \text{res}(2)

and

Type variables: <none>
&\text{m}: \text{memory}

true

and

Type variables: <none>
&\text{m}: \text{memory}

\forall \&1 \&2, (\text{res}(1) \Rightarrow \text{res}(2)) \Rightarrow \text{res}(1) \Rightarrow \text{res}(2)

\textbf{Syntax:} \text{byequiv} (\_ : P \Rightarrow Q). If the goal’s conclusion has the form

\text{Pr}[M_1.p_1(a_{1,1}, \ldots, a_{1,n_1}) @ k_1m_1 : E_1] \leq \text{Pr}[M_2.p_2(a_{2,1}, \ldots, a_{2,n_2}) @ k_2m_2 : E_2] + \text{Pr}[M_2.p_2(a_{2,1}, \ldots, a_{2,n_2}) @ k_2m_2 : B_2],

then \text{byequiv} behaves the same as in the first variant except that the conclusion of the third subgoal says that Q implies !B_2(2) \Rightarrow E_1(1) \Rightarrow E_2(2).

For example, if the current goal is
CHAPTER 3. TACTICS

Type variables: <none>

\( \&m : \text{memory} \)

\[
\Pr[M.f() @ \&m : res] \leq \Pr[N.f() @ \&m : res] + \Pr[N.f() @ \&m : N.bad]
\]

then running

\( \text{byequiv} \ (_ : \text{true} == \neg \text{N.bad(2)} => \text{res}_1 => \text{res}_2) \).

produces the goals

Type variables: <none>

\( \&m : \text{memory} \)

\(\text{pre = true} \)

\( M.f - N.f \)

\(\text{post = } \neg \text{N.bad(2)} => \text{res}_1 => \text{res}_2 \)

and

Type variables: <none>

\( \&m : \text{memory} \)

\(\text{true} \)

\textbf{Fixme} Fatal: Why is the second subgoal pruned? (Compare with first and second variants, where the corresponding subgoal isn’t pruned.) And, if the current goal is

Type variables: <none>

\( \&m : \text{memory} \)

\[
\Pr[M.f() @ \&m : res] \leq \Pr[N.f() @ \&m : res] + \Pr[N.f() @ \&m : N.bad]
\]

then running

\( \text{byequiv}. \)

produces the goals

Type variables: <none>

\( \&m : \text{memory} \)

\(\text{pre = true} \)

\( M.f - N.f \)

\(\text{post = } \neg \text{N.bad(2)} => \text{res}_1 => \text{res}_2 \)

and

Type variables: <none>

\( \&m : \text{memory} \)

\(\text{true} \)
FiXme Fatal: Why is the second subgoal pruned?

Syntax: byequiv \(_ : P \Rightarrow Q \) : \( B_1 \). If the goal’s conclusion has the form

\[
\begin{align*}
&| \Pr[M_1.p_1(a_1,1,\ldots,a_{1,n_1}) @ &m_1 : E_1] - \Pr[M_2.p_2(a_2,1,\ldots,a_{2,n_2}) @ &m_2 : E_2] | <= \\
&\Pr[M_2.p_2(a_2,1,\ldots,a_{2,n_2}) @ &m_2 : B_2],
\end{align*}
\]

then byequiv behaves the same as in the first variant except that the conclusion of the third subgoal says that \( Q \) implies

\[
\langle B_1(1) \iff B_2(2) \rangle \land \neg B_2(2) \Rightarrow (E_1(1) \iff E_2(2))
\]

For example, if the current goal is

```
Type variables: <none>
&m: memory

|\[| \Pr[M.f() @ &m : res] - \Pr[N.f() @ &m : res] | <= \Pr[N.f() @ &m : N.bad]|\]
```

then running

```
byequiv \(_ : \text{true} \Rightarrow M.b\text{ad}(1) = N.b\text{ad}(2) \land (! N.b\text{ad}(2) => ={res}()) \) : M.b\text{ad}
```

produces the goals

```
Type variables: <none>
&m: memory

pre = \text{true}
M.f \neq N.f

post = M.b\text{ad}(1) = N.b\text{ad}(2) \land (! N.b\text{ad}(2) => ={res}())
```

and

```
Type variables: <none>
&m: memory

true
```

and

```
Type variables: <none>
&m: memory

forall \&1 \&2,
M.b\text{ad}(1) = N.b\text{ad}(2) \land (! N.b\text{ad}(2) => ={res}()) =>
(M.b\text{ad}(1) \iff N.b\text{ad}(2)) \land (! N.b\text{ad}(2) => res(1) \iff res(2))
```

Given the lemma

```
lemma L2 \&m :
```

if the current goal is

```
Type variables: <none>
&m: memory

|\[| \Pr[M.f() @ &m : res] - \Pr[N.f() @ &m : res] | <= \Pr[N.f() @ &m : N.bad]|\]
```
then running

\[ \text{byequiv } M.N.f : M.\text{bad}. \]

produces the goals

\begin{align*}
\text{Type variables: } & \langle \text{none} \rangle \\
& \&m : \text{memory} \\
& \text{true}
\end{align*}

and

\begin{align*}
\text{Type variables: } & \langle \text{none} \rangle \\
& \&m : \text{memory} \\
\text{forall } & \&1 \&2, \\
& M.\text{bad}(1) = N.\text{bad}(2) \land (\neg N.\text{bad}(2) \Rightarrow \text{res}) \Rightarrow \\
& (M.\text{bad}(1) \Leftrightarrow N.\text{bad}(2)) \land (\neg N.\text{bad}(2) \Rightarrow \text{res}(1) \Leftrightarrow \text{res}(2))
\end{align*}

\[ \text{byphoare} \]

**Syntax:** \texttt{byphoare} \(_ : P \Rightarrow Q\). If the goal’s conclusion has the form

\[ \text{Pr}[M.p(a_1,\ldots,a_n) @ \&m : E] = e, \]

reduce the goal to three subgoals:

- One with conclusion \texttt{phoare}[M.p : P \Rightarrow Q] = e;
- One whose conclusion says that \(P\) holds, where variables references are looked-up in \&m and references to the formal parameters of \(M.p\) have been replaced by its arguments; and
- One whose conclusion says that \(Q \Leftrightarrow E\).

The argument to \texttt{byphoare} may be replaced by a proof term for \texttt{phoare}[M.p : P \Rightarrow Q] = e, in which case the first subgoal isn’t generated. Furthermore, either or both of \(P\) and \(Q\) may be replaced by \_, asking that the pre- or postcondition be inferred. Supplying no argument to \texttt{byphoare} is the same as replacing both \(P\) and \(Q\) by \_.

The other variants of the tactic behave similarly with regards to the use of proof terms and specification inference.

For example, consider the module

\begin{verbatim}
module M = {
  var x : int
  proc f(y : int) : int = {
    var z : int;
    x <$ [x .. y];
    return x;
  }
}
\end{verbatim}

If the current goal is

\begin{align*}
\text{Type variables: } & \langle \text{none} \rangle \\
& x' : \text{int} \\
& y' : \text{int} \\
& \&m : \text{memory} \\
& \text{range: } x' + 1 = y' \\
& x_.eq : M.\text{x}(m) = x'
\end{align*}

\[ \text{Pr}[M.f(y') @ \&m : \text{res} = x'] = 1/2 \& / 2\& \]
then running

\texttt{byphoare \_ : M.x + 1 = y \land x' = M.x \implies x' = res).}

produces the goals

\begin{verbatim}
Type variables: <none>
x' : int
y' : int
&m : memory
range: x' + 1 = y'
x_eq: M.x{m} = x'

pre = M.x + 1 = y \land x' = M.x

M.f
[=] 1%r / 2%r

post = x' = res
\end{verbatim}

and

\begin{verbatim}
Type variables: <none>
x' : int
y' : int
&m : memory
range: x' + 1 = y'
x_eq: M.x{m} = x'

M.x{m} + 1 = y' \land x' = M.x{m}

forall &hr, x' = res{hr} \iff res{hr} = x'
\end{verbatim}

Given the lemma

\texttt{lemma M_f (x' : int) :}

\texttt{phoare[M.f : M.x + 1 = y \land x' = M.x \implies x' = res] = (1%r / 2%r).}

if the current goal is

\begin{verbatim}
Type variables: <none>
x' : int
y' : int
&m : memory
range: x' + 1 = y'
x_eq: M.x{m} = x'

P_{M.f(y') \& &m : res = x'} = 1%r / 2%r
\end{verbatim}

then running
**CHAPTER 3. TACTICS**

byphoare \( (M_f \ x') \).

produces the goals

**Type variables: <none>**

\[
x': \text{int} \\
y': \text{int} \\
\&m: \text{memory} \\
\text{range: } x' + 1 = y' \\
x_.eq: M.x\{m\} = x'
\]

\[
M.x\{m\} + 1 = y' \land x' = M.x\{m\}
\]

and

**Type variables: <none>**

\[
x': \text{int} \\
y': \text{int} \\
\&m: \text{memory} \\
\text{range: } x' + 1 = y' \\
x_.eq: M.x\{m\} = x'
\]

\[
\text{forall } \&hr, x' = \text{res}\{hr\} <\Rightarrow \text{res}\{hr\} = x'
\]

**Syntax:** byphoare \(_ : P \Rightarrow Q\). If the goal's conclusion has the form

\[
e \Leftarrow P_r[\ M.p(a_1, \ldots, a_n) \ &m : E],
\]

then byphoare behaves as in the first variant except the conclusion of the first subgoal is

**phoare\[M.p : P \Rightarrow Q\] >> e.**

For example, if the current goal is

**Type variables: <none>**

\[
\&m: \text{memory}
\]

\[
1\%r / 2\%r \Leftarrow \text{Pr}[M.f() \ &m : \text{res}]
\]

then running

**byphoare \(_ : \text{true} \Rightarrow \text{res}\).**

produces the goals

**Type variables: <none>**

\[
\&m: \text{memory}
\]

\[
pre = \text{true}
\]

\[
M.f \\
[\Rightarrow 1\%r / 2\%r
\]

\[
post = \text{res}
\]

and

**Type variables: <none>**
CHAPTER 3. TACTICS

&\texttt{m: memory}

\hline
\texttt{true}

\hline

and

\hline

Type variables: <none>

\hline

&\texttt{m: memory}

\hline

\texttt{forall \_\_\_, true}

\hline

\textbf{Fixme} Fatal: It’s confusing how the third goal has been simplified, but not pruned.

Given the lemma

\texttt{lemma M_f : phoare[M.f : true ==> res] >= (1%r / 2%r).}

if the current goal is

\hline

Type variables: <none>

\hline

&\texttt{m: memory}

\hline

1%r / 2%r <= Pr[M.f() @ &m : res]

\hline

then running

\texttt{byphoare M_f.}

produces the goals

\hline

Type variables: <none>

\hline

&\texttt{m: memory}

\hline

\texttt{true}

\hline

and

\hline

Type variables: <none>

\hline

&\texttt{m: memory}

\hline

\texttt{forall \_\_\_, true}

\hline

And, if the current goal is

\hline

Type variables: <none>

\hline

&\texttt{m: memory}

\hline

1%r / 2%r <= Pr[M.f() @ &m : res]

\hline

then running

\texttt{byphoare.}

produces the goals

\hline

Type variables: <none>

\hline

&\texttt{m: memory}

\hline

\texttt{pre = true}
M.f
[>=] 1%r / 2%r

post = res

and

Type variables: <none>
&\text{m}: \text{memory}
true

and

Type variables: <none>
&\text{m}: \text{memory}
forall _, true

Syntax: \text{byphoare} (_ : P \Rightarrow Q). If the goal’s conclusion has the form
\Pr[M.p(a_1,\ldots,a_n) @ &\text{m} : E] <= e,
then \text{byphoare} behaves as in the first variant except the conclusion of the first subgoal is
\text{phoare}[M.p : P \Rightarrow Q] <= e.
For example, if the current goal is

Type variables: <none>
&\text{m}: \text{memory}
\Pr[M.f() @ &\text{m} : \text{res]} <= 1%r / 2%r

then running

\text{byphoare} (_ : \text{true} \Rightarrow \text{res}).

produces the goals

Type variables: <none>
&\text{m}: \text{memory}
\text{pre} = \text{true}

\begin{verbatim}
M.f
[<=] 1%r / 2%r

post = \text{res}
\end{verbatim}

and

Type variables: <none>
&\text{m}: \text{memory}
true

and
FiXme Fatal: It’s confusing how the third goal has been simplified, but not pruned.

Given the lemma

```coq
lemma M_f : phoare[M.f : true ==> res] <= (1%r / 2%r).
```

if the current goal is

```coq
Type variables: <none>

&m: memory

Pr[M.f() @ &m : res] <= 1%r / 2%r
```

then running

```coq
byphoare M_f.
```

produces the goals

```coq
Type variables: <none>

&m: memory

true
```

and

```coq
Type variables: <none>

&m: memory

forall _, true
```

And, if the current goal is

```coq
Type variables: <none>

&m: memory

Pr[M.f() @ &m : res] <= 1%r / 2%r
```

then running

```coq
byphoare.
```

produces the goals

```coq
Type variables: <none>

&m: memory

pre = true

M.f 
[<=] 1%r / 2%r

post = res
```
and

Type variables: <none>

& \text{m: memory}

true

and

Type variables: <none>

& \text{m: memory}

forall \_., true

\text{bypr}

Syntax: \text{bypr} \; e_1 \; e_2. If the goal’s conclusion has the form

\text{equiv}[M. p - N. q : P \Rightarrow Q],

and the \( e_i \) are expressions of the same type possibly involving memories \&1 and \&2 for \( M. p \) and \( N. q \), respectively, then reduce the goal to two subgoals:

- One whose conclusion says that for all memories \&1 and \&2 for \( M. p \) and \( N. q \), if \( e_1 = e_2 \), then \( Q \) holds; and

- One whose conclusion says that, for all memories \&1 and \&2 for \( M. p \) and \( N. q \) and values \( a \) of the common type of the \( e_i \), if \( P \) holds, then the probability of running \( M. p \) in memory \&1 and with arguments consisting of the values of its formal parameters in \&1 and terminating in a memory in which the value of \( e_1 \) (replacing references to \&1 with reference to this memory) is \( a \) is the same as the probability of running \( N. q \) in memory \&2 and with arguments consisting of the values of its formal parameters in \&2 and terminating in a memory in which the value of \( e_2 \) (replacing references to \&2 with reference to this memory) is \( a \).

For example, consider the modules

\begin{verbatim}
module M = {
  var x : bool
  proc f(y : bool) : bool = {
    var b : bool;
    b <$ {0,1};
    return b /\ y;
  }
}.

module N = {
  var x : bool
  proc f(y : bool) : bool = {
    var b, b' : bool;
    b <$ {0,1};
    b' <$ {0,1};
    return (b ^^ b') /\ y;
  }
}.
\end{verbatim}

If the current goal is

Type variables: <none>
CHAPTER 3. TACTICS

pre = \( \{y\} \land M.x{1} = N.x{2}\)

\[ M.f = N.f \]

post = \( \{\text{res}\{1\} \land M.x{1}\} = \{\text{res}\{2\} \land N.x{2}\} \)

then running

\text{bypr} (\text{res}, M.x\{1\}) (\text{res}, N.x\{2\}).

produces the goals

Type variables: <none>

\[ \text{forall} \ &1 \ &2 \ (a : \text{bool} \times \text{bool}), \]

\[ (\text{res}\{1\}, M.x\{1\}) = a \Rightarrow (\text{res}\{2\}, N.x\{2\}) = a \Rightarrow (\text{res}\{1\} \land M.x\{1\}) = (\text{res}\{2\} \land N.x\{2\}) \]

and

Type variables: <none>

\[ \text{forall} \ &1 \ &2 \ (a : \text{bool} \times \text{bool}), \]

\[ =\{y\} \land M.x\{1\} = N.x\{2\} \Rightarrow \]

\[ \text{Pr}[M.f(y\{1\}) @ &1 : \{\text{res}, M.x\} = a] = \]

\[ \text{Pr}[N.f(y\{2\}) @ &2 : \{\text{res}, N.x\} = a] \]

**Syntax:** \text{bypr}. If the goal’s conclusion has the form

\[ \text{hoare}[M.p : P \Rightarrow Q], \]

then reduce the goal to one whose conclusion says that, for all memories \( km \) for \( M.p \) such that \( P(m) \) holds, the probability of running \( M.p \) in memory \( km \) and with arguments consisting of the values of its formal parameters in \( km \) and terminating in a memory satisfying \( !Q \) is 0.

For example, consider the module

```plaintext
module M = {
  var x : bool
  proc f(y : bool) : bool = {
    var z : bool;
    z \in \{0,1\};
    return x \land y \land z;
  }
}.
```

If the current goal is

Type variables: <none>

\[ \text{pre} = \{y\} \land \neg M.x \]

\[ M.f \]

\[ \text{post} = \{\text{res}\} \]

then running

\text{bypr}. 

produces the goal

Type variables: <none>

\[ \forall m, \forall y \{ m \} \Rightarrow \Pr [ M.f(y(m)) ] @ m : \forall \text{res} = \%r \]

\section{exists*}

\textbf{Syntax:} \texttt{exists*} \( e_1, \ldots, e_n \). If the goal’s conclusion is a \textit{pRHL}, \textit{HL} or \textit{pHL} judgment or statement judgements and the \( e_i \) are well-typed expressions typically involving program variables (in the \textit{pRHL} case, the expressions will refer to memories \( \&1 \) and \( \&2 \)), then change the conclusion’s precondition \( P \) to

\[ \texttt{exists} (x_1 \ldots x_n), x_1 = e_2 /\ldots/ x_n = e_n \land P. \]

The tactic can be used in conjunction with \texttt{elim*} (p. 166) when handling a procedure call using a lemma that refers to initial values of program variables. See \texttt{elim*} (p. 166) for an example of this.

For example, if the current goal is

Type variables: <none>

\[ \begin{align*}
\text{pre} &= \{ y \} \land M.x(1) = N.x(2) \\
M.f &= N.f \\
\text{post} &= \{ \text{res} \}
\end{align*} \]

then running

\[ \texttt{exists*} (y + 1){1}, (N.x{2} - y{1}). \]

produces the goal

Type variables: <none>

\[ \begin{align*}
\text{pre} &= \texttt{exists} (f f0 : \text{int}), \\
&\quad (f = y{1} + 1 \land f0 = N.x{2} - y{1}) \land \\
&\quad \{ y \} \land M.x(1) = N.x(2) \\
M.f &= N.f \\
\text{post} &= \{ \text{res} \}
\end{align*} \]

If the current goal is

Type variables: <none>

\begin{align*}
&1 (\texttt{left} ) : M.f \\
&2 (\texttt{right} ) : N.f \\
\text{pre} &= \{ y \} \land M.x(1) = N.x(2) \\
z &\leftarrow (-M.x) + y \quad (1) \quad z \leftarrow N.x - y \\
\text{post} &= M.x(1) + z{1} + M.x(1) = y(2) + z(2) + y(2)
\end{align*}
then running

\texttt{exists*} (y + 1, \texttt{(N.x \cdot y)}).

produces the goal

Type variables: \texttt{<none>}

\&1 \texttt{(left)} : M.f
\&2 \texttt{(right)} : N.f

\texttt{pre} =
\texttt{exists} (f \ f0 : \texttt{int}),
\quad (f = y + 1 \lor f0 = N.x - y) \land
\quad =\{y\} \land M.x = N.x\{2\}

\texttt{z} \leftarrow (-M.x) + y \quad (1) \quad z \leftarrow N.x - y

\texttt{post} = M.x + z + M.x = y + z + y

If the current goal is

Type variables: \texttt{<none>}

\texttt{pre} = 0 \leq y \land 0 \leq M.x

\texttt{M.f}

\texttt{post} = 0 \leq \texttt{res}

then running

\texttt{exists*} (y + M.x - 2).

produces the goal

Type variables: \texttt{<none>}

\texttt{pre} = \texttt{exists} (f : \texttt{int}), f = y + M.x - 2 \land 0 \leq y \land 0 \leq M.x

\texttt{M.f}

\texttt{post} = 0 \leq \texttt{res}

If the current goal is

Type variables: \texttt{<none>}

Context : M.f

\texttt{pre} = 0 \leq y \land 0 \leq M.x

(1) \quad \texttt{z} \leftarrow (-M.x) + y

\texttt{post} = 0 \leq M.x + z + M.x

then running

\texttt{exists*} (y + M.x - 2).
produces the goal

\[
\text{Type variables: <none>}
\]

Context : \( \text{M.f} \)
\[
\text{pre} = \text{exists} (f : \text{int}), f = y + \text{M.x} - 2 \wedge 0 \leq y \wedge 0 \leq \text{M.x}
\]
\[
(1) \ z \leftarrow (-\text{M.x}) + y
\]
\[
\text{post} = 0 \leq \text{M.x} + z + \text{M.x}
\]

\textbf{elim*}

If the goal’s conclusion is a \( \text{pRHL, HL or pHL} \) judgement or statement judgement whose precondition has the form
\[
\text{exists} (x_1 \ldots x_n), P,
\]
then remove the existential quantification from the precondition, and universally quantify the judgement or statement judgement by the \( x_i \).

Such existential quantifications may be introduced by \textbf{sp} (p. 81) or \textbf{exists*} (p. 164).

For example, if the current goal is
\[
\text{Type variables: <none>}
\]
\[
\text{pre} = \\
\quad \text{exists} (f \ f_0 : \text{int}), \\
\quad (f = y(1) + 1 \wedge f_0 = \text{N.x}(2) - y(1)) \wedge \\
\quad =y(1) \wedge \text{M.x}(1) = \text{N.x}(2) \\
\quad \text{M.f} = \text{N.f}
\]
\[
\text{post} = =\text{res}
\]
then running
\textbf{elim*},

produces the goal

\[
\text{Type variables: <none>}
\]
\[
\text{forall} (f \ f_0 : \text{int}), \\
\quad \text{equiv} [ \text{M.f} = \text{N.f} : \\
\quad (f = y(1) + 1 \wedge f_0 = \text{N.x}(2) - y(1)) \wedge \\
\quad =y(1) \wedge \text{M.x}(1) = \text{N.x}(2) \implies =\text{res}]
\]

If the current goal is
\[
\text{Type variables: <none>}
\]
\[
\&1 \ (\textbf{left} ) : \text{M.f} \\
\&2 \ (\textbf{right} ) : \text{N.f}
\]
\[
\text{pre} = \\
\quad \text{exists} (f \ f_0 : \text{int}), \\
\quad (f = y(1) + 1 \wedge f_0 = \text{N.x}(2) - y(1)) \wedge
\]
CHAPTER 3. TACTICS

\[
\begin{align*}
\{y\} \land M.x(1) &= N.x(2) \\
z &\leftarrow (-M.x) + y & \text{(1) } z &\leftarrow N.x - y \\
post &= M.x(1) + z(1) + M.x(1) = y(2) + z(2) + y(2)
\end{align*}
\]

then running

\textit{elim*}.

produces the goal

Type variables: <none>

\[
\begin{align*}
\begin{array}{c}
\text{forall } (f \ f0 : \text{int}), \\
equiv \{ M.f.z &\leftarrow (-M.x(hr)) + M.f.y(hr) - N.f.z \leftarrow N.x(hr) - N.f.y(hr) : \\
(f = y(1) + 1 \land f0 = N.x(2) - y(1)) \land \\
=(y) \land M.x(1) = N.x(2) \Rightarrow \\
M.x(1) + z(1) + M.x(1) = y(2) + z(2) + y(2)\}
\end{array}
\end{align*}
\]

If the current goal is

Type variables: <none>

\[
\begin{align*}
pred = \exists f : \text{int}, f &= y + M.x - 2 \land 0 <= y \land 0 <= M.x \\
M.f
\end{align*}
\]

then running

\textit{elim*}.

produces the goal

Type variables: <none>

\[
\begin{align*}
\begin{array}{c}
\text{forall } (f : \text{int}), \\
\text{hoare} \{ M.f : f = y + M.x - 2 \land 0 <= y \land 0 <= M.x \Rightarrow 0 <= \text{res}\}
\end{array}
\end{align*}
\]

If the current goal is

Type variables: <none>

\[
\begin{align*}
\text{Context } : M.f \\
pred = \exists f : \text{int}, f &= y + M.x - 2 \land 0 <= y \land 0 <= M.x \\
(1) z &\leftarrow (-M.x) + y \\
post &= 0 <= M.x + z + M.x
\end{align*}
\]

then running

\textit{elim*}.

produces the goal
Type variables: <none>

```
forall (f : int),
hoare[ z <- (-M.x) + y :
  f = y + M.x - 2 \ 0 <= y /\ 0 <= M.x ==> 0 <= M.x + z + M.x]
```

As a more realistic example, consider the module
```
module M = {
  proc f(x : int) : int = {
    return x + 1;
  }
  proc g(x : int) : int = {
    var y : int;
    y <@ f(x);
    return y;
  }
};
```
and lemma
```
lemma M_f (x : int) : hoare[M.f : x = x ==> res = x + 1].
```

If the current goal is
```
Type variables: <none>
```
```
Context : M.g
pre = x = -1
(1) y <@ M.f(x)
post = y = 0
```
then running
```
exists* x.
```
produces the goal
```
Type variables: <none>
```
```
Context : M.g
pre = exists (x0 : int), x0 = x /\ x = -1
(1) y <@ M.f(x)
post = y = 0
```
from which running
```
elim=>> x'.
```
produces the goal
```
Type variables: <none>
```
\textbf{x': int}

\underline{Context : M.g}
\pre = x' = x \land x = -1

(1) \ y <\emptyset M.f(x)
\post = y = 0

from which running
\texttt{call \langle M.f \ x'\rangle}.

\underline{produces the goal}

\underline{Type variables: <none>}
\underline{x': int}

\underline{Context : M.g}
\pre = x' = x \land x = -1

\post = \ x' = x \land \textbf{forall} (\textup{result : int}), \textup{result} = x' + 1 \Rightarrow \textup{result} = 0

\section*{hoare}

\textbf{Fixme Fatal: Update waiting for overhaul of pHL.}
\textbf{Syntax: \texttt{hoare <spec>}. Derives a null probability from a HL judgement on the procedure involved. \texttt{hoare} can also be used to derive pHL judgments and certain probability inequalities by automatically applying \texttt{conseq} (p. 136).}

\textbf{Examples:}

\begin{align*}
\texttt{hoare} & \begin{cases} \text{true} \end{cases} f \{ \neg Q \} & \text{hoare} & \begin{cases} P \end{cases} f \{ \neg Q \} \\
\Pr[\langle m, f(x) : Q \rangle] = 0 & \{ P \} f \{ Q \} \leq 0
\end{align*}

\section*{phoare split}

\textbf{Fixme Fatal: Update waiting for overhaul of pHL.}
\textbf{Syntax: \texttt{phoare split \delta_A \delta_B \delta_{AB}. Splits a pHL judgment whose postcondition is a conjunction or disjunction into three pHL judgments following the definition of the probability of a disjunction of events.}

\textbf{Examples:}

\begin{align*}
\texttt{phoare split} & \delta_A \delta_B \delta_{AB} \quad \text{[pHL]} \\
\delta_A + \delta_B - \delta_{AB} \ast \delta & \begin{cases} P \end{cases} c \{ A \} \ast \delta_A \quad \begin{cases} P \end{cases} c \{ B \} \ast \delta_B \quad \begin{cases} P \end{cases} c \{ A \land B \} \ast \delta_{AB} \quad \begin{cases} P \end{cases} c \{ A \lor B \} \ast \delta
\end{align*}
Syntax: **phoare split** $! \delta_i$. Splits a pHL judgment into two judgments whose postcondition are true and the negation of the original postcondition, respectively.

**Examples:**

\[
\text{phoare split } \delta_i \quad [\text{pHL}]
\]
\[
\delta \vdash \delta \cdot \delta \\
\{P\} \lor \delta \cdot \delta \\
\{Q\} \lor \delta
\]

Syntax: **phoare split** $\delta_A \delta_i : \Lambda$. Splits a pHL judgment following an event $A$.

**Examples:**

\[
\text{phoare split } \delta_A \delta_i : \Lambda \\
\delta_A + \delta_i \cdot \delta \\
\{P\} \lor \delta_A \\
\{Q \land \delta\} \lor \delta_i
\]

### 3.4.4 Automated Tactics

**Syntax:** **exfalso**. Combines **conseq** (p. 136), **byequiv** (p. 149), **byphoare** (p. 156), **hoare** (p. 169) and **bypr** (p. 162) to strengthen the precondition into false and discharge the resulting trivial goal.

For example, if the current goal is

Type variables: <none>
CHAPTER 3. TACTICS

pre = true

\[
\begin{align*}
\text{i} & \leftarrow 0 & (1--) & \text{i} & \leftarrow 0 \\
\text{j} & \leftarrow 0 & (2--) & \text{j} & \leftarrow 0 \\
\text{while} (\text{i} \leq 0) \{ & (3--) & \text{while} (\text{i} \leq 0) \{ \\
\text{i} & \leftarrow \text{i} - 1 & (3.1) & \text{i} & \leftarrow \text{i} - 1 \\
\} & (3--) & \}
\end{align*}
\]

post = \{\text{i} \\& \ 0 < \text{i} \& \ \text{i} \leq 0 \}

and

Type variables: <none>

\[
\begin{align*}
& \text{k1 (left)} : M.f \\
& \text{k2 (right)} : N.f \\
pren = \{\text{i} \& \ 0 < \text{i} \& \ \text{i} \leq 0 \\
\text{while} (\text{j} < 10) \{ & (1--) & \text{while} (\text{j} < 20) \{ \\
\text{i} & \leftarrow \text{i} + 2 & (1.1) & \text{i} & \leftarrow \text{i} + 3 \\
\text{j} & \leftarrow \text{j} + 1 & (1.2) & \text{j} & \leftarrow \text{j} + 1 \\
\} & (1--) & \}
\end{align*}
\]

post = \{\text{i} \}

The first of these goals is solved by running

\[
\text{while} (\{\text{i} \& \ \text{i} \leq 0 \} ; \text{auto ; smt}. \\
\]

And running

\[
\text{exfalso.}
\]

reduces the second of these goals to

Type variables: <none>

\[
\forall \text{k1} \ & \text{k2}, =\{\text{i} \& \ 0 < \text{i} \& \ \text{i} \leq 0 \} \Rightarrow \text{false}
\]

which \text{smt} solves.

\text{Fixme Fatal: Perhaps need other examples?}

\text{\textcircled{5} auto}

If the current goal is a \text{pRHL}, \text{HL} or \text{pHL} statement judgement, uses various program logic tactics in an attempt to reduce the goal to a simpler one. Never fails, but may fail to make any progress.

\text{Fixme Fatal: Need better description of when the tactic is applicable and how the tactic works!}

For example, if the current goal is

Type variables: <none>

\[
\text{Context : M.f} \\
\text{pre} = \text{1 <= y < x}
\]
\[ \text{if } (y < x) \{ \]
\[ (1.1) \quad z_1 \leftarrow x \]
\[ (1.2) \quad x \leftarrow y \]
\[ (1.3) \quad y \leftarrow z_1 \]
\[ \} \]
\[ \]
\[ (2--) \quad z_1 \notin [x..y] \]
\[ (3--) \quad z_2 \notin [x - 1..y + 1] \]
\[ \]
\[ \text{post} = 0 \leq z_1 + z_2 \]
\[ \]
then running
\[ \text{auto}. \]
\[ \]
produces the goal
\[ \text{Type variables: } \langle \text{none} \rangle \]
\[ \]
\[ \forall \&hr, \quad 1 \leq y/hr < x/hr \Rightarrow \]
\[ \text{if } y/hr < x/hr \quad \text{then} \]
\[ \forall (z_1 : \text{int}), \quad z_1 \notin [y/hr..x/hr] \Rightarrow \]
\[ \forall (z_2 : \text{int}), \quad z_2 \notin [y/hr - 1..x/hr + 1] \Rightarrow 0 \leq z_1 + z_2 \]
\[ \text{else} \]
\[ \forall (z_1 : \text{int}), \quad z_1 \notin [x/hr..y/hr] \Rightarrow \]
\[ \forall (z_2 : \text{int}), \quad z_2 \notin [x/hr - 1..y/hr + 1] \Rightarrow 0 \leq z_1 + z_2 \]
\[ \]
which \text{progress}; \text{smt} is able to solve. If the current goal is
\[ \text{Type variables: } \langle \text{none} \rangle \]
\[ \]
\[ \text{Context} : N.f \]
\[ \]
\[ \text{pre} = 1 \leq y < x \]
\[ \]
\[ (1) \quad z_1 \notin [x..y] \]
\[ (2) \quad x \leftarrow x - 1 \]
\[ (3) \quad y \leftarrow y + 1 \]
\[ (4) \quad z_2 \notin [x..y] \]
\[ (5) \quad x \leftarrow x - 1 \]
\[ (6) \quad y \leftarrow y + 1 \]
\[ \]
then running
\[ \text{auto}. \]
\[ \]
produce a single goal, which \text{smt} is able to solve. And, if the current goal is
\[ \text{Type variables: } \langle \text{none} \rangle \]
\[ \]
\[ \&1 \text{ (left) } : M.f \]
\[ \&2 \text{ (right) } : N.f \]
CHAPTER 3. TACTICS

\[ pre = \{x, y\} \land 1 < x{1} \leq y{2} \]

\[
\begin{align*}
&if (y < x) \{ \\
&\quad z1 <- x \quad (1.1) \\
&\quad x <- y \quad (1.2) \\
&\quad y <- z1 \quad (1.3) \\
&\} \quad (1--) \\
&\quad z1 <\{x..y\} \quad (2--) \\
&\quad z2 <\{x - 1..y + 1\} \quad (3--) \\
&\quad x <- x - 1 \quad (4--) \\
&\quad y <- y + 1 \quad (5--) \\
&\quad y <- y + 1 \quad (6--)
\end{align*}
\]

\[ post = z1{1} + z2{1} = z1{2} + z2{2} \]

then running

\[auto.\]

produce a single goal, which \texttt{smt} is able to solve.

\[\textcircled{\texttt{sim}}\]

\texttt{sim} attempts to solve a goal whose conclusion is a PRHL judgement or statement judgement by working backwards, propagating and extending a conjunction of equalities between variables of the two programs, verifying that the conclusion’s precondition implies the final conjunction of equalities. It’s capable of working backwards through \texttt{if} and \texttt{while} statements and handing random assignments, but only when the programs are sufficiently similar (thus its name). Sometimes this process only partly succeeds, leaving a statement judgement whose programs are prefixes of the original programs.

\textbf{Syntax:} \texttt{sim}. Without any arguments, \texttt{sim} attempts to infer the conjunction of program variable equalities from the conclusion’s postcondition.

For example, if the current goal is

\[
\begin{align*}
\neg1 & (\texttt{left }): M.f \\
\neg2 & (\texttt{right}): N.f \\
pre & = x{1} = N.u{2} \land y{1} + 1 = N.v{2} \\
i & <- 0 \quad (1--) \\
y & <- y + 1 \quad (2--) \\
&while (j < N.v) \{ \\
&\quad N.u <- N.u + N.u \quad (2.1) \\
&\quad j <- j + 1 \quad (2.2) \\
\} \quad (2--)
\end{align*}
\]

\[
\begin{align*}
while & (i < y) \{ \\
&\quad x <- x + x \quad (3.1) \\
&\quad i <- i + 1 \quad (3.2) \\
\} \quad (3--)
\end{align*}
\]

\[ post = x{1} = N.u{2} \]

then running

\[\texttt{sim}.\]

produces the goal

\[
\begin{align*}
\text{Type variables: <none>}
\end{align*}
\]

\[\neg1 (\texttt{left} ) : M.f \\
\neg2 (\texttt{right} ) : N.f \\
pre = x{1} = N.u{2} \land y{1} + 1 = N.v{2} \\
i & <- 0 \quad (1--) \\
y & <- y + 1 \quad (2--) \\
&while (j < N.v) \{ \\
&\quad N.u <- N.u + N.u \quad (2.1) \\
&\quad j <- j + 1 \quad (2.2) \\
\} \quad (2--)
\end{align*}
\]

\[
\begin{align*}
while & (i < y) \{ \\
&\quad x <- x + x \quad (3.1) \\
&\quad i <- i + 1 \quad (3.2) \\
\} \quad (3--)
\end{align*}
\]

\[ post = x{1} = N.u{2} \]

then running

\[\texttt{sim}.\]

produces the goal

\[
\begin{align*}
\text{Type variables: <none>}
\end{align*}
\]
which \texttt{auto} is able to solve.

\textbf{Syntax:} \texttt{sim} / \phi : \texttt{eqs}. One may give the starting conjunction, \texttt{eqs}, of equalities explicitly, and may also specify an invariant \phi on the global variables of the programs.

For example, if the current goal is

\begin{verbatim}
forall \&1, \&2, (x\{1\} = N.u\{2\} \& y\{1\} = N.v\{2\}) \& 0 < N.v\{2\} => x\{1\} = N.u\{2\} \& 1 < N.v\{2\} + 1
\end{verbatim}

then running

\begin{verbatim}
sim / (0 < N.v\{2\}) : (x\{1\} = N.u\{2\} \& y\{1\} = N.v\{2\}).
\end{verbatim}

produces the goals

\begin{verbatim}
forall \&1 \&2, (x\{1\} = N.u\{2\} \& y\{1\} = N.v\{2\}) \& 0 < N.v\{2\} => x\{1\} = N.u\{2\} \& 1 < N.v\{2\} + 1
\end{verbatim}

and

\begin{verbatim}
forall \&1, \&2, (x\{1\} = N.u\{2\} \& y\{1\} = N.v\{2\}) \& 0 <= y\{1\}
\end{verbatim}
\[ y \leftarrow y + 1 \quad (2) \]

\[ \text{post} = (x(1) = N.u(2) \land y(1) = N.v(2) \land i(1) = j(2)) \land 0 < N.v(2) \]

which \texttt{smt} and \texttt{auto;smt}, respectively, are able to solve.

**Syntax:** \texttt{sim \texttt{proeq}_1 \ldots \texttt{proeq}_n, / \phi : \texttt{eqs}.} In its most general form, one may also supply a sequence of procedure global equality specifications of the form

\[ (M.p - N.q : \texttt{eqs}), \]

where \texttt{eqs} is a conjunction of global variable equalities. When \texttt{sim} encounters a pair of procedure calls consisting of a call to \( M.p \) in the first program and \( N.q \) in the second program, it will generate a subgoal whose conclusion is a PRHL judgment between \( M.p \) and \( N.q \), whose precondition assumes equality of its arguments, \texttt{eqs} and \( \phi \), and whose postcondition requires equality of the calls’ results, \texttt{eqs} and \( \phi \).

One may also replace \( M.p - N.q \) by \_\_, meaning that the same conjunction of global variable equalities is used for all procedure calls.

For example, if the current goal is

```
Type variables: <none>

&1 (left ) : M.h
&2 (right ) : N.h

pre = true

k <- 0
M.x <- 0
M.i <- 0
M.j <- 0
while (k < 10) {
    M.f() ;
    k <- k + 1
}
while (k < 20) {
    M.g() ;
    k <- k + 1
}
post = |M.x{1} + k{1}| = |N.x{2} - k{2}|
```

then running

```
sim (M.f - N.f ; M.i{1} = N.i{2})
    (M.g - N.g ; M.j{1} = N.j{2}) /
    (N.x{1} = -N.x{2}) : (=k).
```

produces the goals

```
Type variables: <none>

forall &1 &2,
    ={k} \land M.x{1} = -N.x{2} \Rightarrow |M.x{1} + k{1}| = |N.x{2} - k{2}|
```

and

```
Type variables: <none>
```
pre = true \land M.i(1) = N.i(2) \land M.x(1) = -N.x(2)
M.f \sim N.f

post = \{res\} \land M.i(1) = N.i(2) \land M.x(1) = -N.x(2)

and

Type variables: <none>

pre = true \land M.j(1) = N.j(2) \land M.x(1) = -N.x(2)
M.g \sim N.g

post = \{res\} \land M.j(1) = N.j(2) \land M.x(1) = -N.x(2)

and

Type variables: <none>

&1 (left) : M.h
&2 (right) : N.h

pre = true
k <- 0
M.x <- 0

(1) k <- 0
(2) N.x <- 0

post = \{k\} \land M.x(1) = -N.x(2)

which smt, proc;auto;smt, proc;auto;smt and auto, respectively, are able to solve.

And, if the current goal is

pre = true
k <- 0
M.x <- 0
M.i <- 0
M.j <- 0

while (k < 10) {
    while (k < 10) {
        M.f()
        k <- k + 1
    }
    \{ (5.1) N.f() (5.2) k <- k + 1 \}
} (5.3)

while (k < 20) {
    while (k < 20) {
        M.g()
        k <- k + 1
    }
} (6.1) N.g() (6.2) k <- k + 1

post = \|M.x(1) + k(1)| = \|N.x(2) - k(2)|

then running
produces the goals

```
forall &1 &2, 
  ={k} /\ M.x{1} = -N.x{2} => `|M.x{1} + k{1}| = `|N.x{2} - k{2}|
```

and

Type variables: <none>

pre =
  true /\ (M.j{1} = N.j{2} /\ M.i{1} = N.i{2}) /\ M.x{1} = -N.x{2}
  M.f ~ N.f

post =
  ={res} /\ 
  (M.j{1} = N.j{2} /\ M.i{1} = N.i{2}) /\ M.x{1} = -N.x{2}

and

Type variables: <none>

pre =
  true /\ (M.j{1} = N.j{2} /\ M.i{1} = N.i{2}) /\ M.x{1} = -N.x{2}
  M.g ~ N.g

post =
  ={res} /\ 
  (M.j{1} = N.j{2} /\ M.i{1} = N.i{2}) /\ M.x{1} = -N.x{2}

and

Type variables: <none>

&1 (left) : M.h
&2 (right) : N.h

pre = true
k <- 0 (1) k <- 0
M.x <- 0 (2) N.x <- 0

post = ={k} /\ M.x{1} = -N.x{2}
```

which smt, proc;auto;smt, proc;auto;smt and auto, respectively, are able to solve.

### 3.4.5 Advanced Tactics

© *fel*

**Syntax:** fel init ctr stepub bound bad conds inv. “fel” stands for “failure event lemma”. To use this tactic, one must load the theory FelTactic. To be applicable, the current goal’s conclusion must have the form
Here:

- \( \text{ub} \) (“upper bound”) is an expression of type \( \text{real} \).
- \( \text{ctr} \) is the counter, an expression of type \( \text{int} \) involving program variables.
- \( \text{bad} \) is an expression of type \( \text{bool} \) involving program variables. It is the “bad” or “failure” event.
- \( \text{inv} \) is an optional invariant on program variables; if it’s omitted, \( \text{true} \) is used.
- \( \text{init} \) is a natural number no bigger than the number of statements in \( M.p \). It is the length of the initial part of the procedure that “initializes” the failure event lemma—causing \( \text{ctr} \) to become 0 and \( \text{bad} \) to become \( \text{false} \) and establishing \( \text{inv} \). The non-initialization part of the procedure may not directly use the program variables on which \( \text{ctr} \), \( \text{bad} \) and \( \text{inv} \) depend. These variables may only be modified by concrete procedures \( M.p \) may directly or indirectly call—such procedures are called oracle procedures. If \( M.p \) directly or indirectly calls an abstract procedure, there must be a module constraint saying that the abstract procedure may not modify the program variables determining the values of \( \text{ctr} \), \( \text{bad} \) and \( \text{inv} \) or that are used by the oracle procedures.
- \( \text{bound} \) is an expression of type \( \text{int} \). It must be the case that 
  \[
  \phi \land \text{inv} \Rightarrow \text{bad} \land \text{ctr} \leq \text{bound}.
  \]
- \( \text{conds} \) is a list of procedure preconditions
  \[
  [N_1.p_1 : \phi_1; \ldots; N_l.p_l : \phi_l],
  \]
  where the \( N_i.p_i \) are procedures, and the \( \phi_i \) are expressions of type \( \text{bool} \) involving program variables and procedure parameters. When a procedure’s precondition is true, it must increase the counter’s value; when it isn’t true, it must not decrease the counter’s value, and must preserve the value of \( \text{bad} \). Whether a procedure’s precondition holds or not, the invariant \( \text{inv} \) must be preserved.
- \( \text{stepub} \) is a function of type \( \text{int} \rightarrow \text{real} \), providing an upper bound as a function of the counter’s current value. When a procedure’s precondition, the invariant \( \text{inv}, \lnot \text{bad} \) and \( 0 \leq \text{ctr} < \text{bound} \) hold, the probability that \( \text{bad} \) becomes set during that call must be upper-bounded by the application of \( \text{stepub} \) to the counter’s value. In addition, it must be the case that the summation of \( \text{stepub} \ i \), as \( i \) ranges from 0 to \( \text{bound} - 1 \), is upper-bounded by \( \text{ub} \).

The subgoals generated by \( \text{fel} \) enforce the above rules. The best way to understand the details is via an example.

For example, consider the declarations

```haskell
op upp : { int | 1 <= upp } as ge1_upp.
op n : { int | 0 <= n } as ge0_n.

module type OR = {
  proc init() : unit
  proc gen() : bool
  proc add(_ : int) : unit
}.

module Or : OR = {
  var won : bool
  var gens : int list
}
```
Here, the oracle has a boolean variable \( \text{won} \), which is the bad event. It also has a list of integers \( \text{gens} \), all of which are within the range 1 to \( \text{upp} \), inclusive—the integers “generated” so far. The counter is the size of \( \text{gens} \). The procedure \( \text{gen} \) randomly generates such an integer, setting \( \text{won} \) to true if the integer was previously generated. And the procedure \( \text{add} \) adds a new integer to the list of generated integers, without possibly setting \( \text{bad} \). Both \( \text{gen} \) and \( \text{add} \) do nothing when the counter reaches the bound \( \text{n} \). The adversary has access to both \( \text{gen} \) and \( \text{bad} \).

If the current goal is

\[
\Pr[\text{G(Adv).main()} \otimes \text{\&m} : \text{Or.won}] \leq (n * (n - 1))^{\frac{1}{2}} / (2 * \text{upp})^{\frac{1}{2}}
\]

then running

\[
fel
\]

1

\[
\text{(size Or.gens)}
\]

\[
\text{(fun c\_tr \Rightarrow c\_tr^{\frac{1}{2}} * (1^{\frac{1}{2}} / \text{upp}^{\frac{1}{2}}))}
\]

\[
n
\]

\[
\text{Or.won}
\]

\[
[\text{Or.gen : (size Or.gens < n)}; \text{Or.add : (size Or.gens < n) / 1 <= x <= upp}]
\]
produces the goals

\[
\begin{align*}
\text{Type variables: } &<\text{none}> \\
\text{Adv: } &\text{ADV}(\text{Or}) \land \text{memory} \\
&\text{bigi predT } (\text{fun } (\text{ctr} : \text{int}) \Rightarrow \text{ctr} \mod r \times (1 \mod r / \text{upp} \mod r)) \ 0 \ n \leq \ (n \times (n - 1)) \mod r / (2 \times \text{upp} \mod r)
\end{align*}
\]

and

\[
\begin{align*}
\text{Type variables: } &<\text{none}> \\
\text{Adv: } &\text{ADV}(\text{Or}) \land \text{memory} \\
&\text{forall } \&m_0, \\
&\text{Or.won}(\&m_0) \Rightarrow \\
&\text{size Or.gens}(\&m_0) \leq n \Rightarrow \text{Or.won}(\&m_0) \land \text{size Or.gens}(\&m_0) \leq n
\end{align*}
\]

and

\[
\begin{align*}
\text{Type variables: } &<\text{none}> \\
\text{Adv: } &\text{ADV}(\text{Or}) \land \text{memory} \\
&\text{Context : } G(\text{Adv}).\text{main} \\
&\text{pre} = tt = tt \land \text{Or.gens} = \text{Or.gens}(\&m) \land \text{Or.won} = \text{Or.won}(\&m) \\
&(1) \text{ Or.init()} \\
&\text{post} = (!\text{Or.won} \land \text{size Or.gens} = 0) \land \text{size Or.gens} \leq n
\end{align*}
\]

and

\[
\begin{align*}
\text{Type variables: } &<\text{none}> \\
\text{Adv: } &\text{ADV}(\text{Or}) \land \text{memory} \\
&\text{pre} = \\
&((0 \leq \text{size Or.gens} \land \text{size Or.gens} < n) \land !\text{Or.won}) \land \\
&\text{size Or.gens} \leq n \land \\
&\text{size Or.gens} < n \land 1 \leq x \leq \text{upp} \\
&\text{Or.add} \\
&[<=] \text{size Or.gens}\mod r \times (1\mod r / \text{upp}\mod r) \\
&\text{post} = \text{Or.won}
\end{align*}
\]

and

\[
\begin{align*}
\text{Type variables: } &<\text{none}> \\
\text{Adv: } &\text{ADV}(\text{Or}) \land \text{memory} \\
&\text{forall } (c : \text{int}),
\end{align*}
\]
hoare\[ Or.add :\\( ((\size Or.gens < n \land 1 <= x <= \upp) \land c = \size Or.gens) \land \size Or.gens <= n) \implies c < \size Or.gens \land \size Or.gens <= n\\)

and

Type variables: <none>

Adv: ADV\{Or\}
&\&m: memory

forall (b : bool) (c : int),
hoare\[ Or.add :
(! (\size Or.gens < n \land 1 <= x <= \upp) \land Or.won = b \land \size Or.gens = c) \land \size Or.gens <= n) \implies (Or.won = b \land c <= \size Or.gens) \land \size Or.gens <= n\]

and

Type variables: <none>

Adv: ADV\{Or\}
&\&m: memory

pre = (((0 <= \size Or.gens \land \size Or.gens < n) \land \neg Or.won) \land \size Or.gens <= n) \land \size Or.gens < n

Or.gen \[<=\] \size Or.gens\%r * (1\%r / \upp\%r)

post = Or.won

and

Type variables: <none>

Adv: ADV\{Or\}
&\&m: memory

forall (c : int),
hoare\[ Or.gen :
(\size Or.gens < n \land c = \size Or.gens) \land \size Or.gens <= n) \implies c < \size Or.gens \land \size Or.gens <= n\]

and

Type variables: <none>

Adv: ADV\{Or\}
&\&m: memory

forall (b : bool) (c : int),
hoare\[ Or.gen :
(! \size Or.gens < n \land Or.won = b \land \size Or.gens = c) \land \size Or.gens <= n) \implies (Or.won = b \land c <= \size Or.gens) \land \size Or.gens <= n\]
**CHAPTER 3. TACTICS**

*eager* is a family of tactics for proving PRHL statement judgements of the form

\[ \text{equiv}[s_1, t_1 - t_2 : P \Rightarrow Q] \]

where the pre- and postconditions \( P \) and \( Q \) are conjunctions of equalities between program variables, and the statement sequences \( s_i \) only read and write global variables. Here \( s_1 \) is in the “eager” position, and its replacement, \( s_2 \), is in the “lazy” position. Some of the tactics work with *eager judgements* of the form

\[ \text{eager}[s_1, M.p - N.q, s_2 : P \Rightarrow Q] \]

where, again, the \( s_i \) only involve global variables, but where \( P \) and \( Q \) may talk about the parameters and results of \( M.p \) and \( N.q \) in the usual way.

The context of our examples is the following *EasyCrypt* script involving variable incrementation oracles \( \text{Or1} \) and \( \text{Or2} \), which only differ in that \( \text{Or2} \) keeps a “transcript” of its operation.

```plaintext
module type OR = {
  proc init() : unit
  proc incr_x() : unit
  proc incr_y() : unit
  proc incr_xy() : unit
  proc incr_yx() : unit
  proc loop(n : int) : bool
};

module Or1 : OR = {
  var x, y : int
  var b : bool
  proc init() : unit = { x <- 0; y <- 0; b <- true; }
  proc incr_x() : unit = { x <- x + 1; }
  proc incr_y() : unit = { y <- y + 1; }
  proc incr_xy() : unit = { incr_x(); incr_y(); }
  proc incr_yx() : unit = { incr_y(); incr_x(); }
  proc loop(n : int) : bool = {
    while (0 < n) {
      if (b) incr_x(); else incr_y();
      b <- !b;
    }
    return !b;
  }
}.

module Or2 : OR = {
  var x, y : int
  var b : bool
  var trace : bool list
  proc init() : unit = { x <- 0; y <- 0; b <- true; trace <- []; }
  proc incr_x() : unit = { x <- x + 1; trace <- trace ++ [true]; }
  proc incr_y() : unit = { y <- y + 1; trace <- trace ++ [false]; }
  proc incr_xy() : unit = { incr_x(); incr_y(); }
  proc incr_yx() : unit = { incr_y(); incr_x(); }
  proc loop(n : int) : bool = {
    while (0 < n) {
      if (b) incr_x(); else incr_y();
      b <- !b;
    }
    return !b;
  }
}```
lemma eager_incr :
eager[Or1.incr_x();, Or1.incr_y - Or2.incr_y, Or2.incr_x(); :
={x, y}(Or1, Or2) ==>{x, y}(Or1, Or2)].
proof.
eager proc.
inline *; auto.
qed.

lemma eager_incr_x :
eager[Or1.incr_x(); Or1.incr_y();, Or1.incr_x -
Or2.incr_x, Or2.incr_y(); Or2.incr_x(); :
={x, y, b}(Or1, Or2) ==>{x, y, b}(Or1, Or2)].
proof.
proc*.
inline*; auto.
qed.

lemma eager_incr_y :
eager[Or1.incr_x(); Or1.incr_y();, Or1.incr_y -
Or2.incr_y, Or2.incr_y(); Or2.incr_x(); :
={x, y, b}(Or1, Or2) ==>{x, y, b}(Or1, Or2)].
proof.
proc*: inline*; auto.
qed.

lemma eager_incr_xy :
eager[Or1.incr_x(); Or1.incr_y();, Or1.incr_xy -
Or2.incr_xy, Or2.incr_y(); Or2.incr_x(); :
={x, y, b}(Or1, Or2) ==>{x, y, b}(Or1, Or2)].
proof.
eager proc.
eager seq 1 1 (incr : Or1.incr_x(); Or1.incr_y(); -
Or2.incr_y(); Or2.incr_x(); :
={x, y}(Or1, Or2) ==>{x, y}(Or1, Or2)) :
(={x, y, b}(Or1, Or2)).
eager call eager_incr.
auto.
eager call eager_incr_x; first auto.
eager call eager_incr_y; first auto.
sim.
qed.

lemma eager_incr_yx :
eager[Or1.incr_x(); Or1.incr_y();, Or1.incr_yx -
Or2.incr_yx, Or2.incr_y(); Or2.incr_x(); :
={x, y, b}(Or1, Or2) ==>{x, y, b}(Or1, Or2)].
proof.
eager proc.
eager seq 1 1 (incr : Or1.incr_x(); Or1.incr_y(); -
Or2.incr_y(); Or2.incr_x(); :
={x, y}(Or1, Or2) ==>{x, y}(Or1, Or2)) :
(={x, y, b}(Or1, Or2)).
[eager call eager_incr; first auto |
eager call eager_incr_y; first auto |
eager call eager_incr_x; first auto | sim].
qed.
lemma eager_loop :
  eager [Or1.incr_x(); Or1.incr_y(); Or1.loop -
  Or2.loop, Or2.incr_y(); Or2.incr_x(); :
  ={n} /
  ={x, y, b}(Or1, Or2) =>>
  ={res} /
  ={x, y, b}(Or1, Or2)].

proof.
  eager proc.
  swap(2) 2 2; wp.
  eager while (incr : Or1.incr_x(); Or1.incr_y(); -
  Or2.incr_y(); Or2.incr_x(); :
  ={n} /
  ={x, y, b}(Or1, Or2) =>>
  ={n} /
  ={x, y, b}(Or1, Or2)).
  eager call eager_incr; first auto.
  trivial.
  swap(2) 2 2; wp.
  eager if.
  trivial.
  move=> &m b'; inline*; auto.
  eager call eager_incr_x; first auto.
  eager call eager_incr_y; first auto.
  sim.
  qed.

module type ADV(O : OR) = 
  {proc * main() : bool {O.incr_x O.incr_y O.incr_xy O.incr_yx O.loop} 
  }.

module G (Adv : ADV) = 
  {proc main1() : bool = 
    var b : bool; 
    Or1.init(); 
    Or1.incr_x(); Or1.incr_y(); 
    b <@ Adv(Or1).main(); 
    return b; 
  }

  proc main2() : bool = 
    var b : bool; 
    Or2.init(); 
    b <@ Adv(Or2).main(); 
    Or2.incr_y(); Or2.incr_x(); 
    return b;
  }

lemma eager_adv (Adv <: ADV{Or1, Or2}) :
  eager [Or1.incr_x(); Or1.incr_y();, Adv(Or1).main -
  Adv(Or2).main, Or2.incr_y(); Or2.incr_x(); :
  ={x, y, b}(Or1, Or2) =>> ={res} /
  ={x, y}(Or1, Or2)].

proof.
  eager proc (incr : Or1.incr_x(); Or1.incr_y(); -
  Or2.incr_y(); Or2.incr_x(); :
  ={x, y}(Or1, Or2) =>> ={x, y}(Or1, Or2))
  ={x, y, b}(Or1, Or2)).
  eager call eager_incr; first auto.
  trivial.
  trivial.
  apply eager_incr_x.
  sim.
  apply eager_incr_y.
  sim.
apply eager_incr_xy.
sim.
apply eager_incr_yx.
sim.
apply eager_loop.
sim.
qed.

lemma G_Adv (Adv <: ADV{Or1, Or2}) :
true ==> ={res} \={x, y}(Or1, Or2)].

proof.
proc.
seq 1 1 : (={x, y, b}(Or1, Or2)); first inline*; auto.
eager call (eager_adv Adv); first auto.
qed.

lemma G_Adv'(Adv <: ADV{Or1, Or2}) :
true ==> ={res} \={x, y}(Or1, Or2)].

proof.
proc.
seq 1 1 : (={x, y, b}(Or1, Or2)); first inline*; auto.
eager (incr : Or1.incr_x(); Or1.incr_y(); ~ Or2.incr_y(); Or2.incr_x(); :
={x, y}(Or1, Or2) ==>{x, y}(Or1, Or2)) :
(={x, y, b}(Or1, Or2)).
eager call eager_incr; first auto.
auto.
eager proc incr (={x, y, b}(Or1, Or2));
[trivial | trivial | apply eager_incr_x | sim |
apply eager_incr_y | sim | apply eager_incr_xy | sim |
apply eager_incr_yx | sim | apply eager_loop | sim].
qed.

Syntax: eager proc. Turn a goal whose conclusion is an eager judgement into one whose
conclusion is a PRHL statement judgement in which the eager judgement’s procedures have been
replaced by their bodies. For example, if the current goal is

```plaintext
eager[ Or1.incr_x();, Or1.incr_y - Or2.incr_y, Or2.incr_x( ); :
Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} ==>
Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}]
```

then running

```plaintext
eager proc.
```

produces the goal

```plaintext
&1 (left ) : Or1.incr_y
&2 (right ) : Or2.incr_y

pre = Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}
```
Or1.incr_x() (1) Or2.y ← Or2.y + 1
Or1.y ← Or1.y + 1 (2) Or2.trace ← Or2.trace ++ [false]
(3) Or2.incr_x()

post = Or1.x{1} = Or2.x{2} /\ Or1.y{1} = Or2.y{2}

**Syntax:** `proc*`. Turn a goal whose conclusion is an eager judgement into one whose conclusion is a PRHL statement judgement in which the eager judgement’s procedures are called, as opposed to being inlined. For example, if the current goal is

```
Type variables: <none>
```

```
eager[ Or1.incr_x();; Or1.incr_y();, Or1.incr_x ~ Or2.incr_x,
Or2.incr_y();; Or2.incr_x() ;
Or1.x{1} = Or2.x{2} /\ 
Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2} ==>
Or1.x{1} = Or2.x{2} /\ 
Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2}]
```

then running

```
proc*.
```

produces the goal

```
Type variables: <none>
```

```
&1 (left) : Or1.incr_x
&2 (right) : Or2.incr_x

pre = 
Or1.x{1} = Or2.x{2} /\ 
Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2}
```

```
Or1.incr_x() (1) r < Or2.incr_x()
Or1.incr_y() (2) Or2.incr_y()
r < Or2.incr_x() (3) Or2.incr_x()
```

```
post = 
Or1.x{1} = Or2.x{2} /\ 
Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2}
```

**Syntax:** `eager call` _p_. Here _p_ is a proof term for an eager judgement. If the goal’s conclusion is a PRHL statement judgement whose programs’ suffixes match the left and right sides of the eager judgment, then consume those suffixes.

For example, if the current goal is

```
Type variables: <none>
```

```
&1 (left) : Or1.incr_xy
&2 (right) : Or2.incr_xy

pre = Or1.x{1} = Or2.x{2} /\ Or1.y{1} = Or2.y{2}
```

```
Or1.incr_x() (1) Or2.incr_y()
Or1.incr_y() (2) Or2.incr_x()
```

```
post = Or1.x{1} = Or2.x{2} /\ Or1.y{1} = Or2.y{2}
```
CHAPTER 3. TACTICS

187

post = Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}

then running

eager call eager_incr.

(see the statement of eager_incr, above) produces the goal

Type variables: <none>

&1 (left) : Or1.incr_xy
&2 (right) : Or2.incr_xy

pre = Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}

post = Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}

Syntax: eager seq n1 n2 (H : s1 - s2 : A ==> B) : C.
Here, the goal’s conclusion must be a pRHL statement judgement whose left and right programs begin and end with s1 and s2, respectively. A first subgoal is generated whose conclusion is the specified pRHL statement judgement, which is made available as H for the subsequent subgoals’s use. The n1 and n2 must be natural numbers saying how many statements from the part of the first program following s1 and from the beginning of the second program to put together with the s1 in a second pRHL statement judgement subgoal. The remaining statements are put together with the si in a third pRHL statement judgement subgoal. And there is a final subgoal whose conclusion is a pRHL statement judgment whose left and right sides are those remaining statements of the second program only.

For example, if the current goal is

Type variables: <none>

&1 (left) : Or1.incr_xy
&2 (right) : Or2.incr_xy

pre =
Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} \ Or1.b{1} = Or2.b{2}

Or1.incr_x() (1) Or2.incr_x()
Or1.incr_y() (2) Or2.incr_y()
Or1.incr_x() (3) Or2.incr_y()
Or1.incr_y() (4) Or2.incr_x()

post =
Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} \ Or1.b{1} = Or2.b{2}

then running

eager seq 1 1 (incr : Or1.incr_x(); Or1.incr_y(); -
Or2.incr_y(); Or2.incr_x();)

={x, y}(Or1, Or2) ==> ={x, y}(Or1, Or2)) :
({x, y, b}(Or1, Or2)).

produces the goals
CHAPTER 3. TACTICS

Type variables: <none>

&1 (left) : Or1.incr_xy
&2 (right) : Or2.incr_xy

pre = Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}

Or1.incr_x() (1) Or2.incr_y()
Or1.incr_y() (2) Or2.incr_x()

post = Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}

and

Type variables: <none>

incr: equiv [ Or1.incr_x(); Or1.incr_y(); - Or2.incr_y();
  Or2.incr_x(); :
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} ==>  
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} ]

&1 (left) : Or1.incr_xy
&2 (right) : Or2.incr_xy

pre =
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} \ Or1.b{1} = Or2.b{2}

Or1.incr_x() (1) Or2.incr_x()
Or1.incr_y() (2) Or2.incr_y()
Or1.incr_x() (3) Or2.incr_x()

post =
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} \ Or1.b{1} = Or2.b{2}

and

Type variables: <none>

incr: equiv [ Or1.incr_x(); Or1.incr_y(); - Or2.incr_y();
  Or2.incr_x(); :
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} ==>  
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} ]

&1 (left) : Or1.incr_xy
&2 (right) : Or2.incr_xy

pre =
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} \ Or1.b{1} = Or2.b{2}

Or1.incr_x() (1) Or2.incr_y()
Or1.incr_y() (2) Or2.incr_y()
Or1.incr_y() (3) Or2.incr_x()

post =
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} \ Or1.b{1} = Or2.b{2}
and

Type variables: <none>

```plaintext
incr: equiv
Or1.incr_x(); Or1.incr_y(); ~ Or2.incr_y();
Or2.incr_x();
Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} ===> 
Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}]
```

&1 (left) : Or2.incr_xy [programs are in sync]
&2 (right) : Or2.incr_xy

pre = {Or2.b, Or2.y, Or2.x}

(1) Or2.incr_y()

post = {Or2.b, Or2.y, Or2.x}

**Syntax:** *eager if*. If the goal’s conclusion is a pRHL statement judgement whose left program consists of \( s_1 \) followed by a conditional, and whose right program consists of a conditional followed by \( s_2 \), reduce the goal to two subgoals using the \( s_i \) together with the “then” and “else” parts of the conditionals, along with auxiliary subgoals verifying that—even after running \( s_1 \)—the conditionals’ boolean expressions are equivalent.

For example, if the current goal is

Type variables: <none>

```plaintext
incr: equiv
Or1.incr_x(); Or1.incr_y(); ~ Or2.incr_y(); Or2.incr_x()
=\( n \) /
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} /
Or1.b{1} = Or2.b{2} ===> 
=\( n \) /
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} /
Or1.b{1} = Or2.b{2}]
```

&1 (left) : Or1.loop
&2 (right) : Or2.loop

pre =
\( =\( n \) /
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} /
Or1.b{1} = Or2.b{2} \ /
0 < n{1}
```

Or1.incr_x()
(1--) if (Or2.b) {
(1.1) Or2.incr_x()
(1--) } else {
(1?1) Or2.incr_y()
(1--) }
```

Or1.incr_y()
(2--) Or2.incr_y()
if (Or1.b) {
(3--) Or2.incr_x()
```
Or1.incr_x()
(3.1)
```
else {
(3--) 
```
Or1.incr_y()
(3?1)
```
}
```

post =
\( =\( n \) /
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} /
(!Or1.b{1}) = !Or2.b{2}]
```

then running
produces the goals

Type variables: <none>

incr: equiv[ 0r1.incr_x(); 0r1.incr_y(); - 0r2.incr_y();; 0r2.incr_x( ); ];
    ==n\ /
    0r1.x{1} = 0r2.x{2} \/
    0r1.y{1} = 0r2.y{2} \/
    0r1.b{1} = 0r2.b{2} ==>
    ==n\ /
    0r1.x{1} = 0r2.x{2} \/
    0r1.y{1} = 0r2.y{2} \/
    0r1.b{1} = 0r2.b{2}]

forall &1 &2,
    (==n\ /
     0r1.x{1} = 0r2.x{2} \/
     0r1.y{1} = 0r2.y{2} \/
     0r1.b{1} = 0r2.b{2}) /\
    0 < n{1} => 0r1.b{1} = 0r2.b{2}

and

Type variables: <none>

incr: equiv[ 0r1.incr_x(); 0r1.incr_y(); - 0r2.incr_y();; 0r2.incr_x( ); ];
    ==n\ /
    0r1.x{1} = 0r2.x{2} \/
    0r1.y{1} = 0r2.y{2} \/
    0r1.b{1} = 0r2.b{2} ==>
    ==n\ /
    0r1.x{1} = 0r2.x{2} \/
    0r1.y{1} = 0r2.y{2} \/
    0r1.b{1} = 0r2.b{2}]

forall &m2 (b1 : bool),
    hoare[ 0r1.incr_x(); 0r1.incr_y(); :
        ((==n \ /
         0r1.x = 0r2.x{m2} \/
         0r1.y = 0r2.y{m2} \/
         0r1.b = 0r2.b{m2}) /\
         0 < n) /\
         0r1.b = b1 ==> 0r1.b = b1]

and

Type variables: <none>

incr: equiv[ 0r1.incr_x(); 0r1.incr_y(); - 0r2.incr_y();; 0r2.incr_x( ); ];
    ==n\ /
    0r1.x{1} = 0r2.x{2} \/
    0r1.y{1} = 0r2.y{2} \/
    0r1.b{1} = 0r2.b{2} ==>
    ==n\ /
    0r1.x{1} = 0r2.x{2} \/
    0r1.y{1} = 0r2.y{2} \/
    0r1.b{1} = 0r2.b{2}]

&1 (left) : 0r1.loop
&2 (right) : 0r2.loop

pre =
    (==n\ /
     0r1.x{1} = 0r2.x{2} \/
     0r1.y{1} = 0r2.y{2} \/
     0r1.b{1} = 0r2.b{2}) /\
    0 < n{1} /\
    0r1.b(hr) = true

0r1.incr_x() (1) 0r2.incr_x()}
\textit{Syntax: eager while} \((H : s_1 \rightarrow s_2 : A \Rightarrow B)\). Like \textit{eager if}, but working with while loops instead of conditionals and featuring an explicit, named \textit{pRHL} statement judgement involving the \(s_i\), available as \(H\) to the subgoals. The subgoal involving the bodies of the while loops uses \(B\) as its invariant. There is also a subgoal whose conclusion is a \textit{pRHL} statement judgement both of whose sides are the body of the second program’s while loop.

\begin{verbatim}
&1 (left) : Or1.loop &2 (right) : Or2.loop
pre =
=(n) \ /
 Or1.x{1} = Or2.x{2} \ /
 Or1.y{1} = Or2.y{2} \ /
 Or1.b{1} = Or2.b{2}

Or1.incr_x() (1) Or2.incr_y()
Or1.incr_y() (2) Or2.incr_y()
Or1.incr_y() (3) Or2.incr_x()

post =
=(n) \ /
 Or1.x{1} = Or2.x{2} \ /
 Or1.y{1} = Or2.y{2} \ /
 (!Or1.b{1}) = !Or2.b{2}
\end{verbatim}
(1.2--) \text{Or2.b} \leftarrow \neg \text{Or2.b}

(1----) \}
\text{Or1.incr_y()}

(2----) \text{Or2.incr_y()}

\textbf{while} \ (0 < n) \{
(3----) \text{Or2.incr_x()}
\textbf{if} \ (\text{Or1.b}) \{
(3.1--) \text{Or1.incr_x()}

(3.1.1)
\text{Or1.incr_y()}

(3.1.2)
\}
\textbf{else} \{
(3.1--) \text{Or1.incr_y()}

(3.1?)
\}
\text{Or1.b} \leftarrow \neg \text{Or1.b}

(3.2--) \}

\text{post} =
(\neg \text{Or1.b}(1) = \neg \text{Or2.b}(2) \land
\text{Or1.x}(1) = \text{Or2.x}(2) \land
\text{Or1.y}(1) = \text{Or2.y}(2) \land \text{Or1.b}(1) = \text{Or2.b}(2)

\}

\text{then running}
\textbf{eager while} \ (\text{incr} : \text{Or1.incr_x()}; \text{Or1.incr_y()}; \neg \text{Or2.incr_y()}; \text{Or2.incr_x()};:
\{n\} \land \{x, y, b\}(\text{Or1, Or2}) =\rightarrow
\{n\} \land \{x, y, b\}(\text{Or1, Or2}).

\text{produces the goals}
\text{Type variables:} \ <\text{none}>\}

&1 \ (\text{left} ) : \text{Or1.loop}
&2 \ (\text{right} ) : \text{Or2.loop}
\text{pre} =
\{n\} \land
\text{Or1.x}(1) = \text{Or2.x}(2) \land
\text{Or1.y}(1) = \text{Or2.y}(2) \land \text{Or1.b}(1) = \text{Or2.b}(2)
\text{Or1.incr_x()}
\text{Or1.incr_y()}
\text{Or2.incr_x()}
\text{Or2.incr_y()}
\text{post} =
\{n\} \land
\text{Or1.x}(1) = \text{Or2.x}(2) \land
\text{Or1.y}(1) = \text{Or2.y}(2) \land \text{Or1.b}(1) = \text{Or2.b}(2)

\text{and}
\text{Type variables:} \ <\text{none}>\}
\text{incr:} \ \textbf{equiv}[\text{Or1.incr_x()}; \text{Or1.incr_y()}; \neg \text{Or2.incr_y()};\text{Or2.incr_x()};:
\{n\} \land
\text{Or1.x}(1) = \text{Or2.x}(2) \land
\text{Or1.y}(1) = \text{Or2.y}(2) \land \text{Or1.b}(1) = \text{Or2.b}(2) =\rightarrow
\{n\} \land
\text{Or1.x}(1) = \text{Or2.x}(2) \land
\text{Or1.y}(1) = \text{Or2.y}(2) \land \text{Or1.b}(1) = \text{Or2.b}(2)]
\textbf{forall} \ &1 \ &2,
\{n\} \land
\text{Or1.x}(1) = \text{Or2.x}(2) \land
\text{Or1.y}(1) = \text{Or2.y}(2) \land \text{Or1.b}(1) = \text{Or2.b}(2) =\rightarrow
$0 \leq n(1) = 0 < n(2)$

and

Type variables: <none>

incr: $equiv$

\[ Or1.incr_x();; Or1.incr_y(); - Or2.incr_y();; \]
\[ Or2.incr_x(); : \]
\[ =\{n\} /\]
\[ Or1.x{1} = Or2.x{2} /\]
\[ Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2} \implies \]
\[ =\{n\} /\]
\[ Or1.x{1} = Or2.x{2} /\]
\[ Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2} ]

&1 (left) : Or1.loop

pre =
\[ =\{n\} /\]
\[ Or1.x{1} = Or2.x{2} /\]
\[ Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2} /\]
\[ 0 < n(1) \]

Or1.incr_x() (1--)

if (Or2.b) {

(1.1) Or2.incr_x()

(1--) else {

(1?) Or2.incr_y()

(1--) }

}

Or1.incr_y() (2--)

if (Or1.b) {

(3--) Or2.incr_y()

Or1.incr_x() (3.1)

} else { (3--)

Or1.incr_y() (3?)

}

Or1.b <- !Or1.b (4--) Or2.incr_x()

}

post =
\[ =\{n\} /\]
\[ Or1.x{1} = Or2.x{2} /\]
\[ Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2} ]

and

Type variables: <none>

incr: $equiv$

\[ Or1.incr_x();; Or1.incr_y(); - Or2.incr_y();; \]
\[ Or2.incr_x(); : \]
\[ =\{n\} /\]
\[ Or1.x{1} = Or2.x{2} /\]
\[ Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2} \implies \]
\[ =\{n\} /\]
\[ Or1.x{1} = Or2.x{2} /\]
\[ Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2} ]

&1 (left) : Or2.loop [programs are in sync]

&2 (right) : Or2.loop

pre = =\{n, Or2.b, Or2.y, Or2.x\}

(1--)

if (Or2.b) {
(1.1) Or2.incr_x()
(1--) } else {
(1?1) Or2.incr_y()
(1--) }
(2--) Or2.b <- !Or2.b

post = ={n, Or2.b, Or2.y, Or2.x}

Syntax: **eager proc** \((H : s_1 \rightarrow s_2 : A \Rightarrow B) \mid eager \ H \ C\). This is the form of **eager proc** that applies when the procedures \(M.p\) and \(N.q\) are abstract. The second variant is where the specified \(\text{pRHL}\) statement judgement has already been introduced by another **eager** tactic. There must be a module restriction saying that the abstract procedures can't directly interfere with the global variables on which the \(s_i\) depend. Subgoals are generated for each pair of “oracles” the abstract procedures are capable of calling, i.e., for each of the procedures that may read/write the global variables used by the \(s_i\).

For example, if the current goal is

Type variables: <none>
Adv: ADV{Or1, Or2}

```plaintext
eager [ Or1.incr_x();; Or1.incr_y();, Adv(Or1).main ~
   Adv(Or2).main, Or2.incr_y();; Or2.incr_x(); :
   Or1.x(1) = Or2.x(2) \land
   Or1.y(1) = Or2.y(2) \land Or1.b(1) = Or2.b(2) ==>
   ={res} \land Or1.x(1) = Or2.x(2) \land Or1.y(1) = Or2.y(2) ]
```

then running

```plaintext
eager proc (incr : Or1.incr_x(); Or1.incr_y(); ~
   Or2.incr_y(); Or2.incr_x(); :
   ={x, y}(Or1, Or2) ==>{x, y}(Or1, Or2))
```

produces the goals

Type variables: <none>
Adv: ADV{Or1, Or2}

```plaintext
&1 (left ) : Top.
&2 (right ) : Top.
pre = Or1.x(1) = Or2.x(2) \land Or1.y(1) = Or2.y(2)
Or1.incr_x()
   (1) Or2.incr_y()
Or1.incr_y()
   (2) Or2.incr_x()
post = Or1.x(1) = Or2.x(2) \land Or1.y(1) = Or2.y(2)
```

and

Type variables: <none>
Adv: ADV{Or1, Or2}

```plaintext
incr: equiv [ Or1.incr_x();; Or1.incr_y(); ~ Or2.incr_y();;
   Or2.incr_x(); :
   Or1.x(1) = Or2.x(2) \land Or1.y(1) = Or2.y(2) ==>
   Or1.x(1) = Or2.x(2) \land Or1.y(1) = Or2.y(2) ]
```
forall &1 &2, 
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} /
Or1.b{1} = Or2.b{2} =>
true /
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} /
Or1.b{1} = Or2.b{2}

and

Type variables: <none>

Adv: ADV{Or1, Or2}
incr: equiv[ Or1.incr_x();; Or1.incr_y(); - Or2.incr_y();; 
Or2.incr_x(); ;
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} =>
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2}]

forall &1 &2, 
={res} /
={glob Adv} /
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} /
Or1.b{1} = Or2.b{2} =>
={res} /
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2}]

and

Type variables: <none>

Adv: ADV{Or1, Or2}
incr: equiv[ Or1.incr_x();; Or1.incr_y(); - Or2.incr_y();; 
Or2.incr_x(); ;
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} =>
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2}]

eager[ Or1.incr_x();; Or1.incr_y();, Or1.incr_x - Or2.incr_x, 
Or2.incr_y();; Or2.incr_x(); ;
true /
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} /
Or1.b{1} = Or2.b{2} =>
={res} /
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} /
Or1.b{1} = Or2.b{2}]

and

Type variables: <none>

Adv: ADV{Or1, Or2}
incr: equiv[ Or1.incr_x();; Or1.incr_y(); - Or2.incr_y();; 
Or2.incr_x(); ;
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2} =>
Or1.x{1} = Or2.x{2} /
Or1.y{1} = Or2.y{2}]

pre = ={Or2.b, Or2.y, Or2.x}
Or2.incr_x - Or2.incr_x

post = ={res, Or2.b, Or2.y, Or2.x}
Adv: ADV(Or1, Or2)
incre: equiv[ Or1.incr_x(); Or1.incr_y(); - Or2.incr_y();
Or2.incr_x(); :
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} =>
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}]

_{eager}_{ Or1.incr_x();; Or1.incr_y();; Or1.incr_y - Or2.incr_y,
  Or2.incr_y();; Or2.incr_x(); :
  true /\ 
  Or1.x{1} = Or2.x{2} /\ Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2} =>
  ={res} /\ 
  Or1.x{1} = Or2.x{2} /\ Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2}]

and

Type variables: <none>

Adv: ADV(Or1, Or2)
incre: equiv[ Or1.incr_x(); Or1.incr_y(); - Or2.incr_y();
Or2.incr_x(); :
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} =>
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}]

pre = ={Or2.b, Or2.y, Or2.x}

Or2.incr_y = Or2.incr_y

post = ={res, Or2.b, Or2.y, Or2.x}

and

Type variables: <none>

Adv: ADV(Or1, Or2)
incre: equiv[ Or1.incr_x(); Or1.incr_y(); - Or2.incr_y();
Or2.incr_x(); :
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} =>
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}]

_{eager}_{ Or1.incr_x();; Or1.incr_y();; Or1.incr xy - Or2.incr_xy,
  Or2.incr_xy();; Or2.incr_x(); :
  true /\ 
  Or1.x{1} = Or2.x{2} /\ Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2} =>
  ={res} /\ 
  Or1.x{1} = Or2.x{2} /\ Or1.y{1} = Or2.y{2} /\ Or1.b{1} = Or2.b{2}]

and

Type variables: <none>

Adv: ADV(Or1, Or2)
incre: equiv[ Or1.incr_x(); Or1.incr_y(); - Or2.incr_y();
Or2.incr_x(); :
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} =>
  Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}]

pre = ={Or2.b, Or2.y, Or2.x}
CHAPTER 3. TACTICS

Or2.incr_xy ~ Or2.incr_xy

post = \{\text{res, Or2.b, Or2.y, Or2.x}\}

and

Type variables: <none>

Adv: ADV\{Or1, Or2\}

incr: \textit{equiv}[ Or1.incr_x(); Or1.incr_y(); - Or2.incr_y();
Or2.incr_x(); :
\begin{align*}
&\text{Or1.x}\{1\} = \text{Or2.x}\{2\} \land \text{Or1.y}\{1\} = \text{Or2.y}\{2\} \implies \\
&\text{Or1.x}\{1\} = \text{Or2.x}\{2\} \land \text{Or1.y}\{1\} = \text{Or2.y}\{2\}\]
\end{align*}

\textit{eager}[ Or1.incr_x(); Or1.incr_y();, Or1.incr_yx - Or2.incr_yx,
Or2.incr_y();; Or2.incr_x(); :
\begin{align*}
&\text{true} \lor \\
&\text{Or1.x}\{1\} = \text{Or2.x}\{2\} \lor \\
&\text{Or1.y}\{1\} = \text{Or2.y}\{2\} \lor \text{Or1.b}\{1\} = \text{Or2.b}\{2\} \implies \\
&\text{\{\text{res}\}} \lor \\
&\text{Or1.x}\{1\} = \text{Or2.x}\{2\} \lor \\
&\text{Or1.y}\{1\} = \text{Or2.y}\{2\} \lor \text{Or1.b}\{1\} = \text{Or2.b}\{2\}\]
\end{align*}

and

Type variables: <none>

Adv: ADV\{Or1, Or2\}

incr: \textit{equiv}[ Or1.incr_x(); Or1.incr_y(); - Or2.incr_y();
Or2.incr_x(); :
\begin{align*}
&\text{Or1.x}\{1\} = \text{Or2.x}\{2\} \land \text{Or1.y}\{1\} = \text{Or2.y}\{2\} \implies \\
&\text{Or1.x}\{1\} = \text{Or2.x}\{2\} \land \text{Or1.y}\{1\} = \text{Or2.y}\{2\}\]
\end{align*}

pre = \{Or2.b, Or2.y, Or2.x\}

Or2.incr_yx ~ Or2.incr_yx

post = \{\text{res, Or2.b, Or2.y, Or2.x}\}

and

Type variables: <none>

Adv: ADV\{Or1, Or2\}

incr: \textit{equiv}[ Or1.incr_x(); Or1.incr_y(); - Or2.incr_y();
Or2.incr_x(); :
\begin{align*}
&\text{Or1.x}\{1\} = \text{Or2.x}\{2\} \land \text{Or1.y}\{1\} = \text{Or2.y}\{2\} \implies \\
&\text{Or1.x}\{1\} = \text{Or2.x}\{2\} \land \text{Or1.y}\{1\} = \text{Or2.y}\{2\}\]
\end{align*}

\textit{eager}[ Or1.incr_x(); Or1.incr_y();, Or1.loop - Or2.loop,
Or2.incr_y();; Or2.incr_x(); :
\begin{align*}
&\text{\{n\}} \lor \\
&\text{Or1.x}\{1\} = \text{Or2.x}\{2\} \lor \\
&\text{Or1.y}\{1\} = \text{Or2.y}\{2\} \lor \text{Or1.b}\{1\} = \text{Or2.b}\{2\} \implies \\
&\text{\{\text{res\}}}} \lor \\
&\text{Or1.x}\{1\} = \text{Or2.x}\{2\} \lor \\
&\text{Or1.y}\{1\} = \text{Or2.y}\{2\} \lor \text{Or1.b}\{1\} = \text{Or2.b}\{2\}\]
\end{align*}

and

Type variables: <none>
CHAPTER 3. TACTICS

Adv: ADV(Or1, Or2)
icr: equiv[ Or1.incr_x(); Or1.incr_y(); - Or2.incr_y();
    Or2.incr_x(); :
    Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} ==>
    Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}]

pre = ={n, Or2.b, Or2.y, Or2.x}
Or2.loop - Or2.loop

post = ={res, Or2.b, Or2.y, Or2.x}

Syntax: eager (H : s1 - s2 : A == B) : C. Reduces a goal whose conclusion is a pRHL
statement judgement of the form

equiv[s1 t1 - t2 s2 : P == Q],

to an eager judgement, along with a subgoal for the specified pRHL statement judgement H,
plus an auxiliary goal.

For example, if the current goal is

Type variables: <none>

Adv: ADV(Or1, Or2)

&1 (left ) : G(Adv).main1
&2 (right ) : G(Adv).main2

pre =
Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2} \ Or1.b{1} = Or2.b{2}

Or1.incr_x()
Or1.incr_y()
Or1.incr_x()

(1) b <@ Adv(Or2).main()
(2) Or2.incr_y()
(3) Or2.incr_x()

post = ={b} \ Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}

then running

eager (incr : Or1.incr_x(); Or1.incr_y(); -
    Or2.incr_y(); Or2.incr_x(); :
    ={x, y}(Or1, Or2) ==>{x, y}(Or1, Or2)) :
    ={x, y, b}(Or1, Or2)).

produces the goals

Type variables: <none>

Adv: ADV(Or1, Or2)

&1 (left ) : G(Adv).main1
&2 (right ) : G(Adv).main2

pre = Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}

Or1.incr_x()
Or1.incr_y()
Or1.incr_y()

(1) Or2.incr_y()
(2) Or2.incr_x()

post = Or1.x{1} = Or2.x{2} \ Or1.y{1} = Or2.y{2}
and

Type variables: <none>

Adv: ADV(Or1, Or2)
incr: equiv\[ Or1.incr_x();; Or1.incr_y(); - Or2.incr_y();
   Or2.incr_x();
   Or1.x{1} = Or2.x(2) \ Or1.y{1} = Or2.y(2) ==>
   Or1.x{1} = Or2.x(2) \ Or1.y{1} = Or2.y(2)\]

&1 (left ) : G(Adv).main1
&2 (right ) : G(Adv).main2

pre =
   Or1.x{1} = Or2.x(2) \ Or1.y{1} = Or2.y(2) \ Or1.b{1} = Or2.b(2)

post =
   Or1.b{1} = Or2.b(2) \ Or1.y{1} = Or2.y(2) \ Or1.x{1} = Or2.x(2)

and

Type variables: <none>

Adv: ADV(Or1, Or2)
incr: equiv\[ Or1.incr_x();; Or1.incr_y(); - Or2.incr_y();
   Or2.incr_x();
   Or1.x{1} = Or2.x(2) \ Or1.y{1} = Or2.y(2) ==>
   Or1.x{1} = Or2.x(2) \ Or1.y{1} = Or2.y(2)\]

eager[ Or1.incr_x();; Or1.incr_y();, Adv(Or1).main -
   Adv(Or2).main, Or2.incr_y();; Or2.incr_x();
   Or1.x{1} = Or2.x(2) \ Or1.y{1} = Or2.y(2) ==>
   (Or1.y{1} = Or2.y(2) \ Or1.x{1} = Or2.x(2)) \ ={res}]
Chapter 4

Structuring Specifications and Proofs

4.1 Theories

4.2 Sections
Chapter 5

EasyCrypt Library
Chapter 6

Advanced Features and Usage
Chapter 7

Examples

7.1 Hashed ElGamal

7.2 BR93

We’ll work through [BR93].
Bibliography


Index of Tactics

admit, 58
algebra, 68
alias, 125
apply, 60
assumption, 48
auto, 171
byequiv, 149
byphoare, 156
bypr, 162
call, 93
case, 64
case-pl, 147
cfold, 126
change, 58
clear, 47
closing goals, 71
congr, 53
conseq, 136
cut, 60
done, 56
eager, 182
elim, 67
elim*, 166
exact, 61
exfalso, 170
exists, 50
exists*, 164
failure recovery, 69
fel, 177
fission, 122
fusion, 123
generalization, 46
goal selection, 70
have, 59
hoare, 169
idtac, 47
if, 86
inline, 106
introduction, 41
kill, 128
left, 48
move, 47
phoare split, 169
pose, 59
proc, 72
progress, 57
rcondf, 113
rcondt, 108
reflexivity, 48
rewrite, 62
right, 49
rnd, 83
seq, 79
sequence, 69
sequence with branching, 69
sim, 173
simplify, 56
skip, 79
smt, 57
sp, 81
split, 50
splitwhile, 119
subst, 54
swap, 103
symmetry, 130
tactic repetition, 70
transitivity, 131
trivial, 55
unroll, 117
while, 89
wp, 82
List of Corrections

Note: Add explanation of new replace tactic, which uses statement patterns. ........ 38
Note: Need explanation of how a proof term may be used in forward reasoning. .... 40
Note: Can it be used in forward reasoning? ............................................ 40
Note: In forward reasoning they aren’t equivalent—why? ............................ 40
Note: Be a bit more detailed about what this tactic does? ............................. 56
Note: Is this the right place to define “convertible”? .................................. 57
Note: Describe progress options. ......................................................... 57
Note: Describe failure states of prover selection. ....................................... 57
Note: Describe dbhint options. .............................................................. 58
Note: Make this a pragma? ................................................................. 58
Note: Missing description of algebra ..................................................... 68
Fatal: Why is the second subgoal pruned? (Compare with first and second variants,
where the corresponding subgoal isn’t pruned.) ..................................... 154
Fatal: Why is the second subgoal pruned? .............................................. 155
Fatal: It’s confusing how the third goal has been simplified, but not pruned. ..... 159
Fatal: It’s confusing how the third goal has been simplified, but not pruned. ..... 161
Fatal: Update waiting for overhaul of pHL ............................................ 169
Fatal: Update waiting for overhaul of pHL ............................................ 169
Fatal: Perhaps need other examples? .................................................... 171
Fatal: Need better description of when the tactic is applicable and how the tactic works! 171