Miscellaneous Isabelle/Isar examples for Higher-Order Logic

Markus Wenzel
http://www.in.tum.de/~wenzelm/

With contributions by Gertrud Bauer and Tobias Nipkow

April 19, 2009

Abstract

Isar offers a high-level proof (and theory) language for Isabelle. We give various examples of Isabelle/Isar proof developments, ranging from simple demonstrations of certain language features to a bit more advanced applications. The "real" applications of Isabelle/Isar are found elsewhere.

Contents

1 Basic logical reasoning

theory *BasicLogic* **imports** *Main* **begin**

1.1 Pure backward reasoning

In order to get a first idea of how Isabelle/Isar proof documents may look like, we consider the propositions I, K, and S. The following (rather explicit) proofs should require little extra explanations.

lemma I: $A \longrightarrow A$
⟨*proof*⟩

lemma K: $A \longrightarrow B \longrightarrow A$
⟨*proof*⟩

lemma S: $(A \longrightarrow B \longrightarrow C) \longrightarrow (A \longrightarrow B) \longrightarrow A \longrightarrow C$
⟨*proof*⟩

Isar provides several ways to fine-tune the reasoning, avoiding excessive detail. Several abbreviated language elements are available, enabling the writer to express proofs in a more concise way, even without referring to any automated proof tools yet.

First of all, proof by assumption may be abbreviated as a single dot.

lemma $A \longrightarrow A$
⟨*proof*⟩

In fact, concluding any (sub-)proof already involves solving any remaining goals by assumption[1]. Thus we may skip the rather vacuous body of the above proof as well.

lemma $A \longrightarrow A$
⟨*proof*⟩

Note that the **proof** command refers to the *rule* method (without arguments) by default. Thus it implicitly applies a single rule, as determined from the syntactic form of the statements involved. The **by** command abbreviates any proof with empty body, so the proof may be further pruned.

lemma $A \longrightarrow A$
⟨*proof*⟩

Proof by a single rule may be abbreviated as double-dot.

lemma $A \longrightarrow A$ ⟨*proof*⟩

Thus we have arrived at an adequate representation of the proof of a tautology that holds by a single standard rule.[2]

Let us also reconsider K. Its statement is composed of iterated connectives. Basic decomposition is by a single rule at a time, which is why our first version above was by nesting two proofs.

[1] This is not a completely trivial operation, as proof by assumption may involve full higher-order unification.

[2] Apparently, the rule here is implication introduction.

The *intro* proof method repeatedly decomposes a goal's conclusion.[3]

lemma $A \longrightarrow B \longrightarrow A$
⟨*proof*⟩

Again, the body may be collapsed.

lemma $A \longrightarrow B \longrightarrow A$
⟨*proof*⟩

Just like *rule*, the *intro* and *elim* proof methods pick standard structural rules, in case no explicit arguments are given. While implicit rules are usually just fine for single rule application, this may go too far with iteration. Thus in practice, *intro* and *elim* would be typically restricted to certain structures by giving a few rules only, e.g. **proof** (*intro impI allI*) to strip implications and universal quantifiers.

Such well-tuned iterated decomposition of certain structures is the prime application of *intro* and *elim*. In contrast, terminal steps that solve a goal completely are usually performed by actual automated proof methods (such as **by** *blast*.

1.2 Variations of backward vs. forward reasoning

Certainly, any proof may be performed in backward-style only. On the other hand, small steps of reasoning are often more naturally expressed in forward-style. Isar supports both backward and forward reasoning as a first-class concept. In order to demonstrate the difference, we consider several proofs of $A \wedge B \longrightarrow B \wedge A$.

The first version is purely backward.

lemma $A \;\&\; B \longrightarrow B \;\&\; A$
⟨*proof*⟩

Above, the *conjunct-1/2* projection rules had to be named explicitly, since the goals B and A did not provide any structural clue. This may be avoided using **from** to focus on the $A \wedge B$ assumption as the current facts, enabling the use of double-dot proofs. Note that **from** already does forward-chaining, involving the *conjE* rule here.

lemma $A \;\&\; B \longrightarrow B \;\&\; A$
⟨*proof*⟩

In the next version, we move the forward step one level upwards. Forward-chaining from the most recent facts is indicated by the **then** command. Thus the proof of $B \wedge A$ from $A \wedge B$ actually becomes an elimination, rather than an introduction. The resulting proof structure directly corresponds

[3] The dual method is *elim*, acting on a goal's premises.

to that of the *conjE* rule, including the repeated goal proposition that is abbreviated as *?thesis* below.

lemma *A* & *B* −−> *B* & *A*
⟨*proof*⟩

In the subsequent version we flatten the structure of the main body by doing forward reasoning all the time. Only the outermost decomposition step is left as backward.

lemma *A* & *B* −−> *B* & *A*
⟨*proof*⟩

We can still push forward-reasoning a bit further, even at the risk of getting ridiculous. Note that we force the initial proof step to do nothing here, by referring to the "-" proof method.

lemma *A* & *B* −−> *B* & *A*
⟨*proof*⟩

With these examples we have shifted through a whole range from purely backward to purely forward reasoning. Apparently, in the extreme ends we get slightly ill-structured proofs, which also require much explicit naming of either rules (backward) or local facts (forward).

The general lesson learned here is that good proof style would achieve just the *right* balance of top-down backward decomposition, and bottom-up forward composition. In general, there is no single best way to arrange some pieces of formal reasoning, of course. Depending on the actual applications, the intended audience etc., rules (and methods) on the one hand vs. facts on the other hand have to be emphasized in an appropriate way. This requires the proof writer to develop good taste, and some practice, of course.

For our example the most appropriate way of reasoning is probably the middle one, with conjunction introduction done after elimination.

lemma *A* & *B* −−> *B* & *A*
⟨*proof*⟩

1.3 A few examples from "Introduction to Isabelle"

We rephrase some of the basic reasoning examples of [5], using HOL rather than FOL.

1.3.1 A propositional proof

We consider the proposition $P \vee P \longrightarrow P$. The proof below involves forward-chaining from $P \vee P$, followed by an explicit case-analysis on the two *identical* cases.

lemma $P \mid P \text{ --> } P$
⟨*proof*⟩

Case splits are *not* hardwired into the Isar language as a special feature. The **next** command used to separate the cases above is just a short form of managing block structure.

In general, applying proof methods may split up a goal into separate "cases", i.e. new subgoals with individual local assumptions. The corresponding proof text typically mimics this by establishing results in appropriate contexts, separated by blocks.

In order to avoid too much explicit parentheses, the Isar system implicitly opens an additional block for any new goal, the **next** statement then closes one block level, opening a new one. The resulting behavior is what one would expect from separating cases, only that it is more flexible. E.g. an induction base case (which does not introduce local assumptions) would *not* require **next** to separate the subsequent step case.

In our example the situation is even simpler, since the two cases actually coincide. Consequently the proof may be rephrased as follows.

lemma $P \mid P \text{ --> } P$
⟨*proof*⟩

Again, the rather vacuous body of the proof may be collapsed. Thus the case analysis degenerates into two assumption steps, which are implicitly performed when concluding the single rule step of the double-dot proof as follows.

lemma $P \mid P \text{ --> } P$
⟨*proof*⟩

1.3.2 A quantifier proof

To illustrate quantifier reasoning, let us prove $(\exists\, x.\ P\ (f\, x)) \longrightarrow (\exists\, y.\ P\ y)$. Informally, this holds because any a with $P\ (f\, a)$ may be taken as a witness for the second existential statement.

The first proof is rather verbose, exhibiting quite a lot of (redundant) detail. It gives explicit rules, even with some instantiation. Furthermore, we encounter two new language elements: the **fix** command augments the context by some new "arbitrary, but fixed" element; the **is** annotation binds term abbreviations by higher-order pattern matching.

lemma $(EX\ x.\ P\ (f\, x)) \text{ --> } (EX\ y.\ P\ y)$
⟨*proof*⟩

While explicit rule instantiation may occasionally improve readability of certain aspects of reasoning, it is usually quite redundant. Above, the basic

proof outline gives already enough structural clues for the system to infer both the rules and their instances (by higher-order unification). Thus we may as well prune the text as follows.

lemma $(EX\ x.\ P\ (f\ x)) \longrightarrow (EX\ y.\ P\ y)$
⟨*proof*⟩

Explicit ∃-elimination as seen above can become quite cumbersome in practice. The derived Isar language element "**obtain**" provides a more handsome way to do generalized existence reasoning.

lemma $(EX\ x.\ P\ (f\ x)) \longrightarrow (EX\ y.\ P\ y)$
⟨*proof*⟩

Technically, **obtain** is similar to **fix** and **assume** together with a soundness proof of the elimination involved. Thus it behaves similar to any other forward proof element. Also note that due to the nature of general existence reasoning involved here, any result exported from the context of an **obtain** statement may *not* refer to the parameters introduced there.

1.3.3 Deriving rules in Isabelle

We derive the conjunction elimination rule from the corresponding projections. The proof is quite straight-forward, since Isabelle/Isar supports non-atomic goals and assumptions fully transparently.

theorem *conjE*: $A\ \&\ B \Longrightarrow (A \Longrightarrow B \Longrightarrow C) \Longrightarrow C$
⟨*proof*⟩

end

2 Cantor's Theorem

theory *Cantor* **imports** *Main* **begin**[4]

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

$$\forall f :: \alpha \to \alpha \to bool.\ \exists S :: \alpha \to bool.\ \forall x :: \alpha.\ f\ x \neq S$$

Viewing types as sets, $\alpha \to bool$ represents the powerset of α. This version of the theorem states that for every function from α to its powerset, some subset is outside its range. The Isabelle/Isar proofs below uses HOL's set theory, with the type $\alpha\ set$ and the operator $range :: (\alpha \to \beta) \to \beta\ set$.

[4]This is an Isar version of the final example of the Isabelle/HOL manual [4].

theorem *EX S. S ~: range (f :: 'a => 'a set)*
⟨*proof*⟩

How much creativity is required? As it happens, Isabelle can prove this theorem automatically using best-first search. Depth-first search would diverge, but best-first search successfully navigates through the large search space. The context of Isabelle's classical prover contains rules for the relevant constructs of HOL's set theory.

theorem *EX S. S ~: range (f :: 'a => 'a set)*
⟨*proof*⟩

While this establishes the same theorem internally, we do not get any idea of how the proof actually works. There is currently no way to transform internal system-level representations of Isabelle proofs back into Isar text. Writing intelligible proof documents really is a creative process, after all.

end

3 Peirce's Law

theory *Peirce* **imports** *Main* **begin**

We consider Peirce's Law: $((A \to B) \to A) \to A$. This is an inherently non-intuitionistic statement, so its proof will certainly involve some form of classical contradiction.

The first proof is again a well-balanced combination of plain backward and forward reasoning. The actual classical step is where the negated goal may be introduced as additional assumption. This eventually leads to a contradiction.[5]

theorem *((A --> B) --> A) --> A*
⟨*proof*⟩

In the subsequent version the reasoning is rearranged by means of "weak assumptions" (as introduced by **presume**). Before assuming the negated goal $\neg A$, its intended consequence $A \to B$ is put into place in order to solve the main problem. Nevertheless, we do not get anything for free, but have to establish $A \to B$ later on. The overall effect is that of a logical *cut*.

Technically speaking, whenever some goal is solved by **show** in the context of weak assumptions then the latter give rise to new subgoals, which may be established separately. In contrast, strong assumptions (as introduced by **assume**) are solved immediately.

theorem *((A --> B) --> A) --> A*
⟨*proof*⟩

[5]The rule involved there is negation elimination; it holds in intuitionistic logic as well.

Note that the goals stemming from weak assumptions may be even left until qed time, where they get eventually solved "by assumption" as well. In that case there is really no fundamental difference between the two kinds of assumptions, apart from the order of reducing the individual parts of the proof configuration.

Nevertheless, the "strong" mode of plain assumptions is quite important in practice to achieve robustness of proof text interpretation. By forcing both the conclusion *and* the assumptions to unify with the pending goal to be solved, goal selection becomes quite deterministic. For example, decomposition with rules of the "case-analysis" type usually gives rise to several goals that only differ in there local contexts. With strong assumptions these may be still solved in any order in a predictable way, while weak ones would quickly lead to great confusion, eventually demanding even some backtracking.

end

4 The Drinker's Principle

theory *Drinker* **imports** *Main* **begin**

Here is another example of classical reasoning: the Drinker's Principle says that for some person, if he is drunk, everybody else is drunk!

We first prove a classical part of de-Morgan's law.

lemma *deMorgan*:
assumes $\neg\ (\forall x.\ P\ x)$
shows $\exists x.\ \neg\ P\ x$
⟨*proof*⟩

theorem *Drinker's-Principle*: $\exists x.\ drunk\ x \longrightarrow (\forall x.\ drunk\ x)$
⟨*proof*⟩

end

5 Correctness of a simple expression compiler

theory *ExprCompiler* **imports** *Main* **begin**

This is a (rather trivial) example of program verification. We model a compiler for translating expressions to stack machine instructions, and prove its correctness wrt. some evaluation semantics.

5.1 Binary operations

Binary operations are just functions over some type of values. This is both for abstract syntax and semantics, i.e. we use a "shallow embedding" here.

types
'val binop = 'val => 'val => 'val

5.2 Expressions

The language of expressions is defined as an inductive type, consisting of variables, constants, and binary operations on expressions.

datatype *('adr, 'val) expr =*
Variable 'adr |
Constant 'val |
Binop 'val binop ('adr, 'val) expr ('adr, 'val) expr

Evaluation (wrt. some environment of variable assignments) is defined by primitive recursion over the structure of expressions.

consts
eval :: ('adr, 'val) expr => ('adr => 'val) => 'val

primrec
eval (Variable x) env = env x
eval (Constant c) env = c
eval (Binop f e1 e2) env = f (eval e1 env) (eval e2 env)

5.3 Machine

Next we model a simple stack machine, with three instructions.

datatype *('adr, 'val) instr =*
Const 'val |
Load 'adr |
Apply 'val binop

Execution of a list of stack machine instructions is easily defined as follows.

consts
exec :: (('adr, 'val) instr) list
=> 'val list => ('adr => 'val) => 'val list

primrec
exec [] stack env = stack
exec (instr # instrs) stack env =
(case instr of
Const c => exec instrs (c # stack) env
| Load x => exec instrs (env x # stack) env
| Apply f => exec instrs (f (hd stack) (hd (tl stack))
 # (tl (tl stack))) env)

constdefs
execute :: (('*adr*, '*val*) *instr*) *list* => ('*adr* => '*val*) => '*val*
execute instrs env == *hd* (*exec instrs* [] *env*)

5.4 Compiler

We are ready to define the compilation function of expressions to lists of stack machine instructions.

consts
compile :: ('*adr*, '*val*) *expr* => (('*adr*, '*val*) *instr*) *list*

primrec
compile (*Variable x*) = [*Load x*]
compile (*Constant c*) = [*Const c*]
compile (*Binop f e1 e2*) = *compile e2* @ *compile e1* @ [*Apply f*]

The main result of this development is the correctness theorem for *compile*. We first establish a lemma about *exec* and list append.

lemma *exec-append*:
exec (*xs* @ *ys*) *stack env* =
exec ys (*exec xs stack env*) *env*
⟨*proof*⟩

theorem *correctness*: *execute* (*compile e*) *env* = *eval e env*
⟨*proof*⟩

In the proofs above, the *simp* method does quite a lot of work behind the scenes (mostly "functional program execution"). Subsequently, the same reasoning is elaborated in detail — at most one recursive function definition is used at a time. Thus we get a better idea of what is actually going on.

lemma *exec-append'*:
exec (*xs* @ *ys*) *stack env* = *exec ys* (*exec xs stack env*) *env*
⟨*proof*⟩

theorem *correctness'*: *execute* (*compile e*) *env* = *eval e env*
⟨*proof*⟩

end

6 Basic group theory

theory *Group* **imports** *Main* **begin**

6.1 Groups and calculational reasoning

Groups over signature $(\times :: \alpha \to \alpha \to \alpha, \mathit{one} :: \alpha, \mathit{inverse} :: \alpha \to \alpha)$ are defined as an axiomatic type class as follows. Note that the parent class *times* is provided by the basic HOL theory.

consts
one :: $'a$
inverse :: $'a$ => $'a$

axclass
group < *times*
group-assoc: $(x * y) * z = x * (y * z)$
group-left-one: $\mathit{one} * x = x$
group-left-inverse: $\mathit{inverse}\ x * x = \mathit{one}$

The group axioms only state the properties of left one and inverse, the right versions may be derived as follows.

theorem *group-right-inverse*: $x * \mathit{inverse}\ x = (\mathit{one}::'a::\mathit{group})$
⟨*proof*⟩

With *group-right-inverse* already available, *group-right-one* is now established much easier.

theorem *group-right-one*: $x * \mathit{one} = (x::'a::\mathit{group})$
⟨*proof*⟩

The calculational proof style above follows typical presentations given in any introductory course on algebra. The basic technique is to form a transitive chain of equations, which in turn are established by simplifying with appropriate rules. The low-level logical details of equational reasoning are left implicit.

Note that "..." is just a special term variable that is bound automatically to the argument[6] of the last fact achieved by any local assumption or proven statement. In contrast to *?thesis*, the "..." variable is bound *after* the proof is finished, though.

There are only two separate Isar language elements for calculational proofs: "**also**" for initial or intermediate calculational steps, and "**finally**" for exhibiting the result of a calculation. These constructs are not hardwired into Isabelle/Isar, but defined on top of the basic Isar/VM interpreter. Expanding the **also** and **finally** derived language elements, calculations may be simulated by hand as demonstrated below.

theorem $x * \mathit{one} = (x::'a::\mathit{group})$
⟨*proof*⟩

[6] The argument of a curried infix expression happens to be its right-hand side.

Note that this scheme of calculations is not restricted to plain transitivity. Rules like anti-symmetry, or even forward and backward substitution work as well. For the actual implementation of **also** and **finally**, Isabelle/Isar maintains separate context information of "transitivity" rules. Rule selection takes place automatically by higher-order unification.

6.2 Groups as monoids

Monoids over signature $(\times :: \alpha \to \alpha \to \alpha, \mathit{one} :: \alpha)$ are defined like this.

axclass *monoid* < *times*
  monoid-assoc: $(x * y) * z = x * (y * z)$
  monoid-left-one: $\mathit{one} * x = x$
  monoid-right-one: $x * \mathit{one} = x$

Groups are *not* yet monoids directly from the definition. For monoids, *right-one* had to be included as an axiom, but for groups both *right-one* and *right-inverse* are derivable from the other axioms. With *group-right-one* derived as a theorem of group theory (see page 12), we may still instantiate *group* $\subseteq$ *monoid* properly as follows.

instance *group* < *monoid*
  ⟨*proof*⟩

The **instance** command actually is a version of **theorem**, setting up a goal that reflects the intended class relation (or type constructor arity). Thus any Isar proof language element may be involved to establish this statement. When concluding the proof, the result is transformed into the intended type signature extension behind the scenes.

6.3 More theorems of group theory

The one element is already uniquely determined by preserving an *arbitrary* group element.

theorem *group-one-equality*: $e * x = x \Longrightarrow \mathit{one} = (e::'a::\mathit{group})$
⟨*proof*⟩

Likewise, the inverse is already determined by the cancel property.

theorem *group-inverse-equality*:
  $x' * x = \mathit{one} \Longrightarrow \mathit{inverse}\ x = (x'::'a::\mathit{group})$
⟨*proof*⟩

The inverse operation has some further characteristic properties.

theorem *group-inverse-times*:
  $\mathit{inverse}\ (x * y) = \mathit{inverse}\ y * \mathit{inverse}\ (x::'a::\mathit{group})$
⟨*proof*⟩

theorem *inverse-inverse*: *inverse* (*inverse* x) = (x::'a::*group*)
⟨*proof*⟩

theorem *inverse-inject*: *inverse* x = *inverse* y ==> x = (y::'a::*group*)
⟨*proof*⟩

end

7 Summing natural numbers

theory *Summation*
imports *Main*
begin[7]

Subsequently, we prove some summation laws of natural numbers (including odds, squares, and cubes). These examples demonstrate how plain natural deduction (including induction) may be combined with calculational proof.

7.1 Summation laws

The sum of natural numbers $0 + \cdots + n$ equals $n \times (n + 1)/2$. Avoiding formal reasoning about division we prove this equation multiplied by 2.

theorem *sum-of-naturals*:
  2 * ($\sum$ i::nat=0..n. i) = n * (n + 1)
  (**is** ?P n **is** ?S n = -)
⟨*proof*⟩

The above proof is a typical instance of mathematical induction. The main statement is viewed as some $?P\ n$ that is split by the induction method into base case $?P\ 0$, and step case $?P\ n \Longrightarrow ?P\ (Suc\ n)$ for arbitrary n.

The step case is established by a short calculation in forward manner. Starting from the left-hand side $?S(n+1)$ of the thesis, the final result is achieved by transformations involving basic arithmetic reasoning (using the Simplifier). The main point is where the induction hypothesis $?S\,n = n \times (n+1)$ is introduced in order to replace a certain subterm. So the "transitivity" rule involved here is actual *substitution*. Also note how the occurrence of "..." in the subsequent step documents the position where the right-hand side of the hypothesis got filled in.

A further notable point here is integration of calculations with plain natural deduction. This works so well in Isar for two reasons.

[7] This example is somewhat reminiscent of the http://isabelle.in.tum.de/library/HOL/ex/NatSum.html, which is discussed in [6] in the context of permutative rewrite rules and ordered rewriting.

1. Facts involved in **also** / **finally** calculational chains may be just anything. There is nothing special about **have**, so the natural deduction element **assume** works just as well.

2. There are two *separate* primitives for building natural deduction contexts: **fix** x and **assume** A. Thus it is possible to start reasoning with some new "arbitrary, but fixed" elements before bringing in the actual assumption. In contrast, natural deduction is occasionally formalized with basic context elements of the form $x : A$ instead.

We derive further summation laws for odds, squares, and cubes as follows. The basic technique of induction plus calculation is the same as before.

theorem *sum-of-odds*:
  $(\sum i{::}nat{=}0..{<}n.\ 2 * i + 1) = n\hat{}Suc\ (Suc\ 0)$
  (**is** *?P n* **is** *?S n* = -)
⟨*proof*⟩

Subsequently we require some additional tweaking of Isabelle built-in arithmetic simplifications, such as bringing in distributivity by hand.

lemmas *distrib* = *add-mult-distrib add-mult-distrib2*

theorem *sum-of-squares*:
  $6 * (\sum i{::}nat{=}0..n.\ i\hat{}Suc\ (Suc\ 0)) = n * (n + 1) * (2 * n + 1)$
  (**is** *?P n* **is** *?S n* = -)
⟨*proof*⟩

theorem *sum-of-cubes*:
  $4 * (\sum i{::}nat{=}0..n.\ i\hat{}3) = (n * (n + 1))\hat{}Suc\ (Suc\ 0)$
  (**is** *?P n* **is** *?S n* = -)
⟨*proof*⟩

Comparing these examples with the tactic script version http://isabelle.in.tum.de/library/HOL/ex/NatSum.html, we note an important difference of how induction vs. simplification is applied. While [6, §10] advises for these examples that "induction should not be applied until the goal is in the simplest form" this would be a very bad idea in our setting.

Simplification normalizes all arithmetic expressions involved, producing huge intermediate goals. With applying induction afterwards, the Isar proof text would have to reflect the emerging configuration by appropriate sub-proofs. This would result in badly structured, low-level technical reasoning, without any good idea of the actual point.

As a general rule of good proof style, automatic methods such as *simp* or *auto* should normally be never used as initial proof methods, but only as terminal ones, solving certain goals completely.

end

8 Pretty syntax for lattice operations

9 Textbook-style reasoning: the Knaster-Tarski Theorem

theory *KnasterTarski*
imports *Main Lattice-Syntax*
begin

9.1 Prose version

According to the textbook [1, pages 93–94], the Knaster-Tarski fixpoint theorem is as follows.[8]

The Knaster-Tarski Fixpoint Theorem. Let L be a complete lattice and f: $L \to L$ an order-preserving map. Then $\bigsqcap \{x \in L \mid f(x) \leq x\}$ is a fixpoint of f.

Proof. Let $H = \{x \in L \mid f(x) \leq x\}$ and $a = \bigsqcap H$. For all $x \in H$ we have $a \leq x$, so $f(a) \leq f(x) \leq x$. Thus $f(a)$ is a lower bound of H, whence $f(a) \leq a$. We now use this inequality to prove the reverse one (!) and thereby complete the proof that a is a fixpoint. Since f is order-preserving, $f(f(a)) \leq f(a)$. This says $f(a) \in H$, so $a \leq f(a)$.

9.2 Formal versions

The Isar proof below closely follows the original presentation. Virtually all of the prose narration has been rephrased in terms of formal Isar language elements. Just as many textbook-style proofs, there is a strong bias towards forward proof, and several bends in the course of reasoning.

theorem *Knaster-Tarski*:
  fixes f :: *'a*::*complete-lattice* $\Rightarrow$ *'a*
  assumes *mono f*
  shows $\exists\, a.\ f\ a = a$
⟨*proof*⟩

Above we have used several advanced Isar language elements, such as explicit block structure and weak assumptions. Thus we have mimicked the particular way of reasoning of the original text.

In the subsequent version the order of reasoning is changed to achieve structured top-down decomposition of the problem at the outer level, while only

[8] We have dualized the argument, and tuned the notation a little bit.

the inner steps of reasoning are done in a forward manner. We are certainly more at ease here, requiring only the most basic features of the Isar language.

theorem *Knaster-Tarski'*:
  fixes f :: $'a$::*complete-lattice* $\Rightarrow$ $'a$
  assumes *mono* f
  shows $\exists a.\ f\ a = a$
⟨*proof*⟩

end

10 The Mutilated Checker Board Problem

theory *MutilatedCheckerboard* **imports** *Main* **begin**

The Mutilated Checker Board Problem, formalized inductively. See [7] and http://isabelle.in.tum.de/library/HOL/Induct/Mutil.html for the original tactic script version.

10.1 Tilings

inductive-set
  tiling :: $'a$ *set set* => $'a$ *set set*
  for A :: $'a$ *set set*
  where
    empty: {} : *tiling A*
  | *Un*: *a* : *A* ==> *t* : *tiling A* ==> *a* <= − *t* ==> *a Un t* : *tiling A*

The union of two disjoint tilings is a tiling.

lemma *tiling-Un*:
  assumes *t* : *tiling A* **and** *u* : *tiling A* **and** *t Int u* = {}
  shows *t Un u* : *tiling A*
⟨*proof*⟩

10.2 Basic properties of "below"

constdefs
  below :: *nat* => *nat set*
  below n == {*i*. *i* < *n*}

lemma *below-less-iff* [*iff*]: (*i*: *below k*) = (*i* < *k*)
  ⟨*proof*⟩

lemma *below-0*: *below 0* = {}
  ⟨*proof*⟩

lemma *Sigma-Suc1*:

$m = n + 1 ==> below\ m <*> B = (\{n\} <*> B)\ Un\ (below\ n <*> B)$
⟨*proof*⟩

lemma *Sigma-Suc2*:
$m = n + 2 ==> A <*> below\ m =$
$(A <*> \{n\})\ Un\ (A <*> \{n + 1\})\ Un\ (A <*> below\ n)$
⟨*proof*⟩

lemmas *Sigma-Suc = Sigma-Suc1 Sigma-Suc2*

10.3 Basic properties of "evnodd"

constdefs
$evnodd :: (nat * nat)\ set => nat => (nat * nat)\ set$
$evnodd\ A\ b == A\ Int\ \{(i, j).\ (i + j)\ mod\ 2 = b\}$

lemma *evnodd-iff*:
$(i, j): evnodd\ A\ b = ((i, j): A\ \ \&\ (i + j)\ mod\ 2 = b)$
⟨*proof*⟩

lemma *evnodd-subset*: $evnodd\ A\ b <= A$
⟨*proof*⟩

lemma *evnoddD*: $x : evnodd\ A\ b ==> x : A$
⟨*proof*⟩

lemma *evnodd-finite*: $finite\ A ==> finite\ (evnodd\ A\ b)$
⟨*proof*⟩

lemma *evnodd-Un*: $evnodd\ (A\ Un\ B)\ b = evnodd\ A\ b\ Un\ evnodd\ B\ b$
⟨*proof*⟩

lemma *evnodd-Diff*: $evnodd\ (A - B)\ b = evnodd\ A\ b - evnodd\ B\ b$
⟨*proof*⟩

lemma *evnodd-empty*: $evnodd\ \{\}\ b = \{\}$
⟨*proof*⟩

lemma *evnodd-insert*: $evnodd\ (insert\ (i, j)\ C)\ b =$
$(if\ (i + j)\ mod\ 2 = b$
$then\ insert\ (i, j)\ (evnodd\ C\ b)\ else\ evnodd\ C\ b)$
⟨*proof*⟩

10.4 Dominoes

inductive-set
$domino :: (nat * nat)\ set\ set$
where
$horiz: \{(i, j), (i, j + 1)\} : domino$
| $vertl: \{(i, j), (i + 1, j)\} : domino$

lemma *dominoes-tile-row*:
  $\{i\}$ <*> *below* $(2 * n)$: *tiling domino*
  (**is** *?B n* : *?T*)
⟨*proof*⟩

lemma *dominoes-tile-matrix*:
  below m <*> *below* $(2 * n)$: *tiling domino*
  (**is** *?B m* : *?T*)
⟨*proof*⟩

lemma *domino-singleton*:
  assumes *d*: *d* : *domino* **and** $b < 2$
  shows *EX i j*. *evnodd d b* = $\{(i, j)\}$ (**is** *?P d*)
  ⟨*proof*⟩

lemma *domino-finite*:
  assumes *d*: *d*: *domino*
  shows *finite d*
  ⟨*proof*⟩

10.5 Tilings of dominoes

lemma *tiling-domino-finite*:
  assumes *t*: *t* : *tiling domino* (**is** *t* : *?T*)
  shows *finite t* (**is** *?F t*)
  ⟨*proof*⟩

lemma *tiling-domino-01*:
  assumes *t*: *t* : *tiling domino* (**is** *t* : *?T*)
  shows *card* (*evnodd t 0*) = *card* (*evnodd t 1*)
  ⟨*proof*⟩

10.6 Main theorem

constdefs
  mutilated-board :: *nat* => *nat* => (*nat* * *nat*) *set*
  mutilated-board m n ==
    below $(2 * (m + 1))$ <*> *below* $(2 * (n + 1))$
      − $\{(0, 0)\}$ − $\{(2 * m + 1, 2 * n + 1)\}$

theorem *mutil-not-tiling*: *mutilated-board m n* ~: *tiling domino*
⟨*proof*⟩

end

11 An old chestnut

theory *Puzzle* **imports** *Main* **begin**[9]

Problem. Given some function $f\colon \mathbb{N} \to \mathbb{N}$ such that $f\ (f\ n) < f\ (Suc\ n)$ for all n. Demonstrate that f is the identity.

theorem
  assumes *f-ax*: $\bigwedge n.\ f\ (f\ n) < f\ (Suc\ n)$
  shows $f\ n = n$
⟨*proof*⟩

end

12 Nested datatypes

theory *NestedDatatype* **imports** *Main* **begin**

12.1 Terms and substitution

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

consts
  subst-term :: $('a \Rightarrow ('a, 'b)\ term) \Rightarrow ('a, 'b)\ term \Rightarrow ('a, 'b)\ term$
  subst-term-list ::
    $('a \Rightarrow ('a, 'b)\ term) \Rightarrow ('a, 'b)\ term\ list \Rightarrow ('a, 'b)\ term\ list$

primrec (*subst*)
  subst-term f (*Var a*) = *f a*
  subst-term f (*App b ts*) = *App b* (*subst-term-list f ts*)
  subst-term-list f [] = []
  subst-term-list f (*t* # *ts*) = *subst-term f t* # *subst-term-list f ts*

A simple lemma about composition of substitutions.

lemma *subst-term* (*subst-term f1 o f2*) *t* =
      subst-term f1 (*subst-term f2 t*)
  and *subst-term-list* (*subst-term f1 o f2*) *ts* =
      subst-term-list f1 (*subst-term-list f2 ts*)
  ⟨*proof*⟩

lemma *subst-term* (*subst-term f1 o f2*) *t* =
  subst-term f1 (*subst-term f2 t*)
⟨*proof*⟩

[9] A question from "Bundeswettbewerb Mathematik". Original pen-and-paper proof due to Herbert Ehler; Isabelle tactic script by Tobias Nipkow.

12.2 Alternative induction

theorem *term-induct'* [*case-names Var App*]:
  assumes *var*: !!*a*. *P* (*Var a*)
    and *app*: !!*b ts*. *list-all P ts* ==> *P* (*App b ts*)
  shows *P t*
⟨*proof*⟩

lemma
  subst-term (*subst-term f1 o f2*) *t* = *subst-term f1* (*subst-term f2 t*)
⟨*proof*⟩

end

13 Hoare Logic

theory *Hoare* **imports** *Main*
uses (~~/*src*/*HOL*/*Hoare*/*hoare-tac.ML*) **begin**

13.1 Abstract syntax and semantics

The following abstract syntax and semantics of Hoare Logic over `WHILE` programs closely follows the existing tradition in Isabelle/HOL of formalizing the presentation given in [10, §6]. See also http://isabelle.in.tum.de/library/Hoare/ and [3].

types
  'a *bexp* = 'a *set*
  'a *assn* = 'a *set*

datatype 'a *com* =
    Basic 'a => 'a
  | *Seq* 'a *com* 'a *com*   ((-;/ -) [*60*, *61*] *60*)
  | *Cond* 'a *bexp* 'a *com* 'a *com*
  | *While* 'a *bexp* 'a *assn* 'a *com*

abbreviation
  Skip (*SKIP*) **where**
  SKIP == *Basic id*

types
  'a *sem* = 'a => 'a => *bool*

consts
  iter :: *nat* => 'a *bexp* => 'a *sem* => 'a *sem*
primrec
  iter 0 b S s s' = (*s* ~: *b* & *s* = *s'*)
  iter (*Suc n*) *b S s s'* =

$(s : b \;\&\; (EX\ s''.\ S\ s\ s'' \;\&\; iter\ n\ b\ S\ s''\ s'))$

consts
$Sem :: 'a\ com => 'a\ sem$
primrec
$Sem\ (Basic\ f)\ s\ s' = (s' = f\ s)$
$Sem\ (c1;\ c2)\ s\ s' = (EX\ s''.\ Sem\ c1\ s\ s'' \;\&\; Sem\ c2\ s''\ s')$
$Sem\ (Cond\ b\ c1\ c2)\ s\ s' =$
$(if\ s : b\ then\ Sem\ c1\ s\ s'\ else\ Sem\ c2\ s\ s')$
$Sem\ (While\ b\ x\ c)\ s\ s' = (EX\ n.\ iter\ n\ b\ (Sem\ c)\ s\ s')$

constdefs
$Valid :: 'a\ bexp => 'a\ com => 'a\ bexp => bool$
$((3|-\ -/\ (2-)/\ -)\ [100,\ 55,\ 100]\ 50)$
$|-\ P\ c\ Q == ALL\ s\ s'.\ Sem\ c\ s\ s' --> s : P --> s' : Q$

syntax (*xsymbols*)
$Valid :: 'a\ bexp => 'a\ com => 'a\ bexp => bool$
$((3\vdash\ -/\ (2-)/\ -)\ [100,\ 55,\ 100]\ 50)$

lemma *ValidI* [*intro?*]:
$(!!s\ s'.\ Sem\ c\ s\ s' ==> s : P ==> s' : Q) ==> |-\ P\ c\ Q$
⟨*proof*⟩

lemma *ValidD* [*dest?*]:
$|-\ P\ c\ Q ==> Sem\ c\ s\ s' ==> s : P ==> s' : Q$
⟨*proof*⟩

13.2 Primitive Hoare rules

From the semantics defined above, we derive the standard set of primitive Hoare rules; e.g. see [10, §6]. Usually, variant forms of these rules are applied in actual proof, see also §13.4 and §13.5.

The *basic* rule represents any kind of atomic access to the state space. This subsumes the common rules of *skip* and *assign*, as formulated in §13.4.

theorem *basic*: $|-\ \{s.\ f\ s : P\}\ (Basic\ f)\ P$
⟨*proof*⟩

The rules for sequential commands and semantic consequences are established in a straight forward manner as follows.

theorem *seq*: $|-\ P\ c1\ Q ==> |-\ Q\ c2\ R ==> |-\ P\ (c1;\ c2)\ R$
⟨*proof*⟩

theorem *conseq*: $P' <= P ==> |-\ P\ c\ Q ==> Q <= Q' ==> |-\ P'\ c\ Q'$
⟨*proof*⟩

The rule for conditional commands is directly reflected by the corresponding semantics; in the proof we just have to look closely which cases apply.

theorem *cond*:
|− (P Int b) c1 Q ==> |− (P Int −b) c2 Q ==> |− P (Cond b c1 c2) Q
⟨*proof*⟩

The *while* rule is slightly less trivial — it is the only one based on recursion, which is expressed in the semantics by a Kleene-style least fixed-point construction. The auxiliary statement below, which is by induction on the number of iterations is the main point to be proven; the rest is by routine application of the semantics of `WHILE`.

theorem *while*:
assumes *body*: *|− (P Int b) c P*
shows *|− P (While b X c) (P Int −b)*
⟨*proof*⟩

13.3 Concrete syntax for assertions

We now introduce concrete syntax for describing commands (with embedded expressions) and assertions. The basic technique is that of semantic "quote-antiquote". A *quotation* is a syntactic entity delimited by an implicit abstraction, say over the state space. An *antiquotation* is a marked expression within a quotation that refers the implicit argument; a typical antiquotation would select (or even update) components from the state.

We will see some examples later in the concrete rules and applications.

The following specification of syntax and translations is for Isabelle experts only; feel free to ignore it.

While the first part is still a somewhat intelligible specification of the concrete syntactic representation of our Hoare language, the actual "ML drivers" is quite involved. Just note that the we re-use the basic quote/antiquote translations as already defined in Isabelle/Pure (see `Syntax.quote_tr` and `Syntax.quote_tr'`).

syntax
-quote :: *'b => ('a => 'b)* ((.'(-').) [0] 1000)
-antiquote :: *('a => 'b) => 'b* ('- [1000] 1000)
-Subst :: *'a bexp ⇒ 'b ⇒ idt ⇒ 'a bexp*
(-[-'/'-] [1000] 999)
-Assert :: *'a => 'a set* ((.{-}.) [0] 1000)
-Assign :: *idt => 'b => 'a com* (('- :=/ -) [70, 65] 61)
-Cond :: *'a bexp => 'a com => 'a com => 'a com*
((0IF -/ THEN -/ ELSE -/ FI) [0, 0, 0] 61)
-While-inv :: *'a bexp => 'a assn => 'a com => 'a com*
((0WHILE -/ INV - //DO - /OD) [0, 0, 0] 61)
-While :: *'a bexp => 'a com => 'a com*
((0WHILE - //DO - /OD) [0, 0] 61)

syntax (*xsymbols*)

-Assert :: *'a => 'a set* ((⦃-⦄) [*0*] *1000*)

translations
.{b}. => *Collect .(b).*
B [a/'x] => *.{'(-update-name x (λ-. a)) ∈ B}.*
'x := a => *Basic .('(-update-name x (λ-. a))).*
IF b THEN c1 ELSE c2 FI => *Cond .{b}. c1 c2*
WHILE b INV i DO c OD => *While .{b}. i c*
WHILE b DO c OD == *WHILE b INV CONST undefined DO c OD*

⟨*ML*⟩

As usual in Isabelle syntax translations, the part for printing is more complicated — we cannot express parts as macro rules as above. Don't look here, unless you have to do similar things for yourself.

⟨*ML*⟩

13.4 Rules for single-step proof

We are now ready to introduce a set of Hoare rules to be used in single-step structured proofs in Isabelle/Isar. We refer to the concrete syntax introduce above.

Assertions of Hoare Logic may be manipulated in calculational proofs, with the inclusion expressed in terms of sets or predicates. Reversed order is supported as well.

lemma [*trans*]: *|- P c Q ==> P' <= P ==> |- P' c Q*
⟨*proof*⟩
lemma [*trans*] : *P' <= P ==> |- P c Q ==> |- P' c Q*
⟨*proof*⟩

lemma [*trans*]: *Q <= Q' ==> |- P c Q ==> |- P c Q'*
⟨*proof*⟩
lemma [*trans*]: *|- P c Q ==> Q <= Q' ==> |- P c Q'*
⟨*proof*⟩

lemma [*trans*]:
|- .{'P}. c Q ==> (!!s. P' s --> P s) ==> |- .{'P'}. c Q
⟨*proof*⟩
lemma [*trans*]:
(!!s. P' s --> P s) ==> |- .{'P}. c Q ==> |- .{'P'}. c Q
⟨*proof*⟩

lemma [*trans*]:
|- P c .{'Q}. ==> (!!s. Q s --> Q' s) ==> |- P c .{'Q'}.
⟨*proof*⟩
lemma [*trans*]:
(!!s. Q s --> Q' s) ==> |- P c .{'Q}. ==> |- P c .{'Q'}.

⟨*proof*⟩

Identity and basic assignments.[10]

lemma *skip* [*intro?*]: |− *P SKIP P*
⟨*proof*⟩

lemma *assign*: |− *P* [´*a*/´*x*] ´*x* := ´*a P*
⟨*proof*⟩

Note that above formulation of assignment corresponds to our preferred way to model state spaces, using (extensible) record types in HOL [2]. For any record field x, Isabelle/HOL provides a functions x (selector) and x-*update* (update). Above, there is only a place-holder appearing for the latter kind of function: due to concrete syntax $\acute{x} := \acute{a}$ also contains *x_update*.[11]

Sequential composition — normalizing with associativity achieves proper of chunks of code verified separately.

lemmas [*trans*, *intro?*] = *seq*

lemma *seq-assoc* [*simp*]: (|− *P c1*;(*c2*;*c3*) *Q*) = (|− *P* (*c1*;*c2*);*c3 Q*)
⟨*proof*⟩

Conditional statements.

lemmas [*trans*, *intro?*] = *cond*

lemma [*trans*, *intro?*]:
|− .{´*P* & ´*b*}. *c1 Q*
==> |− .{´*P* & ~ ´*b*}. *c2 Q*
==> |− .{´*P*}. *IF* ´*b THEN c1 ELSE c2 FI Q*
⟨*proof*⟩

While statements — with optional invariant.

lemma [*intro?*]:
|− (*P Int b*) *c P* ==> |− *P* (*While b P c*) (*P Int* −*b*)
⟨*proof*⟩

lemma [*intro?*]:
|− (*P Int b*) *c P* ==> |− *P* (*While b undefined c*) (*P Int* −*b*)
⟨*proof*⟩

lemma [*intro?*]:

[10] The *hoare* method introduced in §13.5 is able to provide proper instances for any number of basic assignments, without producing additional verification conditions.

[11] Note that due to the external nature of HOL record fields, we could not even state a general theorem relating selector and update functions (if this were required here); this would only work for any particular instance of record fields introduced so far.

$\vdash .\{\acute{}P \;\&\; \acute{}b\}.\ c\ .\{\acute{}P\}.$
$\Longrightarrow \vdash .\{\acute{}P\}.\ \mathit{WHILE}\ \acute{}b\ \mathit{INV}\ .\{\acute{}P\}.\ \mathit{DO}\ c\ \mathit{OD}\ .\{\acute{}P \;\&\; \sim\ \acute{}b\}.$
⟨*proof*⟩

lemma [*intro?*]:
$\vdash .\{\acute{}P \;\&\; \acute{}b\}.\ c\ .\{\acute{}P\}.$
$\Longrightarrow \vdash .\{\acute{}P\}.\ \mathit{WHILE}\ \acute{}b\ \mathit{DO}\ c\ \mathit{OD}\ .\{\acute{}P \;\&\; \sim\ \acute{}b\}.$
⟨*proof*⟩

13.5 Verification conditions

We now load the *original* ML file for proof scripts and tactic definition for the Hoare Verification Condition Generator (see http://isabelle.in.tum.de/library/Hoare/). As far as we are concerned here, the result is a proof method *hoare*, which may be applied to a Hoare Logic assertion to extract purely logical verification conditions. It is important to note that the method requires `WHILE` loops to be fully annotated with invariants beforehand. Furthermore, only *concrete* pieces of code are handled — the underlying tactic fails ungracefully if supplied with meta-variables or parameters, for example.

lemma *SkipRule*: $p \subseteq q \Longrightarrow \mathit{Valid}\ p\ (\mathit{Basic}\ \mathit{id})\ q$
⟨*proof*⟩

lemma *BasicRule*: $p \subseteq \{s.\ f\ s \in q\} \Longrightarrow \mathit{Valid}\ p\ (\mathit{Basic}\ f)\ q$
⟨*proof*⟩

lemma *SeqRule*: $\mathit{Valid}\ P\ c1\ Q \Longrightarrow \mathit{Valid}\ Q\ c2\ R \Longrightarrow \mathit{Valid}\ P\ (c1;c2)\ R$
⟨*proof*⟩

lemma *CondRule*:
$p \subseteq \{s.\ (s \in b \longrightarrow s \in w) \wedge (s \notin b \longrightarrow s \in w')\}$
$\Longrightarrow \mathit{Valid}\ w\ c1\ q \Longrightarrow \mathit{Valid}\ w'\ c2\ q \Longrightarrow \mathit{Valid}\ p\ (\mathit{Cond}\ b\ c1\ c2)\ q$
⟨*proof*⟩

lemma *iter-aux*:
$\forall s\ s'.\ \mathit{Sem}\ c\ s\ s' --> s : I \;\&\; s : b --> s' : I ==>$
$(\bigwedge s\ s'.\ s : I \Longrightarrow \mathit{iter}\ n\ b\ (\mathit{Sem}\ c)\ s\ s' \Longrightarrow s' : I \;\&\; s' \sim: b)$
⟨*proof*⟩

lemma *WhileRule*:
$p \subseteq i \Longrightarrow \mathit{Valid}\ (i \cap b)\ c\ i \Longrightarrow i \cap (-b) \subseteq q \Longrightarrow \mathit{Valid}\ p\ (\mathit{While}\ b\ i\ c)\ q$
⟨*proof*⟩

lemma *Compl-Collect*: $-\ \mathit{Collect}\ b = \{x.\ \neg\ b\ x\}$
⟨*proof*⟩

lemmas *AbortRule* = *SkipRule* — dummy version

⟨*ML*⟩

end

14 Using Hoare Logic

theory *HoareEx* **imports** *Hoare* **begin**

14.1 State spaces

First of all we provide a store of program variables that occur in any of the programs considered later. Slightly unexpected things may happen when attempting to work with undeclared variables.

record *vars* =
  I :: *nat*
  M :: *nat*
  N :: *nat*
  S :: *nat*

While all of our variables happen to have the same type, nothing would prevent us from working with many-sorted programs as well, or even polymorphic ones. Also note that Isabelle/HOL's extensible record types even provides simple means to extend the state space later.

14.2 Basic examples

We look at few trivialities involving assignment and sequential composition, in order to get an idea of how to work with our formulation of Hoare Logic.

Using the basic *assign* rule directly is a bit cumbersome.

lemma
  $\vdash .\{\acute{}(N\text{-}update\ (\lambda\text{-}.\ (2 * \acute{}N))) : .\{\acute{}N = 10\}.\}.\ \acute{}N := 2 * \acute{}N\ .\{\acute{}N = 10\}.$
  ⟨*proof*⟩

Certainly we want the state modification already done, e.g. by simplification. The *hoare* method performs the basic state update for us; we may apply the Simplifier afterwards to achieve "obvious" consequences as well.

lemma $\vdash .\{True\}.\ \acute{}N := 10\ .\{\acute{}N = 10\}.$
  ⟨*proof*⟩

lemma $\vdash .\{2 * \acute{}N = 10\}.\ \acute{}N := 2 * \acute{}N\ .\{\acute{}N = 10\}.$
  ⟨*proof*⟩

lemma $\vdash .\{\acute{}N = 5\}.\ \acute{}N := 2 * \acute{}N\ .\{\acute{}N = 10\}.$
  ⟨*proof*⟩

lemma $|- .\{\acute{}N + 1 = a + 1\}. \acute{}N := \acute{}N + 1 .\{\acute{}N = a + 1\}.$
⟨*proof*⟩

lemma $|- .\{\acute{}N = a\}. \acute{}N := \acute{}N + 1 .\{\acute{}N = a + 1\}.$
⟨*proof*⟩

lemma $|- .\{a = a \,\&\, b = b\}. \acute{}M := a; \acute{}N := b .\{\acute{}M = a \,\&\, \acute{}N = b\}.$
⟨*proof*⟩

lemma $|- .\{True\}. \acute{}M := a; \acute{}N := b .\{\acute{}M = a \,\&\, \acute{}N = b\}.$
⟨*proof*⟩

lemma
$|- .\{\acute{}M = a \,\&\, \acute{}N = b\}.$
$\acute{}I := \acute{}M; \acute{}M := \acute{}N; \acute{}N := \acute{}I$
$.\{\acute{}M = b \,\&\, \acute{}N = a\}.$
⟨*proof*⟩

It is important to note that statements like the following one can only be proven for each individual program variable. Due to the extra-logical nature of record fields, we cannot formulate a theorem relating record selectors and updates schematically.

lemma $|- .\{\acute{}N = a\}. \acute{}N := \acute{}N .\{\acute{}N = a\}.$
⟨*proof*⟩

lemma $|- .\{\acute{}x = a\}. \acute{}x := \acute{}x .\{\acute{}x = a\}.$
⟨*proof*⟩

lemma
Valid $\{s.\ x\ s = a\}$ (*Basic* $(\lambda s.\ x\text{-}update\ (x\ s)\ s)$) $\{s.\ x\ s = n\}$
— same statement without concrete syntax
⟨*proof*⟩

In the following assignments we make use of the consequence rule in order to achieve the intended precondition. Certainly, the *hoare* method is able to handle this case, too.

lemma $|- .\{\acute{}M = \acute{}N\}. \acute{}M := \acute{}M + 1 .\{\acute{}M \sim= \acute{}N\}.$
⟨*proof*⟩

lemma $|- .\{\acute{}M = \acute{}N\}. \acute{}M := \acute{}M + 1 .\{\acute{}M \sim= \acute{}N\}.$
⟨*proof*⟩

lemma $|- .\{\acute{}M = \acute{}N\}. \acute{}M := \acute{}M + 1 .\{\acute{}M \sim= \acute{}N\}.$
⟨*proof*⟩

14.3 Multiplication by addition

We now do some basic examples of actual `WHILE` programs. This one is a loop for calculating the product of two natural numbers, by iterated addition. We first give detailed structured proof based on single-step Hoare rules.

lemma
  $|-\ .\{\acute{}M = 0\ \&\ \acute{}S = 0\}.$
    WHILE $\acute{}M \sim= a$
    DO $\acute{}S := \acute{}S + b;\ \acute{}M := \acute{}M + 1$ *OD*
    $.\{\acute{}S = a * b\}.$
⟨*proof*⟩

The subsequent version of the proof applies the *hoare* method to reduce the Hoare statement to a purely logical problem that can be solved fully automatically. Note that we have to specify the `WHILE` loop invariant in the original statement.

lemma
  $|-\ .\{\acute{}M = 0\ \&\ \acute{}S = 0\}.$
    WHILE $\acute{}M \sim= a$
    INV $.\{\acute{}S = \acute{}M * b\}.$
    DO $\acute{}S := \acute{}S + b;\ \acute{}M := \acute{}M + 1$ *OD*
    $.\{\acute{}S = a * b\}.$
  ⟨*proof*⟩

14.4 Summing natural numbers

We verify an imperative program to sum natural numbers up to a given limit. First some functional definition for proper specification of the problem.

The following proof is quite explicit in the individual steps taken, with the *hoare* method only applied locally to take care of assignment and sequential composition. Note that we express intermediate proof obligation in pure logic, without referring to the state space.

declare *atLeast0LessThan*[*symmetric*,*simp*]

theorem
  $|-\ .\{True\}.$
    $\acute{}S := 0;\ \acute{}I := 1;$
    WHILE $\acute{}I \sim= n$
    DO
      $\acute{}S := \acute{}S + \acute{}I;$
      $\acute{}I := \acute{}I + 1$
    OD
    $.\{\acute{}S = (SUM\ j{<}n.\ j)\}.$
  (**is** $|-$ - (-; *?while*) -)
⟨*proof*⟩

The next version uses the *hoare* method, while still explaining the resulting proof obligations in an abstract, structured manner.

theorem
  $|-$.{*True*}.
    ´*S* := *0*; ´*I* := *1*;
    WHILE ´*I* ~= *n*
    INV .{´*S* = (*SUM j*<´*I*. *j*)}.
    DO
      ´*S* := ´*S* + ´*I*;
      ´*I* := ´*I* + *1*
    OD
    .{´*S* = (*SUM j*<*n*. *j*)}.
⟨*proof*⟩

Certainly, this proof may be done fully automatic as well, provided that the invariant is given beforehand.

theorem
  $|-$.{*True*}.
    ´*S* := *0*; ´*I* := *1*;
    WHILE ´*I* ~= *n*
    INV .{´*S* = (*SUM j*<´*I*. *j*)}.
    DO
      ´*S* := ´*S* + ´*I*;
      ´*I* := ´*I* + *1*
    OD
    .{´*S* = (*SUM j*<*n*. *j*)}.
  ⟨*proof*⟩

14.5 Time

A simple embedding of time in Hoare logic: function *timeit* inserts an extra variable to keep track of the elapsed time.

record *tstate* = *time* :: *nat*

types *'a time* = (|*time* :: *nat*, ... :: *'a*|)

consts *timeit* :: *'a time com* ⇒ *'a time com*
primrec
  timeit (*Basic f*) = (*Basic f*; *Basic*(λ*s*. *s*(|*time* := *Suc* (*time s*)|)))
  timeit (*c1*; *c2*) = (*timeit c1*; *timeit c2*)
  timeit (*Cond b c1 c2*) = *Cond b* (*timeit c1*) (*timeit c2*)
  timeit (*While b iv c*) = *While b iv* (*timeit c*)

record *tvars* = *tstate* +
  I :: *nat*
  J :: *nat*

lemma *lem*: (*0*::*nat*) < *n* ⟹ *n* + *n* ≤ *Suc* (*n* ∗ *n*)

⟨*proof*⟩

lemma |– .{*i* = ´*I* & ´*time* = *0*}.
timeit(
WHILE ´*I* ≠ *0*
INV .{*2*∗´*time* + ´*I*∗´*I* + *5*∗´*I* = *i*∗*i* + *5*∗*i*}.
DO
´*J* := ´*I*;
WHILE ´*J* ≠ *0*
INV .{*0* < ´*I* & *2*∗´*time* + ´*I*∗´*I* + *3*∗´*I* + *2*∗´*J* − *2* = *i*∗*i* + *5*∗*i*}.
DO ´*J* := ´*J* − *1* *OD*;
´*I* := ´*I* − *1*
OD
) .{*2*∗´*time* = *i*∗*i* + *5*∗*i*}.
⟨*proof*⟩

end

References

[1] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, 1990.

[2] W. Naraschewski and M. Wenzel. Object-oriented verification based on record subtyping in Higher-Order Logic. In J. Grundy and M. Newey, editors, *Theorem Proving in Higher Order Logics: TPHOLs '98*, volume 1479 of *LNCS*, 1998.

[3] T. Nipkow. Winskel is (almost) right: Towards a mechanized semantics textbook. *Formal Aspects of Computing*, 10:171–186, 1998.

[4] T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle's Logics: HOL*.

[5] L. C. Paulson. *Introduction to Isabelle*.

[6] L. C. Paulson. *The Isabelle Reference Manual*.

[7] L. C. Paulson. A simple formalization and proof for the mutilated chess board. Technical Report 394, Comp. Lab., Univ. Camb., 1996. http://www.cl.cam.ac.uk/users/lcp/papers/Reports/mutil.pdf.

[8] M. Wenzel. *The Isabelle/Isar Reference Manual*.

[9] M. Wenzel. Isar — a generic interpretative approach to readable formal proof documents. In Y. Bertot, G. Dowek, A. Hirschowitz, C. Paulin, and L. Thery, editors, *Theorem Proving in Higher Order Logics: TPHOLs '99*, LNCS 1690, 1999.

[10] G. Winskel. *The Formal Semantics of Programming Languages.* MIT Press, 1993.