Isabelle/HOLCF Tutorial

May 25, 2015

Contents

1 Domain package examples
   1.1 Generated constants and theorems 3
   1.2 Known bugs 5

2 Fixrec package examples
   2.1 Basic fixrec examples 5
   2.2 Examples using fixrec_simp 5
   2.3 Pattern matching with bottoms 6
   2.4 Skipping proofs of rewrite rules 6
   2.5 Mutual recursion with fixrec 7
   2.6 Looping simp rules 8
   2.7 Using fixrec inside locales 8

3 Definitional domain package 9

1 Domain package examples

theory Domain_ex
imports HOLCF
begin

Domain constructors are strict by default.
domain d1 = d1a / d1b "d1" "d1"

lemma "d1b·⊥·y = ⊥" ⟨proof⟩

Constructors can be made lazy using the lazy keyword.
domain d2 = d2a / d2b (lazy "d2")

lemma "d2b·x ≠ ⊥" ⟨proof⟩

Strict and lazy arguments may be mixed arbitrarily.
domain \( \text{d3} = \text{d3a} \mid \text{d3b} \) (lazy "d2") "d2"

lemma "\( P \ (\text{d3b} \cdot x \cdot y = \bot) \iff P \ (y = \bot) \)" (proof)

Selectors can be used with strict or lazy constructor arguments.

domain \( \text{d4} = \text{d4a} \mid \text{d4b} \) (lazy \( \text{d4b}\_\text{left} :: "d2" \)) (\( \text{d4b}\_\text{right} :: "d2" \))

lemma "\( y \neq \bot \implies \text{d4b}\_\text{left} \cdot (\text{d4b} \cdot x \cdot y) = x \)" (proof)

Mixfix declarations can be given for data constructors.

domain \( \text{d5} = \text{d5a} \mid \text{d5b} \) (lazy "d5") "d5" (infixl ":#:" 70)

lemma "\( \text{d5a} \neq x :#: y :#: z \)" (proof)

Mixfix declarations can also be given for type constructors.

domain \('a, 'b\) lazypair (infixl ":*::" 25) = 
  lpair (lazy \( \text{lfst} :: 'a \)) (lazy \( \text{lsnd} :: 'b \)) (infixl ":*::" 75)

lemma "\( \forall p::('a :*: 'b). p \sqsubseteq \text{lfst} \cdot p :*: \text{lsnd} \cdot p \)" (proof)

Non-recursive constructor arguments can have arbitrary types.

domain \('a, 'b\) d6 = d6 "int lift" "'a \oplus 'b u" (lazy "('a :*: 'b) \times ('b \rightarrow 'a)"")

Indirect recursion is allowed for sums, products, lifting, and the continuous function space. However, the domain package does not generate an induction rule in terms of the constructors.

domain \('a\ d7 = d7a "'a d7 \oplus \text{int lift}" \mid d7b "'a \& 'a d7" \mid d7c (lazy "'a d7 \rightarrow 'a")"
  — Indirect recursion detected, skipping proofs of (co)induction rules

Note that \( \text{d7.induct} \) is absent.

Indirect recursion is also allowed using previously-defined datatypes.

domain \('a\ s\text{list} = \text{SNil} \mid \text{SCons} \ 'a \ "'a s\text{list}"

domain \('a\ s\text{tree} = \text{STip} \mid \text{SBranch} "'a s\text{tree} s\text{list}"

Mutually-recursive datatypes can be defined using the and keyword.

domain \( \text{d8} = \text{d8a} \mid \text{d8b} \ "d8" \) and \( \text{d9} = \text{d9a} \mid \text{d9b} \) (lazy "d9")

Non-regular recursion is not allowed.

Mutually-recursive datatypes must have all the same type arguments, not necessarily in the same order.

domain \('a, 'b\) \text{list}1 = \text{Nil1} \mid \text{Cons1} \ 'a "('b, 'a) list2"
and ('b, 'a) list2 = Nil2 | Cons2 'b "('a, 'b) list1"

Induction rules for flat datatypes have no admissibility side-condition.

domain 'a flattree = Tip | Branch "'a flattree" "'a flattree"

lemma "[P ⊥; P Tip; \(x \neq ⊥; y \neq ⊥; P x; P y\) \implies P (Branch·x·y)]

Trivial datatypes will produce a warning message.

domain triv = Triv triv triv
— domain Domain_ex.triv is empty!

lemma "(x::triv) = ⊥" (proof)

Lazy constructor arguments may have unpointed types.

domain natlist = nnil | ncons (lazy "nat discr") natlist

Class constraints may be given for type parameters on the LHS.

domain ('a::predomain) box = Box (lazy 'a)

domain ('a::countable) stream = snil | scons (lazy "'a discr") "'a stream"

1.1 Generated constants and theorems

domain 'a tree = Leaf (lazy 'a) | Node (left :: "'a tree") (right :: "'a tree")

lemmas tree_abs_bottom_iff =
  iso.abs_bottom_iff [OF iso.intro [OF tree.abs_iso tree.rep_iso]]

Rules about isomorphism

term tree_rep
term tree_abs
thm tree.rep_iso
thm tree.abs_iso
thm tree.iso_rews

Rules about constructors

term Leaf
term Node
thm Leaf_def Node_def
thm tree.nchotomy
thm tree.exhaust
thm tree.compacts
thm tree.con_rews
thm tree.dist_les
thm tree.dist_eqs
thm tree.inverts
thm tree.injects

Rules about case combinator

term tree_case
thm tree.tree_case_def
thm tree.case_rews

Rules about selectors

term left
term right
thm tree.sel_rews

Rules about discriminators

term is_Leaf
term is_Node
thm tree.dis_rews

Rules about monadic pattern match combinators

term match_Leaf
term match_Node
thm tree.match_rews

Rules about take function

term tree_take
thm tree.take_def
thm tree.take_0
thm tree.take_Suc
thm tree.take_rews
thm tree.chain_take
thm tree.take_take
thm tree.deflation_take
thm tree.take_below
thm tree.take lemma
thm tree.lub_take
thm tree.reach
thm tree.finite_induct

Rules about finiteness predicate

term tree.finite
thm tree.finite_def
thm tree.finite

Rules about bisimulation predicate

term tree.bisim
thm tree.bisim_def
thm tree.coinduct
Induction rule
thm tree.induct

1.2 Known bugs

Declaring a mixfix with spaces causes some strange parse errors.
end

2 Fixrec package examples

theory Fixrec_ex
imports HOLCF
begin

2.1 Basic fixrec examples

Fixrec patterns can mention any constructor defined by the domain package, as well as any of the following built-in constructors: Pair, spair, sinl, sinr, up, ONE, TT, FF.

Typical usage is with lazy constructors.

fixrec down :: ''a u → 'a
where "down · (up · x) = x"

With strict constructors, rewrite rules may require side conditions.

fixrec from_sinl :: ''a ⊕ 'b → 'a
where "x ≠ ⊥ ⇒ from_sinl · (sinl · x) = x"

Lifting can turn a strict constructor into a lazy one.

fixrec from_sinl_up :: ''a u ⊕ 'b → 'a
where "from_sinl_up · (sinl · (up · x)) = x"

Fixrec also works with the HOL pair constructor.

fixrec down2 :: ''a u × 'b u → 'a × 'b
where "down2 · (up · x, up · y) = (x, y)"

2.2 Examples using fixrec_simp

A type of lazy lists.

domain 'a llist = lNil | lCons (lazy 'a) (lazy "'a llist")

A zip function for lazy lists.
Notice that the patterns are not exhaustive.

fixrec
lzip :: "'a llist → 'b llist → ('a × 'b) llist"

where
"lzip·(lCons·x·xs)·(lCons·y·ys) = lCons·(x, y)·(lzip·xs·ys)"
| "lzip·lNil·lNil = lNil"

fixrec_simp is useful for producing strictness theorems.

Note that pattern matching is done in left-to-right order.

lemma lzip_stricts [simp]:
"lzip·⊥·ys = ⊥"
"lzip·lNil·⊥ = ⊥"
"lzip·(lCons·x·xs)·⊥ = ⊥"
⟨proof⟩

fixrec_simp can also produce rules for missing cases.

lemma lzip_UNDEFs [simp]:
"lzip·lNil·(lCons·y·ys) = ⊥"
"lzip·(lCons·x·xs)·lNil = ⊥"
⟨proof⟩

2.3 Pattern matching with bottoms

As an alternative to using fixrec_simp, it is also possible to use bottom as a constructor pattern. When using a bottom pattern, the right-hand-side must also be bottom; otherwise, fixrec will not be able to prove the equation.

fixrec
from_sinr_up :: "'a ⊕ 'b ⊥ → 'b"
where
"from_sinr_up·⊥ = ⊥"
| "from_sinr_up·(sinr·(up·x)) = x"

If the function is already strict in that argument, then the bottom pattern does not change the meaning of the function. For example, in the definition of from_sinr_up, the first equation is actually redundant, and could have been proven separately by fixrec_simp.

A bottom pattern can also be used to make a function strict in a certain argument, similar to a bang-pattern in Haskell.

fixrec
seq :: "'a → 'b → 'b"
where
"seq·⊥·y = ⊥"
| "x ≠ ⊥ ⇒ seq·x·y = y"

2.4 Skipping proofs of rewrite rules

Another zip function for lazy lists.
Notice that this version has overlapping patterns. The second equation cannot be proved as a theorem because it only applies when the first pattern fails.

fixrec

\texttt{lzip2 :: 'a llist }→ 'b llist → ('a × 'b) llist"

where

"lzip2·(lCons·x·xs)·(lCons·y·ys) = lCons·(x, y)·(lzip2·xs·ys)"

\}/ (unchecked) "lzip2·xs·ys = 1Nil"

Usually fixrec tries to prove all equations as theorems. The "unchecked" option overrides this behavior, so fixrec does not attempt to prove that particular equation.

Simp rules can be generated later using \texttt{fixrec.simps}.

\textbf{lemma lzip2.simps [simp]:}

"lzip2·(lCons·x·xs)·1Nil = 1Nil"

"lzip2·1 Nil·(lCons·y·ys) = 1 Nil"

"lzip2·1N 11·1N 11 = 1N 11"

\langle proof \rangle

\textbf{lemma lzip2_stricts [simp]:}

"lzip2·⊥·ys = ⊥"

"lzip2·(lCons·x·xs)·⊥ = ⊥"

\langle proof \rangle

\subsection{2.5 Mutual recursion with fixrec}

Tree and forest types.

\textbf{domain 'a tree = Leaf (lazy 'a) | Branch (lazy "'a forest")}

and  

\textbf{domain 'a forest = Empty | Trees (lazy "'a tree") "'a forest"}

To define mutually recursive functions, give multiple type signatures separated by the keyword \texttt{and}.

\textbf{fixrec}

\texttt{map_tree :: "(a → 'b) → (a tree → 'b tree)"

and}

\texttt{map_forest :: "(a → 'b) → (a forest → 'b forest)"

where

"map_tree·f·(Leaf·x) = Leaf·(f·x)"

| "map_tree·f·(Branch·ts) = Branch·(map_forest·f·ts)"

| "map_forest·f·Empty = Empty"

| "ts ≠ ⊥ \implies map_forest·f·(Trees·t·ts) = Trees·(map_tree·f·t)·(map_forest·f·ts)"

\textbf{lemma map_tree_strict [simp]: "map_tree·f·⊥ = ⊥"}

\langle proof \rangle
lemma map_forest_strict [simp]: "map_forest \cdot f \cdot \bot = \bot"
⟨proof⟩

2.6 Looping simp rules
The defining equations of a fixrec definition are declared as simp rules by default. In some cases, especially for constants with no arguments or functions with variable patterns, the defining equations may cause the simplifier to loop. In these cases it will be necessary to use a [simp del] declaration.

fixrec
repeat :: 
\'a \rightarrow \'a llist
where
[simp del]: "repeat \cdot x = 1Cons \cdot x \cdot (repeat \cdot x)"

We can derive other non-looping simp rules for repeat by using the subst method with the repeat.simps rule.

lemma repeat.simps [simp]:
- "repeat \cdot x \neq \bot"
- "repeat \cdot x \neq 1Nil"
- "repeat \cdot x = 1Cons \cdot y \cdot ys \iff x = y \land repeat \cdot x = ys"
⟨proof⟩

lemma llist_case_repeat [simp]:
"llist_case \cdot z \cdot f \cdot (repeat \cdot x) = f \cdot x \cdot (repeat \cdot x)"
⟨proof⟩

For mutually-recursive constants, looping might only occur if all equations are in the simpset at the same time. In such cases it may only be necessary to declare [simp del] on one equation.

fixrec
inf_tree :: 
\'a tree
and
inf_forest :: 
\'a forest
where
[simp del]: "inf_tree = Branch \cdot inf_forest"
| "inf_forest = Trees \cdot inf_tree \cdot (Trees \cdot inf_tree \cdot Empty)"

2.7 Using fixrec inside locales
locale test =
fixes foo :: 
\'a \rightarrow \'a
assumes foo_strict: "foo \cdot \bot = \bot"
begin

fixrec
bar :: 
\'a u \rightarrow \'a
where
"bar \cdot (up \cdot x) = foo \cdot x"

lemma bar_strict: "bar \cdot \bot = \bot"
\section{Definitional domain package}

\begin{verbatim}
theory New_Domain
imports HOLCF
begin

UPDATE: The definitional back-end is now the default mode of the domain package. This file should be merged with Domain_ex.thy.

Provided that \texttt{domain} is the default sort, the \texttt{new_domain} package should work with any type definition supported by the old domain package.

\texttt{domain 'a llist = LNil | LCons (lazy 'a) (lazy "'a llist")}

The difference is that the new domain package is completely definitional, and does not generate any axioms. The following type and constant definitions are not produced by the old domain package.

\texttt{thm type_definition_llist}
\texttt{thm llist_abs_def llist_rep_def}

The new domain package also adds support for indirect recursion with user-defined datatypes. This definition of a tree datatype uses indirect recursion through the lazy list type constructor.

\texttt{domain 'a ltree = Leaf (lazy 'a) | Branch (lazy "'a ltree llist")}

For indirect-recursive definitions, the domain package is not able to generate a high-level induction rule. (It produces a warning message instead.) The low-level reach lemma (now proved as a theorem, no longer generated as an axiom) can be used to derive other induction rules.

\texttt{thm ltree.reach}

The definition of the take function uses map functions associated with each type constructor involved in the definition. A map function for the lazy list type has been generated by the new domain package.

\texttt{thm ltree.take_rews}
\texttt{thm llist_map_def}

\texttt{lemma ltree_induct:}
\begin{verbatim}
  fixes P :: "'a ltree \Rightarrow bool"
  assumes adm: "adm P"
  assumes bot: "P ⊥"
\end{verbatim}
\end{verbatim}
assumes \textit{Leaf}: "\(\forall x. P(\text{Leaf} \cdot x)\)"

assumes \textit{Branch}: "\(\forall f. \forall x. P(f \cdot x) \implies P(\text{Branch} \cdot (\text{llist_map} \cdot f) \cdot l))\)"

shows "\(P \cdot x\)"

\langle \text{proof} \rangle

end