Mechanising the worker/wrapper transformation

Peter Gammie
August 28, 2014

Contents

1 Introduction 2

2 Fixed-point theorems for program transformation 2
  2.1 The rolling rule ................................. 2
  2.2 Least-fixed-point fusion .......................... 3

3 The transformation according to Gill and Hutton 3
  3.1 Worker/wrapper fusion is partially correct ............ 5
  3.2 A non-strict unwrap may go awry .................... 6

4 A totally-correct fusion rule 7

5 Naive reverse becomes accumulator-reverse. 8
  5.1 Hughes lists, naive reverse, worker-wrapper optimisation 8
  5.2 Gill/Hutton-style worker/wrapper ..................... 10
  5.3 Optimise worker/wrapper ........................... 10

6 Unboxing types. 12
  6.1 Factorial example .................................. 12
  6.2 Introducing an accumulator .......................... 14

7 Memoisation using streams. 16
  7.1 Streams ........................................... 16
  7.2 The wrapper/unwrapper functions .................... 17
  7.3 Fibonacci example .................................. 17

8 Tagless interpreter via double-barreled continuations 19
  8.1 Worker/wrapper .................................... 19

9 Backtracking using lazy lists and continuations 21
10 Transforming $O(n^2)$ \textit{nub} into an $O(n \log n)$ one  

10.1 The \textit{nub} function. .................................................. 26

10.2 Optimised data type. ....................................................... 26

11 Optimise “last”.  

11.1 The \textit{last} function. .................................................. 29

12 Concluding remarks  

Bibliography  

1 Introduction

This mechanisation of the worker/wrapper theory of Gill and Hutton (2009) was carried out in Isabelle/HOLCF (Müller et al. 1999; Huffman 2009). It accompanies Gammie (2011). The reader should note that \(oo\) stands for function composition, \(\Lambda\) for continuous function abstraction, \(\cdot\) for continuous function application, \textbf{domain} for recursive-datatype definition.

\[\langle ML\rangle\]

2 Fixed-point theorems for program transformation

We begin by recounting some standard theorems from the early days of denotational semantics. The origins of these results are lost to history; the interested reader can find some of it in Bekić (1984); Manna (1974); Greibach (1975); Stoy (1977); de Bakker et al. (1980); Harel (1980); Plotkin (1983); Winskel (1993); Sangiorgi (2009).

2.1 The rolling rule

The \textit{rolling rule} captures what intuitively happens when we re-order a recursive computation consisting of two parts. This theorem dates from the 1970s at the latest – see Stoy (1977, p210) and Plotkin (1983). The following proofs were provided by Gill and Hutton (2009).

\textbf{lemma} rolling-rule-ltr: \textit{fix}-(\textit{g oo f}) \sqsubseteq \textit{g}-(\textit{fix}-(\textit{f oo g}))  
\langle proof \rangle

\textbf{lemma} rolling-rule-rtl: \textit{g}-(\textit{fix}-(\textit{f oo g})) \sqsubseteq \textit{fix}-(\textit{g oo f})  
\langle proof \rangle

\textbf{lemma} rolling-rule: \textit{fix}-(\textit{g oo f}) = \textit{g}-(\textit{fix}-(\textit{f oo g}))  
\langle proof \rangle
2.2 Least-fixed-point fusion

Least-fixed-point fusion provides a kind of induction that has proven to be very useful in calculational settings. Intuitively it lifts the step-by-step correspondence between \( f \) and \( h \) witnessed by the strict function \( g \) to the fixed points of \( f \) and \( g \):

\[
\begin{array}{c}
\bullet \xrightarrow{h} \bullet \\
g \quad g \\
\bullet \xrightarrow{f} \bullet \\
\end{array} \quad \Rightarrow \quad \begin{array}{c}
\bullet \xrightarrow{\text{fix } h} \\
g \\
\bullet \xrightarrow{\text{fix } f} \\
\end{array}
\]

Fokkinga and Meijer (1991), and also their later Meijer, Fokkinga, and Paterson (1991), made extensive use of this rule, as did Tullsen (2002) in his program transformation tool PATH. This diagram is strongly reminiscent of the simulations used to establish refinement relations between imperative programs and their specifications (de Roever and Engelhardt 1998).

The following proof is close to the third variant of Stoy (1977, p215). We relate the two fixpoints using the rule \( \text{parallel} \_\text{fix} \_\text{ind} \):

\[
\text{adm} \ (\lambda x. \ ?P \ (\text{fst } x) \ (\text{snd } x)) \\
?P \perp \perp \quad \bigwedge x \ y. \quad \text{adm} \ (\lambda x. \ ?P \ (\text{fst } x) \ (\text{snd } x)) \\
?P \ (\text{fix} \cdot \ ?F) \ (\text{fix} \cdot \ ?G)
\]

in a very straightforward way:

\textbf{lemma lfp-fusion:}
\begin{itemize}
  \item assumes \( g \cdot \perp = \perp \)
  \item assumes \( g \circ f = h \circ g \)
  \item shows \( g \cdot (\text{fix} \cdot f) = \text{fix} \cdot h \)
\end{itemize}

\textlangle proof \textrangle

This lemma also goes by the name of \textit{Plotkin's axiom} (Pitts 1996) or \textit{uniformity} (Simpson and Plotkin 2000).

\textlangle proof \textrangle \textlangle proof \textrangle \textlangle proof \textrangle \textlangle proof \textrangle \textlangle proof \textrangle \textlangle proof \textrangle \textlangle proof \textrangle \textlangle proof \textrangle \textlangle proof \textrangle

3 The transformation according to Gill and Hutton

The worker/wrapper transformation and associated fusion rule as formalised by Gill and Hutton (2009) are reproduced in Figure 1, and the reader is referred to the original paper for further motivation and background.

Armed with the rolling rule we can show that Gill and Hutton’s justification of the worker/wrapper transformation is sound. There is a battery of these transformations with varying strengths of hypothesis.
For a recursive definition \( \text{comp} = \text{fix} \cdot \text{body} \) for some \( \text{body} :: A \to A \) and a pair of functions \( \text{wrap} :: B \to A \) and \( \text{unwrap} :: A \to B \) where \( \text{wrap} \circ \text{unwrap} = \text{id}_A \), we have:

\[
\text{comp} = \text{wrap} \cdot \text{work} \\
\text{work} :: B \\
\text{work} = \text{fix} \left( \text{unwrap} \circ \text{body} \circ \text{wrap} \right) 
\]

(the worker/wrapper transformation)

Also:

\[
\left( \text{unwrap} \circ \text{wrap} \right) \text{work} = \text{work} 
\]

(worker/wrapper fusion)

Figure 1: The worker/wrapper transformation and fusion rule of Gill and Hutton (2009).

The first requires \( \text{wrap} \circ \text{unwrap} \) to be the identity for all values.

**Lemma worker-wrapper-id:**

fixes \( \text{wrap} :: 'b::pcpo \to 'a::pcpo \)

fixes \( \text{unwrap} :: 'a \to 'b \)

assumes \( \text{wrap-unwrap}: \text{wrap} \circ \text{unwrap} \) = \text{id}

assumes \( \text{comp-body}: \text{computation} = \text{fix-body} \)

shows \( \text{computation} = \text{wrap} \left( \text{fix} \left( \text{unwrap} \circ \text{body} \circ \text{wrap} \right) \right) \)

\langle \text{proof} \rangle

The second weakens this assumption by requiring that \( \text{wrap} \circ \text{wrap} \) only act as the identity on values in the image of \( \text{body} \).

**Lemma worker-wrapper-body:**

fixes \( \text{wrap} :: 'b::pcpo \to 'a::pcpo \)

fixes \( \text{unwrap} :: 'a \to 'b \)

assumes \( \text{wrap-unwrap}: \text{wrap} \circ \text{unwrap} \circ \text{body} = \text{body} \)

assumes \( \text{comp-body}: \text{computation} = \text{fix-body} \)

shows \( \text{computation} = \text{wrap} \left( \text{fix} \left( \text{unwrap} \circ \text{body} \circ \text{wrap} \right) \right) \)

\langle \text{proof} \rangle

This is particularly useful when the computation being transformed is strict in its argument.

Finally we can allow the identity to take the full recursive context into account. This rule was described by Gill and Hutton but not used.

**Lemma worker-wrapper-fix:**

fixes \( \text{wrap} :: 'b::pcpo \to 'a::pcpo \)

fixes \( \text{unwrap} :: 'a \to 'b \)

assumes \( \text{wrap-unwrap}: \text{fix} \left( \text{wrap} \circ \text{unwrap} \circ \text{body} \right) = \text{fix-body} \)

assumes \( \text{comp-body}: \text{computation} = \text{fix-body} \)

shows \( \text{computation} = \text{wrap} \left( \text{fix} \left( \text{unwrap} \circ \text{body} \circ \text{wrap} \right) \right) \)
proof

Gill and Hutton’s worker-wrapper-fusion rule is intended to allow the transformation of \((\text{unwrap} \circ \text{wrap}) \cdot R\) to \(R\) in recursive contexts, where \(R\) is meant to be a self-call. Note that it assumes that the first worker/wrapper hypothesis can be established.

lemma worker-wrapper-fusion:
  \begin{align*}
  &\text{fixes } \text{wrap} :: \mathcal{b} : \text{pcpo} \to \mathcal{a} : \text{pcpo} \\
  &\text{fixes } \text{unwrap} :: \mathcal{a} \to \mathcal{b} \\
  &\text{assumes } \text{wrap-unwrap}: \text{wrap} \circ \text{unwrap} = \text{ID} \\
  &\text{assumes } \text{work}: \text{work} = \text{fix}(\text{unwrap} \circ \text{body} \circ \text{wrap}) \\
  &\text{shows } (\text{unwrap} \circ \text{wrap}) \cdot \text{work} = \text{work}
  \end{align*}

proof

The following sections show that this rule only preserves partial correctness. This is because Gill and Hutton apply it in the context of the fold/unfold program transformation framework of Burstall and Darlington (1977), which need not preserve termination. We show that the fusion rule does in fact require extra conditions to be totally correct and propose one such sufficient condition.

3.1 Worker/wrapper fusion is partially correct

We now examine how Gill and Hutton apply their worker/wrapper fusion rule in the context of the fold/unfold framework.

The key step of those left implicit in the original paper is the use of the fold rule to justify replacing the worker with the fused version. Schematically, the fold/unfold framework maintains a history of all definitions that have appeared during transformation, and the fold rule treats this as a set of rewrite rules oriented right-to-left. (The unfold rule treats the current working set of definitions as rewrite rules oriented left-to-right.) Hence as each definition \(f = \text{body}\) yields a rule of the form \(\text{body} \implies f\), one can always derive \(f = f\). Clearly this has dire implications for the preservation of termination behaviour.

Tullsen (2002) in his §3.1.2 observes that the semantic essence of the fold rule is Park induction:

\[
\frac{f \cdot ?x = ?x}{\text{fix}_f \subseteq ?x} \quad \text{fix}_\text{least}
\]

viz that \(f \cdot x = x\) implies only the partially correct \(\text{fix}_f \subseteq x\), and not the totally correct \(\text{fix} f = x\). We use this characterisation to show that if \(\text{unwrap}\) is non-strict (i.e. \(\text{unwrap} \perp \neq \perp\)) then there are programs where worker/wrapper fusion as used by Gill and Hutton need only be partially correct.
Consider the scenario described in Figure 1. After applying the worker/wrapper transformation, we attempt to apply fusion by finding a residual expression $body'$ such that the body of the worker, i.e. the expression $unwrap \ oo \ body \ oo \ wrap$, can be rewritten as $body' \ oo \ unwrap \ oo \ wrap$. Intuitively this is the semantic form of workers where all self-calls are fusible. Our goal is to justify redefining $work$ to $fix\cdot body'$, i.e. to establish:

$$fix\cdot (unwrap \ oo \ body \ oo \ wrap) = fix\cdot body'$$

We show that worker/wrapper fusion as proposed by Gill and Hutton is partially correct using Park induction:

**lemma** fusion-partially-correct:
- **assumes** wrap-unwrap: $wrap \ oo \ unwrap = ID$
- **assumes** work: $work = fix\cdot (unwrap \ oo \ body \ oo \ wrap)$
- **assumes** body': $unwrap \ oo \ body \ oo \ wrap = body' \ oo \ unwrap \ oo \ wrap$
- **shows** $fix\cdot body' \subseteq work$

⟨proof⟩

The next section shows the converse does not obtain.

### 3.2 A non-strict $unwrap$ may go awry

If $unwrap$ is non-strict, then it is possible that the fusion rule proposed by Gill and Hutton does not preserve termination. To show this we take a small artificial example. The type $A$ is not important, but we need access to a non-bottom inhabitant. The target type $B$ is the non-strict lift of $A$.

**domain** $A = A$
**domain** $B = B$ (lazy $A$)

The functions $wrap$ and $unwrap$ that map between these types are routine. Note that $wrap$ is (necessarily) strict due to the property $\forall x. \ \forall f. (\forall g. x) = x \implies \forall f. \bot = \bot$.

**fixrec** $wrap :: B \rightarrow A$
**where** $wrap\cdot (B\cdot a) = a$
⟨proof⟩

**fixrec** $unwrap :: A \rightarrow B$
**where** $unwrap = B$

Discharging the worker/wrapper hypothesis is similarly routine.

**lemma** wrap-unwrap: $wrap \ oo \ unwrap = ID$
⟨proof⟩

The candidate computation we transform can be any that uses the recursion parameter $r$ non-strictly. The following is especially trivial.

**fixrec** $body :: A \rightarrow A$
**where** $body\cdot r = A$
The wrinkle is that the transformed worker can be strict in the recursion parameter \( r \), as \( \text{unwrap} \) always lifts it.

\[
\text{fixrec body'} :: B \to B
\text{where body'}(B\cdot a) = B\cdot A\langle \text{proof} \rangle
\]

As explained above, we set up the fusion opportunity:

\[
\text{lemma body-body': unwrapp oo body oo wrapp = body' oo unwrapp oo wrapp}
\langle \text{proof} \rangle
\]

This result depends crucially on \( \text{unwrap} \) being non-strict.

Our earlier result shows that the proposed transformation is partially correct:

\[
\text{lemma fix-body' \sqsubseteq fix-(unwrap oo body oo wrapp)}
\langle \text{proof} \rangle
\]

However it is easy to see that it is not totally correct:

\[
\text{lemma ¬ fix-(unwrap oo body oo wrapp) \sqsubseteq fix-body'}
\langle \text{proof} \rangle
\]

This trick works whenever \( \text{unwrap} \) is not strict. In the following section we show that requiring \( \text{unwrap} \) to be strict leads to a straightforward proof of total correctness.

Note that if we have already established that \( \text{wrapp oo unwrapp} = \text{ID} \), then making \( \text{unwrap} \) strict preserves this equation:

\[
\text{lemma}
\begin{align*}
\text{assumes} & \; \text{wrapp oo unwrapp} = \text{ID} \\
\text{shows} & \; \text{wrapp oo strictify-unwrapp} = \text{ID}
\end{align*}
\langle \text{proof} \rangle
\]

From this we conclude that the worker/wrapper transformation itself cannot exploit any laziness in \( \text{unwrap} \) under the context-insensitive assumptions of \text{worker-wrapper-id}. This is not to say that other program transformations may not be able to.

\langle \text{proof} \rangle

\section{4 A totally-correct fusion rule}

We now show that a termination-preserving worker/wrapper fusion rule can be obtained by requiring \( \text{unwrap} \) to be strict. (As we observed earlier, \( \text{wrapp} \) must always be strict due to the assumption that \( \text{wrapp oo unwrapp} = \text{ID} \).)

Our first result shows that a combined worker/wrapper transformation and fusion rule is sound, using the assumptions of \text{worker-wrapper-id} and the ubiquitous \text{lfp-fusion} rule.

\[
\text{lemma worker-wrapper-fusion-new}:
\]
For a recursive definition \( \text{comp} = \text{body} \) of type \( A \) and a pair of functions \( \text{wrap} :: B \to A \) and \( \text{unwrap} :: A \to B \) where \( \text{wrap} \circ \text{unwrap} = \text{id}_A \) and \( \text{unwrap} \bot = \bot \), define:

\[
\begin{align*}
\text{comp} &= \text{wrap} \text{ work} \\
\text{work} &= \text{unwrap} (\text{body}[\text{wrap work}/\text{comp}]) \\
\end{align*}
\]

(the worker/wrapper transformation)

In the scope of \( \text{work} \), the following rewrite is admissible:

\[
\text{unwrap} (\text{wrap work}) \implies \text{work} \\
\]

(worker/wrapper fusion)

Figure 2: The syntactic worker/wrapper transformation and fusion rule.

\[
\begin{align*}
\text{fixes} \ & \text{wrap} :: 'b::\text{pcpo} \to 'a::\text{pcpo} \\
\text{fixes} \ & \text{unwrap} :: 'a \to 'b \\
\text{fixes} \ & \text{body}' :: 'b \to 'b \\
\text{assumes} \ & \text{wrap-unwrap}: \text{wrap} \circ \text{unwrap} = (\text{id} :: 'a \to 'a) \\
\text{assumes} \ & \text{unwrap-strict}: \text{unwrap} \bot = \bot \\
\text{assumes} \ & \text{body-body}': \text{unwrap} \circ \text{body} \circ \text{unwrap} = \text{body}' \circ (\text{unwrap} \circ \text{wrap}) \\
\text{shows} \ & \text{fix-body} = \text{wrap}(\text{fix-body}') \\
\end{align*}
\]

\[\langle \text{proof} \rangle\]

We can also show a more general result which allows fusion to be optionally performed on a per-recursive-call basis using \textbf{parallel_fix_ind}:

\[
\begin{align*}
\text{lemma} \ & \text{worker-wrapper-fusion-new-general}: \\
\text{fixes} \ & \text{wrap} :: 'b::\text{pcpo} \to 'a::\text{pcpo} \\
\text{fixes} \ & \text{unwrap} :: 'a \to 'b \\
\text{assumes} \ & \text{wrap-unwrap}: \text{wrap} \circ \text{unwrap} = (\text{id} :: 'a \to 'a) \\
\text{assumes} \ & \text{unwrap-strict}: \text{unwrap} \bot = \bot \\
\text{assumes} \ & \text{body-body}': \forall r. (\text{unwrap} \circ \text{wrap}) \cdot r = r \\
\text{shows} \ & \text{fix-body} = \text{wrap}(\text{fix-body}') \\
\end{align*}
\]

\[\langle \text{proof} \rangle\]

This justifies the syntactically-oriented rules shown in Figure 2; note the scoping of the fusion rule.

Those familiar with the “bananas” work of Meijer, Fokkinga, and Paterson (1991) will not be surprised that adding a strictness assumption justifies an equational fusion rule.
5 Naive reverse becomes accumulator-reverse.

5.1 Hughes lists, naive reverse, worker-wrapper optimisation.

The “Hughes” list type.

**type-synonym** ‘a H = ‘a llist → ‘a llist

**definition**

```
list2H :: ‘a llist → ‘a H where
list2H ≡ lappend
```

**lemma** acc-c2a-strict[simp]: list2H·⊥ = ⊥

(proof)

**definition**

```
H2list :: ‘a H → ‘a llist where
H2list ≡ Λ f . f·lnil
```

The paper only claims the homomorphism holds for finite lists, but in fact it holds for all lazy lists in HOLCF. They are trying to dodge an explicit appeal to the equation ⊥ = (Λ x. ⊥), which does not hold in Haskell.

**lemma** H-list-hom-append: list2H·(xs ++ ys) = list2H·xs oo list2H·ys (is ?lhs = ?rhs)

(proof)

**lemma** H-list-hom-id: list2H·lnil = ID

(proof)

**lemma** H2list-list2H-inv: H2list oo list2H = ID

(proof)

Gill and Hutton (2009, §4.2) define the naive reverse function as follows.

**fixrec** lrev :: ‘a llist → ‘a llist

**where**

```
lrev·lnil = lnil
| lrev·(x ::@ xs) = lrev·xs ++ (x ::@ lnil)
```

Note “body” is the generator of lrev-def.

**lemma** lrev-strict[simp]: lrev·⊥ = ⊥

(proof)

**fixrec** lrev-body :: (‘a llist → ‘a llist) → ‘a llist → ‘a llist

**where**

```
lrev-body·r·lnil = lnil
| lrev-body·r·(x ::@ xs) = r·xs ++ (x ::@ lnil)
```

**lemma** lrev-body-strict[simp]: lrev-body·r·⊥ = ⊥
This is trivial but syntactically a bit touchy. Would be nicer to define \(lrev-body\) as the generator of the fixpoint definition of \(lrev\) directly.

**Lemma** \(lrev-lrev-body-eq\): \(lrev = \text{fix}\cdot lrev-body\)

Wrap / unwrap functions.

**Definition**

\[
\text{unwrapH} ::= ('a llist \to 'a llist) \to 'a llist \to 'a H \text{ where}
\]

\[
\text{unwrapH} \equiv \Lambda f \cdot \text{list2H} \cdot (f \cdot xs)
\]

**Lemma** \(\text{unwrapH-strict}[simp]\): \(\text{unwrapH} \cdot \bot = \bot\)

5.2 Gill/Hutton-style worker/wrapper.

**Definition**

\[
lrev-work ::= 'a llist \to 'a H \text{ where}
lrev-work \equiv \text{fix} \cdot (\text{unwrapH} \circ \text{lrev-body} \circ \text{wrapH})
\]

**Definition**

\[
lrev-wrap ::= 'a llist \to 'a llist \text{ where}
lrev-wrap \equiv \text{wrapH} \cdot \text{lrev-work}
\]

**Lemma** \(lrev-lrev-ww-eq\): \(lrev = lrev-wrap\)

5.3 Optimise worker/wrapper.

Intermediate worker.

**Fixrec** \(lrev-body1 ::= ('a llist \to 'a H) \to 'a llist \to 'a H \text{ where}
\]

\[
lrev-body1 \cdot r \cdot \text{lnil} = \text{list2H} \cdot \text{lnil}
\]

\[
lrev-body1 \cdot r \cdot (x :@ xs) = \text{list2H} \cdot (\text{wrapH} \cdot r \cdot xs ++ (x :@ \text{lnil}))
\]

**Definition**

\[
lrev-work1 ::= 'a llist \to 'a H \text{ where}
lrev-work1 \equiv \text{fix}\cdot lrev-body1
\]

**Lemma** \(lrev-body1-lrev-body1-eq\): \(lrev-body1 = \text{unwrapH} \circ \text{lrev-body} \circ \text{wrapH}\)
\begin{proof}
\end{proof}

\textbf{lemma} \ lrev-work1-lrev-work-eq: \ lrev-work1 = \ lrev-work \newline
\begin{proof}
\end{proof}

Now use the homomorphism.

\textbf{fixrec} \ lrev-body2 :: ('a llist \to 'a H) \to 'a llist \to 'a H \newline
\textbf{where} \newline
\begin{quote}
lrev-body2 \cdot r \cdot \text{nil} = \text{ID} \\
lrev-body2 \cdot r \cdot (x :@ xs) = \text{list2H} \cdot (\text{wrapH} \cdot r \cdot xs) \ oo \ \text{list2H} \cdot (x :@ \text{nil})
\end{quote}

\textbf{lemma} \ lrev-body2-strict[simp]: \ lrev-body2 \cdot r \cdot \bot = \bot \newline
\begin{proof}
\end{proof}

\textbf{definition} \newline
\begin{quote}
lrev-work2 :: 'a llist \to 'a H \textbf{ where} \\
lrev-work2 \equiv \text{fix}\cdot lrev-body2
\end{quote}

\textbf{lemma} \ lrev-work2-strict[simp]: \ lrev-work2 \cdot \bot = \bot \newline
\begin{proof}
\end{proof}

\textbf{lemma} \ lrev-body2-lrev-body1-eq: \ lrev-body2 = \ lrev-body1 \newline
\begin{proof}
\end{proof}

\textbf{lemma} \ lrev-work2-lrev-work1-eq: \ lrev-work2 = \ lrev-work1 \newline
\begin{proof}
\end{proof}

Simplify.

\textbf{fixrec} \ lrev-body3 :: ('a llist \to 'a H) \to 'a llist \to 'a H \newline
\textbf{where} \newline
\begin{quote}
lrev-body3 \cdot r \cdot \text{nil} = \text{ID} \\
lrev-body3 \cdot r \cdot (x :@ xs) = r \cdot xs \ oo \ \text{list2H} \cdot (x :@ \text{nil})
\end{quote}

\textbf{lemma} \ lrev-body3-strict[simp]: \ lrev-body3 \cdot r \cdot \bot = \bot \newline
\begin{proof}
\end{proof}

\textbf{definition} \newline
\begin{quote}
lrev-work3 :: 'a llist \to 'a H \textbf{ where} \\
lrev-work3 \equiv \text{fix}\cdot lrev-body3
\end{quote}

\textbf{lemma} \ lrev-wwfusion: \ \text{list2H} \cdot ((\text{wrapH} \cdot \text{lrev-work2}) \cdot xs) = \ lrev-work2 \cdot xs \newline
\begin{proof}
\end{proof}

If we use this result directly, we only get a partially-correct program transformation, see \textbf{Tullsen} (2002) for details.

\textbf{lemma} \ lrev-work3 \sqsubseteq \ lrev-work2 \newline
\begin{proof}
\end{proof}

We can’t show the reverse inclusion in the same way as the fusion law doesn’t
hold for the optimised definition. (Intuitively we haven’t established that it is equal to the original \texttt{lrev} definition.) We could show termination of the optimised definition though, as it operates on finite lists. Alternatively we can use induction (over the list argument) to show total equivalence.

The following lemma shows that the fusion Gill/Hutton want to do is completely sound in this context, by appealing to the lazy list induction principle.

\textbf{Lemma} \texttt{lrev-work3-lrev-work2-eq}: \texttt{lrev-work3} = \texttt{lrev-work2} (\texttt{is ?lhs = ?rhs})

⟨\textbf{proof}⟩

Use the combined worker/wrapper-fusion rule. Note we get a weaker lemma.

\textbf{Lemma} \texttt{lrev3-2-syntactic}: \texttt{lrev-body3} oo (unwrapH oo wrapH) = \texttt{lrev-body2}

⟨\textbf{proof}⟩

\textbf{Lemma} \texttt{lrev-work3-lrev-work2-eq}: \texttt{lrev} = \texttt{wrapH -lrev-work3}

⟨\textbf{proof}⟩

Final syntactic tidy-up.

\textbf{fixrec} \texttt{lrev-body-final} :: ('a list \rightarrow 'a H) \rightarrow 'a list \rightarrow 'a H

\textbf{where}

\texttt{lrev-body-final-r-nil-ys = ys}

\texttt{lrev-body-final-r-\langle x :@ xs \rangle-ys = r-\langle x :@ ys \rangle}

\textbf{definition}

\texttt{lrev-work-final} :: 'a list \rightarrow 'a H

\texttt{lrev-work-final} \equiv \textbf{fix} \cdot \texttt{lrev-body-final}

\textbf{definition}

\texttt{lrev-final} :: 'a list \rightarrow 'a list

\texttt{lrev-final} \equiv \Lambda \texttt{xs}. \texttt{lrev-work-final-\texttt{xs-nil}}

\textbf{lemma} \texttt{lrev-body-final-lrev-body3-eq}: \texttt{lrev-body-final-r-\texttt{xs} = \texttt{lrev-body3-r-\texttt{xs}}}

⟨\textbf{proof}⟩

\textbf{lemma} \texttt{lrev-body-final-lrev-body3-eq}: \texttt{lrev-body-final} = \texttt{lrev-body3}

⟨\textbf{proof}⟩

\textbf{lemma} \texttt{lrev-final-lrev-eq}: \texttt{lrev} = \texttt{lrev-final} (\texttt{is ?lhs = ?rhs})

⟨\textbf{proof}⟩

6 Unboxing types.

The original application of the worker/wrapper transformation was the unboxing of flat types by Peyton Jones and Launchbury (1991). We can model the boxed and unboxed types as (respectively) pointed and unpointed domains in HOLCF. Concretely \texttt{UNat} denotes the discrete domain of naturals,
UNat⊥ the lifted (flat and pointed) variant, and Nat the standard boxed domain, isomorphic to UNat⊥. This latter distinction helps us keep the boxed naturals and lifted function codomains separated; applications of unbox should be thought of in the same way as Haskell’s newtype constructors, i.e. operationally equivalent to ID.

The divergence monad is used to handle the unboxing, see below.

### 6.1 Factorial example.

Standard definition of factorial.

```haskell
fixrec fac :: Nat → Nat
where
  fac·n = If n =B 0 then 1 else n * fac·(n - 1)
```

```haskell
declare fac.simps[simp del]
```

```haskell
lemma fac-strict[simp]: fac·⊥ = ⊥
⟨proof⟩
```

```haskell
definition
  fac-body :: (Nat → Nat) → Nat → Nat
  where
    fac-body ≡ Λ r n. If n =B 0 then 1 else n * r·(n - 1)
```

```haskell
lemma fac-body-strict[simp]: fac-body·r·⊥ = ⊥
⟨proof⟩
```

```haskell
lemma fac-fac-body-eq: fac = fix·fac-body
⟨proof⟩
```

Wrap / unwrap functions. Note the explicit lifting of the co-domain. For some reason the published version of Gill and Hutton (2009) does not discuss this point: if we’re going to handle recursive functions, we need a bottom.

unbox simply removes the tag, yielding a possibly-divergent unboxed value, the result of the function.

```haskell
definition
  unwrapB :: (Nat → Nat) → UNat → UNat⊥
  where
    unwrapB ≡ Λ f. unbox oo f oo box
```

Note that the monadic bind operator op >>= here stands in for the case construct in the paper.

```haskell
definition
  wrapB :: (UNat → UNat⊥) → Nat → Nat
  where
    wrapB ≡ Λ f x. unbox·x >>= f >>= box
```

```haskell
lemma wrapB-unwrapB-body:
  assumes strictF: f·⊥ = ⊥
shows \((\text{wrapB} \circ \text{unwrapB}) \cdot f = f\) (\is \ ?\text{lhs} = ?\text{rhs})

\(\langle\text{proof}\rangle\)

Apply worker/wrapper.

definition
\texttt{fac-work} :: \texttt{UNat} \rightarrow \texttt{UNat} \bot where
\texttt{fac-work} \equiv \texttt{fix} \circ (\texttt{unwrapB} \circ \texttt{fac-body} \circ \texttt{wrapB})

definition
\texttt{fac-wrap} :: \texttt{Nat} \rightarrow \texttt{Nat} where
\texttt{fac-wrap} \equiv \texttt{wrapB} \cdot \texttt{fac-work}

lemma \texttt{fac-fac-ww-eq}: \texttt{fac} = \texttt{fac-wrap} (\is \ ?\text{lhs} = ?\text{rhs})

\(\langle\text{proof}\rangle\)

This is not entirely faithful to the paper, as they don’t explicitly handle the lifting of the codomain.

definition
\texttt{fac-body’} :: (\texttt{UNat} \rightarrow \texttt{UNat} \bot) \rightarrow \texttt{UNat} \rightarrow \texttt{UNat} \bot where
\texttt{fac-body’} \equiv \Lambda \texttt{r n}.
\texttt{unbox} (\texttt{If} \ \texttt{box} \cdot \texttt{n} \equiv \texttt{b} \ 0
\texttt{then} \texttt{1}
\texttt{else} \texttt{unbox} (\texttt{box} \cdot \texttt{n} - 1) >>= \texttt{r} >>= (\Lambda \texttt{b} \cdot \texttt{box} \cdot \texttt{n} * \texttt{box} \cdot \texttt{b}))

lemma \texttt{fac-body’-fac-body}: \texttt{fac-body’} = \texttt{unwrapB} \circ \texttt{fac-body} \circ \texttt{wrapB} (\is \ ?\text{lhs} = ?\text{rhs})

\(\langle\text{proof}\rangle\)

The \texttt{up} constructors here again mediate the isomorphism, operationally doing nothing. Note the switch to the machine-oriented \texttt{if} construct: the test \(n = (\texttt{0}::\texttt{a})\) cannot diverge.

definition
\texttt{fac-body-final} :: (\texttt{UNat} \rightarrow \texttt{UNat} \bot) \rightarrow \texttt{UNat} \rightarrow \texttt{UNat} \bot where
\texttt{fac-body-final} \equiv \Lambda \texttt{r n}.
\texttt{if} \texttt{n} = \texttt{0} \texttt{then} \texttt{up} \cdot \texttt{1} \texttt{else} \texttt{r} \cdot (\texttt{n} -- \texttt{1}) >>= (\Lambda \texttt{b} \cdot \texttt{up} \cdot (\texttt{n} * \texttt{b}))

lemma \texttt{fac-body-final-fac-body’}: \texttt{fac-body-final} = \texttt{fac-body’} (\is \ ?\text{lhs} = ?\text{rhs})

\(\langle\text{proof}\rangle\)

definition
\texttt{fac-work-final} :: \texttt{UNat} \rightarrow \texttt{UNat} \bot where
\texttt{fac-work-final} \equiv \texttt{fix} \cdot \texttt{fac-body-final}

definition
\texttt{fac-final} :: \texttt{Nat} \rightarrow \texttt{Nat} where
\texttt{fac-final} \equiv \Lambda \texttt{n}. \texttt{unbox} \cdot \texttt{n} >>= \texttt{fac-work-final} >>= \texttt{box}

lemma \texttt{fac-fac-final}: \texttt{fac} = \texttt{fac-final} (\is \ ?\text{lhs} = ?\text{rhs})

\(\langle\text{proof}\rangle\)
6.2 Introducing an accumulator.

The final version of factorial uses unboxed naturals but is not tail-recursive. We can apply worker/wrapper once more to introduce an accumulator, similar to §5.

The monadic machinery complicates things slightly here. We use Kleisli composition, denoted \( \Rightarrow \Rightarrow \), in the homomorphism.

Firstly we introduce an “accumulator” monoid and show the homomorphism.

type-synonym \( \texttt{UNatAcc} = \texttt{UNat} \rightarrow \texttt{UNat}^\bot \)

definition \( \texttt{n2a} :: \texttt{UNat} \rightarrow \texttt{UNatAcc} \)

where \( \texttt{n2a} \equiv \Lambda n. \texttt{up}(m \ast \# n) \)

definition \( \texttt{a2n} :: \texttt{UNatAcc} \rightarrow \texttt{UNat} \)

where \( \texttt{a2n} \equiv \Lambda n. a \cdot 1 \)

lemma \( \texttt{a2n-strict} [\texttt{simp}] : \texttt{a2n} \cdot \bot = \bot \)

(\texttt{proof})

lemma \( \texttt{a2n-n2a} : \texttt{a2n} \cdot (\texttt{n2a} \cdot u) = \texttt{up} \cdot u \)

(\texttt{proof})

lemma \( \texttt{A-hom-mult} : \texttt{n2a} \cdot (x \ast \# y) = (\texttt{n2a} \cdot x) \Rightarrow n2a \cdot y \)

(\texttt{proof})

definition \( \texttt{unwrapA} :: (\texttt{UNat} \rightarrow \texttt{UNat}^\bot) \rightarrow \texttt{UNat} \rightarrow \texttt{UNatAcc} \)

where \( \texttt{unwrapA} \equiv \Lambda f n. f \cdot n \Rightarrow n2a \)

lemma \( \texttt{unwrapA-strict} [\texttt{simp}] : \texttt{unwrapA} \cdot \bot = \bot \)

(\texttt{proof})

definition \( \texttt{wrapA} :: (\texttt{UNat} \rightarrow \texttt{UNatAcc}) \rightarrow \texttt{UNat} \rightarrow \texttt{UNat}^\bot \)

where \( \texttt{wrapA} \equiv \Lambda f. \texttt{a2n} \circ f \)

lemma \( \texttt{wrapA-unwrapA-id} : \texttt{wrapA} \circ \texttt{unwrapA} = \texttt{ID} \)

(\texttt{proof})

Some steps along the way.

definition \( \texttt{fac-acc-body1} :: (\texttt{UNat} \rightarrow \texttt{UNatAcc}) \rightarrow \texttt{UNat} \rightarrow \texttt{UNatAcc} \)

where \( \texttt{fac-acc-body1} \equiv \Lambda r n.

\indent \textit{if} \ n = 0 \ \textit{then} \ n2a \cdot 1 \ \textit{else} \ \texttt{wrapA} \cdot r \cdot (n - \# 1) \Rightarrow (\Lambda \texttt{res}. n2a \cdot (n \ast \# \texttt{res})) \)
lemma fac-acc-body1-fac-body-final-eq: fac-acc-body1 = unwrapA oo fac-body-final oo wrapA
⟨proof⟩

Use the homomorphism.

definition fac-acc-body2 :: (UNat → UNatAcc) → UNat → UNatAcc where
fac-acc-body2 ≡ Λ r n.
  if n = 0 then n2a·1 else wrapA·r·(n − # 1) >>= (Λ res. n2a·n >>= n2a·res)

lemma fac-acc-body2-body1-eq: fac-acc-body2 = fac-acc-body1
⟨proof⟩

Apply worker/wrapper.

definition fac-acc-body3 :: (UNat → UNatAcc) → UNat → UNatAcc where
fac-acc-body3 ≡ Λ r n.
  if n = 0 then n2a·1 else n2a·n >>= r·(n − # 1)

lemma fac-acc-body3-body2: fac-acc-body3 oo (unwrapA oo wrapA) = fac-acc-body2
(is ?lhs=?rhs)
⟨proof⟩

lemma fac-work-final-body3-eq: fac-work-final = wrapA·(fix·fac-acc-body3)
⟨proof⟩

definition fac-acc-body-final :: (UNat → UNatAcc) → UNat → UNatAcc where
fac-acc-body-final ≡ Λ r n acc.
  if n = 0 then up·acc else r·(n − # 1)·(n * # acc)

definition fac-acc-work-final :: UNat → UNat⊥ where
fac-acc-work-final ≡ Λ x. fix·fac-acc-body-final·x·1

lemma fac-acc-work-final-fac-acc-work3-eq: fac-acc-body-final = fac-acc-body3 (is ?lhs=?rhs)
⟨proof⟩

lemma fac-acc-work-final-fac-work: fac-acc-work-final = fac-work-final (is ?lhs=?rhs)
⟨proof⟩

7 Memoisation using streams.

7.1 Streams.

The type of infinite streams.
domain  'a Stream = stcons (lazy sthead :: 'a) (lazy sttail :: 'a Stream) (infixr & & 65)
⟨proof⟩
fixrec smap :: ('a → 'b) → 'a Stream → 'b Stream
where
  smap·f·(x & & xs) = f·x & & smap·f·xs
⟨proof⟩
lemma smap-smap: smap·f·(smap·g·xs) = smap·(f oo g)·xs⟨proof⟩
fixrec i-th :: 'a Stream → Nat → 'a
where
  i-th·(x & & xs) = Nat-case·x·(i-th·xs)
abbreviation
  i-th-syn :: 'a Stream ⇒ Nat ⇒ 'a
  (infixl !! 100)
  where
  s !! i ≡ i-th·s·i
  ⟨proof⟩⟨proof⟩⟨proof⟩⟨proof⟩
The infinite stream of natural numbers.
fixrec nats :: Nat Stream
where
  nats = 0 & & smap·(Λ x. 1 + x)·nats

7.2 The wrapper/unwrapper functions.
definition
  unwrapS' :: (Nat → 'a) → 'a Stream
  unwrapS' ≡ Λ f . smap·f·nats
lemma unwrapS'-unfold: unwrapS'·f = f·0 & & smap·(f oo (Λ x. 1 + x))·nats⟨proof⟩
fixrec unwrapS :: (Nat → 'a) → 'a Stream
where
  unwrapS·f = f·0 & & unwrapS·(f oo (Λ x. 1 + x))

The two versions of unwrapS are equivalent. We could try to fold some
definitions here but it’s easier if the stream constructor is manifest.
lemma unwrapS-unwrapS'-eq: unwrapS = unwrapS' (is ?lhs = ?rhs)
⟨proof⟩
definition
  wrapS :: 'a Stream → Nat → 'a
  wrapS ≡ Λ s i . s !! i
Note the identity requires that f be strict. Gill and Hutton (2009, §6.1) do
not make this requirement, an oversight on their part.
In practice all functions worth memoising are strict in the memoised argu-
ment.
lemma `wrapS-unwrapS-id`:
assumes strictF: `(f :: Nat → 'a) ⊥ = ⊥`
shows `unwrapS f !! n = f n`
⟨proof⟩

lemma `wrapS-unwrapS-id`:
`f · ⊥ = ⊥ =⇒ (wrapS oo unwrapS) · f = f`
⟨proof⟩

### 7.3 Fibonacci example.

**Definition**

`fib-body` :: `(Nat → Nat) → Nat → Nat`

`fib-body ≡ Λ r. Nat-case·1·(Nat-case·1·(Λ n. r·n + r·(n + 1)))`

⟨proof⟩

**Definition**

`fib` :: `Nat → Nat`

`fib ≡ fix·fib-body`

⟨proof⟩

Apply worker/wrapper.

**Definition**

`fib-work` :: `Nat Stream`

`fib-work ≡ fix·(unwrapS oo fib-body oo wrapS)`

**Definition**

`fib-wrap` :: `Nat → Nat`

`fib-wrap ≡ wrapS·fib-work`

**Lemma**

`wrapS-unwrapS-fib-body`:

`wrapS oo unwrapS oo fib-body = fib-body`

⟨proof⟩

**Lemma**

`fib-ww-eq`:

`fib = fib-wrap`

⟨proof⟩

Optimise.

**Fixrec**

`fib-work-final` :: `Nat Stream`

and

`fib-f-final` :: `Nat → Nat`

where

`fib-work-final = smap·fib-f-final-nats`

| `fib-f-final = Nat-case·1·(Nat-case·1·(Λ n′. fib-work-final !! n′ + fib-work-final !! (n′ + 1)))`

**Declare**

`fib-f-final.simps[simp del] fib-work-final.simps[simp del]`

**Definition**

`fib-final` :: `Nat → Nat`

`fib-final ≡ Λ n. fib-work-final !! n`

18
This proof is only fiddly due to the way mutual recursion is encoded: we need to use Bekić's Theorem (Bekić 1984)\(^1\) to massage the definitions into their final form.

**lemma** \[\text{fib-work-final-fib-work-eq}: \text{fib-work-final} = \text{fib-work} (\text{is \ ?lhs = ?rhs})\]

**lemma** \[\text{fib-final-fib-eq}: \text{fib-final} = \text{fib} (\text{is \ ?lhs = ?rhs})\]

\(^1\)The interested reader can find some historical commentary in Harel (1980); Sangiorgi (2009).

8 Tagless interpreter via double-barreled continuations

**type-synonym** 'a Cont = ('a \rightarrow 'a) \rightarrow 'a

**definition**

val2cont :: 'a \rightarrow 'a Cont where

val2cont \equiv (Λ a c. c \cdot a)

**definition**

cont2val :: 'a Cont \rightarrow 'a where

cont2val \equiv (Λ f. f \cdot ID)

**lemma** cont2val-val2cont-id: cont2val oo val2cont = ID

\(^1\)The interested reader can find some historical commentary in Harel (1980); Sangiorgi (2009).
lemma eval-body-strictExpr[simp]: eval-body\cdot \bot = \bot
(proof)

lemma eval-eval-body-eq: eval = fix\cdot eval-body
(proof)

8.1 Worker/wrapper
definition unwrapC :: (Expr \to Nat Maybe) \to (Expr \to (Nat \to Nat Maybe) \to Nat Maybe)
where
unwrapC ≡ \lambda g e s f. case g \cdot e of Nothing ⇒ f | Just ⇒ s \cdot n

lemma unwrapC-strict[simp]: unwrapC \cdot \bot = \bot
(proof)

definition wrapC :: (Expr \to (Nat \to Nat Maybe) \to Nat Maybe \to Nat Maybe) \to (Expr
\to Nat Maybe)
where
wrapC ≡ \lambda g e. g \cdot e \cdot Just \cdot Nothing

lemma wrapC-unwrapC-id: wrapC oo unwrapC = ID
(proof)

definition eval-work :: Expr \to (Nat \to Nat Maybe) \to Nat Maybe \to Nat Maybe
where
eval-work ≡ fix\cdot (unwrapC oo eval-body oo wrapC)

definition eval-wrap :: Expr \to Nat Maybe
where
eval-wrap ≡ wrapC \cdot eval-work

fixrec eval-body' :: (Expr \to (Nat \to Nat Maybe) \to Nat Maybe \to Nat Maybe)
\to Expr \to (Nat \to Nat Maybe) \to Nat Maybe \to Nat Maybe
where
eval-body'\cdot r \cdot (Val\cdot n)\cdot s\cdot f = s\cdot n
| eval-body'\cdot r \cdot (Add\cdot x\cdot y)\cdot s\cdot f = (case wrapC\cdot r\cdot x of
  Nothing ⇒ f
  | Just⇒ (case wrapC\cdot r\cdot y of
    Nothing ⇒ f
    | Just⇒ s\cdot (n + m)))
| eval-body'\cdot r \cdot Throw\cdot s\cdot f = f
| eval-body'\cdot r \cdot (Catch\cdot x\cdot y)\cdot s\cdot f = (case wrapC\cdot r\cdot x of
  Nothing ⇒ (case wrapC\cdot r\cdot y of
    Nothing ⇒ f
    | Just⇒ s\cdot n)
  | Just⇒ s\cdot n)

lemma eval-body'-strictExpr[simp]: eval-body'\cdot r\cdot \bot\cdot s\cdot f = \bot
This proof is unfortunately quite messy, due to the simplifier’s inability to cope with HOLCF’s case distinctions.

lemma eval-body'-eval-body-eq: eval-body' = unwrapC oo eval-body oo wrapC

lemma eval-body-final-strictExpr[simp]: eval-body-final·⊥·s·f = ⊥
The language consists of constants, an addition function, a disjunctive choice between expressions, and failure. We give it a direct semantics using the monad of lazy lists of natural numbers, with the goal of deriving an an extensionally-equivalent evaluator that uses double-barrelled continuations. Our theory of lazy lists is entirely standard.

By relaxing the default sort of type variables to `predomain`, our polymorphic definitions can be used at concrete types that do not contain `⊥`. These include those constructed from HOL types using the discrete ordering type constructor `′a discr`, and in particular our interpretation `nat discr` of the natural numbers.

The following standard list functions underpin the monadic infrastructure:

**fixrec lappend :: ′a llist → ′a llist → ′a llist where**
- `lappend··lnil·ys = ys`
- `lappend··(lcons·x·xs)·ys = lcons·x·(lappend·xs·ys)`

**fixrec lconcat :: ′a llist llist → ′a llist where**
- `lconcat··lnil = lnil`
- `lconcat··(lcons·x·xs) = lappend·x·(lconcat·xs)`

**fixrec lmap :: ′a → ′b) → ′a llist → ′b llist where**
- `lmap·f·lnil = lnil`
- `lmap·f·(lcons·x·xs) = lcons·(f·x)·(lmap·f·xs)`

We define the lazy list monad `S` in the traditional fashion:

**type-synonym** `S = nat discr llist`

**definition returnS :: nat discr → S where**
- `returnS = (Λ x. lcons·x·lnil)`

**definition bindS :: S → (nat discr → S) → S where**
- `bindS = (Λ x g. lconcat·(lmap·g·x))`

Unfortunately the lack of higher-order polymorphism in HOL prevents us from providing the general typing one would expect a monad to have in Haskell.

The evaluator uses the following extra constants:

**definition addS :: S → S → S where**
- `addS ≡ (Λ x y. bindS·x·(Λ xv. bindS·y·(Λ yv. returnS·(xv + yv))))`
**definition** disj$S :: S \to S \to S$ where
\[
\text{disj}\!S \equiv \text{lappend}
\]

**definition** fail$S :: S$ where
\[
\text{fail}\!S \equiv \text{lnil}
\]

We interpret our language using these combinators in the obvious way. The only complication is that, even though our evaluator is primitive recursive, we must explicitly use the fixed point operator as the worker/wrapper technique requires us to talk about the body of the recursive definition.

**definition** eval$S$-body :: (expr discr \to nat discr llist) \to (expr discr \to nat discr llist)
\[
\text{eval}\!S\!\!S\!\text{-body} \equiv \Lambda r. e. \text{case undiscr } e \text{ of}
\]
\[
\begin{align*}
\text{const } n & \Rightarrow \text{return}\!S \cdot (\text{Discr } n) \\
\text{add } e_1 e_2 & \Rightarrow \text{add}\!S \cdot (r \cdot (\text{Discr } e_1)) \cdot (r \cdot (\text{Discr } e_2)) \\
\text{disj } e_1 e_2 & \Rightarrow \text{disj}\!S \cdot (r \cdot (\text{Discr } e_1)) \cdot (r \cdot (\text{Discr } e_2)) \\
\text{fail} & \Rightarrow \text{fail}\!S
\end{align*}
\]

**abbreviation** eval$S :: expr discr \to nat discr llist$ where
\[
\text{eval}\!S \equiv \text{fix } \text{eval}\!S\!\!\text{-body}
\]

We aim to transform this evaluator into one using double-barrelled continuations; one will serve as a “success” context, taking a natural number into “the rest of the computation”, and the other outright failure.

In general we could work with an arbitrary observation type ala Reynolds (1974), but for convenience we use the clearly adequate concrete type nat discr llist.

**type-synonym** Obs = nat discr llist
**type-synonym** Failure = Obs
**type-synonym** Success = nat discr \to Failure \to Obs
**type-synonym** K = Success \to Failure \to Obs

To ease our development we adopt what Wand and Vaillancourt (2004, §5) call a “failure computation” instead of a failure continuation, which would have the type unit \to Obs.

The monad over the continuation type K is as follows:

**definition** return$K :: nat discr \to K$ where
\[
\text{return}\!K \equiv (\Lambda x. \Lambda s. f \cdot s \cdot x \cdot f)
\]

**definition** bind$K :: K \to (nat discr \to K) \to K$ where
\[
\text{bind}\!K \equiv (\Lambda x. \Lambda g. \Lambda s. f \cdot x \cdot (\Lambda x v. f'. g \cdot x v \cdot s \cdot f' \cdot f)
\]

Our extra constants are defined as follows:

**definition** add$K :: K \to K \to K$ where
\[ addK \equiv (\Lambda x \ y. \ bindK \cdot x \cdot (\Lambda xv. \ bindK \cdot y \cdot (\Lambda yv. \ returnK \cdot (xv + yv)))) \]

**Definition** \(disjK :: K \to K \to K\) where
\[ disjK \equiv (\Lambda g \ h. \ \Lambda s f. \ g \cdot s \cdot (h \cdot s \cdot f)) \]

**Definition** \(failK :: K\) where
\[ failK \equiv \Lambda s f. \ f \]

The continuation semantics is again straightforward:

**Definition**
\[ evalK-body :: (expr discr \to K) \to (expr discr \to K) \]
where
\[
\begin{align*}
\text{evalK-body} & \equiv \Lambda r \ e. \ \text{case undiscr e of} \\
| \text{const n} & \Rightarrow \text{returnK} \cdot (\text{Discr n}) \\
| \text{add e1 e2} & \Rightarrow \text{addK} \cdot (r \cdot (\text{Discr e1})) \cdot (r \cdot (\text{Discr e2})) \\
| \text{disj e1 e2} & \Rightarrow \text{disjK} \cdot (r \cdot (\text{Discr e1})) \cdot (r \cdot (\text{Discr e2})) \\
| \text{fail} & \Rightarrow \text{failK}
\end{align*}
\]

**Abbreviation**
\[ evalK :: expr discr \to K \]
where
\[ \text{evalK} \equiv \text{fix} \cdot \text{evalK-body} \]

We now set up a worker/wrapper relation between these two semantics.

The kernel of \(unwrap\) is the following function that converts a lazy list into an equivalent continuation representation.

**Definition**
\[ fixrec SK :: S \to K \]
where
\[
\begin{align*}
\text{fixrec SK} & \equiv \Lambda k. \ k \\
| \text{lnil} & = \text{failK} \\
| \text{lcons} \cdot x \cdot xs & = (\Lambda s f. \ s \cdot x \cdot (\text{SK} \cdot xs \cdot s \cdot f))
\end{align*}
\]

**Definition**
\[ unwrap :: (expr discr \to nat discr llist) \to (expr discr \to K) \]
where
\[ \text{unwrap} \equiv \Lambda r e. \ (\text{SK} \cdot (r \cdot e)) \langle \text{proof} \rangle \langle \text{proof} \rangle \]

Symmetrically \(wrap\) converts an evaluator using continuations into one generating lazy lists by passing it the right continuations.

**Definition**
\[ KS :: K \to S \]
where
\[ \text{KS} \equiv (\Lambda k. \ k \cdot \text{lcons-lnil}) \]

**Definition**
\[ wrap :: (expr discr \to K) \to (expr discr \to nat discr llist) \]
where
\[ \text{wrap} \equiv \Lambda r e. \ (\text{KS} \cdot (r \cdot e)) \langle \text{proof} \rangle \langle \text{proof} \rangle \]

The worker/wrapper condition follows directly from these definitions.

**Lemma**
\[ KS-SK-id: \]
\[ \text{KS} \cdot (\text{SK} \cdot xs) = xs \]
\[ \langle \text{proof} \rangle \]

**Lemma**
\[ wrap-unwrap-id: \]
\[ \text{wrap} \circ \text{unwrap} = \text{ID} \]

24
The worker/wrapper transformation is only non-trivial if wrap and unwrap do not witness an isomorphism. In this case we can show that we do not even have a Galois connection.

**lemma** cfun-not-below:
\[ f \cdot x \not\sqsubseteq g \cdot x \implies f \not\sqsubseteq g \]

**lemma** unwrap-wrap-not-under-id:
\[ \text{unwrap oo wrap} \not\subseteq \text{ID} \]

We now apply worker_wrapper_id:

**definition** eval-work :: expr discr \to K where
\[
eval-work \equiv \text{fix} \cdot (\text{unwrap oo evalS-body oo wrap})
\]

**definition** eval-ww :: expr discr \to nat discr llist where
\[
eval-ww \equiv \text{wrap} \cdot \text{eval-work}
\]

**lemma** evalS = eval-ww

We now show how the monadic operations correspond by showing that SK witnesses a monad morphism (Wadler 1992, §6). As required by Danvy et al. (2001, Definition 2.1), the mapping needs to hold for our specific operations in addition to the common monadic scaffolding.

**lemma** SK-returnS-returnK:
\[
\text{SK} \cdot (\text{returnS} \cdot x) = \text{returnK} \cdot x
\]

**lemma** SK-lappend-distrib:
\[
\text{SK} \cdot (\text{lappend} \cdot xs \cdot ys) \cdot s \cdot f = \text{SK} \cdot xs \cdot s \cdot (\text{SK} \cdot ys \cdot s \cdot f)
\]

**lemma** SK-bindS-bindK:
\[
\text{SK} \cdot (\text{bindS} \cdot x \cdot g) = \text{bindK} \cdot (\text{SK} \cdot x) \cdot (\text{SK} \cdot g)
\]

**lemma** SK-addS-distrib:
\[
\text{SK} \cdot (\text{addS} \cdot x \cdot y) = \text{addK} \cdot (\text{SK} \cdot x) \cdot (\text{SK} \cdot y)
\]

**lemma** SK-disjS-disjK:
\[
\text{SK} \cdot (\text{disjS} \cdot xs \cdot ys) = \text{disjK} \cdot (\text{SK} \cdot xs) \cdot (\text{SK} \cdot ys)
\]

**lemma** SK-failS-failK:
These lemmas directly establish the precondition for our all-in-one worker/wrapper and fusion rule:

**lemma** evalS-body-evalK-body:
\[
\text{unwrap} \circ \text{evalS-body} \circ \text{wrap} = \text{evalK-body} \circ \text{unwrap} \circ \text{wrap}
\]

**theorem** evalS-evalK:
\[
\text{evalS} = \text{wrap} \cdot \text{evalK}
\]

This proof can be considered an instance of the approach of Hutton et al. (2010), which uses the worker/wrapper machinery to relate two algebras. This result could be obtained by a structural induction over the syntax of the language. However our goal here is to show how such a transformation can be achieved by purely equational means; this has the advantage that our proof can be locally extended, e.g. the full language of Danvy et al. (2001) simply by proving extra equations. In contrast the higher-order language of Wand and Vaillancourt (2004) is beyond the reach of this approach.

10 Transforming $O(n^2)$ nub into an $O(n \lg n)$ one

Andy Gill’s solution, mechanised.

10.1 The nub function.

**fixrec** nub :: Nat list \rightarrow Nat list

**where**
\[
nub-\text{nil} = \text{nil}
| \ nub-(x :@ xs) = x :@ nub-(\text{filter}-(\neg \circ (\Lambda \ y. x = B y)) \circ xs)
\]

**lemma** nub-strict[simp]: nub-\bot = \bot

**fixrec** nub-body :: (Nat list \rightarrow Nat list) \rightarrow Nat list \rightarrow Nat list

**where**
\[
nub-body.f-\text{nil} = \text{nil}
| \ nub-body.f-(x :@ xs) = x :@ f-(\text{filter}-(\neg \circ (\Lambda \ y. x = B y)) \circ xs)
\]

**lemma** nub-nub-body-eq: nub = fix-nub-body

(\text{proof})
10.2 Optimised data type.

Implement sets using lazy lists for now. Lifting up HOL’s ‘a set type causes continuity grief.

**type-synonym** NatSet = Nat llist

**definition**

\[ SetEmpty :: NatSet \text{ where } \]
\[ SetEmpty \equiv \text{lnil} \]

**definition**

\[ SetInsert :: \text{Nat} \to \text{NatSet} \to \text{NatSet} \text{ where } \]
\[ SetInsert \equiv \text{lcons} \]

**definition**

\[ SetMem :: \text{Nat} \to \text{NatSet} \to \text{tr} \text{ where } \]
\[ SetMem \equiv \text{bmember}\cdot(\text{bpred } (\text{op } =)) \]

**lemma** \[ \text{SetMem-strict}[\text{simp}]: \text{SetMem}\cdot x \cdot \bot = \bot \text{⟨proof⟩} \]

**lemma** \[ \text{SetMem-SetEmpty}[\text{simp}]: \text{SetMem}\cdot x \cdot \text{SetEmpty} = \text{FF} \text{⟨proof⟩} \]

**lemma** \[ \text{SetMem-SetInsert}: \text{SetMem}\cdot v \cdot (\text{SetInsert}\cdot x \cdot s) = (\text{SetMem}\cdot v \cdot s \text{ orelse } x =_B v) \text{⟨proof⟩} \]

AndyG’s new type.

**domain** \[ R = R \text{ (lazy resultR :: Nat llist) (lazy exceptR :: NatSet)} \]

**definition**

\[ \text{nextR} :: R \to (\text{Nat } \ast R) \text{ Maybe} \text{ where } \]
\[ \text{nextR} = (\Lambda r. \text{case } \text{dropWhile}\cdot(\Lambda x. \text{SetMem}\cdot x \cdot (\text{exceptR}\cdot r))\cdot(\text{resultR}\cdot r) \text{ of } \]
\[ \text{init} \Rightarrow \text{Nothing} \]
\[ | x :@ xs \Rightarrow \text{Just}\cdot(x, R\cdot xs\cdot(\text{exceptR}\cdot r))) \]

**lemma** \[ \text{nextR-strict1}[\text{simp}]: \text{nextR}\cdot \bot = \bot \text{⟨proof⟩} \]

**lemma** \[ \text{nextR-strict2}[\text{simp}]: \text{nextR}\cdot (R\cdot \bot \cdot S) = \bot \text{⟨proof⟩} \]

**lemma** \[ \text{nextR-lnil}[\text{simp}]: \text{nextR}\cdot (R\cdot \text{lnil}\cdot S) = \text{Nothing} \text{⟨proof⟩} \]

**definition**

\[ \text{filterR} :: \text{Nat } \to R \to R \text{ where } \]
\[ \text{filterR} \equiv (\Lambda v r. R\cdot (\text{resultR}\cdot r)\cdot(\text{SetInsert}\cdot v \cdot (\text{exceptR}\cdot r))) \]

**definition**

\[ \text{c2a} :: \text{Nat llist } \to R \text{ where } \]
\[ \text{c2a} \equiv \Lambda xs. R\cdot xs\cdot \text{SetEmpty} \]

**definition**

\[ \text{a2c} :: R \to \text{Nat llist} \text{ where } \]
\[ a2c \equiv \Lambda r. \ lfilter (\Lambda v. \ neg (\set\negr v. (\except\r r)))\cdot (\result\r r) \]

**Lemma a2c-strict[simp]:** \( a2c \bot = \bot \)  
(proof)

**Lemma a2c-c2a-id:** \( a2c \circ c2a = \text{ID} \)  
(proof)

**Definition**
\[
\text{wrap} :: (R \rightarrow \text{Nat list}) \rightarrow \text{Nat list} \rightarrow \text{Nat list}
\text{where}
\text{wrap} \equiv \Lambda f x. \ f \cdot (c2a\cdot x)
\]

**Definition**
\[
\text{unwrap} :: (\text{Nat list} \rightarrow \text{Nat list}) \rightarrow R \rightarrow \text{Nat list}
\text{where}
\text{unwrap} \equiv \Lambda f r. \ f \cdot (a2c\cdot r)
\]

**Lemma unwrap-strict[simp]:** \( \text{unwrap} \cdot \bot = \bot \)  
(proof)

**Lemma wrap-unwrap-id:** \( \text{wrap} \circ \text{unwrap} = \text{ID} \)  
(proof)

Equivalences needed for later.

**Lemma TR-deMorgan:** \( \neg (x \circ\lor y) = (\neg x \circ\land \neg y) \)  
(proof)

**Lemma case-maybe-case:**
\[
\text{(case (case L of lnil \Rightarrow \text{Nothing} | x ::@ x \Rightarrow \text{Just} \cdot (h \cdot x \cdot x)) \ of}
\text{Nothing \Rightarrow f | \text{Just} \cdot (a, b) \Rightarrow g \cdot a \cdot b)
\]
\[
\text{= (case L of lnil \Rightarrow f | x ::@ x \Rightarrow g \cdot (\text{fst} \cdot (h \cdot x \cdot x)) \cdot (\text{snd} \cdot (h \cdot x \cdot x)))}
\]
(proof)

**Lemma case-a2c-case-caseR:**
\[
\text{(case a2c \cdot w of lnil \Rightarrow f | x ::@ x \Rightarrow g \cdot x \cdot x)
\]
\[
\text{= (case nextR \cdot w of Nothing \Rightarrow f | \text{Just} \cdot (x, r) \Rightarrow g \cdot x \cdot (a2c \cdot r)) (is \ ?lhs = ?rhs)}
\]
(proof)

**Lemma filter-filterR:** \( \text{lfilter} \cdot (neg \circ o) \cdot (\Lambda y. \ x =_B y)) \cdot (a2c \cdot r) = a2c \cdot (\text{filterR} \cdot x \cdot r) \)  
(proof)

Apply worker/wrapper. Unlike Gill/Hutton, we manipulate the body of the worker into the right form then apply the lemma.

**Definition**
\[
\text{nub-body}' :: (R \rightarrow \text{Nat list}) \rightarrow R \rightarrow \text{Nat list}
\text{where}
\text{nub-body}' \equiv \Lambda f r. \ \text{case a2c \cdot r of lnil \Rightarrow lnil}
\text{| x ::@ x \Rightarrow x ::@ f \cdot (c2a \cdot (\text{lfilter} \cdot (neg \circ o \cdot (\Lambda y. \ x =_B y))) \cdot x)}
\]

**Lemma nub-body-nub-body'-eq:** \( \text{unwrap} \circ \text{nub-body} \circ \text{unwrap} = \text{nub-body}' \)
\begin{proof}

definition nub-body'' :: (R \rightarrow \text{Nat list}) \rightarrow R \rightarrow \text{Nat list} where
nub-body'' \equiv \Lambda f r. \text{case nextR} r \text{ of Nothing} \Rightarrow \text{lnil}
| \text{Just}(x, xs) \Rightarrow x :@ f \cdot (c2a \cdot (\text{lfilter} \cdot (\text{neg oo} \cdot (\Lambda y. x =_B y)) \cdot (a2c \cdot xs)))

lemma nub-body'\text{-}nub-body''\text{-eq}: nub-body' = nub-body''
\end{proof}

\begin{proof}

definition nub-body''\text{'} :: (R \rightarrow \text{Nat list}) \rightarrow R \rightarrow \text{Nat list} where
nub-body''\text{'} \equiv (\Lambda f r. \text{case nextR} r \text{ of Nothing} \Rightarrow \text{lnil}
| \text{Just}(x, xs) \Rightarrow x :@ f \cdot (\text{filterR} \cdot x \cdot xs))

lemma nub-body''\text{'-}nub-body''\text{''-eq}: nub-body''\text{'} = nub-body''\text{''} \text{ oo } (\text{unwrap oo wrap})
\end{proof}

Finally glue it all together.

\begin{proof}

lemma nub-wrap-nub-body''\text{'}: nub = wrap \cdot (\text{fix} \cdot nub-body''\text{''})
\end{proof}

end

11 Optimise “last”.

Andy Gill’s solution, mechanised. No fusion, works fine using their rule.

11.1 The last function.

fixrec llast :: 'a list \rightarrow 'a
where
llast.(x :@ yys) = (case yys of \text{lnil} \Rightarrow x | y :@ ys \Rightarrow llast\cdot yys)

lemma llast-strict[simp]: llast.\bot = \bot
\end{proof}

fixrec llast-body :: ('a list \rightarrow 'a) \rightarrow 'a list \rightarrow 'a
where
llast-body.f.(x :@ yys) = (case yys of \text{lnil} \Rightarrow x | y :@ ys \Rightarrow f \cdot yys)

lemma llast-llast-body: llast = fix-llast-body
\end{proof}

definition wrap :: ('a \rightarrow 'a list \rightarrow 'a) \rightarrow ('a list \rightarrow 'a)
where
wrap \equiv \Lambda f \cdot (x :@ xs). f \cdot x \cdot xs
**definition** \textit{unwrap} :: ('a list → 'a) → ('a → 'a list → 'a) where \textit{unwrap} ≡ Λ f x xs. f·(x :@ xs)

**lemma** \textit{unwrap-strict}[simp]: \textit{unwrap}·⊥ = ⊥

**lemma** \textit{wrap-unwrap-ID}: \textit{wrap} oo \textit{unwrap} oo \textit{llast-body} = \textit{llast-body}

**definition** \textit{llast-worker} :: ('a → 'a list → 'a) → 'a → 'a list → 'a where \textit{llast-worker} ≡ Λ r x yys. \text{case} yys of \textit{lnil} ⇒ x | x :@ ys ⇒ r·y·ys

**definition** \textit{llast'} :: 'a list → 'a where \textit{llast'} ≡ \textit{wrap}·(fix-\textit{llast-worker})

**lemma** \textit{llast-worker-llast-body}: \textit{llast-worker} = \textit{unwrap} oo \textit{llast-body} oo \textit{wrap}

**lemma** \textit{llast'‐llast}: \textit{llast'} = \textit{llast} (is ?lhs = ?rhs)

**end**

12 Concluding remarks

Gill and Hutton provide two examples of fusion: accumulator introduction in their §4, and the transformation in their §7 of an interpreter for a language with exceptions into one employing continuations. Both involve strict \textit{unwrap}s and are indeed totally correct.

The example in their §5 demonstrates the unboxing of numerical computations using a different worker/wrapper rule and does not require fusion. In their §6 a non-strict \textit{unwrap} is used to memoise functions over the natural numbers using the rule considered here. It should in fact use the same rule as the unboxing example as the scheme only correctly memoises strict functions. We can see this by considering a base case missing from their inductive proof, viz that if \textit{f} :: Nat → a is not strict – in fact constant, as Nat is a flat domain – then \textit{f}·⊥ ≠ ⊥ = (map \textit{f} [0..]) !! ⊥, where \textit{xs} !! \textit{n} is the \textit{n}th element of \textit{xs}.

References


