# Shivers’ Control Flow Analysis

Joachim Breitner

May 28, 2015

## Abstract

In his dissertation [3], Olin Shivers introduces a concept of control flow graphs for functional languages, provides an algorithm to statically derive a safe approximation of the control flow graph and proves this algorithm correct. In this research project [1], Shivers’ algorithms and proofs are formalized using the HOLCF extension of the logic HOL in the theorem prover Isabelle.

## Contents

I. The definitions

1. Syntax

2. Standard semantics

3. Exact nonstandard semantics

4. Abstract nonstandard semantics

II. The main results

5. The exact call cache is a map
   5.1. Preparations
   5.2. The proof

6. The abstract semantics is correct
   6.1. Abstraction functions
   6.2. Lemmas about abstraction functions
   6.3. Approximation relation
   6.4. Lemmas about the approximation relation
First, we define the syntax tree of a program in our toy functional language, using continuation passing style, corresponding to section 3.2 in Shivers’ dissertation.

We assume that the program to be investigated is already parsed into a syntax tree. Furthermore, we assume that distinct labels were added to distinguish different code positions and that the program has been alphatised, i.e. that each variable name is only
bound once. This binding position is, as a convenience, considered part of the variable name.

\[\text{type-synonym} \ label = \text{nat} \]
\[\text{type-synonym} \ var = \ label \times \text{string} \]

\[\text{definition} \ binder :: \ var \Rightarrow \ label \ \text{where} \ [\text{simp}]: \ binder \ v = \text{fst} \ v \]

The syntax consists now of lambda abstractions, call expressions and values, which can either be lambdas, variable references, constants or primitive operations. A program is a lambda expression.

Shivers’ language has as the set of basic values integers plus a special value for false. We simplified this to just the set of integers. The conditional \text{If} considers zero as false and any other number as true.

Shivers also restricts the values in a call expression: No constant maybe be used as the called value, and no primitive operation may occur as an argument. This restriction is dropped here and just leads to runtime errors when evaluating the program.

\[\text{datatype} \ prim = \text{Plus label} \mid \text{If label label} \]
\[\text{datatype} \ lambda = \Lambda label \ \text{var list call} \]
\[\text{and} \ \text{call} = \text{App label val val list} \]
\[\text{and} \ \text{val} = \text{L lambda} \mid \text{R label var} \mid \text{C label int} \mid \text{P prim} \]

\[\text{datatype-compat} \ \text{lambda call val} \]

\[\text{type-synonym} \ prog = \text{lambda} \]

\[\text{lemmas} \ \text{mutual-lambda-call-var-inducts} =\]
\[\text{compat-lambda.induct} \]
\[\text{compat-call.induct} \]
\[\text{compat-val.induct} \]
\[\text{compat-val-list.induct} \]
\[\text{compat-nat-char-list-prod-lambda-prod-list.induct} \]
\[\text{compat-nat-char-list-prod-lambda-prod.induct} \]

Three example programs. These were generated using the Haskell implementation of Shivers’ algorithm that we wrote as a prototype[2].

\[\text{abbreviation} \ ex1 == (\Lambda 1 [(1,"cont'"))(\text{App} 2 (\text{R} 3 (1,"cont'"))(\text{C} 4 0)) \]
\[\text{abbreviation} \ ex2 == (\Lambda 1 [(1,"cont'"))(\text{App} 2 (\text{P} (\text{Plus} 3)) [(\text{C} 4 1), (\text{C} 5 1), (\text{R} 6 (1,"cont'")))]) \]
\[\text{abbreviation} \ ex3 == (\Lambda 1 [(1,"cont'"))(\text{Let} 2 [(2,"rec'"),(\text{Lambda} 3 [(3,"p'"),(3,"i'"),(3,"c'"))(\text{App} 4 (\text{P} (\text{If} 5 6))(\text{R} 7 (3,"i'")), (\text{L} (\text{Lambda} 8 ))) (\text{App} 9 (\text{P} (\text{Plus} 10))(\text{R} 11 (3,"p'")), (\text{R} 12 (3,"i'")), (\text{L} (\text{Lambda} 13 [13,"p'"])) (\text{App} 14 (\text{P} (\text{Plus} 15))(\text{R} 16 (3,"i'")), (\text{C} 17 (\text{C} 4 0)))](\text{App} 19 (\text{R} 20 (2,"rec'"))(\text{R} 21 (13,"p'")))) \}

3
2. Standard semantics

theory Eval
  imports HOLCF HOLCFUtils CPSScheme
begin

We begin by giving the standard semantics for our language. Although this is not actually used to show any results, it is helpful to see that the later algorithms “look similar” to the evaluation code and the relation between calls done during evaluation and calls recorded by the control flow graph.

We follow the definition in Figure 3.1 and 3.2 of Shivers’ dissertation, with the clarifications from Section 4.1. As explained previously, our set of values encompasses just the integers, there is no separate value for \textit{false}. Also, values and procedures are not distinguished by the type system.

Due to recursion, one variable can have more than one currently valid binding, and due to closures all bindings can possibly be accessed. A simple call stack is therefore not sufficient. Instead we have a \textit{contour counter}, which is increased in each evaluation step. It can also be thought of as a time counter. The variable environment maps tuples of variables and contour counter to values, thus allowing a variable to have more than one active binding. A contour environment lists the currently visible binding for each binding position and is preserved when a lambda expression is turned into a closure.

\begin{verbatim}
  type-synonym contour = nat
  type-synonym benv = label -> contour
  type-synonym closure = lambda × benv

  The set of semantic values consist of the integers, closures, primitive operations and a special value \textit{Stop}. This is passed as an argument to the program and represents the terminal continuation. When this value occurs in the first position of a call, the program terminates.

  datatype d = DI int
  | DC closure
  | DP prim
  | Stop

  type-synonym venv = var × contour → d
\end{verbatim}
The function $A$ evaluates a syntactic value into a semantic datum. Constants and
primitive operations are left untouched. Variable references are resolved in two stages:
First the current binding contour is fetched from the binding environment $\beta$, then the
stored value is fetched from the variable environment $ve$. A lambda expression is bundled
with the current contour environment to form a closure.

```
fun $evalV :: val \Rightarrow benv \Rightarrow venv \Rightarrow d (A)
where $A (C - i) \beta ve = DI i
| $A (P prim) \beta ve = DP prim
| $A (R - var) \beta ve =
  (case $\beta (binder var) of
    Some l \Rightarrow (case ve (var,l) of Some d \Rightarrow d))
| $A (L lam) \beta ve = DC (lam, \beta)
```

The answer domain of our semantics is the set of integers, lifted to obtain an additional
element denoting bottom. Shivers distinguishes runtime errors from non-termination.
Here, both are represented by $\bot$.

```
type-synonym ans = int lift
```

To be able to do case analysis on the custom datatypes $lambda$, $d$, $call$ and $prim$ inside
a function defined with $fixrec$, we need continuity results for them. These are all of the
same shape and proven by case analysis on the discriminator.

```
lemma cont2cont-case-lambda [simp, cont2cont]:
  assumes $\forall a b c. cont (\lambda x. f x a b c)$
  shows $cont (\lambda x. case-lambda (f x) l)$
  ⟨proof⟩

lemma cont2cont-case-d [simp, cont2cont]:
  assumes $\forall y. cont (\lambda x. f1 x y)$
    and $\forall y. cont (\lambda x. f2 x y)$
    and $\forall y. cont (\lambda x. f3 x y)$
    and $cont (\lambda x. f4 x)$
  shows $cont (\lambda x. case-d (f1 x) (f2 x) (f3 x) (f4 x) d)$
  ⟨proof⟩

lemma cont2cont-case-call [simp, cont2cont]:
  assumes $\forall a b c. cont (\lambda x. f1 x a b c)$
    and $\forall a b c. cont (\lambda x. f2 x a b c)$
  shows $cont (\lambda x. case-call (f1 x) (f2 x) c)$
  ⟨proof⟩

lemma cont2cont-case-prim [simp, cont2cont]:
  assumes $\forall y. cont (\lambda x. f1 x y)$
    and $\forall y z. cont (\lambda x. f2 x y z)$
  shows $cont (\lambda x. case-prim (f1 x) (f2 x) p)$
  ⟨proof⟩
```
As usual, the semantics of a functional language is given as a denotational semantics. To that end, two functions are defined here: \( \mathcal{F} \) applies a procedure to a list of arguments. Here closures are unwrapped, the primitive operations are implemented and the terminal continuation \( \text{Stop} \) is handled. \( \mathcal{C} \) evaluates a call expression, either by evaluating procedure and arguments and passing them to \( \mathcal{F} \), or by adding the bindings of a \( \text{Let} \) expression to the environment.

Note how the contour counter is incremented before each call to \( \mathcal{F} \) or when a \( \text{Let} \) expression is evaluated.

With mutually recursive equations, such as those given here, the existence of a function satisfying these is not obvious. Therefore, the \texttt{fixrec} command from the HOLCF package is used. This takes a set of equations and builds a functional from that. It mechanically proofs that this functional is continuous and thus a least fixed point exists. This is then used to define \( \mathcal{F} \) and \( \mathcal{C} \) and proof the equations given here. To use the HOLCF setup, the continuous function arrow \( \rightarrow \) with application operator \( \cdot \) is used and our types are wrapped in \texttt{discr} and \texttt{lift} to indicate which partial order is to be used.

\begin{verbatim}
type-synonym fstate = (d x d list x venv x contour)
type-synonym cstate = (call x benv x venv x contour)

fixrec evalF :: fstate discr → ans (F)
  and evalC :: cstate discr → ans (C)
  where evalF::fstate = (case undiscr fstate of
    (DC (Lambda lab vs c, β), as, ve, b) ⇒
      (if length vs = length as
      then let β' = β (lab ↦→ b);
        ve' = map-upds ve (map (λv.(v,b)) vs) as
        in C·(Discr (c,β',ve',b))
      else ⊥)
    | (DP (Plus c),[DI a1, DI a2, cnt],ve,b) ⇒
      let b' = Suc b;
        β = [c ↦→ b]
      in F·(Discr (cnt,[DI (a1 + a2)],ve,b'))
    | (DP (prim.If ct cf),[DI v, contt, contf],ve,b) ⇒
      (if v ≠ 0
      then let b' = Suc b;
        β = [ct ↦→ b]
      in F·(Discr (contt,[],ve,b'))
      else let b' = Suc b;
        β = [cf ↦→ b]
      in F·(Discr (contf,[],ve,b')))
    | (Stop,[DI i],-,-) ⇒ Def i
    | - ⇒ ⊥
  )
  | C·cstate = (case undiscr cstate of
    (App lab f vs,β,ve,b) ⇒
\end{verbatim}
let \( f' = A f \beta ve; \)
\( as = map (\lambda v. A v \beta ve) vs; \)
\( b' = Suc b \)
in \( F.(Discr (f', as, ve, b')) \)
\( \) (Let \( lab \) \( ls \) \( c', \beta, ve, b' \) \( \Rightarrow \)
let \( b' = Suc b; \)
\( \beta' = \beta (lab \mapsto b'); \)
\( ve' = ve ++ map-of (map (\lambda (v, l). (\lambda v. (L l) \beta' ve)) ls) \)
in \( C.(Discr (c', \beta', ve', b')) \)
\)

To evaluate a full program, it is passed to \( F \) with proper initializations of the other arguments. We test our semantics function against two example programs and observe that the expected value is returned.

**definition** evalCPS :: prog \( \Rightarrow \) ans \((PR)\)
where \( PR \) \( l \) = (let \( ve = empty; \)
\( \beta = empty; \)
\( f = A (L l) \beta ve \)
in \( F.(Discr (f,[Stop], ve, 0)) \))

**lemma** correct-ex1: \( PR \) \( ex1 = Def 0 \)
(\( proof \))

**lemma** correct-ex2: \( PR \) \( ex2 = Def 2 \)
(\( proof \))

3. Exact nonstandard semantics

**theory** ExCF
**imports** HOLCF HOLCFUtils CPSScheme Utils
**begin**

We now alter the standard semantics given in the previous section to calculate a control flow graph instead of the return value. At this point, we still “run” the program in full, so this is not yet the static analysis that we aim for. Instead, this is the reference for the correctness proof of the static analysis: If an edge is recorded here, we expect it to be found by the static analysis as well.

In preparation of the correctness proof we change the type of the contour counters. Instead of plain natural numbers as in the previous sections we use lists of labels, remembering at each step which part of the program was just evaluated.
Note that for the exact semantics, this is information is not used in any way and it would have been possible to just use natural numbers again. This is reflected by the preorder instance for the contours which only look at the length of the list, but not the entries.

\textbf{definition} contour = (UNIV::label list set)

\textbf{typedef} contour = contour

(\textit{proof})

\textbf{definition} initial-contour (b\textsubscript{0})
where b\textsubscript{0} = Abs-contour []

\textbf{definition} nb
where nb b c = Abs-contour (c ≠ Rep-contour b)

\textbf{instantiation} contour :: preorder
begin
\textbf{definition} le-contour-def: b ≤ b′ ←→ length (Rep-contour b) ≤ length (Rep-contour b′)
\textbf{definition} less-contour-def: b < b′ ←→ length (Rep-contour b) < length (Rep-contour b′)
\textbf{instance} (\textit{proof})
end

Three simple lemmas helping Isabelle to automatically prove statements about contour numbers.

\textbf{lemma} nb-le-less[iff]: nb b c ≤ b′ ←→ b < b′
(\textit{proof})

\textbf{lemma} nb-less[iff]: b′ < nb b c ←→ b′ ≤ b
(\textit{proof})

\textbf{declare} less-imp-le[where 'a = contour, intro]

The other types used in our semantics functions have not changed.

\textbf{type-synonym} benv = label ↦ contour
\textbf{type-synonym} closure = \textit{lambda} × benv

\textbf{datatype} d = DI int
| DC closure
| DP prim
| Stop

\textbf{type-synonym} venv = var × contour → d

As we do not use the type system to distinguish procedural from non-procedural values, we define a predicate for that.

\textbf{primrec} isProc
where $\text{isProc} \ (\text{DI} -) = \text{False}$
| $\text{isProc} \ (\text{DC} -) = \text{True}$
| $\text{isProc} \ (\text{DP} -) = \text{True}$
| $\text{isProc} \ \text{Stop} = \text{True}$

To please HOLCF, we declare the discrete partial order for our types:

instantiation $\text{contour} :: \text{discrete-cpo}$
begin
definition $\text{[simp]}$: $(x :: \text{contour}) \sqsubseteq y \iff x = y$
instance $\langle \text{proof} \rangle$
end

instantiation $d :: \text{discrete-cpo}$ begin
definition $\text{[simp]}$: $(x :: d) \sqsubseteq y \iff x = y$
instance $\langle \text{proof} \rangle$
end

instantiation $\text{call} :: \text{discrete-cpo}$ begin
definition $\text{[simp]}$: $(x :: \text{call}) \sqsubseteq y \iff x = y$
instance $\langle \text{proof} \rangle$
end

The evaluation function for values has only changed slightly: To avoid worrying about incorrect programs, we return zero when a variable lookup fails. If the labels in the program given are correct, this will not happen. Shivers makes this explicit in Section 4.1.3 by restricting the function domains to the valid programs. This is omitted here.

fun $\text{evalV} :: \text{val} \Rightarrow \text{benv} \Rightarrow \text{venv} \Rightarrow d \ (A)$
where $A \ (C \ - \ i) \ \beta \ \text{ve} = \text{DI} \ i$
| $A \ (P \ \text{prim}) \ \beta \ \text{ve} = \text{DP} \ \text{prim}$
| $A \ (R \ - \ \text{var}) \ \beta \ \text{ve} =$
  $(\text{case} \ \beta \ (\text{binder} \ \text{var}) \ \text{of} \\    \text{Some} \ \text{l} \Rightarrow (\text{case} \ \text{ve} \ (\text{var,} \ l) \ \text{of} \ \text{Some} \ \text{d} \Rightarrow d \ | \ \text{None} \Rightarrow \text{DI} \ 0) \\    | \ \text{None} \Rightarrow \text{DI} \ 0) \\    | \ A \ (L \ \text{lam}) \ \beta \ \text{ve} = \text{DC} \ (\text{lam,} \ \beta$)

To be able to do case analysis on the custom datatypes $\text{lambda}$, $d$, $\text{call}$ and $\text{prim}$ inside a function defined with $\text{fixrec}$, we need continuity results for them. These are all of the same shape and proven by case analysis on the discriminator.

lemma $\text{cont2cont-case-lambda} \ [\text{simp, cont2cont}]$
  assumes $\wedge a \ b \ c. \ \text{cont} \ (\lambda x. \ f \ x \ a \ b \ c)$
  shows $\text{cont} \ (\lambda x. \ \text{case-lambda} \ (f \ x) \ l)$
(proof)

lemma $\text{cont2cont-case-d} \ [\text{simp, cont2cont}]$
  assumes $\wedge y. \ \text{cont} \ (\lambda x. \ f1 \ x \ y)$
  and $\wedge y. \ \text{cont} \ (\lambda x. \ f2 \ x \ y)$
and \( \forall y. \) cont \((\lambda x. f_3 x y)\)
and cont \((\lambda x. f_4 x)\)
shows cont \((\lambda x. \text{case-d} (f_1 x) (f_2 x) (f_3 x) (f_4 x) d)\)
(proof)

lemma cont2cont-case-call [simp, cont2cont]:
assumes \( \forall a \ b \ c.\) cont \((\lambda x. f_1 x \ a \ b \ c)\)
and \( \forall a \ b \ c.\) cont \((\lambda x. f_2 x \ a \ b \ c)\)
shows cont \((\lambda x. \text{case-call} (f_1 x) (f_2 x) c)\)
(proof)

lemma cont2cont-case-prim [simp, cont2cont]:
assumes \( \forall y.\) cont \((\lambda x. f_1 x \ y)\)
and \( \forall y \ z.\) cont \((\lambda x. f_2 x \ y \ z)\)
shows cont \((\lambda x. \text{case-prim} (f_1 x) (f_2 x) p)\)
(proof)

Now, our answer domain is not any more the integers, but rather call caches. These are represented as sets containing tuples of call sites (given by their label) and binding environments to the called value. The argument types are unaltered.

In the functions \( F \) and \( C \), upon every call, a new element is added to the resulting set. The \( \text{STOP} \) continuation now ignores its argument and returns the empty set instead. This corresponds to Figure 4.2 and 4.3 in Shivers’ dissertation.

type-synonym ccache = ((label \times \text{benv}) \times d) \text{set}
type-synonym ans = ccache
type-synonym fstate = (d \times d \text{list} \times \text{venv} \times \text{contour})
type-synonym cstate = (\text{call} \times \text{benv} \times \text{venv} \times \text{contour})

fixrec evalF :: fstate discr \rightarrow ans (\text{F})
and evalC :: cstate discr \rightarrow ans (\text{C})
where \( \text{F-fstate} = (\text{case undiscr fstate of} \)
\((\text{DC (Lambda lab vs c, } \beta, \text{ as, ve, b)}) \Rightarrow \)
\((\text{if length vs = length as}\)
\(\text{then let } \beta' = \beta (\text{lab } \mapsto b); \)
\(\text{ve'} = \text{map-upds ve (map (lambda v. } (v,b)) \text{ vs) as}\)
\(\text{in C.(Discr (c,} \beta', \text{ve',b)})\)
else \(\bot\))
\((\text{DP (Plus c),[DI a1, DI a2, cnt],ve,b)}) \Rightarrow \)
\((\text{if isProc cnt}\)
\(\text{then let b'} = \text{nb b c;}\)
\(\beta = [c \mapsto b]\)
\(\text{in F.(Discr (cnt,[DI (a1 + a2)],ve,b'))}\)
\(\cup \{((c,} \beta),\text{cnt}\})\)
else \(\bot\))
\((\text{DP (prim.If ct cf),[DI v, contt, conf],ve,b)}) \Rightarrow \)
(if isProc contt \land isProc contf
then
  (if v \neq 0
  then let b' = nb b ct;
  \beta = [ct \mapsto b]
  in (F.(Discr (contt,[],ve,b'))
  \cup \{((ct, \beta),contt)\})
  else let b' = nb b cf;
  \beta = [cf \mapsto b]
  in (F.(Discr (contf,[],ve,b')))
  \cup \{((cf, \beta),contf)\})
else \bot)
| (Stop,[DI i],\_,\_) \Rightarrow \{\}
| \_ \Rightarrow \bot
)

| C-estate = (case undiscr estate of
| (App lab f vs,\beta,ve,b) \Rightarrow

| let f' = A f \beta ve;
| as = map (\lambda v. A v \beta ve) vs;
| b' = nb b lab
| in if isProc f'
| then F.(Discr (f',as,ve,b')) \cup \{((lab, \beta),f')\}
| else \bot
| (Let lab ls c',\beta,ve,b) \Rightarrow

| let b' = nb b lab;
| \beta' = \beta (lab \mapsto b');
| ve' = ve ++ map-of (map (\lambda (v,l). ((v,b'), A (L l) \beta' ve)) ls)
| in C.(Discr (c',\beta',ve',b'))
)

In preparation of later proofs, we give the cases of the generated induction rule names
and also create a large rule to deconstruct the an value of type jstate into the various
cases that were used in the definition of F.

lemmas evalF-evalC-induct = evalF-evalC.induct[case-names Admissibility Bottom Next]

lemmas cl-cases = prod.exhaust[OF lambda.exhaust, of - \lambda a - . a]

lemmas ds-cases-plus = list.exhaust[
  OF - d.exhaust, of - - \lambda a - a,
  OF - list.exhaust, of - - \lambda - x - , x,
  OF - d.exhaust, of - - \lambda - - a - a,
  OF - list.exhaust,of - - \lambda - - x - x,
  OF - list.exhaust of - - \lambda - - - - - x. x
]

lemmas ds-cases-if = list.exhaust[OF - d.exhaust, of - - \lambda a - a,
  OF - list.exhaust[OF - list.exhaust[OF - list.exhaust, of - - \lambda - x. x], of - - \lambda - x. x], of - - \lambda - x - x]

lemmas ds-cases-stop = list.exhaust[OF - d.exhaust, of - - \lambda a - a,
  OF - list.exhaust, of - - \lambda - x. x]
lemmas fstate-case = prod-cases[\ OF d.exhaust, of - \ x - - - , x,
  OF - cl-cases prim.exhaust, of - \ \ y - - - - a \ a \ y - - - - a, a,
  OF - case-split ds-cases-plus ds-cases-if ds-cases-stop,
  of - \ y- as - - - - - vs - . length vs = length as \ ds - - - - ds \ y - ds - - - - ds \ y - ds - - - - ds,
  case-names x Closure y x x Plus x x x x x x x x x x If-True If-False x x x x x
]

The exact semantics of a program again uses $\mathcal{F}$ with properly initialized arguments. For
the first two examples, we see that the function works as expected.

definition evalCPS :: prog $\Rightarrow$ ans (PR)
  where PR l = (let ve = empty;
    $\beta$ = empty;
    $f$ = A (L l) $\beta$ ve
  in $\mathcal{F}$:(Discr ($f$,Stop,ve,b0)))

lemma correct-ex1: PR ex1 = {((2,[1 $\mapsto$ b0]), Stop)}
(proof)

lemma correct-ex2: PR ex2 = {((2, [1 $\mapsto$ b0]), DP (Plus 3)),
  ((3, [3 $\mapsto$ nb b0 2]), Stop)}
(proof)

end

4. Abstract nonstandard semantics

theory AbsCF
  imports HOLCF HOLCFUtils CPSScheme Utils SetMap
begin

default-sort type

After having defined the exact meaning of a control graph, we now alter the algorithm
into a statically computable. We note that the contour pointer in the exact semantics is
taken from an infinite set. This is unavoidable, as recursion depth is unbounded. But if
this were not the case and the set were finite, the function would be calculable, having
finite range and domain.

Therefore, we make the set of contour counter values finite and accept that this makes
our result less exact, but calculable. We also do not work with values any more but only
remember, for each variable, what possible lambdas can occur there. Because we do not
have exact values any more, in a conditional expression, both branches are taken.

We want to leave the exact choice of the finite contour set open for now. Therefore, we
define a type class capturing the relevant definitions and the fact that the set is finite. Isabelle expects type classes to be non-empty, so we show that the unit type is in this type class.

```lean
class contour = finite +
  fixes nba :: 'a ⇒ label ⇒ 'a (nba)
  and a-initial-contour :: 'a (n0)

instantiation unit :: contour
begin
  definition nba - = ()
  definition n0 = ()
  instance ⟨proof⟩
end
```

Analogous to the previous section, we define types for binding environments, closures, procedures, semantic values (which are now sets of possible procedures) and variable environment. Their types are parametrized by the chosen set of abstract contours.

The abstract variable environment is a partial map to sets in Shivers’ dissertation. As he does not need to distinguish between a key not in the map and a key mapped to the empty set, this presentation is redundant. Therefore, I encoded this as a function from keys to sets of values. The theory SetMap contains functions and lemmas to work with such maps, symbolized by an appended dot (e.g. {}, ∪).

```lean
type-synonym 'c a-benv = label ⇒ 'c (- benv [1000])
type-synonym 'c a-closure = lambda × 'c benv (- closure [1000])
datatype 'c proc (- proc [1000])
  = PC 'c closure
  | PP prim
  | AStop
type-synonym 'c a-d = 'c proc set (- d [1000])
type-synonym 'c a-venv = var × 'c ⇒ 'c d (- venv [1000])
```

The evaluation function now ignores constants and returns singletons for primitive operations and lambda expressions.

```lean
fun evalV-a :: val ⇒ 'c benv ⇒ 'c venv ⇒ 'c d (A)
  where A (C - i) β ve = {}
  | A (P prim) β ve = {PP prim}
  | A (R - var) β ve =
    (case β (binder var) of
      Some l ⇒ ve (var,l)
    | None ⇒ {})
```
\[ \hat{A} (L \text{ lam} \beta \text{ ve} = \{PC (\text{lam}, \beta)\} \]

The types of the calculated graph, the arguments to \( \hat{F} \) and \( \hat{C} \) resemble closely the types in the exact case, with each type replaced by its abstract counterpart.

\[
\begin{align*}
\text{type-synonym} \ 'c\ a-ccache &= (('c\ label \times 'c\ benv) \times 'c\ proc)\ set\ (\cdot\ ccache\ [1000]) \\
\text{type-synonym} \ 'c\ a-ans &= 'c\ ccache\ (\cdot\ ans\ [1000]) \\
\text{type-synonym} \ 'c\ a-fstate &= ('c\ proc \times 'c\ venv)\ set\ (\cdot\ fstate\ [1000]) \\
\text{type-synonym} \ 'c\ a-cstate &= (\cdot\ call \times 'c\ benv \times 'c\ venv)\ set\ (\cdot\ cstate\ [1000])
\end{align*}
\]

And yet again, cont2cont results need to be shown for our custom data types.

\[
\begin{align*}
\text{lemma} \ cont2cont-case-lambda \ [\text{simp, cont2cont}]: \\
&\text{assumes } \lambda a\ b\ c.\ \text{cont} (\lambda x\ . f\ x\ a\ b\ c) \\
&\text{shows } \text{cont} (\lambda x.\ \text{case-lambda} (f\ x)\ l) \\
&\text{⟨proof}⟩
\end{align*}
\]

\[
\begin{align*}
\text{lemma} \ cont2cont-case-proc \ [\text{simp, cont2cont}]: \\
&\text{assumes } \lambda y.\ \text{cont} (\lambda x.\ f1\ x\ y) \\
&\text{and } \lambda y.\ \text{cont} (\lambda x.\ f2\ x\ y) \\
&\text{and } \text{cont} (\lambda x.\ f3\ x) \\
&\text{shows } \text{cont} (\lambda x.\ \text{case-proc} (f1\ x)\ (f2\ x)\ (f3\ x)\ d) \\
&\text{⟨proof}⟩
\end{align*}
\]

\[
\begin{align*}
\text{lemma} \ cont2cont-case-call \ [\text{simp, cont2cont}]: \\
&\text{assumes } \lambda a\ b\ c.\ \text{cont} (\lambda x.\ f1\ x\ a\ b\ c) \\
&\text{and } \lambda a\ b\ c.\ \text{cont} (\lambda x.\ f2\ x\ a\ b\ c) \\
&\text{shows } \text{cont} (\lambda x.\ \text{case-call} (f1\ x)\ (f2\ x)\ c) \\
&\text{⟨proof}⟩
\end{align*}
\]

\[
\begin{align*}
\text{lemma} \ cont2cont-case-prim \ [\text{simp, cont2cont}]: \\
&\text{assumes } \lambda y.\ \text{cont} (\lambda x.\ f1\ x\ y) \\
&\text{and } \lambda y\ z.\ \text{cont} (\lambda x.\ f2\ x\ y\ z) \\
&\text{shows } \text{cont} (\lambda x.\ \text{case-prim} (f1\ x)\ (f2\ x)\ p) \\
&\text{⟨proof}⟩
\end{align*}
\]

We can now define the abstract nonstandard semantics, based on the equations in Figure 4.5 and 4.6 of Shivers’ dissertation. In the \( A Stop \) case, \( \{} \) is returned, while for wrong arguments, \( ⊥ \) is returned. Both actually represent the same value, the empty set, so this is just an aesthetic difference.

\[
\begin{align*}
\text{fixrec} \ a-evalF : 'c::contour \ fstate\ discr \rightarrow 'c\ \text{ans}\ (\hat{F}) \\
\text{and} \ a-evalC : 'c::contour \ cstate\ discr \rightarrow 'c\ \text{ans}\ (\hat{C}) \\
\text{where} \ \hat{F}\cdot\ fstate = (\text{case}\ \text{anddiscr}\ fstate\ of\ \\
&\quad (PC (\text{Lambda}\ lab\ vs\ c,\ β),\ as,\ ve,\ b) \Rightarrow \\
&\quad \quad (\text{if}\ \text{length}\ vs = \text{length}\ as \Rightarrow \\
&\quad \quad \quad \text{then let } β' = β (lab \mapsto b); \\
\end{align*}
\]

14
Again, we name the cases of the induction rule and build a nicer case analysis rule for arguments of type fstate.

lemmas a-evalF-evalC-induct = a-evalF-a-evalC.induct[case-names Admissibility Bottom Next]

fun a-evalF-cases
where a-evalF-cases (PC (Lambda lab vs c, β)) as ve b = undefined
| a-evalF-cases (PP (Plus cp)) [a1, a2, cnt] ve b = undefined
| a-evalF-cases (PP (prim.If cp1 cp2)) [ve,cnt,cntf] ve b = undefined
| a-evalF-cases AStop [v] ve b = undefined
lemmas a-fstate-case-x = a-evalF-cases.cases[
    OF case-split, of - λ- vs - - as - - . length vs = length as,
    case-names Closure Closure-inv Plus If Stop]

lemmas a-cl-cases = prod.exhaust[OF lambda.exhaust, of - λ a - . a]
lemmas a-ds-cases = list.exhaust[
    OF - list.exhaust, of - - λ- x. x,
    OF - - list.exhaust ,of - - λ- - - x. x ,
    OF - - - list.exhaust,of - - λ- - - - x. x ]
lemmas a-ds-cases-stop = list.exhaust[OF - list.exhaust, of - - λ- x. x]
lemmas a-fstate-case = prod-cases4[OF proc.exhaust, of - λx - - - . x,
    OF a-cl-cases prim.exhaust, of - λ - - - a . a - λ - - - a. a,
    OF case-split a-ds-cases a-ds-cases a-ds-cases-stop,
    of - λ- as - - - - vs - . length vs = length as - λ - ds - - - - . ds λ - ds - - - -. ds λ - ds - - . ds]

Not surprisingly, the abstract semantics of a whole program is defined using \( \widehat{F} \) with suitably initialized arguments. The function \( \text{the-elem} \) extracts a value from a singleton set. This works because we know that \( \hat{A} \) returns such a set when given a lambda expression.

definition evalCPS-a :: prog ⇒ ('c::contour) ans (\( \widehat{PR} \))
    where \( \widehat{PR} \) l = (let ve = \{\};
            \( \beta = \text{empty} ; \)
            \( f = \hat{A} (L l) \beta ve \)
            in \( \widehat{F}·(\text{Discr (the-elem f,}\{(\text{AStop})\},ve,\hat{b}_0)) \))
end

Part II.
The main results

5. The exact call cache is a map

theory ExCFSV
imports ExCF
begin

5.1. Preparations

Before we state the main result of this section, we need to define
• the set of binding environments occurring in a semantic value (which exists only if it is a closure),

• the set of binding environments in a variable environment, using the previous definition,

• the set of contour counters occurring in a semantic value and

• the set of contour counters occurring in a variable environment.

fun benv-in-d :: d ⇒ benv set
  where benv-in-d (DC ((l, β))) = {β}
       | benv-in-d d' = {}

definition benv-in-ve :: venv ⇒ benv set
  where benv-in-ve ve = \{benv-in-d d | d . d ∈ ran ve\}

fun contours-in-d :: d ⇒ contour set
  where contours-in-d (DC ((l, β))) = ran β
       | contours-in-d d' = {}

definition contours-in-ve :: venv ⇒ contour set
  where contours-in-ve ve = \{contours-in-d d | d . d ∈ ran ve\}

The following 6 lemmas allow us to calculate the above definition, when applied to constructs used in our semantics function, e.g. map updates, empty maps etc.

lemma benv-in-ve-upds:
  assumes eq-length: length vs = length ds
      and \∀ β ∈ benv-in-ve ve . Q β
      and \∀ d' ∈ set ds . \∀ β ∈ benv-in-d d' . Q β
  shows \∀ β ∈ benv-in-ve (ve(map (λv. (v, b'')) vs \serialization→ ds)). Q β
  (proof)

lemma benv-in-eval:
  assumes \∀ β' ∈ benv-in-ve ve . Q β'
      and Q β
  shows \∀ β ∈ benv-in-d (A v β ve). Q β
  (proof)

lemma contours-in-ve-empty[simp]: contours-in-ve empty = {}
  (proof)

lemma contours-in-ve-upds:
  assumes eq-length: length vs = length ds
      and \∀ b' ∈ contours-in-ve ve . Q b'
      and \∀ d' ∈ set ds . \∀ b' ∈ contours-in-d d' . Q b'
  shows \∀ b' ∈ contours-in-ve (ve(map (λv. (v, b'')) vs \serialization→ ds)). Q b'
  (proof)
lemma contours-in-ve-upds-binds:
  assumes ∀ b′ ∈ contours-in-ve ve. Q b′
  and ∀ b′ ∈ ran β′. Q b′
  shows ∀ b′ ∈ contours-in-ve (ve ++ map-of (map (λ(v,l). ((v,b′), A (L l) β′ ve))) bs). Q b′
⟨proof⟩

lemma contours-in-eval:
  assumes ∀ b′ ∈ contours-in-ve ve. Q b′
  and ∀ b′ ∈ ran β′. Q b′
  shows ∀ b′ ∈ contours-in-d (A f β ve). Q b′
⟨proof⟩

5.2. The proof

The set returned by \( \mathcal{F} \) and \( \mathcal{C} \) is actually a partial map from callsite/binding environment pairs to called values. The corresponding predicate in Isabelle is \emph{single-valued}.

We would like to show an auxiliary result about the contour counter passed to \( \mathcal{F} \) and \( \mathcal{C} \) (such that it is an unused counter when passed to \( \mathcal{F} \) and others) first. Unfortunately, this is not possible with induction proofs over fixed points: While proving the inductive case, one does not show results for the function in question, but for an information-theoretical approximation. Thus, any previously shown results are not available. We therefore intertwine the two inductions in one large proof.

This is a proof by fixpoint induction, so we have are obliged to show that the predicate is admissible and that it holds for the base case, i.e. the empty set. For the proof of admissibility, \emph{HOLCF} provides a number of introduction lemmas that, together with some additions in \emph{HOLCFUtils} and the continuity lemmas, mechanically proove admissibility. The base case is trivial.

The remaining case is the preservation of the properties when applying the recursive equations to a function known to have the desired property. Here, we break the proof into the various cases that occur in the definitions of \( \mathcal{F} \) and \( \mathcal{C} \) and use the induction hypotheses.

lemma cc-single-valued′:
  \[
  \begin{align*}
  \forall b′ ∈ contours-in-ve ve. b′ & < b \\
  \forall b′ ∈ contours-in-d d. b′ & < b \\
  \forall d′ ∈ set ds. \forall b′ ∈ contours-in-d d′. b′ & < b
  \end{align*}
  \Rightarrow
  \begin{align*}
  \text{single-valued} (\mathcal{F}(\Discr (d,ds,ve,b))) \\
  \land (\forall ((lab,\beta),t) ∈ \mathcal{F}(\Discr (d,ds,ve,b))). \exists b′. b′ ∈ \text{ran } \beta \land b \leq b′
  \end{align*}
\]
and $[ b \in \text{ran } \beta' \\
\forall b' \in \text{ran } \beta', b' \leq b \\
\forall b' \in \text{contours-in-ve } ve, b' \leq b ] \\
\Rightarrow \\
(\text{single-valued } (C \cdot (\text{Discr } (e, \beta', ve, b)))) \\
\land (\forall ((\text{lab}, \beta), t) \in C \cdot (\text{Discr } (e, \beta', ve, b)), \exists b', b' \in \text{ran } \beta \land b \leq b') \\
\langle \text{proof} \rangle \\
\text{lemma single-valued } (P \cdot R \prog) \\
\langle \text{proof} \rangle \\
\text{end}

6. The abstract semantics is correct

theory AbsCFCorrect
  imports AbsCF ExCF
begin

default-sort type

The intention of the abstract semantics is to safely approximate the real control flow. This means that every call recorded by the exact semantics must occur in the result provided by the abstract semantics, which in turn is allowed to predict more calls than actually done.

6.1. Abstraction functions

This relation is expressed by abstraction functions and approximation relations. For each of our data types, there is an abstraction function $\text{abs-<type>}$, mapping the value from the exact setup to the corresponding value in the abstract view. The approximation relation then expresses the fact that one abstract value of such a type is safely approximated by another.

Because we need an abstraction function for contours, we extend the $\text{contour}$ type class by the abstraction functions and two equations involving the $\text{nb}$ and $b_0$ symbols.

class contour-a = contour + 
  fixes abs-cnt :: contour $\Rightarrow \alpha$
  assumes abs-cnt-nb[simp]: $\text{abs-cnt}(\text{nb } b \text{ lab}) = \tilde{\text{nb}} (\text{abs-cnt } b) \text{ lab}$
  and abs-cnt-initial[simp]: $\text{abs-cnt}(b_0) = \tilde{b}_0$

instantiation unit :: contour-a
begin
definition abs-cnt - = ()
instance ⟨proof⟩
end

It would be unwieldly to always write out \(\text{abs-}<\text{type}>\ x\). We would rather like to write \(|x|\) if the type of \(x\) is known, as Shivers does it as well. Isabelle allows one to use the same syntax for different symbols. In that case, it generates more than one parse tree and picks the (hopefully unique) tree that typechecks.

Unfortunately, this does not work well in our case: There are eight \(\text{abs-}<\text{type}>\) functions and some expressions later have multiple occurrences of these, causing an exponential blow-up of combinations.

Therefore, we use a module by Christian Sternagel and Alexander Krauss for ad-hoc overloading, where the choice of the concrete function is done at parse time and immediately. This is used in the following to set up the the symbol \(|-|\) for the family of abstraction functions.

```plaintext
consts abs :: 'a ⇒ 'b (|-)

adhoc-overloading
abs abs-cnt

definition abs-benv :: benv ⇒ 'c::contour-a benv
  where abs-benv β = map-option abs-cnt o β

adhoc-overloading
abs abs-benv

primrec abs-closure :: closure ⇒ 'c::contour-a closure
  where abs-closure (l,β) = (l,|β|)

adhoc-overloading
abs abs-closure

primrec abs-d :: d ⇒ 'c::contour-a d
  where abs-d (DI i) = {}
    | abs-d (DP p) = {PP p}
    | abs-d (DC cl) = {PC |cl|}
    | abs-d (Stop) = {AStop}

adhoc-overloading
abs abs-d

definition abs-venv :: venv ⇒ 'c::contour-a venv
  where abs-venv ve = (λ(v,b-a). U {case ve (v,b) of Some d ⇒ |d| | None ⇒ {}} | b. |b| = b-a })

adhoc-overloading
```

20
6.2. Lemmas about abstraction functions

Some results about the abstraction functions.

**Lemma** `abs-benv-empty [simp]`: `|empty|` = `empty`

(proof)

**Lemma** `abs-benv-upd [simp]`: `|β(c→b)|` = `|β| (c `→` |b| )`

(proof)

**Lemma** `the-elem-is-Proc`:

- assumes `isProc cnt`
- shows `the-elem |cnt| ∈ |cnt|`

(proof)

**Lemma** `[simp]`: `|{|}|` = `{}` (proof)

**Lemma** `abs-cache-singleton [simp]`: `|{(c,β,d)}|` = `{((c, |β| ), p) | p. p ∈ |d|}`

(proof)

**Lemma** `abs-venv-empty [simp]`: `|empty|` = `{}`.

(proof)

6.3. Approximation relation

The family of relations defined here capture the notion of safe approximation.

21
consts approx :: 'a ⇒ 'a ⇒ bool (≈)

definition venv-approx :: 'c venv ⇒ 'c venv ⇒ bool
  where venv-approx = smap-less

adhoc-overloading
  approx venv-approx

definition ccache-approx :: 'c ccache ⇒ 'c ccache ⇒ bool
  where ccache-approx = less-eq

adhoc-overloading
  approx ccache-approx

definition d-approx :: 'c d ⇒ 'c d ⇒ bool
  where d-approx = less-eq

adhoc-overloading
  approx d-approx

definition ds-approx :: 'c d list ⇒ 'c d list ⇒ bool
  where ds-approx = list-all2 d-approx

adhoc-overloading
  approx ds-approx

inductive fstate-approx :: 'c fstate ⇒ 'c fstate ⇒ bool
  where [ ve ≅ ve'; ds ≅ ds' ]
    ⇒ fstate-approx (proc,ds,ve,b) (proc,ds',ve',b)

adhoc-overloading
  approx fstate-approx

inductive cstate-approx :: 'c cstate ⇒ 'c cstate ⇒ bool
  where [ ve ≅ ve' ] ⇒ cstate-approx (c,β,ve,b) (c,β,ve',b)

adhoc-overloading
  approx cstate-approx

6.4. Lemmas about the approximation relation

Most of the following lemmas reduce an approximation statement about larger structures, as they are occurring the semantics functions, to statements about the components.

lemma venv-approx-trans[trans]:
  fixes ve1 ve2 ve3 :: 'c venv
  shows [ ve1 ≃ ve2; ve2 ≃ ve3 ] ⇒ (ve1 ≃ ve3)
  ⟨proof⟩
lemma abs-venv-union: \(|ve1 ++ ve2| \subseteq |ve1| \cup |ve2|
\langle proof \rangle

lemma abs-venv-map-of-rev: \(|map-of (rev l)| \subseteq \cup. (map (\lambda (v,k). |[v \mapsto k]| ) l)
\langle proof \rangle

lemma abs-venv-map-of: \(|map-of l| \subseteq \cup. (map (\lambda (v,k). |[v \mapsto k]| ) l)
\langle proof \rangle

lemma abs-venv-singleton: |[(v,b) \mapsto d]| = \{ (v,b) := d \}.
\langle proof \rangle

lemma ccache-approx-empty[simp]:
  \begin{align*}
  \text{fixes } x :: 'c ccache \\
  \text{shows } \{ \} \subseteq x \\
  \langle proof \rangle
  \end{align*}

lemmas ccache-approx-trans[trans] = subset-trans[where \(a = ((\text{label } 'c benv) \times 'c p\text{roc}),
folded ccache-approx-def]
lemmas Un-mono-approx = Un-mono[where \(a = ((\text{label } 'c benv) \times 'c p\text{roc}), folded ccache-approx-def]
lemmas Un-upper1-approx = Un-upper1[where \(a = ((\text{label } 'c benv) \times 'c p\text{roc}), folded ccache-approx-def]
lemmas Un-upper2-approx = Un-upper2[where \(a = ((\text{label } 'c benv) \times 'c p\text{roc}), folded ccache-approx-def]

lemma abs-ccache-union: \(|c1 \cup c2| \subseteq |c1| \cup |c2|
\langle proof \rangle

lemma d-approx-empty[simp]: \{\} \subseteq (d::'c \tilde{d})
\langle proof \rangle

lemma ds-approx-empty[simp]: [] \subseteq []
\langle proof \rangle

6.5. Lemma 7

Shivers’ lemma 7 says that \(\hat{A}\) safely approximates \(A\).

lemma lemma7:
  \begin{align*}
  \text{assumes } |ve::venv| \subseteq ve-a \\
  \text{shows } |A f \beta ve| \subseteq \hat{A} f \beta |ve-a \\
  \langle proof \rangle
  \end{align*}
6.6. Lemmas 8 and 9

The main goal of this section is to show that \( \hat{\mathcal{F}} \) safely approximates \( \mathcal{F} \) and that \( \hat{\mathcal{C}} \) safely approximates \( \mathcal{C} \). This has to be shown at once, as the functions are mutually recursive and requires a fixed point induction. To that end, we have to augment the set of continuity lemmas.

**lemma** cont2cont-abs-ccache[cont2cont,simp]:
- **assumes** \( \text{cont } f \)
- **shows** \( \text{cont} (\lambda x. \text{abs-ccache}(f x)) \)

Shivers proves these lemmas using parallel fixed point induction over the two fixed points (the one from the exact semantics and the one from the abstract semantics). But it is simpler and equivalent to just do induction over the exact semantics and keep the abstract semantics functions fixed, so this is what I am doing.

**lemma** lemma89:
- **fixes** \( f\text{state-a} :: 'c::contour-a \hat{f\text{state}} \text{ and } c\text{state-a} :: 'c::contour-a \hat{c\text{state}} \)
- **shows** \( |f\text{state}| \leq f\text{state-a} \Rightarrow |\hat{\mathcal{F}} \cdot (\text{Discr } f\text{state})| \leq \hat{\mathcal{F}} \cdot (\text{Discr } f\text{state-a}) \)
- \( |c\text{state}| \leq c\text{state-a} \Rightarrow |\hat{\mathcal{C}} \cdot (\text{Discr } c\text{state})| \leq \hat{\mathcal{C}} \cdot (\text{Discr } c\text{state-a}) \)

And finally, we lift this result to \( \hat{\mathcal{P}\mathcal{R}} \) and \( \mathcal{P}\mathcal{R} \).

**lemma** lemma6: \( |\mathcal{P}\mathcal{R} l| \leq \hat{\mathcal{P}\mathcal{R}} l \)

And finally, we lift this result to \( \hat{\mathcal{P}\mathcal{R}} \) and \( \mathcal{P}\mathcal{R} \).

7. Generic Computability

**theory** Computability
**imports** HOLCF HOLCFUtils
**begin**

Shivers proves the computability of the abstract semantics functions only by generic and slightly simplified example. This theory contains the abstract treatment in Section 4.4.3. Later, we will work out the details apply this to \( \hat{\mathcal{P}\mathcal{R}} \).

7.1. Non-branching case

After the following lemma (which could go into Set-Interval), we show Shivers’ Theorem 10. This says that the least fixed point of the equation

\[
f x = g x \cup f (r x)
\]
is given by
\[ f \; x = \bigcup_{i \geq 0} g \; (r^i \; x). \]

The proof follows the standard proof of showing an equality involving a fixed point:
First we show that the right hand side fulfills the above equation and then show that
our solution is less than any other solution to that equation.

**lemma** *insert-greaterThan:*
\[
\text{insert} \; (\text{n::nat}) \; \{ \text{n<..} \} = \{ \text{n..} \}
\]

**lemma** *theorem10:*
\[
\text{fixes} \; g :: 'a::cpo \to 'b::type \; \text{set} \; \text{and} \; r :: 'a \to 'a
\]
\[
\text{shows} \; \text{fix} \cdot (\Lambda \; f \; x. \; g \cdot x \cup f \cdot (r \cdot x)) = (\Lambda \; x. \; (\bigcup \; i. \; g \cdot (r^i \cdot x)))
\]

7.2. Branching case

Actually, our functions are more complicated than the one above: The abstract semantics
functions recurse with multiple arguments. So we have to handle a recursive equation
of the kind
\[ f \; x = g \; x \cup \bigcup_{a \in R \; x} f \; r. \]

By moving to the power-set relatives of our function, e.g.
\[ g \; Y = \bigcup_{a \in A} g \; a \quad \text{and} \quad R \; Y = \bigcup_{a \in R} R \; a \]

the equation becomes
\[ f \; Y = g \; Y \cup f \; (R \; Y) \]

(which is shown in Lemma 11) and we can apply Theorem 10 to obtain Theorem 12.

We define the power-set relative for a function together with some properties.

**definition** *powerset-lift:*
\[
\text{powerset-lift} :: ('a::cpo \to 'b::type \; \text{set}) \to 'a \to 'b \; \text{set} \; ()
\]
\[
\text{where} \; f = (\Lambda \; S. \; \bigcup \; y \in S. \; f \cdot y)
\]

**lemma** *powerset-lift-singleton[simp]:*
\[
\text{f} \cdot \{ x \} = f \cdot x
\]

**lemma** *powerset-lift-union[simp]:*
\[
\text{f} \cdot (A \; \cup \; B) = f \cdot A \; \cup \; f \cdot B
\]

25
Lemma 11 shows that if a function satisfies the relation with the branching \( R \), its powerset function satisfies the powerset variant of the equation.

**Lemma 11:**

| fixes \( f :: 'a \rightarrow 'b set \) and \( g :: 'a \rightarrow 'b set \) and \( R :: 'a \rightarrow 'a set \)
| assumes \( \forall x. f \cdot x = g \cdot x \cup (\bigcup y \in R \cdot x. f \cdot y) \)
| shows \( f \cdot S = g \cdot S \cup f (R \cdot S) \)

Theorem 10 as it will be used in Theorem 12.

**Lemmas** theorem10ps = theorem10[if g r] for g r

Now we can show Lemma 12: If \( F \) is the least solution to the recursive power-set equation, then \( x \mapsto F \cdot x \) is the least solution to the equation with branching \( R \).

We fix the type variable \( 'a \) to be a discrete cpo, as otherwise \( x \mapsto \{ x \} \) is not continuous.

**Lemma 12:**

| fixes \( g :: 'a::discrete-cpo \rightarrow 'b::type set \) and \( R :: 'a \rightarrow 'a set \)
| assumes \( F \cdot fix: F = fix (\Lambda f x. g \cdot x \cup (\bigcup y \in R \cdot x. f \cdot y)) \)
| shows \( fix (\Lambda f x. g \cdot x \cup (\bigcup y \in R \cdot x. f \cdot y)) = (\Lambda x. F \cdot \{ x \}) \)

**end**

8. The abstract semantics is computable

**theory** AbsCFComp

**imports** AbsCF Computability FixTransform CPSUtils MapSets
begin

default-sort type

The point of the abstract semantics is that it is computable. To show this, we exploit the special structure of \( \hat{F} \) and \( \hat{C} \): Each call adds some elements to the result set and joins this with the results from a number of recursive calls. So we separate these two actions into separate functions. These take as arguments the direct sum of \( \hat{f}_{\text{state}} \) and \( \hat{c}_{\text{state}} \), i.e. we treat the two mutually recursive functions now as one.

\textit{abs-g} gives the local result for the given argument.

\begin{verbatim}
fixrec abs-g :: ('c::contour \hat{f}_{\text{state}} + 'c \hat{c}_{\text{state}}) discr \rightarrow 'c \hat{a}_{\text{ans}}
where abs-g-x = (case undiscr x of
    (Inl (PC (Lambda lab vs c, \beta), as, ve, b)) \Rightarrow 
        let
            b' = \hat{nb} b c;
            \beta = [c \mapsto b]
        in 
            \{(c, \beta, cont) | cont . cont \in cnts\}
    | (Inl (PP (Plus c), [-,cnts], ve, b)) \Rightarrow 
        let
            b' = \hat{nb} b c;
            \beta = [ct \mapsto b]
        in 
            \{(ct, \beta, cnt) | cnt . cnt \in cntts\}
    | (Inl (AStop), [-, -]) \Rightarrow \}
    | (Inl -) \Rightarrow ⊥
    | (Inr (App lab f vs \beta, ve, b)) \Rightarrow 
        let
            fs = \hat{A} f \beta ve;
            as = map (λv. \hat{A} v \beta ve) vs;
            b' = \hat{nb} b lab
        in 
            \{(l, \beta, f') | f' . f' \in fs\}
    | (Inr (Let lab ls c, as, ve, b)) \Rightarrow \}
)
\end{verbatim}

\textit{abs-R} gives the set of arguments passed to the recursive calls.

\begin{verbatim}
fixrec abs-R :: ('c::contour \hat{f}_{\text{state}} + 'c \hat{c}_{\text{state}}) discr \rightarrow ('c::contour \hat{f}_{\text{state}} + 'c \hat{c}_{\text{state}}) discr set
where abs-R-x = (case undiscr x of
    (Inl (PC (Lambda lab vs c, \beta), as, ve, b)) \Rightarrow 
        if length vs = length as then let
            \beta' = \beta (lab \mapsto b);
            ve' = ve \cup. (\cup. (map (λ(v,a). \{(v,b) := a\}) (zip vs as)))
    \end{verbatim}
Therefore, we define the set of possible procedures, of possible arguments to \( \hat{\text{proc-poss}} \).

AStop

The initial argument vector, as created by \( \hat{\text{PR}} \).

definition initial-r :: prog ⇒ ('c::contour fstate + 'c cstate) discr
  where initial-r prog = Discr (Inl
    (the-elem (\( \hat{\text{A}} \) (L prog) empty {}), [(AStop)], {}, \( \hat{\vec{b}}_0 \))

8.1. Towards finiteness

We need to show that the set of possible arguments for a given program \( p \) is finite. Therefore, we define the set of possible procedures, of possible arguments to \( \hat{\mathcal{F}} \), or possible arguments to \( \hat{\mathcal{C}} \) and of possible arguments.

definition proc-poss :: prog ⇒ 'c::contour proc set
  where proc-poss p = PC ' (lambdas p × maps-over (labels p) UNIV) ∪ PP ' prim's p ∪ {AStop}

definition fstate-poss :: prog ⇒ 'c::contour a-fstate set
  where fstate-poss p = (proc-poss p × NList (Pow (proc-poss p))) (call-list-lengths p) ×
\(\text{smaps-over} \ (\text{vars} \ p \times \text{UNIV}) \ (\text{proc-poss} \ p \times \text{UNIV})\)

**definition** \(\text{cstate-poss} :: \text{prog} \Rightarrow \text{contour} \ a-cstate \text{ set}\)

**where** \(\text{cstate-poss} \ p = (\text{calls} \ p \times \text{maps-over} \ (\text{labels} \ p) \ \text{UNIV} \times \text{smaps-over} \ (\text{vars} \ p \times \text{UNIV}) \ (\text{proc-poss} \ p) \times \text{UNIV})\)

**definition** \(\text{arg-poss} :: \text{prog} \Rightarrow (\text{\textquotesingle c::contour} \ a-fstate + \text{\textquotesingle c} \ a-cstate) \text{ discr set}\)

**where** \(\text{arg-poss} \ p = \text{Discr} \ (\text{fstate-poss} \ p <\leftrightarrow \text{cstate-poss} \ p)\)

Using the auxiliary results from **CPSUtils**, we see that the argument space as defined here is finite.

**lemma** \(\text{finite-arg-space}: \text{finite} \ (\text{arg-poss} \ p)\)

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

But is it closed? I.e. if we pass a member of \(\text{arg-poss}\) to \(\text{abs-R}\), are the generated recursive call arguments also in \(\text{arg-poss}\)? This is shown in **arg-space-complete**, after proving an auxiliary result about the possible outcome of a call to \(\mathcal{A}\) and an admissibility lemma.

**lemma** \(\text{evalV-possible}:\)

**assumes** \(f: f \in \mathcal{A} \ d \beta \ ve\)

**and** \(d: d \in \text{vals} \ p\)

**and** \(ve: ve \in \text{smaps-over} \ (\text{vars} \ p \times \text{UNIV}) \ (\text{proc-poss} \ p)\)

**and** \(\beta: \beta \in \text{maps-over} \ (\text{labels} \ p) \ \text{UNIV}\)

**shows** \(f \in \text{proc-poss} \ p\)

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

**lemma** \(\text{adm-subset}: \text{cont} \ (\lambda x. f x) \implies \text{adm} \ (\lambda x. f x \subseteq S)\)

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

**lemma** \(\text{arg-space-complete}:\)

\(\text{state} \in \text{arg-poss} \ p \implies \text{abs-R} \cdot \text{state} \subseteq \text{arg-poss} \ p\)

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

This result is now lifted to the powerset of \(\text{abs-R}\).

**lemma** \(\text{arg-space-complete-ps}: \text{states} \subseteq \text{arg-poss} \ p \implies (\text{abs-R}) \cdot \text{states} \subseteq \text{arg-poss} \ p\)

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

We are not so much interested in the finiteness of the set of possible arguments but rather of the the set of occurring arguments, when we start with the initial argument. But as this is of course a subset of the set of possible arguments, this is not hard to show.

**lemma** \(\text{UN-iterate-less}:\)

**assumes** \(\text{start}: x \in S\)

**and** \(\text{step}: \forall y. y \leq S \implies (f \cdot y) \subseteq S\)

29
shows (∪ i. iterate i.f.{x}) ⊆ S
(proof)

lemma args-finite: finite (∪ i. iterate i.(abs-R).{initial-r p}) (is finite ?S)
(proof)

8.2. A decomposition

The functions abs-g and abs-R are derived from ˆF and ˆC. This connection has yet to expressed explicitly.

lemma Un-commute-helper:(a ∪ b) ∪ (c ∪ d) = (a ∪ c) ∪ (b ∪ d)
(proof)

lemma a-evalF-decomp:
  ˆF = fst (sum-to-tup.(fix.(Λ f x. (∪ y∈abs-R·x. f·y) ∪ abs-g·x)))
(proof)

8.3. The iterative equation

Because of the special form of ˆF (and thus ˆPR) derived in the previous lemma, we can apply our generic results from Computability and express the abstract semantics as the image of a finite set under a computable function.

lemma a-evalF-iterative:
  ˆF·(Discr x) = abs-g·(∪ i. iterate i.(abs-R).{Discr (Inl x)})
(proof)

lemma a-evalCPS-interative:
  ˆPR prog = abs-g·(∪ i. iterate i.(abs-R).{initial-r prog})
(proof)

end

Part III.
The auxiliary theories

9. Syntax tree helpers

theory CPSUtils
imports CPSScheme
begin

This theory defines the sets lambdas p, calls p, calls p, vars p, labels p and primsp as
the subexpressions of the program \( p \). Finiteness is shown for each of these sets, and some rules about how these sets relate. All these rules are proven more or less the same ways, which is very inelegant due to the nesting of the type and the shape of the derived induction rule.

It would be much nicer to start with these rules and define the set inductively. Unfortunately, that approach would make it very hard to show the finiteness of the sets in question.

\[
\text{fun } \text{lambdas} :: \lambda \Rightarrow \text{lambda set}
\]
\[
\text{and } \text{lambdasC} :: \text{call } \Rightarrow \text{lambda set}
\]
\[
\text{and } \text{lambdasV} :: \text{val } \Rightarrow \text{lambda set}
\]
\[
\text{where}
\]
\[
\text{lambdas} \ (\Lambda \ l \ vs \ c) = (\{\Lambda \ l \ vs \ c\} \cup \text{lambdasC} \ c)
\]
\[
\text{lambdasC} \ (\text{App} \ l \ d \ ds) = \text{lambdasV} \ d \cup (\text{UNION} \ (\text{set} \ ds) \ \text{lambdasV})
\]
\[
\text{lambdasC} \ (\text{Let} \ l \ binds \ c') = (\text{UNION} \ (\text{set} \ binds) \ (\lambda (-,l). \ \text{lambdas} \ l)
\]
\[
\cup \ \text{lambdasC} \ c')
\]
\[
\text{lambdasV} \ (L \ l) = \text{lambdas} \ l
\]
\[
\text{lambdasV} \ - = \{\}
\]

\[
\text{fun } \text{calls} :: \lambda \Rightarrow \text{call set}
\]
\[
\text{and } \text{callsC} :: \text{call } \Rightarrow \text{call set}
\]
\[
\text{and } \text{callsV} :: \text{val } \Rightarrow \text{call set}
\]
\[
\text{where}
\]
\[
\text{calls} \ (\Lambda \ l \ vs \ c) = \text{callsC} \ c
\]
\[
\text{callsC} \ (\text{App} \ l \ d \ ds) = \{\text{App} \ l \ d \ ds\} \cup \text{callsV} \ d \cup (\text{UNION} \ (\text{set} \ ds) \ \text{callsV})
\]
\[
\text{callsC} \ (\text{Let} \ l \ binds \ c') = \{\text{Let} \ l \ binds \ c'\}
\]
\[
\cup (\text{UNION} \ (\text{set} \ binds) \ (\lambda (-,l). \ \text{calls} \ l)
\]
\[
\cup \ \text{callsC} \ c')
\]
\[
\text{callsV} \ (L \ l) = \text{calls} \ l
\]
\[
\text{callsV} \ - = \{\}
\]

\text{lemma finite-lambdas[simp]::finite (lambdas l) and finite (lambdasC c) finite (lambdasV v)}
\text{(proof)}

\text{lemma finite-calls[simp]:: finite (calls l) and finite (callsC c) finite (callsV v)}
\text{(proof)}

\[
\text{fun } \text{vars} :: \lambda \Rightarrow \text{var set}
\]
\[
\text{and } \text{varsC} :: \text{call } \Rightarrow \text{var set}
\]
\[
\text{and } \text{varsV} :: \text{val } \Rightarrow \text{var set}
\]
\[
\text{where}
\]
\[
\text{vars} \ (\Lambda - vs \ c) = \text{set} \ vs \cup \text{varsC} \ c
\]
\[
\text{varsC} \ (\text{App} - a \ as) = \text{varsV} \ a \cup \text{UNION} \ (\text{set} \ as) \ \text{varsV}
\]
\[
\text{varsC} \ (\text{Let} - binds \ c') = \text{UNION} \ (\text{set} \ binds) \ (\lambda (v,l). \ \{v\} \cup \text{vars} \ l) \cup \text{varsC} \ c'
\]
\[
\text{varsV} \ (L \ l) = \text{vars} \ l
\]
\[
\text{varsV} \ (R - v) = \{v\}
\]
\[
\text{varsV} \ - = \{\}
\]

\text{lemma finite-vars[simp]::finite (vars l) and finite (varsC c) finite (varsV v)}
\text{(proof)}
fun label :: lambda + call ⇒ label
where label (Inl (Lambda l - -)) = l
    | label (Inr (App l - -)) = l
    | label (Inr (Let l - -)) = l

fun labels :: lambda ⇒ label set
and labelsC :: call ⇒ label set
and labelsV :: val ⇒ label set
where labels (Lambda l vs c) = {l} ∪ labelsC c
    | labelsC (App l a as) = {l} ∪ labelsV a ∪ UNION (set as) labelsV
    | labelsC (Let l binds c′) = {l} ∪ UNION (set binds) (λ(v,l). labels l) ∪ labelsC c′
    | labelsV (L l) = labels l
    | labelsV (R l v) = {l}
    | labelsV - = {}

lemma finite-labels[simp]: finite (labels l) and finite (labelsC c) finite (labelsV v)
⟨proof⟩

fun prims :: lambda ⇒ prim set
and primsC :: call ⇒ prim set
and primsV :: val ⇒ prim set
where prims (Lambda - vs c) = primsC c
    | primsC (App - a as) = primsV a ∪ UNION (set as) primsV
    | primsC (Let - binds c′) = UNION (set binds) (λ(-,l). prims l) ∪ primsC c′
    | primsV (L l) = prims l
    | primsV (R l v) = {l}
    | primsV (P prim) = {prim}
    | primsV (C l v) = {}

lemma finite-prims[simp]: finite (prims l) and finite (primsC c) finite (primsV v)
⟨proof⟩

fun vals :: lambda ⇒ val set
and valsC :: call ⇒ val set
and valsV :: val ⇒ val set
where vals (Lambda - vs c) = valsC c
    | valsC (App - a as) = valsV a ∪ UNION (set as) valsV
    | valsC (Let - binds c′) = UNION (set binds) (λ(-,l). vals l) ∪ valsC c′
    | valsV (L l) = {L l} ∪ vals l
    | valsV (R l v) = {R l v}
    | valsV (P prim) = {P prim}
    | valsV (C l v) = {C l v}

lemma
fixes list2 :: (var × lambda) list and t :: var × lambda
shows lambdas1: Lambda l vs c ∈ lambdas x ⇒ c ∈ calls x
and Lambda l vs c ∈ lambdasC y ⇒ c ∈ callsC y
and Lambda l vs c ∈ lambdasV z ⇒ c ∈ callsV z
and $\forall z \in \text{set list.} \ \Lambda l \ vs \ c \in \text{lambda } V z \rightarrow c \in \text{calls } V z$
and $\forall z \in \text{set list2.} \ \Lambda l \ vs \ c \in \text{lambda } (\text{snd } x) \rightarrow c \in \text{calls } (\text{snd } x)$
and $\Lambda l \ vs \ c \in \text{lambda } (\text{snd } t) \Rightarrow c \in \text{calls } (\text{snd } t)$
(proof)

**Lemma**

shows lambda2: $\Lambda l \ vs \ c \in \text{lambda } x \Rightarrow l \in \text{labels } x$
and $\Lambda l \ vs \ c \in \text{lambda } C y \Rightarrow l \in \text{labels } C y$
and $\Lambda l \ vs \ c \in \text{lambda } V z \Rightarrow l \in \text{labels } V z$
and $\forall z \in \text{set list.} \ \Lambda l \ vs \ c \in \text{lambda } V z \rightarrow l \in \text{labels } V z$
and $\forall x \in \text{set (list2 :: (var } \times \text{ lambda) list).} \ \Lambda l \ vs \ c \in \text{lambda } (\text{snd } x) \rightarrow l \in \text{labels } (\text{snd } x)$
and $\Lambda l \ vs \ c \in \text{lambda } (\text{snd } (t:: \text{var } \times \text{ lambda})) \Rightarrow l \in \text{labels } (\text{snd } t)$
(proof)

**Lemma**

shows lambda3: $\Lambda l \ vs \ c \in \text{lambda } x \rightarrow \text{ set vs } \subseteq \text{vars } x$
and $\Lambda l \ vs \ c \in \text{lambda } C y \rightarrow \text{ set vs } \subseteq \text{vars } C y$
and $\Lambda l \ vs \ c \in \text{lambda } V z \rightarrow \text{ set vs } \subseteq \text{vars } V z$
and $\forall z \in \text{set list.} \ \Lambda l \ vs \ c \in \text{lambda } V z \rightarrow \text{ set vs } \subseteq \text{vars } V z$
and $\forall x \in \text{set (list2 :: (var } \times \text{ lambda) list).} \ \Lambda l \ vs \ c \in \text{lambda } (\text{snd } x) \rightarrow \text{ set vs } \subseteq \text{vars } (\text{snd } x)$
and $\Lambda l \ vs \ c \in \text{lambda } (\text{snd } (t:: \text{var } \times \text{ lambda})) \Rightarrow \text{ set vs } \subseteq \text{vars } (\text{snd } t)$
(proof)

**Lemma**

shows app1: $\text{App } l \ d \ ds \in \text{calls } x \Rightarrow d \in \text{vals } x$
and $\text{App } l \ d \ ds \in \text{calls } C y \Rightarrow d \in \text{vals } C y$
and $\text{App } l \ d \ ds \in \text{calls } V z \Rightarrow d \in \text{vals } V z$
and $\forall z \in \text{set list.} \ \text{App } l \ d \ ds \in \text{calls } V z \rightarrow d \in \text{vals } V z$
and $\forall x \in \text{set (list2 :: (var } \times \text{ lambda) list).} \ \text{App } l \ d \ ds \in \text{calls } (\text{snd } x) \rightarrow d \in \text{vals } (\text{snd } x)$
and $\text{App } l \ d \ ds \in \text{calls } (\text{snd } (t:: \text{var } \times \text{ lambda})) \Rightarrow d \in \text{vals } (\text{snd } t)$
(proof)

**Lemma**

shows app2: $\text{App } l \ d \ ds \in \text{calls } x \Rightarrow \text{ set ds } \subseteq \text{vals } x$
and $\text{App } l \ d \ ds \in \text{calls } C y \Rightarrow \text{ set ds } \subseteq \text{vals } C y$
and $\text{App } l \ d \ ds \in \text{calls } V z \Rightarrow \text{ set ds } \subseteq \text{vals } V z$
and $\forall z \in \text{set list.} \ \text{App } l \ d \ ds \in \text{calls } V z \rightarrow \text{ set ds } \subseteq \text{vals } V z$
and $\forall x \in \text{set (list2 :: (var } \times \text{ lambda) list).} \ \text{App } l \ d \ ds \in \text{calls } (\text{snd } x) \rightarrow \text{ set ds } \subseteq \text{vals } (\text{snd } x)$
and $\text{App } l \ d \ ds \in \text{calls } (\text{snd } (t:: \text{var } \times \text{ lambda})) \Rightarrow \text{ set ds } \subseteq \text{vals } (\text{snd } t)$
(proof)

**Lemma**

shows let1: $\text{Let } l \ binds \ c' \in \text{calls } x \rightarrow l \in \text{labels } x$
and $\text{Let } l \ binds \ c' \in \text{calls } C y \Rightarrow l \in \text{labels } C y$
and $\text{Let } l \ binds \ c' \in \text{calls } V z \Rightarrow l \in \text{labels } V z$
and $\forall z \in \text{set list.} \ \text{Let } l \ binds \ c' \in \text{calls } V z \rightarrow l \in \text{labels } V z$
\[\forall x \in \text{set} (\text{list}2 :: (\text{var} \times \text{lambda}) \text{list}) \Rightarrow \text{let} \text{l binds} \ c' \in \text{calls} (\text{snd} \ t) \Rightarrow \text{l} \in \text{labels} (\text{snd} \ x)\]

\[\text{let} \text{l binds} \ c' \in \text{calls} (\text{snd} \ t :: \text{var} \times \text{lambda}) \Rightarrow \text{l} \in \text{labels} (\text{snd} \ t)\]

(proof)

lemma
shows let2: \text{Let} \text{l binds} \ c' \in \text{calls} \ x \Rightarrow c' \in \text{calls} \ x
and \text{Let} \text{l binds} \ c' \in \text{calls} C \ y \Rightarrow c' \in \text{calls} C \ y
and \text{Let} \text{l binds} \ c' \in \text{calls} V \ z \Rightarrow c' \in \text{calls} V \ z
and \forall z \in \text{set list}. \text{Let} \text{l binds} \ c' \in \text{calls} V \ z \Rightarrow c' \in \text{calls} V \ z
and \forall x \in \text{set} (\text{list}2 :: (\text{var} \times \text{lambda}) \text{list}) \Rightarrow \text{Let} \text{l binds} \ c' \in \text{calls} (\text{snd} \ x) \Rightarrow c' \in \text{calls} (\text{snd} \ x)
and \text{Let} \text{l binds} \ c' \in \text{calls} (\text{snd} \ t :: \text{var} \times \text{lambda}) \Rightarrow c' \in \text{calls} (\text{snd} \ t)
(proof)

lemma
shows let3: \text{Let} \text{l binds} \ c' \in \text{calls} \ x \Rightarrow \text{fst} \ ' \text{set binds} \subseteq \text{vars} \ x
and \text{Let} \text{l binds} \ c' \in \text{calls} C \ y \Rightarrow \text{fst} \ ' \text{set binds} \subseteq \text{vars} C \ y
and \text{Let} \text{l binds} \ c' \in \text{calls} V \ z \Rightarrow \text{fst} \ ' \text{set binds} \subseteq \text{vars} V \ z
and \forall z \in \text{set list}. \text{Let} \text{l binds} \ c' \in \text{calls} V \ z \Rightarrow \text{fst} \ ' \text{set binds} \subseteq \text{vars} V \ z
and \forall x \in \text{set} (\text{list}2 :: (\text{var} \times \text{lambda}) \text{list}) \Rightarrow \text{Let} \text{l binds} \ c' \in \text{calls} (\text{snd} \ x) \Rightarrow \text{fst} \ ' \text{set binds} \subseteq \text{vars} (\text{snd} \ x)
and \text{Let} \text{l binds} \ c' \in \text{calls} (\text{snd} \ t :: \text{var} \times \text{lambda}) \Rightarrow \text{fst} \ ' \text{set binds} \subseteq \text{vars} (\text{snd} \ t)
(proof)

lemma
shows let4: \text{Let} \text{l binds} \ c' \in \text{calls} \ x \Rightarrow \text{snd} \ ' \text{set binds} \subseteq \text{lam} \\text{das} \ x
and \text{Let} \text{l binds} \ c' \in \text{calls} C \ y \Rightarrow \text{snd} \ ' \text{set binds} \subseteq \text{lam} \\text{das} C \ y
and \text{Let} \text{l binds} \ c' \in \text{calls} V \ z \Rightarrow \text{snd} \ ' \text{set binds} \subseteq \text{lam} \\text{das} V \ z
and \forall z \in \text{set list}. \text{Let} \text{l binds} \ c' \in \text{calls} V \ z \Rightarrow \text{snd} \ ' \text{set binds} \subseteq \text{lam} \\text{das} V \ z
and \forall x \in \text{set} (\text{list}2 :: (\text{var} \times \text{lambda}) \text{list}) \Rightarrow \text{Let} \text{l binds} \ c' \in \text{calls} (\text{snd} \ x) \Rightarrow \text{snd} \ ' \text{set binds} \subseteq \text{lam} \\text{das} (\text{snd} \ x)
and \text{Let} \text{l binds} \ c' \in \text{calls} (\text{snd} \ t :: \text{var} \times \text{lambda}) \Rightarrow \text{snd} \ ' \text{set binds} \subseteq \text{lam} \\text{das} (\text{snd} \ t)
(proof)

lemma
shows vals1: \text{P} \text{prim} \in \text{vals} \ p \Rightarrow \text{prim} \in \text{prims} \ p
and \text{P} \text{prim} \in \text{vals} C \ y \Rightarrow \text{prim} \in \text{prims} C \ y
and \text{P} \text{prim} \in \text{vals} V \ z \Rightarrow \text{prim} \in \text{prims} V \ z
and \forall z \in \text{set list}. \text{P} \text{prim} \in \text{vals} V \ z \Rightarrow \text{prim} \in \text{prims} V \ z
and \forall x \in \text{set} (\text{list}2 :: (\text{var} \times \text{lambda}) \text{list}) \Rightarrow \text{P} \text{prim} \in \text{vals} (\text{snd} \ x) \Rightarrow \text{prim} \in \text{prims} (\text{snd} \ x)
and \text{P} \text{prim} \in \text{vals} (\text{snd} \ t :: \text{var} \times \text{lambda}) \Rightarrow \text{prim} \in \text{prims} (\text{snd} \ t)
(proof)

lemma
shows vals2: \text{R} \text{l var} \in \text{vals} \ p \Rightarrow \text{var} \in \text{vars} \ p
and \text{R} \text{l var} \in \text{vals} C \ y \Rightarrow \text{var} \in \text{vars} C \ y
and \text{R} \text{l var} \in \text{vals} V \ z \Rightarrow \text{var} \in \text{vars} V \ z
\[
\forall z \in \text{set list}.\ R\ l\ \text{var} \in \text{vals}V\ z \Rightarrow \text{var} \in \text{vars}V\ z
\]
\[
\forall x \in \text{set}\ (\text{list2} :: (\text{var} \times \lambda\ \text{list})).\ R\ l\ \text{var} \in \text{vals}\ (\text{snd}\ x) \Rightarrow \text{var} \in \text{vars}\ (\text{snd}\ x)
\]
\[
R\ l\ \text{var} \in \text{vals}\ (\text{snd}\ (t::\text{var}\times\lambda\text{lambda})) \Rightarrow \text{var} \in \text{vars}\ (\text{snd}\ t)
\]

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

**lemma**

showsvals3: L l \in \text{vals} p \Rightarrow l \in \text{lambdas} p

and L l \in \text{valsC} y \Rightarrow l \in \text{lambdasC} y

and L l \in \text{valsV} z \Rightarrow l \in \text{lambdasV} z

\[
\forall z \in \text{set list}.\ L l \in \text{valsV} z \Rightarrow l \in \text{lambdasV} z
\]
\[
\forall x \in \text{set}\ (\text{list2} :: (\text{var} \times \lambda\ \text{list})).\ L l \in \text{vals}\ (\text{snd}\ x) \Rightarrow l \in \text{lambdas}\ (\text{snd}\ x)
\]
\[
L l \in \text{vals}\ (\text{snd}\ (t::\text{var}\times\lambda\text{lambda})) = \Rightarrow l \in \text{lambdas}\ (\text{snd}\ t)
\]

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

**definition** nList :: 'a set \Rightarrow \text{nat} \Rightarrow 'a list set

where nList A n \equiv \{l.\ \text{set}\ l \leq A \land \text{length}\ l = n\}

**lemma** finite-nList[intro]:

assumes finA: finite A

shows finite (nList A n)

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

**definition** NList :: 'a set \Rightarrow \text{nat} set \Rightarrow 'a list set

where NList A N \equiv \bigcup n \in N.\ nList A n

**lemma** finite-Nlist[intro]:

\[\begin{array}{c}
\text{finite}\ A;\ \text{finite}\ N
\end{array} \Rightarrow \text{finite}\ (NList A N)

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

**definition** call-list-lengths

where call-list-lengths p = \{0,1,2,3\} \cup (\lambda c.\ \text{case}\ c\ \text{of}\ (\text{App}\ -\ -\ ds) \Rightarrow \text{length}\ ds | - \Rightarrow 0)\ ' \text{calls}\ p

**lemma** finite-call-list-lengths[simp]: finite (call-list-lengths p)

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

end

10. General utility lemmas

theory Utils imports Main

begin

This is a potpourri of various lemmas not specific to our project. Some of them could very well be included in the default Isabelle library.
Lemmas about the single-valued predicate.

lemma single-valued-empty[simp]: single-valued {}
(proof)

lemma single-valued-insert:
  assumes single-valued rel
  and \( \forall x \ y \cdot [(x,y) \in \text{rel}; x=a] \implies y = b \)
  shows single-valued (insert (a,b) \text{rel})
(proof)

Lemmas about \text{ran}, the range of a finite map.

lemma ran-upd: \text{ran} \((m \ (k \mapsto v))\) \subseteq \text{ran} \ m \cup \{v\}
(proof)

lemma ran-map-of: \text{ran} \ (\text{map-of} \ x) \subseteq \text{snd} \circ \, \text{set} \ x
(proof)

lemma ran-concat: \text{ran} \ (m1 ++ m2) \subseteq \text{ran} \ m1 \cup \text{ran} \ m2
(proof)

lemma ran-upds:
  assumes eq-length: \text{length} \ ks = \text{length} \ vs
  shows \text{ran} \ (\text{map-upds} \ m \ ks \ vs) \subseteq \text{ran} \ m \cup \text{set} \ vs
(proof)

lemma ran-upd-mem[simp]: \( v \in \text{ran} \ (m \ (k \mapsto v)) \)
(proof)

Lemmas about \text{map}, \text{zip} and \text{fst/snd}

lemma map-fst-zip: \text{length} \ x = \text{length} \ y \implies \text{map} \ \text{fst} \ (\text{zip} \ x \ y) = x
(proof)

lemma map-snd-zip: \text{length} \ x = \text{length} \ y \implies \text{map} \ \text{snd} \ (\text{zip} \ x \ y) = y
(proof)

end

11. Set-valued maps

theory SetMap
  imports Main
begin

For the abstract semantics, we need methods to work with set-valued maps, i.e. functions from a key type to sets of values. For this type, some well known operations are
introduced and properties shown, either borrowing the nomenclature from finite maps (sdom, sran,...) or of sets (\{\}, \cup,...).

**definition**

\[ \text{sdom} :: ('a => 'b set) => 'a set \]
\[ \text{sdom} \ m = \{a. \ m \ a \sim = \{\}\} \]

**definition**

\[ \text{sran} :: ('a => 'b set) => 'b set \]
\[ \text{sran} \ m = \{b. \ EX \ a. \ b \in \ m \ a\} \]

**lemma** \[ \text{sranI}: b \in m a \Rightarrow b \in \text{sran} \ m \]

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

**lemma** \[ \text{sdom-not-mem[elim]}: a \notin \text{sdom} \ m \Rightarrow m \ a = \{\} \]

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

**definition** \[ \text{smap-empty} (\{\}.\) \]
\[ \text{where} \ \{\}. \ k = \{\} \]

**definition** \[ \text{smap-union} :: ('a::type => 'b::type set) => ('a => 'b set) => ('a => 'b set) \]
\[ \text{where} \ \text{smap1} \cup. \text{smap2} k = \text{smap1} k \cup \text{smap2} k \]

**primrec** \[ \text{smap-Union} :: ('a::type => 'b::type set) list => 'a => 'b set (\cup.-) \]
\[ \text{where} \ [\text{simp}]:\cup. \ [] = \{\}. \]
\[ | \cup. (m#ms) = m \cup \cup. ms \]

**definition** \[ \text{smap-singleton} :: 'a::type => 'b::type set => 'a => 'b set (\{. := -.\}) \]
\[ \text{where} \ \{k := vs\}. = \{\}. \ (k := vs) \]

**definition** \[ \text{smap-less} :: ('a => 'b set) => ('a => 'b set) => bool (\cdot \subseteq. \cdot \ [50, 51] 50) \]
\[ \text{where} \ \text{smap-less} m1 m2 = (\forall k. \ m1 \ k \subseteq m2 \ k) \]

**lemma** \[ \text{sdom-empty[simp]}: \text{sdom} \ \{\}. = \{\} \]

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

**lemma** \[ \text{sdom-singleton[simp]}: \text{sdom} \ \{k := vs\}. \subseteq \{k\} \]

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

**lemma** \[ \text{sran-singleton[simp]}: \text{sran} \ \{k := vs\}. = vs \]

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

**lemma** \[ \text{sran-empty[simp]}: \text{sran} \ \{\}. = \{\} \]

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

**lemma** \[ \text{sdom-union[simp]}: \text{sdom} \ (m \cup. n) = \text{sdom} \ m \cup \text{sdom} \ n \]

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

**lemma** \[ \text{sran-union[simp]}: \text{sran} \ (m \cup. n) = \text{sran} \ m \cup \text{sran} \ n \]

\[ \langle \text{proof} \rangle \]
lemma smap-empty[simp]: \{\} \subseteq \{\}.
⟨proof⟩

lemma smap-less-refl: m \subseteq m
⟨proof⟩

lemma smap-less-trans[trans]: [ m1 \subseteq m2; m2 \subseteq m3 ] \implies m1 \subseteq m3
⟨proof⟩

lemma smap-union-monolemma: [ ve1 \subseteq ve1'; ve2 \subseteq ve2' ] \implies ve1 \cup ve2 \subseteq ve1' \cup ve2'
⟨proof⟩

lemma smap-Union-union: m1 \cup \bigcup ms = \bigcup (m1 \# ms)
⟨proof⟩

lemma smap-Union-monolemma: 
  assumes list-all2 smap-less ms1 ms2
  shows \bigcup ms1 \subseteq \bigcup ms2
⟨proof⟩

lemma smap-singleton-monolemma: v \subseteq v' \implies \{ k := v \} \subseteq \{ k := v' \}.
⟨proof⟩

lemma smap-union-comm: m1 \cup m2 = m2 \cup m1
⟨proof⟩

lemma smap-union-empty1[simp]: \{\} \cup m = m
⟨proof⟩

lemma smap-union-empty2[simp]: m \cup \{\} = m
⟨proof⟩

lemma smap-union-assoc [simp]: (m1 \cup m2) \cup m3 = m1 \cup (m2 \cup m3)
⟨proof⟩

lemma smap-Union-append[simp]: \bigcup (m1 @ m2) = \bigcup m1 = \bigcup m2
⟨proof⟩

lemma smap-Union-rev[ simp]: \bigcup (rev l) = \bigcup l
⟨proof⟩

lemma smap-Union-map-rev[ simp]: \bigcup (map f (rev l)) = \bigcup (map f l)
⟨proof⟩

end
12. Sets of maps

theory MapSets
imports SetMap Utils
begin

In the section about the finiteness of the argument space, we need the fact that the set
of maps from a finite domain to a finite range is finite, and the same for the set-valued
maps defined in SetMap. Both these sets are defined (maps-over, smaps-over) and the
finiteness is shown.

definition maps-over :: 'a::type set ⇒ 'b::type set ⇒ ('a → 'b) set
  where maps-over A B = {m. dom m ⊆ A ∧ ran m ⊆ B}

lemma maps-over-empty[simp]:
  empty ∈ maps-over A B
⟨proof⟩

lemma maps-over-upd:
  assumes m ∈ maps-over A B
  and v ∈ A and k ∈ B
  shows m(v ↦ k) ∈ maps-over A B
⟨proof⟩

lemma maps-over-finite[intro]:
  assumes finite A and finite B shows finite (maps-over A B)
⟨proof⟩

definition smaps-over :: 'a::type set ⇒ 'b::type set ⇒ ('a ⇒ 'b set) set
  where smaps-over A B = {m. sdom m ⊆ A ∧ sran m ⊆ B}

lemma smaps-over-empty[simp]:
  {}. ∈ smaps-over A B
⟨proof⟩

lemma smaps-over-singleton:
  assumes k ∈ A and vs ⊆ B
  shows {k := vs}. ∈ smaps-over A B
⟨proof⟩

lemma smaps-over-un:
  assumes m1 ∈ smaps-over A B and m2 ∈ smaps-over A B
  shows m1 ∪. m2 ∈ smaps-over A B
⟨proof⟩

lemma smaps-over-Union:
  assumes set ms ⊆ smaps-over A B
  shows ∪. ms ∈ smaps-over A B
⟨proof⟩
lemma smaps-over-im:
\[ \{ f \in m : m \in \text{smaps-over } A B \} \implies f \in B \]
(proof)

lemma smaps-over-finite[intro]:
assumes finite A and finite B shows finite (smaps-over A B)
(proof)
end

13. HOLCF Utility lemmas

theory HOLCFUtils imports HOLCF begin

We use HOLCF to define the denotational semantics. By default, HOLCF does not turn the regular set type into a partial order, so this is done here. Some of the lemmas here are contributed by Brian Huffman.

We start by making the type bool a pointed chain-complete partial order.

instantiation bool :: po begin
definition x \subseteq y \iff (x \rightarrow y)
instance (proof)
end

instance bool :: chfin (proof)

instance bool :: pcpo (proof)

lemma is-lub-bool: S \ll (True \in S) (proof)

lemma lub-bool: lub S = (True \in S) (proof)

lemma bottom-eq-False[simp]: \bot = False (proof)

To convert between the squared syntax used by HOLCF and the regular, round syntax for sets, we state some of the equivalencies.

40
instantiation set :: (type) po
begin
  definition
    $A \sqsubseteq B \leftrightarrow A \subseteq B$
  instance (proof)
end

lemma sqsubset-is-subset: $A \sqsubseteq B \leftrightarrow A \subseteq B$
  (proof)

lemma is-lub-set: $S \ll\cup S$
  (proof)

lemma lub-is-union: lub $S = \bigcup S$
  (proof)

instance set :: (type) cpo
  (proof)

lemma emptyset-is-bot[simp]: $\{\} \sqsubseteq S$
  (proof)

instance set :: (type) pcpo
  (proof)

lemma bot-bool-is-emptyset[simp]: $\bot = \{\}$
  (proof)

To actually use these instance in fixrec definitions or fixed-point inductions, we need continuity requirements for various boolean and set operations.

lemma cont2cont-disj [simp, cont2cont]:
  assumes f: cont ($\lambda x. f x$) and g: cont ($\lambda x. g x$)
  shows cont ($\lambda x. f x \lor g x$)
  (proof)

lemma cont2cont-imp[simp, cont2cont]:
  assumes f: cont ($\lambda x. \neg f x$) and g: cont ($\lambda x. g x$)
  shows cont ($\lambda x. f x \rightarrow g x$)
  (proof)

lemma cont2cont-Collect [simp, cont2cont]:
  assumes $\forall y. \text{cont} (\lambda x. f x y)$
  shows cont ($\lambda x. \{ y. f x y \}$)
  (proof)

lemma cont2cont-mem [simp, cont2cont]:
  assumes cont ($\lambda x. f x$)
  shows cont ($\lambda x. y \in f x$)
lemma cont2cont-union [simp, cont2cont]:
  cont (λx. f x) ⊢ cont (λx. g x)
  ⊢ cont (λx. f x ∪ g x)
(proof)

lemma cont2cont-insert [simp, cont2cont]:
  assumes cont (λx. f x)
  shows cont (λx. insert y (f x))
(proof)

lemmas adm-subset = adm-below[where 'a::type set, unfolded sqsubset-is-subset]

lemma cont2cont-UNION[cont2cont,simp]:
  assumes cont f
  and ∀ y. cont (λx. g x y)
  shows cont (λx. ∪ y ∈ f x. g x y)
(proof)

lemma cont2cont-Let-simple[simp,cont2cont]:
  assumes cont (λx. g x t)
  shows cont (λx. let y = t in g x y)
(proof)

lemma cont2cont-case-list [simp, cont2cont]:
  assumes ∀ y. cont (λx. f1 x)
  and ∀ y z. cont (λx. f2 x y z)
  shows cont (λx. case-list (f1 x) (f2 x) l)
(proof)

As with the continuity lemmas, we need admissibility lemmas.

lemma adm-not-mem:
  assumes cont (λx. f x)
  shows adm (λx. y /∈ f x)
(proof)

lemma adm-id[simp]: adm (λx . x)
(proof)

lemma adm-Not[simp]: adm Not
(proof)

lemma adm-prod-split:
  assumes adm (λp. f (fst p) (snd p))
  shows adm (λ(x,y). f x y)
(proof)
lemma adm-ball':
  assumes \( \forall y. \text{adm} (\lambda x. y \in A x \rightarrow P x y) \)
  shows \( \text{adm} (\lambda x. \forall y \in A x . P x y) \)
 ⟨proof⟩

lemma adm-not-conj:
  \([\text{adm} (\lambda x. \neg P x); \text{adm} (\lambda x. \neg Q x)] \implies \text{adm} (\lambda x. \neg (P x \land Q x))\]
 ⟨proof⟩

lemma adm-single-valued:
  assumes cont (\( \lambda x. f x \))
  shows \( \text{adm} (\lambda x. \text{single-valued} (f x)) \)
 ⟨proof⟩

To match Shivers’ syntax we introduce the power-syntax for iterated function application.

abbreviation niceiterate ((-) [1000] 1000)
  where niceiterate \( f i \equiv \text{iterate} i \cdot f \)
end

14. Fixed point transformations

theory FixTransform
imports HOLCF
begin

default-sort type

In his treatment of the computabily, Shivers gives proofs only for a generic example and leaves it to the reader to apply this to the mutually recursive functions used for the semantics. As we carry this out, we need to transform a fixed point for two functions (implemented in HOLCF as a fixed point over a tuple) to a simple fixed point equation. The approach here works as long as both functions in the tuple have the same return type, using the equation
\[ X^A \cdot X^B = X^{A+B}. \]

Generally, a fixed point can be transformed using any retractable continuous function:

lemma fix-transform:
  assumes \( \forall x. g \cdot (f \cdot x) = x \)
  shows \( \text{fix} \cdot F = g \cdot (\text{fix} \cdot (f \circ F \circ g)) \)
 ⟨proof⟩
The functions we use here convert a tuple of functions to a function taking a direct sum as parameters and back. We only care about discrete arguments here.

**definition** `tup-to-sum` :: `(′a discr → ′c) × (′b discr → ′c) → (′a + ′b) discr → ′c::cpo`

**where**

\[
\text{tup-to-sum} = (\Lambda \ p \ s . \ (\lambda (f,g). \\
\text{case undiscr } s \ \text{of } \text{Inl } x \Rightarrow f(\text{Discr } x) \\
\text{Inr } x \Rightarrow g(\text{Discr } x)) \ p)
\]

**definition** `sum-to-tup` :: `((′a + ′b) discr → ′c) → (′a discr → ′c) × (′b discr → ′c::cpo)`

**where**

\[
\text{sum-to-tup} = (\Lambda f . \ (\Lambda x . f(\text{Discr (Inl (undiscr } x))))), \\
(\Lambda x . f(\text{Discr (Inr (undiscr } x))))
\]

As so often when working with HOLCF, some continuity lemmas are required.

**lemma** `cont2cont-case-sum[simp,cont2cont]`:

assumes `cont f` and `cont g`

shows `cont (λx. case-sum (f x) (g x) s)`

(\[ proof \]

**lemma** `cont2cont-circ[simp,cont2cont]`:

`cont (λf. f ◦ g)`

(\[ proof \]

**lemma** `cont2cont-split-pair[cont2cont,simp]`:

assumes `f1: cont f`

and `f2: ∃ x. cont (f x)`

and `g1: cont g`

and `g2: ∃ x. cont (g x)`

shows `cont (λ(a, b). (f a b, g a b))`

(\[ proof \]

Using these continuity lemmas, we can show that our function are actually continuous and thus allow us to apply them to a value.

**lemma** `sum-to-tup-app`:

\[
\text{sum-to-tup} \cdot f = (\Lambda x . f(\text{Discr (Inl (undiscr } x))))), \ (\Lambda x . f(\text{Discr (Inr (undiscr } x)))))
\]

(\[ proof \]

**lemma** `tup-to-sum-app`:

\[
\text{tup-to-sum} \cdot p = (\Lambda s . (\lambda (f,g). \\
\text{case undiscr } s \ \text{of } \text{Inl } x \Rightarrow f(\text{Discr } x) \\
\text{Inr } x \Rightarrow g(\text{Discr } x)) \ p)
\]

(\[ proof \]

Generally, lambda abstractions with discrete domain are continous and can be resolved immediately.

**lemma** `discr-app[simp]`:

\[
(\Lambda s . f s)(\text{Discr } x) = f (\text{Discr } x)
\]
Our transformation functions are inverse to each other, so we can use them to transform a fixed point.

**lemma** tup-to-sum-to-tup\([\text{simp}]:\)
  
  shows \(\text{sum-to-tup} \circ (\text{tup-to-sum} \cdot F) = F\)

**lemma** fix-transform-pair-sum:
  
  shows \(\text{fix} \cdot F = \text{sum-to-tup} \circ (\text{fix} \circ (\text{tup-to-sum} \circ F \circ \text{sum-to-tup}))\)

After such a transformation, we want to get rid of these helper functions again. This is done by the next two simplification lemmas.

**lemma** tup-sum-oo\([\text{simp}]:\)
  
  assumes \(f_1: \text{cont } F\)
  
  and \(f_2: \forall x. \text{cont } (F x)\)
  
  and \(g_1: \text{cont } G\)
  
  and \(g_2: \forall x. \text{cont } (G x)\)
  
  shows \(\text{tup-to-sum} \circ (\lambda p. (\lambda (a, b). (F a b, G a b)) p) \circ \text{sum-to-tup} = (\lambda f s. \left(\text{case } \text{undiscr } s \text{ of } \right.\)
  
  \(\text{Inl } x \Rightarrow F (\lambda s. f \cdot (\text{Discr } (\text{Inl } (\text{undiscr } s))))\)
  
  \(\left. (\lambda s. f \cdot (\text{Discr } (\text{Inr } (\text{undiscr } s)))) \cdot (\text{Discr } x)\right)\)
  
  \| \text{Inr } x \Rightarrow G (\lambda s. f \cdot (\text{Discr } (\text{Inl } (\text{undiscr } s))))\)
  
  \(\left. (\lambda s. f \cdot (\text{Discr } (\text{Inr } (\text{undiscr } s)))) \cdot (\text{Discr } x)\right)\)

**lemma** fst-sum-to-tup\([\text{simp}]:\)
  
  \(\text{fst} \circ (\text{sum-to-tup} \cdot x) = (\lambda xa. x \cdot (\text{Discr } (\text{Inl } (\text{undiscr } xa))))\)

\end