Flow Logic and Operational Semantics

Flemming Nielson

Computer Science Department
University of Aarhus
DK-8000 Aarhus C, Denmark

Hanne Riis Nielson

Computer Science Department
University of Aarhus
DK-8000 Aarhus C, Denmark

Abstract
Flow logic is a “fast prototyping” approach to program analysis that shows great promise of being able to deal with a wide variety of languages and calculi for computation. However, seemingly innocent choices in the flow logic as well as in the operational semantics may inhibit proving the analysis correct. Our main conclusion is that environment based semantics is more flexible than either substitution based semantics or semantics making use of structural congruences (like alpha-renaming).

1 Introduction
Flow logic facilitates the specification of program analyses [10] that automatically predict properties of programs holding in all executions. It allows to deal with a wide variety of languages; examples include the lambda-calculus with side-effects (a fragment of Standard ML) or communications (a fragment of Concurrent ML), several object based calculi, and a process algebra (the π-calculus). Analyses may be described in a succinct form (akin to program logic) or in a more verbose form (taking the form of constraint satisfaction); also they may be described at an abstract level of reasoning (using coinductive techniques) or in a more compositional manner (using inductive techniques). This allows to use the approach to first sketch the analysis, next refine it and prove it correct, and finally obtain an efficient implementation; furthermore, the development may be firmly rooted upon existing program analysis technology and insights, rather than having to start from scratch.

Structural operational semantics similarly allows to deal with a wide variety of languages. There are many choices that needs to be made concerning
how to define the semantics: e.g. having small-step or big-step transitions, using environments or performing direct substitution, making use of evaluation contexts or having explicit rules for reduction in context. Many of these choices are seemingly innocent in the sense that they do not affect the “meaning” of the language being defined; and indeed different formulations of the semantics can often be proved equivalent (although the proofs are sometimes quite laborious).

This might suggest that one could deal with a new language or calculus in the following way: first the syntax and informal meaning is defined, then the program analysis is developed simultaneously with the operational semantics, and finally they are consolidated with respect to one another (and in particular the analysis is proved correct). One advantage of this approach is that the fine details of the language definition are consolidated not only by semantic considerations but also by more pragmatic considerations concerning the ease with which programs can be validated not to have anomalous behaviour; we believe that this is a key issue in designing languages that are both theoretically well-behaved and pragmatically useful. Another advantage is that the methods would then be more likely to scale up to “real life” languages because different teams of researchers could be responsible for different aspects of the development; this is a major parameter for the success of formal methods in software engineering and is often neglected in purely theoretical studies.

In our experience the above approach is fraught with problems. One reason is that the structure, size and complexity of the correctness proofs depend on characteristic of the flow logic (e.g. whether it is abstract or compositional) as well as on characteristic of the operational semantics (e.g. whether it uses environments or direct substitution). In some cases the choices may “contradict” one another so that no proof of correctness is possible and the analysis or semantics has to be changed. It is therefore important to identify general guidelines concerning what complications are likely to arise for what combinations – in order that the use of formal methods in this area may become a craft rather than a (black) art.

Our main conclusion is that environment based semantics is more flexible than either substitution based semantics or semantics making use of structural congruences (like alpha-renaming) in terms of being able to accommodate a variety of specification styles for program analysis.

2 Setting the Scene

For simplicity this paper concentrates on an untyped lambda-calculus although analogous considerations apply to the more advanced object based and concurrent calculi mentioned above. The pure untyped lambda-calculus has the following syntax:

$$e \in \text{Exp}$$
$$e ::= x \mid \text{fn } x \Rightarrow e \mid e \ e$$
where \( \text{Var} \) is an unspecified countably infinite set

The succinct formulations of flow logic considered here do not require that all program points are made explicit; so there is no need to place explicit labels on all subexpressions (as in [9]) or to convert programs into “A-normal-form” (as in [4]). Instead we shall assume that all function abstractions have initially been alpha-renamed so as to have distinct formal parameters that are also disjoint from the set of global variables, \( \text{FV}(e) \), of the program of interest, \( e \).

Often program analysis is formulated as the demand to compute the best (or least) analysis information, \( \rho \), that pertains to a program, \( e \): \( \rho = A(e) \). Here we shall take the more flexible approach that a piece of analysis information, \( \rho \), needs to be validated with respect to the program, \( e \): \( \rho \models e \) (yielding \( \text{tt} \) or \( \text{ff} \)). On the one hand this allows to develop algorithms for computing the best analysis information [11,5] and on the other hand it offers promise of analysing not only closed systems: whenever new expressions emerge from the environment it can be checked whether or not the current analysis has duly recorded all the possible effects of these expressions. The ability to analyse open systems is particularly important for calculi and languages dealing with distribution and mobility of software.

Example 2.1 To give an example of the analysis consider the following simple program, \( e \), (in a slight extension of the syntax):

\[
\text{letrec } g = (\text{fn } x => (g \ g)) \\
\text{in } g (\text{fn } y => y)
\]

Here a function \( g \) is defined that ignores its parameter and calls itself recursively upon itself; the function is then called with the identity function as parameter.

We shall next consider an analysis that is called a control flow analysis [15,16], a closure analysis [12,14] or a set based analysis [6]. To do so we first define the abstract environment \( \rho \) by:

\[
\rho(g) = \{\text{fn } x => (g \ g)\} \\
\rho(x) = \{\text{fn } x => (g \ g), \text{fn } y => y\} \\
\rho(y) = \emptyset
\]

The analysis of the program, \( e \), then amounts to a judgement of the form

\[
\rho \models e : \emptyset
\]

saying that it will be correct to stipulate that \( g \) is bound to the recursive function itself, that the formal parameter \( x \) is bound to the recursive function or the identity function, that the formal parameter \( y \) is bound to nothing (corresponding to the fact that \( y \) is neither called), and that the program never returns any function (corresponding to the fact that \( g \) loops forever).

To validate the analysis we will encounter other judgements like

\[
\rho \models \text{fn } x => (g \ g) : \{\text{fn } x => (g \ g)\}
\]
\[ \hat{\rho} \models \text{fn } y \Rightarrow y : \{ \text{fn } y \Rightarrow y \} \]
\[ \hat{\rho} \models g \ g : \emptyset \]
\[ \hat{\rho} \models g \ (\text{fn } y \Rightarrow y) : \emptyset \]

and to make this precise we need to clarify how the judgements, \( \hat{\rho} \models e : W \), are defined; this will be the subject of Section 4 after having defined the operational semantics in Section 3.

3 Operational Semantics

Let us now start on our first task: the definition of the operational semantics. As already indicated there are a number of choices to be made. Here we shall just consider three kinds of semantics: a substitution based semantics in the manner of the \( \lambda \)-calculus [1], a structural operational semantics with environments in the manner of [13] and a variant involving explicit alpha-renaming of bound variables (in the manner of the structural congruence used in process algebras like the \( \pi \)-calculus).

All of these semantics are small-step and this is advantageous for the ability to express the correctness of looping programs and for programs with concurrency. The general form of the correctness result then is a subject reduction result:

- if the analysis \( \hat{\rho} \) is acceptable for the expression \( e_1 \)
- and if \( e_1 \) evolves into \( e_2 \)
- then the analysis \( \hat{\rho} \) is acceptable for the expression \( e_2 \).

If a big-step semantics had been used then looping programs\(^1\) as well as concurrent programs would present obstacles to the development.

Substitution based semantics

Perhaps the simplest kind of operational semantics uses substitutions rather than environments. In this case the operational semantics is given by a judgement of the form

\[ e_1 \xrightarrow{g} e_2 \]

saying that one step of evaluation of \( e_1 \) yields \( e_2 \). To define the judgement it is helpful to clarify that the expressions playing the role of values (i.e. fully evaluated expressions) are simply those function abstractions that only contain global variables:

\[ v \in \text{Val} \]
\[ v ::= \text{fn } x \Rightarrow e \text{ provided that } \text{FV}(\text{fn } x \Rightarrow e) \subseteq \text{FV}(e) \]

Here the set \( \text{FV}(e) \) of free variables of an expression \( e \) is defined in the standard way: \( \text{FV}(x) = \{ x \} \), \( \text{FV}(\text{fn } x \Rightarrow e) = \text{FV}(e) \setminus \{ x \} \) and \( \text{FV}(e_1 , e_2) = \text{FV}(e_1) \cup \text{FV}(e_2) \).

\(^1\) Assuming a standard inductive interpretation of big-step semantics.
The semantics is then defined by the following standard axioms and inference rules; intuitively we shall only be interested in evaluating upon expressions whose only free variables are among the global ones, but formally it suffices that this condition holds for the values:

\[
\begin{align*}
    e_1 & \xrightarrow{s} e_1' \\
    e_1 \cdot e_2 & \xrightarrow{s} e_1' \cdot e_2 \\
    e_2 & \xrightarrow{s} e_2' \\
    v_1 \cdot e_2 & \xrightarrow{s} v_1 \cdot e_2' \\
    v_1 \cdot v_2 & \xrightarrow{s} v_1[\mathit{x} \mapsto v_2] \text{ if } v_1 = (\mathit{fn} \ \mathit{x} \mapsto e)
\end{align*}
\]

Here \(e[\mathit{x} \mapsto v]\) denotes the expression \(e\) with all free occurrences of the variable \(x\) replaced by the value \(v\). Since the formal parameters were assumed to be distinct from the global variables, \(\text{FV}(e)\), no variable capture can take place; hence there is no need for alpha-renaming any formal parameter and therefore the formal parameters continue to be distinct from the global variables. As usual these axioms and rules are to be interpreted inductively, meaning that the judgement is defined by what can be obtained using the axioms and rules and nothing else.

**Environment based semantics**

A somewhat more complex semantics is obtained by using environments instead of substitutions. Following the pattern in [13] we need to *extend the syntax* of the language in order to define the structural operational semantics. The changes needed for the extended syntax are as follows:

\[
\begin{align*}
    ie & \in \mathbb{I}\mathbb{E}\mathbb{x}p \\
    ie ::= x \mid \mathit{fn} \ \mathit{x} \mapsto e \mid ie \cdot ie \mid \mathit{close} \ (\mathit{fn} \ \mathit{x} \mapsto e) \ \mathit{in} \ \rho \mid \mathit{bind} \ \rho \ \mathit{in} \ ie \\
    \rho & \in \mathbb{E}\mathbb{n}\mathbb{v} \\
    \rho ::= [\ ] \mid \rho[\mathit{x} \mapsto v] \\
    v & \in \mathbb{I}\mathbb{V}a\mathbb{l} \\
    v ::= \mathit{close} \ (\mathit{fn} \ \mathit{x} \mapsto e) \ \mathit{in} \ \rho
\end{align*}
\]

The expression \(\mathit{close} \ (\mathit{fn} \ \mathit{x} \mapsto e) \ \mathit{in} \ \rho\) encapsulates an unevaluated abstraction \(\mathit{fn} \ \mathit{x} \mapsto e\) with an environment \(\rho\) that gives values to all the free variables in \(\mathit{fn} \ \mathit{x} \mapsto e\); this construct is needed because we have decided to design a semantics using environments. The expression \(\mathit{bind} \ \rho \ \mathit{in} \ ie\) encapsulates a partly evaluated expression \(ie\) with a local environment \(\rho\); this construct is needed because we have decided to design a small-step semantics. Note that we retain the distinction between unevaluated expressions, \(e \in \mathbb{E}\mathbb{x}p\), and partly evaluated (or intermediate) expressions, \(ie \in \mathbb{I}\mathbb{E}\mathbb{x}p\), in order to clarify the precise points where partly evaluated expressions may occur; this will prove helpful when reasoning about the analysis. Finally, (intermediate) values are just closures, and environments are lists of mappings from variables to values: we write \(\rho[\mathit{x} \mapsto v]\) for the environment \(\rho\) augmented such that the variable \(x\)
now maps to the value v; if there is more than one binding for a given variable we always use the rightmost (most recent) one.

The operational semantics is given by a judgement of the form:

$$\rho \vdash ie_1 \overset{e}{\to} ie_2$$

Here $\rho$ is the environment in which the expression is to be evaluated. It is defined by the following standard axioms and inference rules:

$$\rho \vdash x \overset{e}{\to} v \text{ if } \rho(x) = v$$

$$\rho \vdash (\text{fn } x \Rightarrow e) \overset{e}{\to} (\text{close } (\text{fn } x \Rightarrow e) \text{ in } \rho)$$

$$\rho \vdash ie_1 \overset{e}{\to} ie'_1 \text{ if } \rho \vdash ie_1 \overset{e}{\to} ie_2 \overset{e}{\to} ie'_2$$

$$\rho \vdash v_1 ie_2 \overset{e}{\to} v_1 ie'_2$$

$$\rho \vdash v_1 v_2 \overset{e}{\to} (\text{bind } \rho_1[x \mapsto v_2] \text{ in } e) \text{ if } v_1 = (\text{close } (\text{fn } x \Rightarrow e) \text{ in } \rho_1)$$

$$\rho \vdash (\text{bind } \rho_1 \text{ in } ie_1) \overset{e}{\to} (\text{bind } \rho_1 \text{ in } ie'_1)$$

$$\rho \vdash (\text{bind } \rho_1 \text{ in } v_1) \overset{e}{\to} v_1$$

Once again this definition is to be interpreted inductively.

Explicit alpha-renaming

Let us finally consider a variation of the environment-based semantics where there is an explicit rule for alpha-renaming the bound variable of an abstraction. This will allow us to illustrate some of the difficulties that will emerge when analysing process calculi like the $\pi$-calculus where a structural congruence (containing alpha-renaming) is defined and incorporated into the semantics.

The operational semantics is then given by a judgement of the form:

$$\rho \vdash ie_1 \overset{e_0}{\to} ie_2$$

As above $\rho$ is the environment in which the expression is to be evaluated. The inductive definition is given by

analougues of the axioms and rules given for $\overset{e}{\to}$

$$\rho \vdash ie =_\alpha ie'$$

$$\rho \vdash ie \overset{e_0}{\to} ie'' \overset{e_0}{\to} ie' =_\alpha ie''$$

$$\rho \vdash ie \overset{e_0}{\to} ie''$$

where $ie =_\alpha ie'$ denotes that $ie$ is equivalent to $ie'$ modulo alpha-renaming (of formal parameters).

A similar modification, $\overset{s_\alpha}{\to}$, is possible for the substitution based sematics; we shall write $\overset{a}{\to}$ when it is not of any importance whether we refer to $\overset{e}{\to}$ or $\overset{s_\alpha}{\to}$. 

6
4 Flow Logic

Let us now turn to our second task: the specification of the program analysis. As already indicated there are a number of choices to be made. Here we shall concentrate on an abstract specification (in the manner of abstract interpretation [2]), a compositional (or syntax-directed) specification, and a specification using representations of expressions. We shall only be concerned with specifying how to check that a proposed solution is indeed acceptable; the existence of “best” (or least) acceptable solutions is treated in [9,5,11]. Also we shall only deal with succinct specifications as they exhibit a logical flavour that is well suited for semantic considerations.

4.1 Abstract Specification

The most general approach is motivated by the considerations of the collecting semantics (static semantics [2]) in abstract interpretation and works well for open systems. Here the judgement

$$\hat{\rho} \vdash^A e : W$$

expresses that the pair $$(\hat{\rho}, W)$$ is an acceptable analysis for the expression $e$: the $W$ component describes the set of function abstractions that $e$ could result in and the $$\hat{\rho}$$ component describes the set of function abstractions that the variables inside $e$ could be bound to. It is defined by the following clauses:

$$\hat{\rho} \vdash^A x : W \iff \hat{\rho}(x) \subseteq W$$

$$\hat{\rho} \vdash^A \text{fn } x \Rightarrow e : W \iff \{\text{fn } x \Rightarrow e\} \subseteq W$$

$$\hat{\rho} \vdash^A e_1, e_2 : W \iff \exists W_1, W_2 : \hat{\rho} \vdash^A e_1 : W_1 \land \hat{\rho} \vdash^A e_2 : W_2 \land \forall (\text{fn } x \Rightarrow e') \in W_1 : \exists W^' : W_2 \subseteq \hat{\rho}(x) \land \hat{\rho} \vdash^A e' : W^' \land W^' \subseteq W$$

The axiom for variables is straightforward: since the abstract environment records the set of abstract values that the variable can be bound to, we just ensure that this set is part of the set of abstract variables that can result from the expression. Also the axiom for function abstractions is straightforward: a function abstraction gives rise to a single abstract value and we ensure that it is part of what can result from the expression. The rule for function applications is a bit more complex. First we must verify that the analysis is correct as regards the operator part and as regards the operand part. For each possible function being applied, we then “link” the abstract values for the actual parameter to those for the formal parameter, we verify that the analysis is correct as regards the body of the function being called, and finally we “link” the abstract values from the function body into those of the application itself.

This definition is appropriate for open systems because at the function application we analyse the body of the function actually being called rather than assuming that it is part of the program in question and that it has already
been analysed. Hence the functions called can be allowed to come from the environment, e.g. from a library or from the arguments being supplied to the program in question.

**The need for coinduction**

There remains the problem of ensuring that the clauses displayed above do in fact define a relation, \( \bar{\rho} \models e : W \), for each expression \( e \). This is complicated by the fact that the definition is not syntax-directed: in the clause for function application we perform an analysis of an expression that need not be a subexpression of the function application in question.

The remedy is standard: we need to interpret the clauses coinductively [9]. To do so we regard the clauses as defining a function

\[
S : \mathcal{P}(\text{AEnv} \times \text{Exp} \times \text{AVal}) \rightarrow \mathcal{P}(\text{AEnv} \times \text{Exp} \times \text{AVal})
\]

that operates over sets of triples of the form \((\bar{\rho}, e, W)\) where \( \bar{\rho} \in \text{AEnv}, e \in \text{Exp}, W \in \text{AVal}, \text{AEnv} = \text{Var} \rightarrow \text{AVal}, \text{AVal} = \mathcal{P}(\text{Exp}^{\text{fin}}) \) and \( \text{Exp}^{\text{fin}} \) is the set of function abstractions in \( \text{Exp} \). The result of \( S(S) \) is defined by combining the effect of all the clauses except that any occurrence of \( \bar{\rho}' \models e' : W' \) on the right hand side is replaced by \((\bar{\rho}', e', W') \in S\). We shall omit the detailed definition of \( S \) but merely note that the function \( S \) is monotonic. By Tarski’s Theorem [17] it follows that \( S \) has a complete lattice of fixed points. The least fixed point corresponds to the standard inductive interpretation of the clauses whereas the greatest fixed point corresponds to a coinductive definition [8,3].

By taking the coinductive interpretation of the clauses above we obtain the desired definition of \( \bar{\rho} \models e : W \). By reasoning similar to the one in [9] it follows that there always exists a least (or best) analysis that is acceptable in the manner of the above clauses; in particular this means that all programs can be analysed as should not be surprising since one can simply pretend that all function abstractions can reach all places.

**The extended language**

Let us now pause a moment and think ahead. In case the analysis is to be validated with respect to the environment based semantics we will likely have to analyse also the extensions to the syntax. This calls for adding the following clauses

\[
\bar{\rho} \models \text{close (fn} \ x \ => \ e \ \text{in} \ \rho \ : \ W \ \text{iff} \ \{\text{fn} \ x \ => \ e\} \subseteq W \land \rho \ \mathcal{R}^A \ \bar{\rho}
\]

\[
\bar{\rho} \models \text{bind} \ \rho \ \text{in} \ ie : W \ \text{iff} \ \exists W' : \bar{\rho} \models ie' : W' \land W' \subseteq W \land \rho \ \mathcal{R}^A \ \bar{\rho}
\]

(as well as changing the \( e_1, e_2 \) above to be \( ie_1, ie_2 \)). The auxiliary relation \( \mathcal{R}^A \) ensures that the entities encapsulated in the environments have been properly analysed and it is defined by:

\[
\rho \ \mathcal{R}^A \ \bar{\rho} \ \text{iff} \ \forall x \in \text{dom(}\rho) : \forall y_x, e_x, \rho_x : \]

8
(\rho(x) = \text{close (} \text{fn } y_x \Rightarrow e_x \text{)} \text{ in } \rho_x) \Rightarrow
((\text{fn } y_x \Rightarrow e_x) \subseteq \rho(x) \land \rho_x \mathcal{R}^A \hat{\rho})

It is immediate that the auxiliary relation \mathcal{R}^A is well-defined: in each recursive call the environment gets smaller. The overall collection of clauses is then interpreted coinductively as before.

Semantic correctness
Let us now consider the possibility of proving the specification of the analysis correct. Recall that this takes the form of a subject reduction result:

if the analysis \hat{\rho} is acceptable for the expression \( e_1 \)
and if \( e_1 \) evolves into \( e_2 \)
then the analysis \hat{\rho} is acceptable for the expression \( e_2 \).

(Clearly the detailed formulations depend on the semantics used; they will be spelled out in detail as part of the proofs.)

**Proposition 4.1** The possibility of proving the analysis correct with respect to the semantics is given by the following table:

<table>
<thead>
<tr>
<th></th>
<th>( \models^A )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( s \rightarrow )</td>
<td>no</td>
</tr>
<tr>
<td>( e \rightarrow )</td>
<td>yes</td>
</tr>
</tbody>
</table>
| \( 
\) | no |

**Proof.** In each case we must begin with clearly formulating the correctness statement and then either disprove it by means of an example or conduct a formal proof. For the substitution based semantics the subject reduction result reads as follows:

\[ \forall \hat{\rho}, W, e_1, e_2 : (\hat{\rho} \models e_1 : W \land e_1 \xrightarrow{s} e_2) \Rightarrow (\hat{\rho} \models e_2 : W) \]

To disprove this we shall take \( e_1 = (\text{fn } x \Rightarrow (\text{fn } y \Rightarrow (\text{fn } z \Rightarrow x)) (\text{fn } u \Rightarrow u) \),
\( e_2 = (\text{fn } y \Rightarrow y) (\text{fn } z \Rightarrow (\text{fn } u \Rightarrow u)) \), \( \hat{\rho}(x) = \{\text{fn } u \Rightarrow u\}, \hat{\rho}(y) = \{\text{fn } z \Rightarrow x\}, \hat{\rho}(z) = \emptyset, \hat{\rho}(u) = \emptyset \), and \( W = \{\text{fn } z \Rightarrow x\} \).

For the environment based semantics the subject reduction result reads as follows:

\[ \forall \hat{\rho}, W, i e_1, i e_2, \rho : (\hat{\rho} \models^A i e_1 : W \land \rho \mathcal{R}^A \hat{\rho} \land \rho \vdash i e_1 \xrightarrow{e} i e_2) \Rightarrow (\hat{\rho} \models^A i e_2 : W) \]

We proceed by induction on \( \rho \vdash i e_1 \xrightarrow{e} i e_2 \). In several cases we make use of the lemma

if \( \hat{\rho} \models^A e : W_1 \) and \( W_1 \subseteq W_2 \) then \( \hat{\rho} \models^A e : W_2 \)

that can be proved by inspecting each of the clauses defining \( \models^A \) in turn.
The negative result for $\not\rightarrow$ holds for $s\not\rightarrow$ as well as $e\not\rightarrow$ (assuming that the correctness statements are analogues of those displayed above). In the case of $s\not\rightarrow$ one takes $e_1 = (\lambda x \Rightarrow (\lambda y \Rightarrow y) (\lambda z \Rightarrow z)) (\lambda u \Rightarrow u)$, $e_2 = (\lambda y \Rightarrow y) (\lambda v \Rightarrow v)$, $\rho(x) = \{\lambda u \Rightarrow u\}$, $\rho(y) = \{\lambda z \Rightarrow z\}$, $\rho(z) = \emptyset$, $\rho(u) = \emptyset$, $\rho(v) = \emptyset$, and $W = \{\lambda z \Rightarrow z\}$. The proof in the case of $e\not\rightarrow$ is similar.

**Remark**

Given the lemma in the proof of Proposition 4.1 it might seem that one could simplify the clauses for $\models$ by not writing all constraints explicitly in all clauses: one could consider adding a clause saying that $\hat{\rho} \models e : W_2$ if $\exists W_1 : W_1 \subseteq W_2 \land \hat{\rho} \models e : W_1$ and then the clause for function abstractions would simply read $\hat{\rho} \models \lambda x \Rightarrow e : \{\lambda x \Rightarrow e\}$ and “similarly” for the other clauses. This is indeed a common trick used in (inductively defined) type systems but unfortunately it turns out to be problematic for the (coinductively defined) clauses here. The reason is that the coinductive interpretation of the revised definition of $\models$ yields the relation that is universally true (because of the ability to take $W_1 = W_2$)! So to allow the simplifications (as is done in [11]) one needs a more sophisticated way of interpreting the clauses (and the offending clause must not be added).

### 4.2 Compositional Specification

In order to obtain a specification that is readily implementable one usually needs to proceed in a more syntax-directed manner. This amounts to checking the bodies of functions when they are “defined” rather than when they are called. One problem with this approach is that we may then end up analysing the bodies of functions that are never called; this can be remedied by adding a reachability component to the analysis (see e.g. [5]) but for conciseness of the presentation we shall abstain from doing so. Another problem with this approach is that we then confine the attention to closed systems: we cannot deal with functions that are not part of the program in question (or some *a priori* given library or set of arguments to the program).

Analysing function bodies when “defined” then necessitates an additional component to the analysis: a mechanism for ensuring that the set of function abstractions that can result from the body will be known at all relevant application points. Since we have assumed that all function abstractions have initially been alpha-renamed to have distinct formal parameters, it makes sense to use the formal parameter as the unique identifier for the function abstraction in question. We then extend the global analysis information, $\rho$, to contain a component $\rho(x \Rightarrow) = W$ whenever the body of $\lambda x \Rightarrow e$ may yield $W$ (just as $\hat{\rho}(x) = W$ whenever the formal parameter of $\lambda x \Rightarrow e$ may be bound to abstract values from $W$).

With these preparations we can then define a judgement of the form
\[ \hat{\rho} \models^C e : W \]

for expressing that the pair \((\hat{\rho}, W)\) is an acceptable analysis for the expression \(e\) and bearing in mind that the domain of \(\hat{\rho}\) is larger than in the abstract specification. The judgement is defined by the following clauses:

\[ \hat{\rho} \models^C x : W \iff \hat{\rho}(x) \subseteq W \]

\[ \hat{\rho} \models^C \text{fn } x \Rightarrow e : W \iff \{ \text{fn } x \Rightarrow e \} \subseteq W \land \hat{\rho} \models^C e : \hat{\rho}(x\Rightarrow) \]

\[ \hat{\rho} \models^C e_1 , e_2 : W \iff \exists W_1 , W_2 : \hat{\rho} \models^C e_1 : W_1 \land \hat{\rho} \models^C e_2 : W_2 \land \forall (\text{fn } x \Rightarrow e') \in W_1 : W_2 \subseteq \hat{\rho}(x) \land \hat{\rho}(x\Rightarrow) \subseteq W \]

Unlike the abstract specification there is no need to rely on a coinductive definition because the specification is purely compositional (or syntax-directed); however, there is no harm in viewing the specification as being a coinductive definition because the coinductive and inductive definitions turn out to agree (and on philosophical grounds one might indeed argue that one should continue to stress the fact that the specification is coinductive)!

**The extended language**

Looking ahead to possibly using the environment based semantics for validating the analysis there once more is the need to analyse the extensions to the syntax. This calls for adding the following clauses:

\[ \hat{\rho} \models^C \text{close } (\text{fn } x \Rightarrow e) \text{ in } \rho : W \iff \{ \text{fn } x \Rightarrow e \} \subseteq W \land \rho \mathcal{R}^C \hat{\rho} \land \hat{\rho} \models^C e : \hat{\rho}(x\Rightarrow) \]

\[ \hat{\rho} \models^C \text{bind } \rho \text{ in } i\rho' : W \iff \exists i\rho' : \hat{\rho} \models^C i\rho' : W' \land W' \subseteq W \land \rho \mathcal{R}^C \hat{\rho} \]

(as well as changing the \(e_1 , e_2\) above to be \(ie_1 , ie_2\)). The auxiliary relation \(\mathcal{R}^C\) is defined as follows:

\[ \rho \mathcal{R}^C \hat{\rho} \iff \forall x \in \text{dom}(\rho) : \forall y_x , e_x , \rho_x : \]

\[ (\rho(x) = \text{close } (\text{fn } y_x \Rightarrow e_x) \text{ in } \rho_x) \Rightarrow \]

\[ (\{ \text{fn } y_x \Rightarrow e_x \} \subseteq \hat{\rho}(x) \land \rho_x \mathcal{R}^C \hat{\rho} \land \hat{\rho} \models^C e_x : \hat{\rho}(y_x\Rightarrow)) \]

It is now slightly more tricky to ensure that the analysis and the auxiliary relation are well-defined since they depend recursively upon one another. One possibility is to use mathematical induction on \(n\) to prove that \(\hat{\rho} \models^C e : W\) and \(\rho \mathcal{R}^C \hat{\rho}\) are well-defined whenever the size of \(e\) and \(\rho\) is at most \(n\); here the size may be taken to be the finite number of ASCII characters needed to represent the entity.

**Relationship between the specifications**

We said above that the abstract and compositional specifications differ because we did not include a reachability component. Indeed, once this is done along the lines of [5] one can establish an equivalence result between the two
specifications. To give the flavour of this result we state without proof the
following weaker fact that holds for the analyses as defined here; it says that
(for closed systems) all acceptable analyses with respect to the compositional
specification are also acceptable with respect to the abstract specification.

**Fact 4.2** Let $e_s$ be the given program, let $\text{Exp}_s$ be the set of subexpressions
of $e_s$ and let $\text{Exp}^\text{fn}_s$ be the set of function abstractions in $e_s$. Assuming that
all $\rho(x)$ and $W$ are restricted to be subsets of $\text{Exp}^\text{fn}_s$, i.e. $AVal = \mathcal{P}(\text{Exp}^\text{fn}_s)$,
we have

$$\hat{\rho} \models e_s : W \iff \hat{\rho} \models e_s : W.$$  

The opposite implication need not hold; as an example take $\rho(x) = \emptyset$, $\rho(y) = \emptyset$,
$\rho(z) = \emptyset$, $W = \emptyset$ and consider $e_s = (\text{fn}\ x \mapsto (\text{fn}\ y \mapsto y) (\text{fn}\ z \mapsto z)).$

**Semantic correctness**

Let us now consider the possibility of establishing a subject reduction result
for this analysis.

**Proposition 4.3** The possibility of proving the analysis correct with respect
to the semantics is given by the following table:

<table>
<thead>
<tr>
<th>$\overset{s}{\rightarrow}$</th>
<th>$\overset{e}{\rightarrow}$</th>
<th>$\overset{a}{\rightarrow}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

**Proof.** For the substitution based semantics the subject reduction result
reads as follows:

$$\forall \hat{\rho}, W, e_1, e_2 : (\hat{\rho} \models^{\text{C}} e_1 : W \land e_1 \overset{\overset{s}{\rightarrow}}{\rightarrow} e_2) \Rightarrow (\hat{\rho} \models^{\text{C}} e_2 : W)$$

To disprove this statement we proceed as in the proof of Proposition 4.1.

For the environment based semantics the subject reduction result reads as follows:

$$\forall \hat{\rho}, W, i e_1, i e_2, \rho : (\hat{\rho} \models^{\text{C}} i e_1 : W \land \rho \overset{\text{RC}}{\rightarrow}^{\text{C}} \hat{\rho} \land \rho \vdash i e_1 \overset{\overset{e}{\rightarrow}}{\rightarrow} i e_2) \Rightarrow (\hat{\rho} \models^{\text{C}} i e_2 : W)$$

We proceed by induction on $\rho \vdash i e_1 \overset{\overset{e}{\rightarrow}}{\rightarrow} i e_2$. In several cases we make use of
the lemma

$$\text{if } \hat{\rho} \models^{\text{C}} e : W_1 \text{ and } W_1 \subseteq W_2 \text{ then } \hat{\rho} \models^{\text{C}} e : W_2$$

that can be proved by inspecting each of the clauses defining $\models^{\text{C}}$ in turn.

The negative result for $\overset{a}{\rightarrow}$ holds for $\overset{\overset{s}{\rightarrow}}{\rightarrow}$ as well as $\overset{\text{En}}{\rightarrow}$ (assuming
that the correctness statements are analogues of those displayed above); it
may be proved as in the proof of Proposition 4.1. \qed
4.3 Representations of Expressions

In terms of implementing the compositional analysis it would seem that we are carrying a lot of useless baggage around: the complete function bodies. This suggests defining a modified analysis that just uses representations of functions. Given our assumption that all function abstractions in the given program have initially been alpha-renamed so as to have distinct formal parameters, it makes sense to let $\text{fn}\ x$ serve as a representation of $\text{fn}\ x \Rightarrow e$. We then define the judgement

$$\hat{\rho} \triangleright e : W$$

by the following clauses that are rather directly obtained from those for $\vdash^C$:

$$\hat{\rho} \triangleright x : W \iff \hat{\rho}(x) \subseteq W$$

$$\hat{\rho} \triangleright \text{fn}\ x \Rightarrow e : W \iff \{\text{fn}\ x\} \subseteq W \land \hat{\rho} \triangleright e : \hat{\rho}(x\Rightarrow)$$

$$\hat{\rho} \triangleright e_1, e_2 : W \iff \exists W_1, W_2 : \hat{\rho} \triangleright e_1 : W_1 \land \hat{\rho} \triangleright e_2 : W_2 \land \forall (\text{fn}\ x \in W_1 : W_2 \subseteq \hat{\rho}(x) \land \hat{\rho}(x\Rightarrow) \subseteq W$$

The extended language

The clauses relevant for the extensions to the syntax are minor variations of those considered before:

$$\hat{\rho} \triangleright \text{close}\ (\text{fn}\ x \Rightarrow e) \text{ in } \rho : W \iff \{\text{fn}\ x\} \subseteq W \land \rho \mc\ R^{CR} \land \hat{\rho} \triangleright e : \hat{\rho}(x\Rightarrow)$$

$$\hat{\rho} \triangleright \text{bind } \rho \text{ in } i\epsilon : W \iff \exists W' : \hat{\rho} \triangleright i\epsilon : W' \land W' \subseteq W \land \rho \mc\ R^{CR} \hat{\rho}$$

Finally, the definition of the auxiliary relation $R^{CR}$ is obtained from the one for $R^C$:

$$\rho \mc R^{CR} \hat{\rho} \iff \forall x \in \text{dom}(\rho) : \forall y_x, e_x, \rho_x :$$

$$(\rho(x) = \text{close}\ (\text{fn}\ y_x \Rightarrow e_x) \text{ in } \rho_x) \Rightarrow$$

$$\{\text{fn}\ y_x\} \subseteq \hat{\rho}(x) \land \rho_x \mc R^{CR} \hat{\rho} \land \hat{\rho} \triangleright e_x : \hat{\rho}(y_x\Rightarrow)$$

Well-definedness of these definitions follows as for the compositional specification.

Relationship between the specifications

Intuitively the two compositional specifications should be equivalent because the body of a function abstraction is not used to carry any information. We state without proof the following fact; it states an equivalence result for closed systems.

Fact 4.4 Let $e_*$ be the given program, let $\text{Exp}_*$ be the set of subexpressions of $e_*$ and let $\text{Exp}_*^{fn}$ be the set of function abstractions in $e_*$. Writing $\text{ret}(W) = \{(\text{fn}\ x) | (\text{fn}\ x \Rightarrow e) \in W\}$ and assuming that all $\hat{\rho}(x)$ and $W$ are restricted
to be subsets of $\text{Exp}^\text{in}$, i.e. $\text{AVal} = \mathcal{P}(\text{Exp}^\text{in})$, we have

$$\hat{\rho} \models^c e_1 : W \Rightarrow (\text{ret} \circ \hat{\rho}) \models^c e_1 : \text{ret}(W)$$

Furthermore, writing $\exp(W) = \{(\text{fn } x \Rightarrow e) \in \text{Exp}, (\text{fn } x) \in W\}$ and assuming that all $\hat{\rho}(x)$ and $W$ are restricted to be subsets of $\text{ret}(\text{Exp}^\text{in})$, i.e. $\text{AVal} = \mathcal{P}(\text{ret}(\text{Exp}^\text{in}))$, we have

$$(\exp \circ \hat{\rho}) \models^c e_1 : \exp(W) \Leftrightarrow \hat{\rho} \models^c e_1 : W$$

Note that $\exp(W)$ produces exactly the same number of elements as in $W$ given our assumption that all function abstractions have initially been alpha-renamed to have distinct formal parameters.

**Semantic correctness**

The use of representations of expressions rather the expressions themselves turns out to facilitate establishing an analogue of a subject reduction result that defeated us earlier.

**Proposition 4.5** The possibility of proving the analysis correct with respect to the semantics is given by the following table:

<table>
<thead>
<tr>
<th>$\models^c$</th>
<th>$\models^c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\rightarrow$</td>
<td>yes</td>
</tr>
<tr>
<td>$\leftarrow$</td>
<td>yes</td>
</tr>
<tr>
<td>$\downarrow$</td>
<td>no</td>
</tr>
</tbody>
</table>

**Proof.** For the substitution based semantics the subject reduction result reads as follows:

$$\forall \hat{\rho}, W, e_1, e_2 : (\hat{\rho} \models^c e_1 : W \land e_1 \xrightarrow{s} e_2) \Rightarrow (\hat{\rho} \models^c e_2 : W)$$

The proof is by induction on $e_1 \xrightarrow{s} e_2$. For $(\text{fn } x \Rightarrow e) \leftarrow \rightarrow e[x \mapsto v_2]$ we use the lemma

if $\hat{\rho} \models e : W_1$ and $W_1 \subseteq W_2$ then $\hat{\rho} \models^c e : W_2$

(that can be proved by inspecting each of the clauses defining $\models^c$ in turn) and also the lemma

if $\hat{\rho} \models e : W$ and $\hat{\rho} \models^c \hat{\rho}(x)$ then $\hat{\rho} \models^c e[x \mapsto v] : W$

(that can be proved by structural induction on $e$) and we also use the fact that no variable capture can take place in $e[x \mapsto v]$ (because if $v$ is a value then $\text{FV}(v) \subseteq \text{FV}(e_1)$ and the set of formal parameters is disjoint from the set of global variables, $\text{FV}(e_1)$).

For the environment based semantics the subject reduction result reads as follows:
\[ \forall \hat{\rho}, W, i_1, i_2, \rho : (\hat{\rho} \models i_1 : W \land \rho \mathcal{R}_C \hat{\rho} \land \rho \vdash i_1 \xrightarrow{E} i_2) \Rightarrow (\hat{\rho} \not\models i_2 : W) \]

For the proof we proceed as in the proof of the corresponding case in Proposition 4.3.

The negative result for \( \xrightarrow{=} \) holds for \( \xrightarrow{s} \) as well as \( \xrightarrow{E} \) (assuming that the correctness statements are analogues of those displayed above); it may be proved as in the proof of Proposition 4.3.  \( \square \)

Representations of expressions for abstract specification

The reader might wonder whether it is only in the case of compositional specifications that it is possible to work with representations of expressions rather than the expressions themselves. In the Appendix we shall show that it is indeed possible to do so for abstract specifications although the resulting specification, \( \mathcal{A}_R \), is not of interest because the analysis is much coarser than the other analyses.

5 Conclusion

Flow Logic is by no means the first approach to formulating program analyses in a logical form. However, in our view it is the first approach that aims at integrating the insights from existing program analysis technologies (such as data flow analysis, control flow analysis and abstract interpretation) into a common form that is applicable to a wide variety of programming languages. This then motivates the current investigation into the relative usefulness of different kinds of semantics.

The technical results concerning the possibility of proving the analyses correct may be summarised as follows\(^2\):

<table>
<thead>
<tr>
<th></th>
<th>( \mathcal{A} )</th>
<th>( \mathcal{C} )</th>
<th>( \mathcal{C}_R )</th>
<th>( \mathcal{A}_R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \xrightarrow{s} )</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>(yes)</td>
</tr>
<tr>
<td>( \xrightarrow{E} )</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>(yes)</td>
</tr>
<tr>
<td>( \xrightarrow{=} )</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>

Here \( \models \) and \( \models_{CR} \) are equally precise (Fact 4.4) and only “slightly coarser” than \( \models \) (Fact 4.2) whereas \( \models_{AR} \) is so coarse as to be of no interest (Fact A.1). The table clearly shows that the environment based semantics is more flexible than either substitution based semantics or semantics making use of structural congruences\(^3\) (like alpha-renaming) in terms of being able to accomodate a

\( ^2 \) We refer to the Appendix for the missing entry.

\( ^3 \) Current work on the \( \pi \)-calculus studies techniques aimed at overcoming some of these difficulties; this involves changing the syntax of the language so as to contain “markers” for all entities that are not invariant under the congruence.
variety of specification styles for program analysis.

In our view it is easiest to develop a correct and useful program analysis if one proceeds as follows:

- *begin by developing an abstract specification.*

This is particularly so for novel calculi involving distribution and mobility because abstract specifications are able to deal with open systems. Also one is less likely to fail to observe that the compositional specifications restrict themselves to closed systems and that a reachability component is needed in order to obtain the same precision as in the abstract specification.

In order to establish semantic correctness by means of a subject reduction result it is a general principle that:

- *the analysis information should remain invariant under evaluation.*

As we have seen this puts severe demands on the choice of operational semantics: one is more or less forced to abandon working with a simple substitution based semantics in order to work with a more complex environment based semantics; unfortunately, (in keeping with [13]) this requires “artificial” extensions to the syntax, that then also have to be analysed thereby reducing the level of abstraction of the reasoning.

We believe that a compositional (or syntax-directed) specification is a prerequisite for obtaining an efficient implementation. As was explained above, this involves restricting the attention to closed systems. The development in Section 4.2 is semi-compositional [7] in the sense that all expressions considered are subexpressions of the given program; however, semi-compositionality does not suffice for having a free choice between using environment based or substitution based semantics. To achieve this we used representations of expressions in Section 4.3.

In this paper we have only considered succinct specifications and have ignored the verbose formulations of flow logic that are likely to be needed in order to obtain an efficient implementation. One further principle worth stating is that:

- *explicit program points (in the form of labelling all subexpressions [9] or demanding all expressions to be in “A-normalform” [4]) are needed for verbose formulations but not for succinct specifications.*

For the succinct formulations considered in this paper we merely assumed that all function abstractions had initially been alpha-renamed so as to have distinct formal parameters that were also distinct from the global variables. We refer to [11] for how to transform a succinct specification into a more verbose specification and to [5] for an example of how a verbose specification may be implemented.
Acknowledgements

This research was supported in part by the DART-AROS project funded by the Danish Research Councils. We wish to thank Chiara Bodei, Pierpaolo Degano, Chris Hankin, Carolyn Talcott and Mitch Wand for discussions about semantics based program analysis; Torben Amtoft provided helpful comments on a previous version.

References


A Representations of Expressions for Abstract Specification

In this appendix we show that it is possible to use representations of expressions also for abstract specifications, although the resulting analysis is so coarse as to be of little interest.

So let us define a judgement

\[ \hat{\rho} \models e : W \]

by the following clauses:

\[ \hat{\rho} \models x : W \quad \text{iff} \quad \hat{\rho}(x) \subseteq W \]

\[ \hat{\rho} \models \text{fn } x => e : W \quad \text{iff} \quad \{\text{fn } x\} \subseteq W \]

\[ \hat{\rho} \models e_1, e_2 : W \quad \text{iff} \quad \exists W_1, W_2 : \hat{\rho} \models e_1 : W_1 \land \hat{\rho} \models e_2 : W_2 \land \forall (\text{fn } x) \in W_1 : \forall e' : \exists W' : W_2 \subseteq \hat{\rho}(x) \land \hat{\rho} \models e' : W' \land W' \subseteq W \]

For completeness sake we also list the clauses for the extended syntax:

\[ \hat{\rho} \models \text{close} (\text{fn } x => e) \text{ in } \rho : W \quad \text{iff} \quad \{\text{fn } x\} \subseteq W \land \rho \mathcal{R}^{AR} \hat{\rho} \]

\[ \hat{\rho} \models \text{bind } \rho \text{ in } i e' : W \quad \text{iff} \quad \exists W' : \hat{\rho} \models i e' : W' \land W' \subseteq W \land \rho \mathcal{R}^{AR} \hat{\rho} \]

The definition of the auxiliary relation then is:

\[ \rho \mathcal{R}^{AR} \hat{\rho} \quad \text{iff} \quad \forall x \in \text{dom}(\rho) : \forall y_x, e_x, \rho_x : \]

\[ (\rho(x) = \text{close} (\text{fn } y_x => e_x) \text{ in } \rho_x) \Rightarrow (\{\text{fn } y_x\} \subseteq \hat{\rho}(x) \land \rho_x \mathcal{R}^{AR} \hat{\rho}) \]

Relationship between the specifications

The following result shows that the only acceptable analysis for unevaluated programs is the one that says that all function abstractions can reach all places. For the formal statement we need a few preparations. First note that an expression in the original syntax is either an application, a variable or a
function abstraction; if it is an application it can be “maximally expanded” into one of the forms \(((x_1 e_1) e_2) \cdots e_n\) or \(((\text{fn } y \Rightarrow e) e_1 e_2) \cdots e_n\) (for \(n > 0\)). To get access to the variable \(x\) occurring to the very left, if indeed such a variable exists, we shall define the set \(\text{LV}(e)\) as follows: \(\text{LV}(x) = \{x\}\), \(\text{LV}(\text{fn } x \Rightarrow e) = \emptyset\) and \(\text{LV}(e_1 e_2) = \text{LV}(e_1)\). Clearly \(\text{LV}(e)\) contains at most one element.

**Fact A.1** Let \(e_\ast\) be the given program and suppose that it is an application (i.e., it is not a variable or a function abstraction), that \(\forall x \in \text{LV}(e_\ast) : \rho(x) \neq \emptyset\) and that (for all \(x\)) \(\rho(x)\) and \(W\) are restricted to be subsets of \(\text{ret}(\text{Exp}^{fn})\) where \(\text{ret}(W) = \{(\text{fn } x) \mid (\text{fn } x \Rightarrow e) \in W\}\) and \(\text{Exp}^{fn}\) is the set of function abstractions;

\[
\text{if } \rho \models_{AR} e_\ast : W \text{ then } \forall x : \rho(x) = \text{ret}(\text{Exp}^{fn}) \text{ and } W = \text{ret}(\text{Exp}^{fn}).
\]

**Proof (sketch).** The key to the proof is that in the clause for application we can choose \(e' = (\text{fn } x_i \Rightarrow x_i) e_j\) where \(x_i\) ranges through all variables and \(e_j\) ranges through all function abstractions. For the proof note that since \(e_\ast\) is an application it can be “maximally expanded”: either into \(((x_1 e_1) e_2) \cdots e_n\) (for \(n > 0\)) in which case we know that \(\rho(x) \neq \emptyset\), or else into \(((\text{fn } y \Rightarrow e) e_1 e_2) \cdots e_n\) (for \(n > 0\)); in both cases we prove the desired result by induction on \(n\).

**Semantic correctness**

Despite our lack of interest in this analysis let us nonetheless consider the possibility of establishing a subject reduction result; in the table below we put answers in parantheses in order to remind us that the analysis is substantially coarser than those previously considered.

**Proposition A.2** The possibility of proving the analysis correct with respect to the semantics is given by the following table:

<table>
<thead>
<tr>
<th>(\rightarrow)</th>
<th>(\models_{AR})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(s)</td>
<td>(\text{(yes)})</td>
</tr>
<tr>
<td>(e)</td>
<td>(\text{(yes)})</td>
</tr>
<tr>
<td>(\sigma_s)</td>
<td>(\text{(yes)})</td>
</tr>
<tr>
<td>(\sigma_e)</td>
<td>(\text{(no)})</td>
</tr>
</tbody>
</table>

**Proof (sketch).** The formulations of the subject reduction results are much as in the proofs of Proposition 4.1; we shall dispense with repeating them here.

We first consider the case of the substitution based semantics. One way to prove the result is to proceed as in the proof of the corresponding case in Proposition 4.5. — A more “abstract” way of proving the result proceeds as follows where we must take care to restrict all \(\rho(x)\) and \(W\) to be subsets
of \( \text{ret}(\text{Exp}^n) \). If an expression (in the original syntax) can evaluate into another then it must be an application and hence it must expand into either \(((x \, e_1 \, e_2) \, \cdots \, e_n) \) (for \( n > 0 \)) or else \(((\text{fn} \, y \Rightarrow e) \, e_1 \, e_2 \, \cdots \, e_n) \) (for \( n > 0 \)). In fact the first case cannot arise because variables are not values. This leaves us with the second case where it follows from Fact A.1 that the \( \bar{\rho} \) and \( W \) in question must state that all function abstractions reach everywhere; but this suffices for analysing an arbitrary expression since all constraints are then vacuously fulfilled.

We next consider the case of the environment based semantics where we proceed as in the proof of the corresponding case in Proposition 4.1.

The positive result for \( \xrightarrow{s_a} \) may be proved as in the “abstract” way of proving \( \xrightarrow{s} \) above: if there is any possibility of using alpha-renaming we know by Fact A.1 that the \( \bar{\rho} \) and \( W \) in question must state that all function abstractions reach everywhere; but then alpha-renaming is not harmful.

The negative result for \( \xrightarrow{e_a} \) may be obtained as follows: let \( \forall x : \bar{\rho}(x) = \emptyset, W = \{\text{fn} \, x \Rightarrow x\}, \, \rho = [], \, ie_1 = \text{fn} \, x \Rightarrow x \) and \( ie_2 = \text{close} (\text{fn} \, y \Rightarrow y) \) in \([\]. □