ROPAS
Research On Program Analysis System
National Creative Research Initiative Center
Korea Advanced Institute of Science and Technology

ROPAS MEMO
2000-9
November 2, 2000

A Proof Method for the Correctness of Modularized kCFAs[*]

Oukseh Lee and Kwangkeun Yi

Division of Computer Science
Korea Advanced Institute of Science and Technology
{cookcu; kwang}@ropas.kaist.ac.kr

November 2, 2000

Abstract

This article is about our findings when we tried to derive a modular version from a whole-program control-flow analysis (CFA). Deriving a modular version from a whole-program kCFA makes the resulting analysis polyvariant at module-level. Hence the correctness of its modularized version cannot be proven in general with respect to the original kCFA. A convenient stepping-stone to prove the correctness of a modularized version is a whole-program kCFA that is polyvariant at module-level.

Because CFA is a basis of almost all analyses for higher-order programs, our result can be seen as a general hint of using the *module-variant* whole-program analysis in order to ease the correctness proof for a modularized version. Our work can also be seen as a formal investigation, for CFA, of the folklore that modularization improves the analysis accuracy.

1 Introduction

Modular analyses, which analyze incomplete programs such as modules, are practical alternatives to whole-program analysis for large-scale realistic programs. A whole-program analysis needs the entire program text as its input, and it has to solve a large set of equations at once. If some parts of the program are modified, it has to re-analyze the entire program. A modular analysis, on the other hand, does not need the entire program and re-analyzes only the dependent parts of the modified module.

This article is about our findings when we tried to derive a modular version from a whole-program control-flow analysis (CFA) [Shi91, NN97], to be used inside a modularized version of our exception analysis[YR01, YR97, YR98]:

- Deriving a modular version (in the framework of incremental analysis) from a whole-program kCFA [Shi91, NN97] makes the resulting analysis polyvariant at module-level.

[*]This work is supported by Creative Research Initiatives of the Korean Ministry of Science and Technology.

- Hence the correctness of its modularized version cannot be proven in general with respect to the original kCFA.
- A convenient stepping-stone to prove the correctness of a modularized version (instead of proving it against the program semantics) is a whole-program kCFA that is polyvariant at module-level.

Example 1 As an example that modularization improves the accuracy, consider a CFA of the following two higher-order code-fragments:

$$\begin{array}{l}\texttt{id = }\lambda\texttt{x.x}\\ \texttt{dec = id }\lambda\texttt{y.y-1}\end{array} \quad \text{and} \quad \texttt{inc = id }\lambda\texttt{z.z+1.}$$

The goal of CFA is to safely estimate which functions flow into each expression. Suppose we analyze the two fragments together. Because of the two calls to `id`, `id`'s formal parameter `x` is bound to both λ`y.y-1` and λ`z.z+1`. This information is propagated back to the call sites that we conclude `inc` has λ`y.y-1` (a false-flow) as well as λ`z.z+1`. On the other hand, analyzing the left fragment in isolation concludes that `id` has λ`x.x` and `dec` has λ`y.y-1`. Analyzing the second fragment with this information concludes that `inc` has only λ`z.z+1`. $\Box$

After we describe the model for our modular analysis in Section 2, we first show the case for 0CFA. After the definition of 0CFA in Section 3, we present its modular version 0CFA/m in Section 4, and show in Section 5 that it is not a safe extension of the original 0CFA. In Section 6 we define a module-variant 0CFA and prove in Section 7 that the modular version is correct for this module-variant 0CFA. In Section 8, we show that the same holds for kCFA in general: we show that modularized version kCFA/m is not a safe extension of kCFA yet is a safe extension of the whole-program module-variant kCFA. We conclude in Section 9.

2 Incremental Model for Modular Analysis

We assume that a modular analysis works inside an incremental compilation environment [AM94]. A module consists of variable declarations ("`x =` e") and a signature that enlists a subset of the declared variables visible from the other modules. Module M depends on another module M', written $M' \sqsubset M$, if and only if module M uses variables of module M'. We assume that there exists a dependency between modules and we analyze modules in sequence by their topological order, as in the incremental compilation system. We do not consider circular dependencies, for which iterative analysis of involved modules is necessary.

Figure 1 illustrates our incremental model of modular analysis. For each module in its dependence order, we analyze it and export some of the analysis results that subsequent modules may need. This exported results will be used by modules that depend on the current one. For a given module $M = (\mathit{decl}, \mathit{sig})$, let the analysis phase be $\mathcal{A}(M, \delta)$ with

$$\mathcal{A} : \mathit{Module} \times \mathit{Results} \rightarrow \mathit{Results}.$$

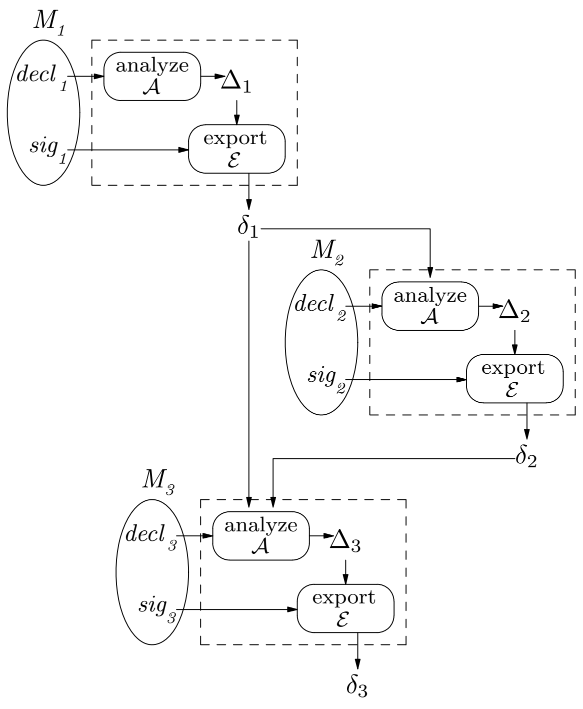

Figure 1: Incremental model for modular analysis. Module M_2 uses names declared in M_1, and M_3 uses those of M_1 and M_2.

The second input δ is the exported results from the modules that M depends on. Let the result of this analysis be Δ. From Δ, we export only some parts of it that subsequent modules may need. Let this export phase be $\mathcal{E}(\Delta, \mathit{sig})$ with

$$\mathcal{E} : \mathit{Results} \times \mathit{Signature} \to \mathit{Results}.$$

For a program that consists of modules $M_1, \cdots, M_n$, each module M_i's analysis result Δ_i and its exported set δ_i (in Figure 1) are defined as $\Delta_i = \mathcal{A}\left(M_i, \cup_{M_j \sqsubset M_i} \delta_j\right)$ and $\delta_i = \mathcal{E}(\Delta_i, \mathit{sig}_i)$, where sig_i is the signature of M_i. The final analysis result $\mathit{Sol}(M_1, \cdots, M_n)$ for the whole-program is $\Delta_1 \cup \cdots \cup \Delta_n$.

It is clear that this model has an inherent effect of polyvariant analysis; a module's analysis result is separately copied in analyzing subsequent modules. Our point here is to show how to ease the correctness proof of a modularized version when we move a whole-program analysis into this modular analysis model.

3 0CFA

The whole-program 0CFA [Shi91], whose modular version we are designing, is shown in Figure 2. We present 0CFA in the style similar to [HM97]. An input program is a sequence of declarations, and an expression is either a function, an application, a

$$\begin{array}{llll}
\mathit{Label}\ \ l & \mathit{Var}\ \ x & \mathit{Constant}\ \ c & \\
\mathit{Expr} & e & ::= & x \mid \lambda x.e^l \mid e^l\ e^l \mid c \\
\mathit{Decl} & d & ::= & x = e^l \\
\mathit{Program} & \wp & ::= & d^* \\
 & & & \\
\mathit{Node} & n & ::= & x \mid l \mid \lambda x.e^l \\
\mathit{Edge} & g & ::= & n \rightarrow n
\end{array}$$

$$\frac{x = e^l \in \wp}{x \rightarrow l} \qquad \frac{(e_1^{l_1}\ e_2^{l_2})^l \in \wp \quad l_1 \rightarrow \lambda x.e^{l_0}}{l \rightarrow l_0 \quad x \rightarrow l_2}$$

$$\frac{x^l \in \wp}{l \rightarrow x} \qquad \frac{n \rightarrow m \quad m \rightarrow \lambda x.e^l}{n \rightarrow \lambda x.e^l}$$

$$\frac{(\lambda x.e^{l_0})^l \in \wp}{l \rightarrow \lambda x.e^{l_0}}$$

Figure 2: The language and its 0CFA.

variable, or a non-function constant. The analysis computes edge "$n \rightarrow m$" between two nodes n and m. Nodes are syntactic objects: the variables or sub-expressions of the input program. All variables and labels are assumed distinct. Edge "$n \rightarrow m$" indicates that n may have the values of m (or, values of m may flow into n.). Applying the rules of Figure 2, we collect such edges until no more additions are possible. This process terminates because the number of nodes are finite for a given program. Edge "$n \rightarrow \lambda x.e^l$" in the final result indicates that n may evaluate into (or, is bound to) function $\lambda x.e^l$ in the input program. The correctness of 0CFA is known [Shi91, NN97].

4 0CFA/m: A Modularized 0CFA

We present a modular version of 0CFA in Figure 3. Rules in the analysis phase $\mathcal{A}(M, \delta)$ are the same as the rules in the whole-program 0CFA except that instead of examining the whole-program text, they only examine the current module M and the exported edges δ from the referenced modules. The premise "$\in M$ or δ" means "is a sub-expression in either module M or a node of δ." In the export phase $\mathcal{E}(\Delta, \mathit{sig})$, we conservatively export all the edges that can be needed by subsequent modules. The starting point is the signature. For a variable x in the signature, x's bindings are needed to analyze subsequent modules:

$$\frac{x \in \mathit{sig}}{x \in \mathit{Needed}}\ (\mathit{Sig}).$$

If variable x is needed to analyze subsequent modules ($x \in \mathit{Needed}$), then (1) its analysis result ($x \rightarrow \lambda y.e^l$) is exported and (2) we record ($FV(\lambda y.e^l) \subseteq \mathit{Needed}$) that the free

$$
\begin{array}{llll}
\textit{Signature} & \textit{sig} & ::= & \{x_1, \cdots, x_n\} \\
\textit{Declaration} & \textit{decl} & ::= & d^* \\
\textit{Module} & M & ::= & (\textit{decl}, \textit{sig}) \\[1ex]
\textit{Node} & n & ::= & x \mid l \mid \lambda x.e^l \\
\textit{Edge} & g & ::= & n \to n
\end{array}
$$

Analysis phase. $\mathcal{A}(M, \delta)$ = edge-set Δ closed from module M and imported edges δ by the five rules:

$$
\frac{x = e^l \in M}{x \to l}\ (\textit{Dec}) \qquad \frac{\begin{array}{c}(e_1^{l_1}\ e_2^{l_2})^l \in M \text{ or } \delta \\ l_1 \to \lambda x.e^{l_0}\end{array}}{l \to l_0 \quad x \to l_2}\ (\textit{App})
$$

$$
\frac{x^l \in M \text{ or } \delta}{l \to x}\ (\textit{Var}) \qquad \frac{\begin{array}{c}n \to m \\ m \to \lambda x.e^l\end{array}}{n \to \lambda x.e^l}\ (\textit{Tr})
$$

$$
\frac{(\lambda x.e^{l_0})^l \in M \text{ or } \delta}{l \to \lambda x.e^{l_0}}\ (\textit{Lam})
$$

Export phase. $\mathcal{E}(\Delta, \textit{sig})$ = exported-edge-set δ closed by the two rules:

$$
\frac{x \in \textit{sig}}{x \in \textit{Needed}}\ (\textit{Sig})
$$

$$
\frac{x \in \textit{Needed} \quad x \to \lambda y.e^l \in \Delta}{FV(\lambda y.e^l) \subseteq \textit{Needed} \quad x \to \lambda y.e^l}\ (\textit{ExportFn})
$$

Figure 3: 0CFA/m: a modularized 0CFA.

variables of the function are needed to analyze subsequent modules:

$$
\frac{x \in \textit{Needed} \quad x \to \lambda y.e^l \in \Delta}{FV(\lambda y.e^l) \subseteq \textit{Needed} \quad x \to \lambda y.e^l}\ (\textit{ExportFn}).
$$

Algorithm for 0CFA/m is the same as for 0CFA: we add edges by applying the rules until no more additions are possible. Note that we export code-segments in (*ExportFn*) and re-use them in (*Var*), (*Lam*), and (*App*). For an efficient implementation of 0CFA/m, we can replace code-segments by equivalent edges using simplification algorithms [FF99].

5 0CFA/m is Not a Safe Extension of 0CFA

This modular analysis 0CFA/m is more accurate than 0CFA.

Example 2 Consider the program (consisting of two modules) and its modular analysis:

$$\left(\begin{array}{l}\texttt{f = }(\lambda\texttt{x.x}^2)^1\\ \texttt{g = }(\texttt{f}^4\ (\lambda\texttt{y.y}^6)^5)^3\end{array},\ \{\texttt{f,g}\}\right) \quad\text{and}\quad \left(\texttt{h = }(\texttt{f}^8\ (\lambda\texttt{z.z}^{10})^9)^7\ ,\ \{\texttt{h}\}\right).$$

If we analyze the whole program by 0CFA, the result includes a false-flow edge $\texttt{h} \rightarrow \lambda\texttt{y.y}$ because

$$\begin{tikzcd} \texttt{h} \arrow[r] & (\texttt{f}\ \lambda\texttt{z.z}) \arrow[r] & \texttt{x} \arrow[r] \arrow[dr] & \lambda\texttt{z.z} \\ & & & \lambda\texttt{y.y} \end{tikzcd}$$

In presenting analysis results, we will not show transitively-closed edges.

However, if we analyze the two modules by 0CFA/m this false-flow edge is avoided. Analyzing the first module returns

$$\begin{array}{l}\texttt{f} \rightarrow 1 \rightarrow \lambda\texttt{x.x}^2,\\ \texttt{g} \rightarrow 3 \rightarrow 2 \rightarrow \texttt{x} \rightarrow 5 \rightarrow \lambda\texttt{y.y}^6,\\ 6 \rightarrow \texttt{y},\end{array}$$

among which 0CFA/m exports only two edges: $\texttt{f} \rightarrow \lambda\texttt{x.x}^2$ and $\texttt{g} \rightarrow \lambda\texttt{y.y}^6$. Note that $\texttt{x} \rightarrow \lambda\texttt{y.y}^6$ is not included. With the exported edges from the first module, analyzing the second module returns

$$\texttt{h} \rightarrow 7 \rightarrow 2 \rightarrow \texttt{x} \rightarrow 9 \rightarrow \lambda\texttt{z.z}^{10}.$$

The false-flow edge $\texttt{h} \rightarrow \lambda\texttt{y.y}^6$ is absent. □

This situation does not mean that 0CFA/m is incorrect; 0CFA/m is still correct (with respect to the program semantics), but because modularization makes the resulting analysis polyvariant, 0CFA/m fails to be a safe extension of the original 0CFA. Because 0CFA/m is more accurate than the whole 0CFA, the correctness relation between CFAs is

$$\begin{array}{rl}\text{Semantics} \subseteq \text{0CFA} & \text{(correctness of 0CFA)}\\ \text{0CFA/m} \subseteq \text{0CFA} & \text{(0CFA/m is not correct w.r.t. 0CFA)}\end{array}$$

where $A \subseteq B$ means that the result of B includes that of A.

In order to prove the correctness of 0CFA/m, instead of proving with respect to the program semantics, we suggest a method using a stepping-stone. If there exists an analysis A such that we can easily prove that A is correct (Semantics $\subseteq A$), and that A is more accurate than 0CFA/m ($A \subseteq$ 0CFA/m), then A makes it easy to prove the correctness of 0CFA/m.

It seems that such analysis A must be polyvariant at module-level. In Example 2, there are two applications whose function part is `f`: (`f` λ`y.y`) in M_1 and (`f` λ`z.z`) in M_2. In 0CFA, both application nodes link to `x`: (`f` λ`y.y`)$\rightarrow$`x` and (`f` λ`z.z`)$\rightarrow$`x`. The former `x` is bound to λ`y.y` and the latter `x` to λ`z.z`. These two distinct bindings for `x` can be separated ("polyvariant") if we differentiate the variable `x` by the two modules M_1 and M_2.

We show that such analysis A is a whole-program analysis that is polyvariant at module-level. We call it *module-variant 0CFA*. This analysis is a convenient stepping-stone to proving the correctness of 0CFA/m because:

$$
\begin{array}{llll}
\textit{Module} & M & & \\
\textit{ModEnv} & \sigma & \in & \textit{Var} \rightarrow \textit{Module} \\
\textit{Value} & v & ::= & (\lambda x.e^l, \sigma) \\
\textit{Solution} & S & \in & (\textit{Var} + \textit{Label}) \times \textit{Module} \rightarrow \textit{Value}
\end{array}
$$

$$
\begin{array}{lllll}
(\textit{var}) & S \models^\sigma_M x^l & \text{iff} & S(x, \sigma(x)) \subseteq S(l, M) & \\
(\textit{fn}) & S \models^\sigma_M (\lambda x.e^{l_0})^l & & & \\
 & & \text{iff} & (\lambda x.e^{l_0}, \sigma|_{FV(\lambda x.e^{l_0})}) \in S(l, M) & \\
(\textit{app}) & S \models^\sigma_M (e_1^{l_1}\ e_2^{l_2})^l & & & \\
 & & \text{iff} & S \models^\sigma_M e_1^{l_1} \quad \wedge & \\
 & & & S \models^\sigma_M e_2^{l_2} \quad \wedge & \\
 & & & \forall (\lambda x.e^{l_0}, \sigma') \in S(l_1, M) : & \\
 & & & \qquad S \models^{\sigma'[x \mapsto M]}_M e^{l_0} \quad \wedge & \\
 & & & \qquad S(l_2, M) \subseteq S(x, M) \quad \wedge & \\
 & & & \qquad S(l_0, M) \subseteq S(l, M) & \\
(\textit{con}) & S \models^\sigma_M c^l & \text{iff} & \text{true} & \\
(\textit{let}) & S \models^\sigma_M (\texttt{let}\ x = e^{l_1}\ \texttt{in}\ e^{l_2})^l & & & \\
 & & \text{iff} & S \models^\sigma_{M'} e^{l_1} \quad \wedge & \\
 & & & S \models^{\sigma[x \mapsto M']}_M e^{l_2} \quad \wedge & \\
 & & & S(l_1, M') \subseteq S(x, M') \quad \wedge & \\
 & & & S(l_2, M) \subseteq S(l, M) & \\
 & & & \text{where } x = e^{l_1} \text{ is in module } M' &
\end{array}
$$

Figure 4: Module-variant 0CFA.

- the proof is between two static analyses (0CFA/m and module-variant 0CFA) that have a smaller gap than that between a static analysis (0CFA/m) and the program semantics, and
- the correctness of module-variant 0CFA is free since it is an instance of the infinitary CFA of Nielson and Nielson [NN97].

6 Module-Variant 0CFA

6.1 Definition

Module-variant 0CFA distinguishes the same expression label (or variable) by the originating modules whose evaluations need its values. For example, if $\lambda x.x$ is called from modules M_1 and M_2 with actual argument expressions e_1 and e_2, respectively, then we distinguish the formal parameter x by M_1 and M_2, binding e_1 to (x, M_1) and e_2 to (x, M_2). The function's body expression x also has two instances, indexed by M_1 and M_2, whose values are respectively those of e_1 and e_2.

The exact definition of the module-variant 0CFA is shown in Figure 4. In order to achieve its correctness freely, we define it as an instance of the infinitary CFA [NN97].

In order to fit with the program syntax in the infinitary CFA, we assume that a program is not just a collection of declarations (a collection of modules) but a single nested let-expression.

Throughout this paper, we say "a program $\wp$ consists of modules $M_1, \cdots, M_n$" to imply that the program is a nested let-expression that has exactly the declarations of the modules in the topological order of their dependencies, and whose innermost let-body is a dummy constant. For example, a program that consists of two modules $M_1 = (x = e_1\ y = e_2, \{x\}), M_2 = (z = x, \{z\})$ is expressed "$\texttt{let}\ x = e_1\ \texttt{in}\ \texttt{let}\ y = e_2\ \texttt{in}\ \texttt{let}\ z = x\ \texttt{in}\ c$." We assume that all the declarations in a merged let-expression have their associated module names.

Judgment "$S \models^{\sigma}_{M} e^l$" means solution S respects the situation that evaluating expressions of module M under environment σ needs to evaluate e. Environment σ maps free variables of e into the modules whose evaluation bind them. This environment determines the variable's module indices for the polyvariant effect.

For the input program $\wp$ that consists of modules $M_1, \cdots, M_n$, its module-variant 0CFA is defined [NN97] as the least S such that $S \models^{\emptyset}_{\varepsilon} \wp$ where $\emptyset$ is the empty module-context environment and ε is a dummy module index for the whole program.

Let's consider the rules, case by case.

Case (var). If a variable is necessary ($S \models^{\sigma}_{M} x^l$) for evaluating expressions of module M then the values $S(l, M)$ of its label must include those $S(x, \sigma(x))$ of the variable.

Case (fn). If an immediate function expression is needed ($S \models^{\sigma}_{M} (\lambda x.e^{l_0})^l$) for module M then the analysis result $S(l, M)$ at the label must include it.

Case (app). If an application is necessary ($S \models^{\sigma}_{M} (e_1^{l_1}\ e_2^{l_2})^l$) for evaluating expressions in module M, we propagate the same module context to its sub-expressions and to the body of the called function, and we determine value-flows across the call. The application's sub-expressions have the same module context: $S \models^{\sigma}_{M} e_1^{l_1} \wedge S \models^{\sigma}_{M} e_2^{l_2}$. For each function ($\forall(\lambda x.e^{l_0}, \sigma') \in S(l_1, M)$) that can be called, (1) its formal parameter x and its body e^{l_0} have the same module context: $S \models^{\sigma'[x \mapsto M]}_{M} e^{l_0}$, (2) values of argument expression e^{l_2} flow to the formal parameter x: $S(l_2, M) \subseteq S(x, M)$, and (3) values of body expression e^{l_0} flow to the call expression $(e_1^{l_1}\ e_2^{l_2})^l$: $S(l_0, M) \subseteq S(l, M)$. Note that a module-variant effect occurs because the function's argument and body have the call expression's module index.

Case (let). Everything is the same as in the application case, except that because the let-binding "x=e^{l_1}" is a declaration in a module, we have to use this module context for the variable x and its definition e^{l_1}.

6.2 Module-Variant 0CFA is Correct

Because the module-variant 0CFA is an instance of the infinitary control flow analysis [NN97], it is correct by Theorem 4.1 of Nielson and Nielson [NN97].

Our module-variant 0CFA is instantiated as the following. For the context domains, whose elements are used to enable polyvariance, we choose as follows:

$$\begin{aligned} \widehat{Mem} &\stackrel{\triangle}{=} Module \\ \widehat{MC} &\stackrel{\triangle}{=} Module \end{aligned}$$

Hence the projection is defined as $\pi(M,\sigma) \stackrel{\triangle}{=} M$. For the instantiators (of Table 3 [NN97, p.339]) we choose as follows. For application expression, we ensure that the context of a function body (M_0) and the context of its argument (M_x) are the same as the context of the application (M):

$$\mathcal{I}^{fn}_{app}(\sigma, M, \sigma', M'_0, e^l; M_0, M_x) \stackrel{\triangle}{=} M_0 = M_x = M.$$

For let-expression, we ensure that the context of a declaration (M_1) and the context of its declared variable (M_x) are the same as their associated module (M'):

$$\begin{aligned}&\mathcal{I}_{let}(\sigma, M, (\texttt{let } x \texttt{=} e^{l_1} \texttt{ in } e^{l_2})^l; M_1, M_2, M_x)\\ &\qquad \stackrel{\triangle}{=} (M = M_2) \wedge (M_x = M_1 = M') \text{ where } x \texttt{=} e^{l_1} \in M'.\end{aligned}$$

For other cases, instantiators does not change the context:

$$\begin{aligned}&\mathcal{I}_{fn}(\sigma, M, (\lambda x.e^{l_0})^l; M_0) \stackrel{\triangle}{=} M_0 = M\\ &\mathcal{I}_{app}(\sigma, M, (e_1^{l_1}\ e_2^{l_2})^l; M_1, M_2) \stackrel{\triangle}{=} M_1 = M_2 = M.\end{aligned}$$

7 0CFA/m is a Safe Extension of Module-Variant 0CFA

We prove this by showing that there exists a solution S of the module-variant 0CFA that is covered by the result of 0CFA/m. Definition 2 defines a solution S that is covered by the result of 0CFA/m, and Theorem 1 asserts that the S is a solution of the module-variant 0CFA. We write Needed_M to denote the *Needed* set of the exporting phase in analyzing module M by 0CFA/m (See Figure 3).

Definition 1 (x reaches M via M') *Let Δ_M be the solved edges in analyzing module M by 0CFA/m.*

- *Variable x reaches M_n via M_0 iff $M_0 = M_n$ and $x \in \Delta_{M_n}$, or there exists a path $M_0 \sqsubset M_1 \cdots \sqsubset M_n$ such that for all $0 \leq i < n$, $x \in \mathit{Needed}_{M_i}$.*
- *Expression e^l reaches M iff e^l is in module M or e^l occurs in the exported edges from the referenced modules of M.*
- *Environment σ reaches M iff, for all x in $dom(\sigma)$, x reaches M via $\sigma(x)$.*

Definition 2 ($|\mathit{Sol}_{\mathrm{0CFA/m}}(M_1, \cdots, M_n)|$) *Let $\mathit{Sol}_{\mathrm{0CFA/m}}(M_1, \cdots, M_n)$ be the result edges from analyzing modules $M_1, \cdots, M_n$ by 0CFA/m. Its corresponding form $|\mathit{Sol}_{\mathrm{0CFA/m}}(M_1, \cdots, M_n)|$ in the solution space for the module-variant 0CFA is defined as:*

$$\begin{aligned}&|\mathit{Sol}_{\mathrm{0CFA/m}}(M_1, \cdots, M_n)|(n, M) =\\ &\quad \{(\lambda x.e^l, \sigma) \mid n \rightarrow \lambda x.e^l \in \Delta_M,\ \sigma \text{ reaches } M,\ dom(\sigma) = FV(\lambda x.e^l)\}\end{aligned}$$

where Δ_M is the 0CFA/m's solution for module M.

Fact. By definition, $|\mathit{Sol}_{\mathrm{0CFA/m}}(\cdot)|$ is "covered by" $\mathit{Sol}_{\mathrm{0CFA/m}}(\cdot)$: if $(\lambda x.e^l, \_) \in |\mathit{Sol}_{\mathrm{0CFA/m}}(\cdot)|(n, M)$ then $(n \rightarrow \lambda x.e^l) \in \mathit{Sol}_{\mathrm{0CFA/m}}(\cdot)$.

Theorem 1 (Correctness of 0CFA/m) *Let program $\wp$, as a let-expression, consist of modules $M_1, \cdots, M_n$. $|Sol_{\text{0CFA/m}}(M_1, \cdots, M_n)| \models^{\emptyset}_{\varepsilon} \wp$ holds, where $\emptyset$ is the empty module-context environment and ε is a dummy module index for the whole program.*

Proof. Let $S = |Sol_{\text{0CFA/m}}(M_1, \cdots, M_n)|$. Judgment $S \models^{\sigma}_{M} e^l$ holds if it is included in the greatest fixed point of the function

$$F : \textit{Judgments} \rightarrow \textit{Judgments}$$

derived from Figure 4 [NN97]. $F(Q)$ gives us a set of left-hand side judgments asserted by the rules of Figure 4 assuming that judgments in Q hold. If we find a set Q of judgments such that $(S \models^{\emptyset}_{\varepsilon} \wp) \in Q$ and $Q \subseteq F(Q)$, then by the co-induction principle [MT91], Q is included in the greatest fixed point of F and $S \models^{\emptyset}_{\varepsilon} \wp$ holds.

Therefore, the module-variant 0CFA's solution, which is defined as the least X such that $X \models^{\emptyset}_{\varepsilon} \wp$, is included in the modularized solution $Sol_{\text{0CFA/m}}(M_1, \cdots, M_n)$.

Appendix A has the co-induction proof. □

The correctness relation between CFAs becomes:

$$\text{Semantics} \subseteq \text{module-variant 0CFA} \subseteq \text{0CFA/m} \subseteq \text{0CFA}.$$

Note that the module-variant 0CFA is not a modular analysis. It is a *whole-program* analysis, found as facilitating the correctness proof of the modular 0CFA (0CFA/m).

8 Modularizing kCFA

The next question is: what if we modularize already polyvariant CFAs? The answer is that modularization of an polyvariant CFA can make the result analysis more polyvariant than the original CFA.

Example 3 As an example that modularization of kCFA [Shi91] improves the accuracy, consider 1CFA of the following two higher-order code-fragments:

$$\left(\begin{array}{l} \texttt{f = (}\lambda\texttt{x.(}\lambda\texttt{z.z) x)} \\ \texttt{g = f }\lambda\texttt{y.y} \end{array} , \{\texttt{f,g}\} \right) \quad \text{and} \quad \left(\texttt{h = f }\lambda\texttt{w.w} , \{\texttt{h}\} \right).$$

First consider the 1CFA for the whole program consisting of three declarations. Because 1CFA distinguishes the same variable by the call sites which bind the variable, it cannot distinguish the two dynamic calls to λ`z.z` inside `f`, which occurred for `g` and `h`. That is, the two instances of `z` are not distinguished. Hence, it concludes that `h` can evaluate to both λ`w.w` and λ`y.y`. However, analyzing modules separately, we can export from the first module `f` $\rightarrow$ `(`λ`x.(`λ`z.z) x)` and `g` $\rightarrow$ λ`y.y`, and conclude that `h` can evaluate to only λ`w.w`. For any k in kCFA, we can show similar counter-example where its modular version is more accurate than kCFA. □

Example 4 As an example that modularizing the polymorphic-splitting CFA [WJ98] improves the accuracy, consider the following two higher-order code-fragments:

$$\left(\begin{array}{l} \texttt{f = }\lambda\texttt{x.x} \\ \texttt{g = }\lambda\texttt{y.(f y)} \\ \texttt{h = g }\lambda\texttt{z.z} \end{array} , \{\texttt{g,h}\} \right) \quad \text{and} \quad \left(\texttt{i = g }\lambda\texttt{w.w} , \{\texttt{i}\} \right)$$

Analyzing these four declarations together, the polymorphic-splitting CFA concludes that `i` can be evaluated to both λ`z.z` and λ`w.w`, because it cannot distinguish the two calls to `f` inside `g`, which occurred for `h` and `i`. However, analyzing modules separately, we can export, from the first module, `f` $\rightarrow$ λ`x.x`, `g` $\rightarrow$ λ`y.(f y)` and `h` $\rightarrow$ λ`z.z`, and conclude that `i` can be evaluated to only λ`w.w`. $\square$

Hence the correctness of modularized versions of kCFA and the polymorphic-splitting CFA *cannot* be proven in general with respect to the original ones. We can prove the correctness of their modularized versions, as in 0CFA, using their module-variant versions. The module-variant versions are achieved simply by coupling the original versions with the module-variant 0CFA.

In the following sections we will present kCFA, its modular version kCFA/m, a module-variant kCFA, and the proof that kCFA/m is a safe extension of the module-variant kCFA. Although we will not show the case of the polymorphic-splitting CFA, it is similar to that of kCFA.

8.1 kCFA

Figure 5 is kCFA, whose modular version will be presented in the next section. The rules are basically the same as in 0CFA, except that the nodes in the resulting control flow graph are indexed by the active-call sequence. An active-call sequence C is a sequence of call-sites that are currently active. For kCFA, the sequence's length is at most k; we keep only the most recent k call-sites. We write ϵ for the empty call-site sequence. The context information of the current active-call sequence is propagated by the relation "$C, \sigma \vdash e^l$," which indicates that expression e can be executed when the active-call sequence is C and the call environment is σ. A call environment maps variables to their active-call sequences at their bindings. Edge "$n \rightarrow m$" indicates that n may have the values of m. A single expression (or variable) in program has distinct instances in the analysis result, identified by different call-sequence indices.

For example, consider the (App_k) rule:

$$\frac{C, \sigma \vdash (e_1^a\, e_2^b)^l \quad a_C \rightarrow (\lambda x.e^{l'}, \sigma')}{\begin{array}{c} l \oplus C, \sigma'[x \mapsto l \oplus C] \vdash e^{l'} \\ x_{l\oplus C} \rightarrow b_C \quad l_C \rightarrow {l'}_{l\oplus C} \end{array}} \; (App_k)$$

For an application expression l at context (C, σ), suppose its function part a_C is $(\lambda x.e^{l'}, \sigma')$. The actual parameter b_C of the current context C is bound to the formal parameter: $x_{l\oplus C} \rightarrow b_C$. The incremented call-sequence context for x reflects the new call at l. The return value ${l'}_{l\oplus C}$ from the body becomes the value of the application: $l_C \rightarrow {l'}_{l\oplus C}$. The body expression's context reflects the new call at l: $l \oplus C, \sigma'[x \mapsto l \oplus C] \vdash e^{l'}$.

Applying the rules of Figure 5, we collect edges and relations until no more additions are possible. This process terminate because the number of nodes are finite for a given program.

kCFA is correct; it is straightforward to show by co-induction that a program's kCFA solution is a model for the program's uniform-kCFA [NN97].

$$\begin{array}{llcl}
\mathit{Label} & l, a, b & \in & \mathit{Lab} \\
\mathit{Context} & C, \epsilon & \in & \mathit{Lab}^{\leq k} \\
\mathit{ConEnv} & \sigma & \in & \mathit{Var} \to \mathit{Context} \\
\mathit{Node} & n & ::= & x_C \mid l_C \mid (\lambda x.e^l, \sigma) \\
\mathit{Edge} & g & ::= & n \to n
\end{array}$$

$$\frac{x = e^l \in \wp}{x_\epsilon \to l_\epsilon \quad \epsilon, \sigma \vdash e^l}\ (\mathit{Dec}_k\wp)$$
$$\text{where } \sigma \supseteq \{y \mapsto \epsilon \mid y \in \mathit{FV}(e)\}$$

$$\frac{C, \sigma \vdash x^l}{l_C \to x_{\sigma(x)}}\ (\mathit{Var}_k)$$

$$\frac{C, \sigma \vdash (\lambda x.e^{l_0})^l}{l_C \to \left(\lambda x.e^{l_0}, \sigma|_{\mathit{FV}(\lambda x.e^{l_0})}\right)}\ (\mathit{Lam}_k)$$

$$\frac{C, \sigma \vdash (e_1^{l_1}\ e_2^{l_2})^l}{C, \sigma \vdash e_1^{l_1} \quad C, \sigma \vdash e_2^{l_2}}\ (\mathit{Appd}_k)$$

$$\frac{C, \sigma \vdash (e_1^a\ e_2^b)^l \quad a_C \to (\lambda x.e^{l'}, \sigma')}{\begin{array}{c} l \oplus C, \sigma'[x \mapsto l \oplus C] \vdash e^{l'} \\ l_C \to l'_{l \oplus C} \quad x_{l \oplus C} \to b_C \end{array}}\ (\mathit{App}_k)$$
$$\text{where } l \oplus (l_n \cdots l_1) = \begin{cases} l l_n \cdots l_1 & \text{if } n < k; \\ l l_n \cdots l_2 & \text{if } n = k. \end{cases}$$

$$\frac{n_{C_1} \to m_{C_2} \quad m_{C_2} \to (\lambda x.e^l, \sigma)}{n_{C_1} \to (\lambda x.e^l, \sigma)}\ (\mathit{Tr}_k)$$

Figure 5: kCFA.

8.2 kCFA/m: A Modularized kCFA

Our modularized version kCFA/m is achieved similarly to 0CFA/m. Rules in the analysis phase $\mathcal{A}(M, \delta)$ are identical to those in the whole-program kCFA except that rule $(\mathit{Dec}_k\wp)$ is replaced by rule (Dec_k) that examines only the current module text. In the export phase $\mathcal{E}(\Delta, \mathit{sig})$, we conservatively export all the edges that can be needed by subsequent modules. The starting point is the signature. For a variable x in the signature, x's bindings are needed to analyze subsequent modules because subsequent modules can directly refer to x, hence:

$$\frac{x \in \mathit{sig}}{x_\epsilon \in \mathit{Needed}}\ (\mathit{Sig}_k).$$

Note that every declared variable in modules has no call-site (ϵ) when it is bound to values. If the binding of variable x_C is needed to analyze subsequent modules ($x_C \in \mathit{Needed}$), then (1) its analysis result ($x_C \to (\lambda y.e^l, \sigma)$) is exported and (2) the

Analysis phase. $\mathcal{A}(M, \delta)$ = edge-set Δ closed from module M and δ by the identical rules in kCFA, except that rule (Dec$_{k\wp}$) is replaced by rule (Dec$_k$):

$$\frac{x = e^l \in M}{x_\epsilon \to l_\epsilon \quad \epsilon, \sigma \vdash e^l}\ (\mathit{Dec}_k)$$
$$\text{where } \sigma \supseteq \{y \mapsto \epsilon \mid y \in \mathit{FV}(e)\}$$

Export phase. $\mathcal{E}(\Delta, \mathit{sig})$ = exported-edge-set δ closed by the two rules:

$$\frac{x \in \mathit{sig}}{x_\epsilon \in \mathit{Needed}}\ (\mathit{Sig}_k)$$

$$\frac{x_C \in \mathit{Needed} \quad x_C \to (\lambda y.e^l, \sigma) \in \Delta}{\begin{array}{c} x_C \to (\lambda y.e^l, \sigma) \\ \left\{ z_{\sigma(z)} \mid z \in \mathit{dom}(\sigma) \right\} \subseteq \mathit{Needed} \end{array}}\ (\mathit{ExportFn}_k)$$

Figure 6: kCFA/m.

bindings of the free variables in the function values are needed to analyze subsequent modules ($\left\{ z_{\sigma(z)} \mid z \in \mathit{dom}(\sigma) \right\} \subseteq \mathit{Needed}$):

$$\frac{x_C \in \mathit{Needed} \quad x_C \to (\lambda y.e^l, \sigma) \in \Delta}{\begin{array}{c} x_C \to (\lambda y.e^l, \sigma) \\ \left\{ z_{\sigma(z)} \mid z \in \mathit{dom}(\sigma) \right\} \subseteq \mathit{Needed} \end{array}}\ (\mathit{ExportFn}_k)$$

8.3 kCFA/m is Not a Safe Extension of kCFA

The result of kCFA/m does not always include that of kCFA.

Example 5 Let us analyze the two modules in Example 3 by 1CFA/m:

$$M_1 = \left(\begin{array}{l} \texttt{f = } (\lambda\texttt{x.}((\lambda\texttt{z.z}^5)^3\ \texttt{x}^4)^2)^1 \\ \texttt{g = } (\texttt{f}^7\ (\lambda\texttt{y.y}^9)^8)^6 \end{array},\ \{\texttt{f},\texttt{g}\} \right)$$
$$M_2 = \left(\texttt{h = } (\texttt{f}^{11}\ (\lambda\texttt{w.w}^{13})^{12})^{10}\ ,\ \{\texttt{h}\} \right)$$

Analyzing the first module returns

$$\begin{array}{l} 7_\epsilon \to \texttt{f}_\epsilon \to 1_\epsilon \to \lambda\texttt{x.}((\lambda\texttt{z.z}^5)^3\ \texttt{x}^4)^2, \\ \texttt{g}_\epsilon \to 6_\epsilon \to 2_6 \to 5_2 \to \texttt{z}_2 \to 4_6 \to \texttt{x}_6 \to 8_\epsilon \to \lambda\texttt{y.y}^9, \\ 3_6 \to (\lambda\texttt{z.z}^5)_6, \end{array}$$

among which 1CFA/m exports only two edges

$$\texttt{f}_\epsilon \to \lambda\texttt{x.}((\lambda\texttt{z.z}^5)^3\ \texttt{x}^4)^2 \text{ and } \texttt{g}_\epsilon \to \lambda\texttt{y.y}^9.$$

Note that $z_2 \to \lambda\texttt{y.y}^9$ is not included. Analyzing the second module returns

$$\begin{array}{l} \texttt{h}_\epsilon \to 10_\epsilon \to 2_{10} \to 5_2 \to \texttt{z}_2 \to 4_{10} \to \texttt{x}_{10} \to 12_\epsilon \to \lambda\texttt{w.w}^{13}, \\ 3_{10} \to \lambda\texttt{z.z}^5. \end{array}$$

Thus 1CFA/m concludes that `h` can evaluate to only λ`w.w`. On the other hand, as discussed in Example 3, 1CFA for the whole-program concludes that `h` has λ`y.y` (a false-flow) as well as λ`w.w`. $\square$

8.4 Module-Variant kCFA

kCFA/m is a correct analysis, which can be proven, not with respect to the original kCFA, but with respect to a module-variant kCFA.

Our module-variant kCFA is a "conjunctive" combination of the original kCFA and the module-variant 0CFA (in Figure 7). A context of the module-variant kCFA is a pair containing an active-call sequence of length up to k (as in kCFA) *and* a module index (as in module-variant 0CFA). The way to manipulate the call sequence follows that of kCFA, and the way to manipulate the module index follows that of the module-variant 0CFA. For example, in (*app*), if the context of a call-site labeled l is a pair containing a call sequence C and module M, then the context of the called function's body is a pair, $l \oplus C$ (as in kCFA) and M (as in the module-variant 0CFA). This module-variant kCFA is achieved straightforwardly; a general recipe for combining two CFAs is illustrated in Appendix C. Because such a combined CFA is also an instance of the infinitary CFA of Nielson and Nielson [NN97], the module-variant kCFA's correctness follows from Theorem 4.1 in [NN97].

For the input program $\wp$ that consists of modules $M_1, \cdots, M_n$, its module-variant kCFA is defined [NN97] as the least S such that $S \models^{\emptyset}_{\epsilon,\varepsilon} \wp$, where $\emptyset$ is the empty environment, ϵ is the empty context sequence, and ε is a dummy module index for the whole program.

8.5 kCFA/m is a Safe Extension of Module-Variant kCFA

The proof technique is exactly the same as in the case for 0CFA/m. We prove by showing that there exists a solution S of the module-variant kCFA that is covered by the result of kCFA/m. Definition 5 defines a solution S that is covered by the result of kCFA/m, and Theorem 2 asserts that the S is a solution of the module-variant kCFA.

Definition 3 (x_C reaches M via M') *Let Δ_M be the solved edges in analyzing module M by kCFA/m.*

- *Variable x_C reaches M_n via M_0 if and only if $M_0 = M_n$ and $x_C \in \Delta_{M_n}$, or there exists a path $M_0 \sqsubset M_1 \sqsubset \cdots \sqsubset M_n$ such that for all $0 \le i < n$, $x_C \in Needed_{M_i}$.*
- *Environment σ reaches M if and only if, for all $x \mapsto (C, M') \in \sigma$, x_C reaches M via M'*

Definition 4 ($|\sigma|$) *For a given environment σ of the module-variant kCFA, the corresponding environment $|\sigma|$ for kCFA/m is $\{x \mapsto C \mid x \mapsto (C, M) \in \sigma\}$.*

Definition 5 ($|Sol_{k\mathrm{CFA/m}}(M_1, \cdots, M_n)|$) *Let $Sol_{k\mathrm{CFA/m}}(M_1, \cdots, M_n)$ be the result edges from analyzing modules $M_1, \cdots, M_n$ by kCFA/m. Its corresponding form $|Sol_{k\mathrm{CFA/m}}(M_1, \cdots, M_n)|$ in the solution space for the module-variant kCFA is defined as:*

$$|Sol_{k\mathrm{CFA/m}}(M_1, \cdots, M_n)|(n, (C, M)) = \\ \left\{(\lambda x.e^l, \sigma) \;\middle|\; n_C \to (\lambda x.e^l, |\sigma|) \in \Delta_M,\ \sigma \text{ reaches } M,\ dom(\sigma) = FV(\lambda x.e^l)\right\}$$

$$\begin{array}{rccl}
\textit{ContMod} & (C,M) & \in & \textit{Lab}^{\leq k} \times \textit{Module} \\
\textit{ContModEnv} & \sigma & \in & \textit{Var} \to \textit{ContMod} \\
\textit{Value} & v & ::= & (\lambda x.e^l, \sigma) \\
\textit{Solution} & S & \in & (\textit{Var} + \textit{Label}) \times \textit{ContMod} \to \textit{Value}
\end{array}$$

$$\begin{array}{lll}
(\textit{var}) & S \models^{\sigma}_{C,M} x^l & \text{iff } S(x,\sigma(x)) \subseteq S(l,(C,M)) \\
(\textit{fn}) & S \models^{\sigma}_{C,M} (\lambda x.e^{l_0})^l & \text{iff } (\lambda x.e^{l_0}, \sigma|_{FV(\lambda x.e^{l_0})}) \in S(l,(C,M)) \\
(\textit{app}) & S \models^{\sigma}_{C,M} (e_1^{l_1}\ e_2^{l_2})^l & \text{iff } S \models^{\sigma}_{C,M} e_1^{l_1} \quad \wedge \\
 & & \quad S \models^{\sigma}_{C,M} e_2^{l_2} \quad \wedge \\
 & & \quad \forall (\lambda x.e^{l_0}, \sigma') \in S(l_1,(C,M)) : \\
 & & \qquad S \models^{\sigma'[x\mapsto(l\oplus C,M)]}_{l\oplus C,M} e^{l_0} \quad \wedge \\
 & & \qquad S(l_2,(C,M)) \subseteq S(x,(l\oplus C,M)) \quad \wedge \\
 & & \qquad S(l_0,(l\oplus C,M)) \subseteq S(l,(C,M)) \\
(\textit{con}) & S \models^{\sigma}_{C,M} c^l & \text{iff true} \\
(\textit{let}) & S \models^{\sigma}_{C,M} (\texttt{let } x = e_1^{l_1} \texttt{ in } e_2^{l_2})^l & \text{iff } S \models^{\sigma}_{C,M'} e_1^{l_1} \quad \wedge \\
 & & \quad S \models^{\sigma[x\mapsto(C,M')]}_{C,M} e_2^{l_2} \quad \wedge \\
 & & \quad S(l_1,(C,M')) \subseteq S(x,(C,M')) \quad \wedge \\
 & & \quad S(l_2,(C,M)) \subseteq S(l,(C,M)) \\
 & & \quad \text{where } x = e^{l_1} \text{ is in module } M'
\end{array}$$

Figure 7: Module-variant kCFA = kCFA $\times$ the module-variant 0CFA.

where Δ_M is the kCFA/m's solution for module M.

Fact. By definition, $|Sol_{k\text{CFA/m}}(\cdot)|$ is "covered by" $Sol_{k\text{CFA/m}}(\cdot)$: if $(\lambda x.e^l, \sigma) \in |Sol_{k\text{CFA/m}}(\cdot)|(n,(C,M))$ then $n_C \to (\lambda x.e^l, |\sigma|) \in Sol_{k\text{CFA/m}}(\cdot)$.

Theorem 2 (Correctness of kCFA/m) *Let program $\wp$, as a let-expression, consist of modules $M_1, \cdots, M_n$. $|Sol_{k\text{CFA/m}}(M_1,\cdots,M_n)| \models^{\emptyset}_{\epsilon,\varepsilon} \wp$ holds, where $\emptyset$ is the empty environment, ϵ is the empty context sequence, and ε is a dummy module index for the whole program.*

Proof. Let $S = |Sol_{k\text{CFA/m}}(M_1,\cdots,M_n)|$. $F(Q)$ gives us a set of left-hand-side judgments asserted by the rules of Figure 7 assuming that judgments in Q hold. If we find a set Q of judgments such that $(S \models^{\emptyset}_{\epsilon,\varepsilon} \wp) \in Q$ and $Q \subseteq F(Q)$, then by the co-induction principle [MT91], Q is included in the greatest fixed point of F and $S \models^{\emptyset}_{\epsilon,\varepsilon} \wp$ holds.

Therefore, the module-variant kCFA's solution, which is defined as the least X such that $X \models^{\emptyset}_{\epsilon,\varepsilon} \wp$, is included in the modularized solution $Sol_{k\text{CFA/m}}(M_1,\cdots,M_n)$.

See Appendix B for the co-induction proof. □

9 Conclusion

Modular analyses, which are necessary in practice for analyzing large-scale programs, are usually designed *after* whole-program analyses' cost-accuracy balance is assured by extensive tests against realistic programs. A cost-effective, practical program analysis is achieved by first finding an effective whole-program analysis and then modularizing it. This practice is observed also in literature; only recently have modular versions of particular flow analyses been reported [CRL99, CmWH00, FF99].

However, deriving a correct modular version from a given whole-program analysis has received little attention. For example, the abstract interpretation framework [CC77, CC92] does not yet cover the practice of designing modular analyses; it assumes that the whole-program text is available a priori. Within the type system framework, modular analysis is considered free [TJ94, Ban97, PS92, PL99, TJ92]. This is because the type environment, which has the analysis solution for the free variables (i.e., other modules), are manifest in the typing rules. Also, the notion of principal types and type polymorphism coincide very well with the modular analysis model [Ban97]. But the type-based modular analyses are limited to typed languages.

In this article we reported that deriving a modular version from a whole-program kCFA (for any k in the framework of incremental analysis) makes the resulting analysis polyvariant at module-level. Hence the correctness of its modularized version cannot be proven in general with respect to the original kCFA. In order to prove the correctness of a modularized version, we presented a method using, as a convenient stepping-stone, a whole-program kCFA that is polyvariant at module-level.

Last question is: how far-reaching is the principle of module-variant analysis? If CFAs are already polyvariant at module-level (e.g. one in [WJ98, pages 178]), then their modularizations cannot improve their accuracies, hence no need for module-variant versions to facilitate the correctness proof. For any analysis in general, we conjecture the same is true (modularization of an analysis can make it polyvariant at module-level), because CFA is a basis of almost all analyses for higher-order programs.

Our result can be seen as a general hint of using the *module-variant* whole-program analysis in order to ease the correctness proof for a modularized version. Our work can also be seen as a formal investigation, for CFA, of the folklore that modularization improves the analysis accuracy.

Appendix

A Proof of Theorem 1

Theorem 1. *Let a program $\wp$, as a let-expression, consists of modules $M_1, \cdots, M_n$. $|Sol_{\mathrm{0CFA/m}}(M_1, \cdots, M_n)| \models^{\emptyset}_{\varepsilon} \wp$ holds, where $\emptyset$ is the empty module-context environment and ε is a dummy module index for the whole program.*

Proof. Let $S = |Sol_{\mathrm{0CFA/m}}(M_1, \cdots, M_n)|$. Judgment $S \models^{\sigma}_{M} e^l$ holds if it is included in the greatest fixed point of the function

$$F : \mathit{Judgments} \rightarrow \mathit{Judgments}$$

derived from Figure 4 [NN97]. $F(Q)$ gives us a set of left-hand side judgments asserted by the rules of Figure 4 assuming that judgments in Q hold. If we find a set Q of judgments such that $(S \models^{\emptyset}_{\varepsilon} \wp) \in Q$ and $Q \subseteq F(Q)$, then by the co-induction principle [MT91], Q is included in the greatest fixed point of F and $S \models^{\emptyset}_{\varepsilon} \wp$ holds.

Let Q be

$$\begin{array}{l}
\left\{S \models^{\sigma}_{M} c^{l} \mid \text{constant } c\right\} \cup \\
\left\{\begin{array}{ll} S \models^{\sigma}_{\varepsilon} (\texttt{let } x\texttt{=}e_1^{l_1} \texttt{ in } e_2^{l_2})^{l} \mid & \\ \quad (\texttt{let } x\texttt{=}e_1^{l_1} \texttt{ in } e_2^{l_2})^{l} \in \wp, & \\ \quad \sigma \subseteq \{y \mapsto M_i \mid \exists i.\, y = e \in M_i\}, & \\ \quad \mathit{dom}(\sigma) \supseteq FV(\texttt{let } x\texttt{=}e_1^{l_1} \texttt{ in } e_2^{l_2}) & \end{array}\right\} \cup \\
\left\{\begin{array}{ll} S \models^{\sigma}_{M} e^{l} \mid & e^{l} \text{ reaches } M,\ \sigma|_{FV(e)} \text{ reaches } M, \\ & \mathit{dom}(\sigma) \supseteq FV(e) \end{array}\right\}.
\end{array}$$

Obviously, $(S \models^{\emptyset}_{\varepsilon} \wp) \in Q$ because $FV(\wp) = \emptyset$. We need to show $Q \subseteq F(Q)$. We prove this by case analysis for the judgments in Q.

- **case** (*var*): Consider $S \models^{\sigma}_{M} x^{l}$ from Q. We need to prove that $(S \models^{\sigma}_{M} x^{l}) \in F(Q)$. By (*var*), it is enough to prove that $S(x, \sigma(x)) \subseteq S(l, M)$. Suppose that $S(x, \sigma(x))$ includes $(\lambda y.e^{l_0}, \sigma')$. By the definition of S,

$$x \rightarrow \lambda y.e^{l_0} \in \Delta_{\sigma(x)}, \tag{1}$$
$$\sigma' \text{ reaches } \sigma(x), \text{ and} \tag{2}$$
$$\mathit{dom}(\sigma') = FV(\lambda y.e^{l_0}). \tag{3}$$

Because $(S \models^{\sigma}_{M} x^{l}) \in Q$, by the definition of Q,

$$x^{l} \text{ reaches } M, \tag{4}$$
$$\sigma|_{FV(x)} \text{ reaches } M,\ \mathit{dom}(\sigma) \supseteq FV(x). \tag{5}$$

(5) implies that x reaches M via $\sigma(x)$. Thus by (1) and (*ExportFn*),

$$x \rightarrow \lambda y.e^{l_0} \in \Delta_M, \text{ and} \tag{6}$$

the variables in $FV(\lambda y.e^{l_0})$ reaches M via $\sigma(x)$. Thus by (2) and (3),

$$\sigma' \text{ reaches } M. \tag{7}$$

By (*Var*), (4) implies that

$$l \rightarrow x \in \Delta_M. \tag{8}$$

By (6), (8) and (*Tr*),

$$l \rightarrow \lambda y.e^{l_0} \in \Delta_M. \tag{9}$$

Therefore by the definition of S, (3), (7), and (9) imply $S(l, M)$ includes $(\lambda y.e^{l_0}, \sigma')$.

- **case** (*fn*): Consider $S \models^{\sigma}_{M} (\lambda x.e^{l_0})^l$ from Q. We need to prove that $(S \models^{\sigma}_{M} (\lambda x.e^{l_0})^l) \in F(Q)$. By (*fn*), it is enough to prove that $(\lambda x.e^{l_0}, \sigma|_{FV(\lambda x.e^{l_0})}) \in S(l, M)$. Because $(S \models^{\sigma}_{M} (\lambda x.e^{l_0})^l) \in Q$, by the definition of Q,

$$\sigma|_{FV(\lambda x.e^{l_0})} \text{ reaches } M, \tag{10}$$
$$dom(\sigma) \supseteq FV(\lambda x.e^{l_0}), \tag{11}$$

and $(\lambda x.e^{l_0})^l$ reaches M. Then by (*Lam*),

$$l \to \lambda x.e^{l_0} \in \Delta_M. \tag{12}$$

Therefore by the definition of S, (10), (11), and (12) imply $(\lambda x.e^{l_0}, \sigma|_{FV(\lambda x.e^{l_0})}) \in S(l, M)$.

- **case** (*app*): Consider $S \models^{\sigma}_{M} (e_1^{l_1}\ e_2^{l_2})^l$ from Q. We need to prove that $(S \models^{\sigma}_{M} (e_1^{l_1}\ e_2^{l_2})^l) \in F(Q)$. By (*app*), it is enough to prove that
  - $(S \models^{\sigma}_{M} e_1^{l_1}) \in Q$, $(S \models^{\sigma}_{M} e_2^{l_2}) \in Q$, and
  - $\forall (\lambda x.e^{l_0}, \sigma') \in S(l_1, M)$: $(S \models^{\sigma'[x \mapsto M]}_{M} e^{l_0}) \in Q$, $S(l_2, M) \subseteq S(x, M)$, and $S(l_0, M) \subseteq S(l, M)$.

We prove the first sub-case: $(S \models^{\sigma}_{M} e_1^{l_1}) \in Q$ and $(S \models^{\sigma}_{M} e_2^{l_2}) \in Q$. Because $(S \models^{\sigma}_{M} (e_1^{l_1}\ e_2^{l_2})^l) \in Q$, by the definition of Q,

$$(e_1^{l_1}\ e_2^{l_2})^l \text{ reaches } M, \tag{13}$$
$$\sigma|_{FV(e_1^{l_1}\ e_2^{l_2})} \text{ reaches } M, \text{ and} \tag{14}$$
$$dom(\sigma) \supseteq FV(e_1^{l_1}\ e_2^{l_2}). \tag{15}$$

(13) implies that $e_1^{l_1}$ and $e_2^{l_2}$ reach M, (14) implies $\sigma|_{FV(e_1)}$ and $\sigma|_{FV(e_2)}$ reach M, and (15) implies $dom(\sigma) \supseteq FV(e_1) \cup FV(e_2)$. Therefore by the definition of Q, $(S \models^{\sigma}_{M} e_1^{l_1}) \in Q$ and $(S \models^{\sigma}_{M} e_2^{l_2}) \in Q$.

Now we prove the second sub-case. Suppose that $(\lambda x.e^{l_0}, \sigma') \in S(l_1, M)$. By the definition of S,

$$l_1 \to \lambda x.e^{l_0} \in \Delta_M, \tag{16}$$
$$dom(\sigma') = FV(\lambda x.e^{l_0}), \text{ and } \sigma' \text{ reaches } M. \tag{17}$$

By (13), (16) and (*App*),

$$x \to l_2 \in \Delta_M, \text{ and} \tag{18}$$
$$l \to l_0 \in \Delta_M. \tag{19}$$

(16) implies

$$e^{l_0} \text{ reaches } M. \tag{20}$$

Because x occurs in Δ_M by (18), x reaches M via M by definition. Thus by (17),

$$\sigma'[x \mapsto M] \text{ reaches } M. \tag{21}$$

Because $FV(e) \subseteq FV(\lambda x.e^{l_0}) \cup \{x\}$, by (17),

$$dom(\sigma'[x \mapsto M]) \supseteq FV(e). \tag{22}$$

Then by the definition of Q, (20), (21), and (22) imply $(S \models_M^{\sigma'[x\mapsto M]} e^{l_0}) \in Q$.

Now we prove that (18) implies $S(l_2, M) \subseteq S(x, M)$. Suppose that $x \to l_2 \in \Delta_M$ and $(\lambda y.e_3^{l_3}, \sigma_3) \in S(l_2, M)$. Then by the definition of S, σ_3 reaches M, $dom(\sigma_3) = FV(\lambda y.e_3^{l_3})$, and $l_2 \to \lambda y.e_3 \in \Delta_M$. By (*Tr*), $x \to \lambda y.e_3 \in \Delta_M$. Then by the definition of S, $(\lambda y.e_3^{l_3}, \sigma_3) \in S(x, M)$. We can prove similarly that (19) implies $S(l, M) \subseteq S(l_0, M)$.

- **case** (*const*): Consider $S \models_M^\sigma c^l \in Q$. By (*const*), it always holds thus it is included in $F(Q)$.

- **case** (*let*): Consider $S \models_\varepsilon^\sigma (\texttt{let}\ x\texttt{=}e_1^{l_1}\ \texttt{in}\ e_2^{l_2})^l$ from Q. We need to prove that $(S \models_\varepsilon^\sigma (\texttt{let}\ x\texttt{=}e_1^{l_1}\ \texttt{in}\ e_2^{l_2})^l) \in F(Q)$. By (*let*), it is enough to prove that $(S \models_M^\sigma e_1^{l_1}) \in Q$, $(S \models_\varepsilon^{\sigma[x\mapsto M]} e_2^{l_2}) \in Q$, $S(l_1, M) \subseteq S(x, M)$, and $S(l_2, \varepsilon) \subseteq S(l, \varepsilon)$ where $x\texttt{=}e_1^{l_1} \in M$. Because $x\texttt{=}e_1^{l_1} \in M$,

$$e_1^{l_1} \text{ reaches } M. \tag{23}$$

By the definition of Q,

$$\sigma \subseteq \{y \mapsto M_i \mid \exists i.y\texttt{=}e \in M_i\} \text{ and} \tag{24}$$

$$dom(\sigma) \supseteq FV(\texttt{let}\ x\texttt{=}e_1^{l_1}\ \texttt{in}\ e_2^{l_2}). \tag{25}$$

Because $FV(\texttt{let}\ x\texttt{=}e_1^{l_1}\ \texttt{in}\ e_2^{l_2}) \supseteq FV(e_1)$, (25) implies

$$dom(\sigma) \supseteq FV(e_1). \tag{26}$$

Because e_1 is a top-level expression in module M, $FV(e_1)$ only consists of names declared in modules. Hence (24) implies

$$\sigma|_{FV(e_1)} \text{ reaches } M. \tag{27}$$

Then by the definition of Q, (23), (26) and (27) imply $(S \models_M^\sigma e_1^{l_1}) \in Q$.

$e_2^{l_2}$ is a let-expression or a constant. If $e_2^{l_2}$ is a constant, by the definition of Q, $(S \models_\varepsilon^{\sigma[x\mapsto M]} e_2^{l_2}) \in Q$. If $e_2^{l_2}$ is a let-expression, because (24) implies $\sigma[x \mapsto M] \subseteq \{y \mapsto M_i \mid \exists i.y\texttt{=}e \in M_i\}$ and (25) implies $FV(e_2) \subseteq FV(\texttt{let}\ x\texttt{=}e_1^{l_1}\ \texttt{in}\ e_2^{l_2}) \cup \{x\} \subseteq dom(\sigma[x \mapsto M])$, by the definition of Q, $(S \models_\varepsilon^{\sigma[x\mapsto M]} e_2^{l_2}) \in Q$.

Because $x\texttt{=}e_1^{l_1} \in M$, by (*Dec*), $x \to l_1 \in \Delta_M$, from which, similarly to the last part of the (*app*) case, we can prove $S(l_1, M) \subseteq S(x, M)$. Because l and l_2 are not used in 0CFA/m, $S(l, \varepsilon) = S(l_2, \varepsilon) = \emptyset$. $\square$

B Proof of Theorem 2

Theorem 2. *Let a program $\wp$, as a let-expression, consists of modules $M_1, \cdots, M_n$. $|Sol_{k\mathrm{CFA/m}}(M_1, \cdots, M_n)| \models^{\emptyset}_{\epsilon,\varepsilon} \wp$ holds, where $\emptyset$ is the empty environment, ϵ is the empty context sequence, and ε is a dummy module index for the whole program.*

Proof. Let $S = |Sol_{k\mathrm{CFA/m}}(M_1, \cdots, M_n)|$. $F(Q)$ gives us a set of left-hand-side judgments asserted by the rules of Figure 7 assuming that judgments in Q hold. If we find a set Q of judgments such that $(S \models^{\emptyset}_{\epsilon,\varepsilon} \wp) \in Q$ and $Q \subseteq F(Q)$, then by the co-induction principle [MT91], Q is included in the greatest fixed point of F and $S \models^{\emptyset}_{\epsilon,\varepsilon} \wp$ holds.

Let Q be

$$\begin{array}{l}
\left\{S \models^{\sigma}_{C,M} c^l \mid \text{constant } c\right\} \cup \\
\left\{\begin{array}{l} S \models^{\sigma}_{\epsilon,\varepsilon} (\texttt{let } x \texttt{=} e_1^{l_1} \texttt{ in } e_2^{l_2})^l \mid \\ \qquad (\texttt{let } x \texttt{=} e_1^{l_1} \texttt{ in } e_2^{l_2})^l \in \wp, \\ \qquad \sigma \subseteq \{y \mapsto (\epsilon, M_i) \mid \exists i.\, y \texttt{=} e \in M_i\}, \\ \qquad dom(\sigma) \supseteq FV(\texttt{let } x \texttt{=} e_1^{l_1} \texttt{ in } e_2^{l_2}) \end{array}\right\} \cup \\
\left\{\begin{array}{ll} S \models^{\sigma}_{C,M} e^l \mid & (C, |\sigma| \vdash e^l) \in \Delta_M,\ \sigma|_{FV(e)} \text{ reaches } M, \\ & dom(\sigma) \supseteq FV(e) \end{array}\right\}.
\end{array}$$

Obviously, $(S \models^{\emptyset}_{\epsilon,\varepsilon} \wp) \in Q$ because $FV(\wp) = \emptyset$. We need to show $Q \subseteq F(Q)$. We prove this by case analysis for the judgments in Q.

- **case** (*var*): Consider $S \models^{\sigma}_{C,M} x^l$ from Q. We need to prove that $(S \models^{\sigma}_{C,M} x^l) \in F(Q)$. By (*var*), it is enough to prove that $S(x, \sigma(x)) \subseteq S(l, (C, M))$. Let $\sigma(x)$ be (C', M'). Suppose that $S(x, \sigma(x))$ includes $(\lambda y.e^{l_0}, \sigma')$. Then by the definition of S,

$$x_{C'} \to (\lambda y.e^{l_0}, |\sigma'|) \in \Delta_{M'}, \tag{28}$$
$$\sigma' \text{ reaches } M', \text{ and} \tag{29}$$
$$dom(\sigma') = FV(\lambda y.e^{l_0}). \tag{30}$$

  Because $(S \models^{\sigma}_{C,M} x^l) \in Q$, by the definition of Q,

$$(C, |\sigma| \vdash x^l) \in \Delta_M, \tag{31}$$
$$\sigma|_{FV(x)} \text{ reaches } M, \text{ and } dom(\sigma) \supseteq FV(x). \tag{32}$$

  Because (32) implies that $x_{C'}$ reaches M via M', by (28) and (*ExportFn$_k$*),

$$x_{C'} \to (\lambda y.e^{l_0}, |\sigma'|) \in \Delta_M \tag{33}$$

  and for all $z \in dom(\sigma')$, $z_{|\sigma'|(z)}$ reaches M via M'. Thus by (29) and (30),

$$\sigma' \text{ reaches } M. \tag{34}$$

  By (31), (*Var$_k$*), and $|\sigma|(x) = C'$, $l_C \to x_{C'} \in \Delta_M$. Then by (33) and (*Tr$_k$*),

$$l_C \to (\lambda y.e^{l_0}, |\sigma'|) \in \Delta_M. \tag{35}$$

  Then by the definition of S, (30), (34), and (35) imply $(\lambda y.e^{l_0}, \sigma') \in S(l, (C, M))$.

- **case** (*fn*): Consider $S \models^{\sigma}_{C,M} (\lambda x.e^{l_0})^l$ from Q. We need to prove that $(S \models^{\sigma}_{C,M} (\lambda x.e^{l_0})^l) \in F(Q)$. By (*fn*), it is enough to prove that $(\lambda x.e^{l_0}, \sigma|_{FV(\lambda x.e^{l_0})}) \in S(l,(C,M))$. Because $(S \models^{\sigma}_{C,M} (\lambda x.e^{l_0})^l) \in Q$, by the definition of Q,

$$\sigma|_{FV(\lambda x.e^{l_0})} \text{ reaches } M, \tag{36}$$
$$\mathit{dom}(\sigma) \supseteq FV(\lambda x.e^{l_0}), \text{ and} \tag{37}$$
$$(C, |\sigma| \vdash (\lambda x.e^{l_0})^l) \in \Delta_M. \tag{38}$$

  By (Lam_k), (38) implies

$$l_C \to (\lambda x.e^{l_0}, (|\sigma|)|_{FV(\lambda x.e^{l_0})}) \in \Delta_M. \tag{39}$$

  Therefore by the definition of S, (36), (37), and (39) imply $(\lambda x.e^{l_0}, \sigma|_{FV(\lambda x.e^{l_0})}) \in S(l,(C,M))$.

- **case** (*app*): Consider $S \models^{\sigma}_{C,M} (e_1^{l_1}\ e_2^{l_2})^l$ from Q. We need to prove that $(S \models^{\sigma}_{C,M} (e_1^{l_1}\ e_2^{l_2})^l) \in F(Q)$. By (*app*), it is enough to prove that

  – $(S \models^{\sigma}_{C,M} e_1^{l_1}) \in Q$, $(S \models^{\sigma}_{C,M} e_2^{l_2}) \in Q$, and

  – $\forall (\lambda x.e^{l_0}, \sigma') \in S(l_1,(C,M))$: $(S \models^{\sigma'[x \mapsto (l\oplus C, M)]}_{l\oplus C,M} e^{l_0}) \in Q$, $S(l_2,(C,M)) \subseteq S(x,(l\oplus C,M))$, and $S(l_0,(l\oplus C,M)) \subseteq S(l,(C,M))$.

  We prove the first sub-case: $(S \models^{\sigma}_{C,M} e_1^{l_1}) \in Q$ and $(S \models^{\sigma}_{C,M} e_2^{l_2}) \in Q$. Because $(S \models^{\sigma}_{C,M} (e_1^{l_1}\ e_2^{l_2})^l) \in Q$, by the definition of Q,

$$(C, \sigma \vdash (e_1^{l_1}\ e_2^{l_2})^l) \in \Delta_M, \tag{40}$$
$$\sigma|_{FV(e_1^{l_1}\ e_2^{l_2})} \text{ reaches } M, \text{ and} \tag{41}$$
$$\mathit{dom}(\sigma) \supseteq FV(e_1^{l_1}\ e_2^{l_2}). \tag{42}$$

  By $(Appd_k)$, (40) implies $(C, \sigma \vdash e_1^{l_1}) \in \Delta_M$ and $(C, \sigma \vdash e_2^{l_2}) \in \Delta_M$. (41) implies that $\sigma|_{FV(e_1)}$ and $\sigma|_{FV(e_2)}$ reaches M. (42) implies $\mathit{dom}(\sigma) \supseteq FV(e_1) \cup FV(e_2)$. Therefore by the definition of Q, $(S \models^{\sigma}_{C,M} e_1^{l_1}) \in Q$ and $(S \models^{\sigma}_{C,M} e_2^{l_2}) \in Q$.

  Now we prove the second sub-case. Suppose that $(\lambda x.e^{l'}, \sigma') \in S(l_1,(C,M))$. By the definition of S,

$$l_{1C} \to (\lambda x.e^{l'}, |\sigma'|) \in \Delta_M, \tag{43}$$
$$\sigma' \text{ reaches } M, \text{ and} \tag{44}$$
$$\mathit{dom}(\sigma') \supseteq FV(\lambda x.e^{l'}). \tag{45}$$

  By (40), (43) and (App_k),

$$(l\oplus C, |\sigma'|[x \mapsto l\oplus C] \vdash e^{l'}) \in \Delta_M, \tag{46}$$
$$l_C \to l'_{l\oplus C} \in \Delta_M, \text{ and} \tag{47}$$
$$x_{l\oplus C} \to l_{2C} \in \Delta_M. \tag{48}$$

Because $x_{l\oplus M}$ is in Δ_M by (48), $x_{l\oplus M}$ reaches M via M by definition. Thus by (44),

$$\sigma'[x \mapsto (l \oplus C, M)] \text{ reaches } M. \tag{49}$$

Because $FV(e) \subseteq FV(\lambda x.e^{l_0}) \cup \{x\}$, (45) implies

$$dom(\sigma'[x \mapsto (l \oplus C, M)]) \supseteq FV(e). \tag{50}$$

Then by the definition of Q, (46), (49), and (50) imply $(S \models^{\sigma'[x\mapsto(l\oplus C,M)]}_{l\oplus C,M} e^{l_0}) \in Q$.

Now we prove that (47) implies $S(l', (l \oplus C, M)) \subseteq S(l, (C, M))$. Suppose that $l_C \to l'_{l\oplus C} \in \Delta_M$ and $(\lambda y.e_3^{l_3}, \sigma_3) \in S(l', (l \oplus C, M))$. By the definition of S, σ_3 reaches M, $dom(\sigma_3) = FV(\lambda y.e_3^{l_3})$ and $l'_{l\oplus C} \to (\lambda y.e_3^{l_3}, |\sigma_3|)_{C_3} \in \Delta_M$. Then by (Tr_k), $l_C \to (\lambda y.e_3^{l_3}, |\sigma_3|) \in \Delta_M$. By the definition of S, $(\lambda y.e_3^{l_3}, \sigma_3) \in S(l, (C, M))$. We can prove similarly that (48) implies $S(l_2, (C, M)) \subseteq S(x, (l \oplus C, M))$.

- **case** (*const*): Consider $S \models^{\sigma}_{C,M} c^l$ from Q. By (*const*), it always holds, thus it is included in $F(Q)$.

- **case** (*let*): Consider $S \models^{\sigma}_{\epsilon,\varepsilon} (\texttt{let } x = e_1^{l_1} \texttt{ in } e_2^{l_2})^l$ from Q. We need to prove that $(S \models^{\sigma}_{\epsilon,\varepsilon} (\texttt{let } x = e_1^{l_1} \texttt{ in } e_2^{l_2})^l) \in F(Q)$. By (*let*), it is enough to prove that $(S \models^{\sigma}_{\epsilon,M} e_1^{l_1}) \in Q$, $(S \models^{\sigma[x\mapsto(\epsilon,M)]}_{\epsilon,\varepsilon} e_2^{l_2}) \in Q$, $S(l_1, (\epsilon, M)) \subseteq S(x, (\epsilon, M))$, and $S(l_2, (\epsilon, \varepsilon)) \subseteq S(l, (\epsilon, \varepsilon))$ where $x = e_1^{l_1} \in M$.

  By the definition of Q,

$$\sigma \subseteq \{y \mapsto (\epsilon, M_i) \mid \exists i. y = e \in M_i\}, \text{ and} \tag{51}$$
$$dom(\sigma) \supseteq FV(\texttt{let } x = e_1^{l_1} \texttt{ in } e_2^{l_2}). \tag{52}$$

  Because $FV(\texttt{let } x = e_1^{l_1} \texttt{ in } e_2^{l_2}) \supseteq FV(e_1)$, (52) implies

$$dom(\sigma) \supseteq FV(e_1). \tag{53}$$

  Because e_1 is a top-level expression in module M, $FV(e_1)$ only consists of names declared in modules. Hence (51) implies

$$\sigma|_{FV(e_1)} \text{ reaches } M. \tag{54}$$

  Because $x = e_1^{l_1} \in M$, by (51), (53), and (Dec_k),

$$(\epsilon, |\sigma| \vdash e_1^{l_1}) \in \Delta_M, \text{ and} \tag{55}$$
$$x_\epsilon \to l_{1\epsilon} \in \Delta_M. \tag{56}$$

  By the definition of Q, (53), (54), and (55) imply $(S \models^{\sigma}_{\epsilon,M} e_1^{l_1}) \in Q$.

  $e_2^{l_2}$ is a let-expression or a constant. If $e_2^{l_2}$ is a constant, by the definition of Q, $(S \models^{\sigma[x\mapsto(\epsilon,M)]}_{\epsilon,\varepsilon} e_2^{l_2}) \in Q$. If $e_2^{l_2}$ is a let-expression, because (51) implies $\sigma[x \mapsto (\epsilon, M)] \subseteq \{y \mapsto (\epsilon, M_i) \mid \exists i. y = e \in M_i\}$ and (52) implies $FV(e_2) \subseteq$

$FV(\texttt{let}\ x = e_1^{l_1}\ \texttt{in}\ e_2^{l_2}) \cup \{x\} \subseteq dom(\sigma[x \mapsto (\epsilon, M)])$, by the definition of Q, $(S \models_{\epsilon,\varepsilon}^{\sigma[x\mapsto(\epsilon,M)]} e_2^{l_2}) \in Q$.

We can prove that (56) implies $S(l_1, (\epsilon, M)) \subseteq S(x, (\epsilon, M))$ similarly to the last part of the (*app*) case. Because l and l_2 are not used in kCFA/m, $S(l, (\epsilon, \varepsilon)) = S(l_2, (\epsilon, \varepsilon)) = \emptyset$. □

C Coupled CFA

For two CFAs A and B defined as an instance of the infinitary CFA, the coupled CFA $(A \times B)$ of A and B is defined as follows. The context is the pair of the contexts of A and B, and the label distinguisher is also the pair of those of A and B:

$$\begin{array}{rcl} \widehat{Mem} & \triangleq & \widehat{Mem}_A \times \widehat{Mem}_B \\ \widehat{MEnv} & \triangleq & Var \to (\widehat{Mem}_A \times \widehat{Mem}_B) \\ \widehat{MC} & \triangleq & \widehat{MC}_A \times \widehat{MC}_B. \end{array}$$

Then the projection function π is defined by those of A and B:

$$\pi(m, \sigma)] \triangleq (\pi_A(m^A, \sigma^A), \pi_B(m^B, \sigma^B))$$

where $(m_1, m_2)^A \triangleq m_1$, $(m_1, m_2)^B \triangleq m_2$, and

$$\begin{array}{l} \sigma^A \triangleq \left\{x \mapsto m^A \mid x \mapsto m \in \sigma\right\} \\ \sigma^B \triangleq \left\{x \mapsto m^B \mid x \mapsto m \in \sigma\right\}. \end{array}$$

The instantiators have to ensure the conditions of the instantiators of A and B; that is, an instantiator $\mathcal{I}(m, \sigma, e^l; m')$ is defined as:

$$\begin{array}{rcl} \mathcal{I}(m, \sigma, e^l; m') & \triangleq & \mathcal{I}_A(m^A, \sigma^A, e^l; m'^A) \\ & \wedge & \mathcal{I}_B(m^B, \sigma^B, e^l; m'^B). \end{array}$$

The coupled CFA is an instance of the infinitary CFA, and is more accurate than both A and B.

References

[AM94] Andrew W. Appel and David B. MacQueen. Separate compilation for Standard ML. In *Proceedings of the SIGPLAN Conference on Programming Language Design and Implementation*, pages 13–23, June 1994.

[Ban97] Anindya Banerjee. A modular, polyvariant, and type-based closure analysis. In *ACM SIGPLAN International Conference on Functional Programming*, pages 1–10, 1997.

[CC77] Patrick Cousot and Radhia Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proceedings of The ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 238–252, 1977.

[CC92] Patrick Cousot and Radhia Cousot. Inductive definitions, semantics and abstract interpretation. In *Proceedings of The ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 83–94, 1992.

[CmWH00] Ben-Chung Cheng and Wen mei W. Hwu. Modular interprocedural pointer analysis using access paths: Design, implementation, and evaluation. In *Proceedings of the SIGPLAN Conference on Programming Language Design and Implementation*, pages 57–69, June 2000.

[CRL99] Ramkrishna Chatterjee, Barbara G. Ryder, and William A. Landi. Relevant context inference. In *Proceedings of The ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 133–146, January 1999.

[FF99] Cormac Flanagan and Matthias Felleisen. Componential set-based analysis. *ACM Transactions on Programming Languages and Systems*, 21(2):370–416, March 1999.

[HM97] Nevin Heintze and David McAllester. Linear-time subtransitive control flow analysis. In *Proceedings of the SIGPLAN Conference on Programming Language Design and Implementation*, pages 261–272, June 1997.

[MT91] Robin Milner and Mads Tofte. Co-induction in relational semantics. *Theoretical Computer Science*, 87:209–220, 1991.

[NN97] Flemming Nielson and Hanne Riis Nielson. Infinitary control flow analysis: a collecting semantics for closure analysis. In *Proceedings of The ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 332–345, January 1997.

[PL99] François Pessaux and Xavier Leroy. Type-based analysis of uncaught exceptions. In *Proceedings of The ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 276–290, January 1999.

[PS92] Jens Palsberg and Michael I. Schwartzbach. Safety analysis versus type inference. *Information and Computation*, 118(1):128–141, 1992.

[Shi91] Olin Shivers. *Control-Flow Analysis of Higher-Order Languages*. PhD thesis, Carnegie Mellon University, May 1991. Technical Report CMU-CS-91-145.

[TJ92] Jean-Piere Talpin and Pierre Jouvelot. Polymorphic type, region and effect inference. *Journal of Functional Programming*, 2(3):245–271, July 1992.

[TJ94] Yan Mei Tang and Pierre Jouvelot. Separate abstract interpretation for control-flow analysis. In *Lecture Notes in Computer Science*, volume 789, pages 224–243. Springer-Verlag, proceedings of the theoretical aspect in computer science edition, 1994.

[WJ98] Andrew K. Wright and Suresh Jagannathan. Polymorphic splitting: an effective polyvariant flow analysis. *ACM Transactions on Programming Languages and Systems*, 20(1):166–207, 1998.

[YR97] Kwangkeun Yi and Sukyoung Ryu. Towards a cost-effective estimation of uncaught exceptions in SML programs. In *Proceedings of the 4th International Static Analysis Symposium*, volume 1302 of *Lecture Notes in Computer Science*, pages 98–113. Springer-Verlag, 1997.

[YR98] Kwangkeun Yi and Sukyoung Ryu. SML/NJ Exception Analyzer 0.98, 1998. `http://compiler.kaist.ac.kr/pub/exna/exna-README.html`.

[YR01] Kwangkeun Yi and Sukyoung Ryu. A cost-effective estimation of uncaught exceptions in Standard ML programs. *Theoretical Computer Science*, 273(1), 2001. Extended version of [YR97] (to appear).