Control-flow analysis of function call and returns by abstract interpretation
Jan Midtgaard, Thomas Jensen

To cite this version:

HAL Id: inria-00574944
https://inria.hal.science/inria-00574944
Submitted on 9 Mar 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Control-Flow Analysis of Function Calls and Returns by Abstract Interpretation

Jan Midtgaard  
Roskilde University  
jmid@ruc.dk

Thomas P. Jensen  
CNRS  
thomas.jensen@irisa.fr

Abstract
We derive a control-flow analysis that approximates the interprocedural control-flow of both function calls and returns in the presence of first-class functions and tail-call optimization. In addition to an abstract environment, our analysis computes for each expression an abstract control stack, effectively approximating where function calls return across optimized tail calls. The analysis is systematically calculated by abstract interpretation of the stack-based \( C_{EK} \) abstract machine of Flanagan et al. using a series of Galois connections. Abstract interpretation provides a unifying setting in which we 1) prove the equivalence between the composition of a continuation-passing style (CPS) transformation followed by an abstract interpretation of a stack-less CPS machine, and 2) extract an equivalent constraint-based formulation, thereby providing a rational reconstruction of a constraint-based control-flow analysis from abstract interpretation principles.

Categories and Subject Descriptors F.3.2 [Logics and Meanings of Programs]: Semantics of Programming Languages—Program Analysis

General Terms Languages, Theory, Verification

Keywords Control flow analysis, abstract interpretation, tail-call optimization, continuation-passing style, direct style, constraint-based analysis

1. Introduction
The control flow of a functional program is expressed in terms of function calls and returns. As a result, iteration in functional programs is expressed using recursive functions. In order for this approach to be feasible, language implementations perform tail-call optimization of function calls [Clinger, 1998], by not pushing a stack frame on the control stack at call sites in tail position. Consequently functions do not necessarily return control to their caller. Control-flow analysis (CFA) has long been a staple of program optimization and verification. Surprisingly, research on control-flow analysis has focused on calls: A textbook CFA [Nielson et al., 1999]. Our systematic approximation of a known operational semantics leads to a CFA that “will determine where the flow of control may be transferred to in the case of a function return.” The resulting analysis thereby approximates both call and return information for a higher-order, direct-style language. Interestingly it does so by approximating the control stack.

Consider the example program in Fig. 1(a). The program contains three functions: two named function \( f \) and \( g \) and an anonymous function \( \text{fn } x => x \). A standard direct-style CFA can determine that the application of \( f \) in each branch of the conditional will call the anonymous function \( \text{fn } x => x \) at run time. Building a call-graph based on this output gives rise to Fig. 1(b), where we have named the main expression of the program main. In addition to the above resolved call, our analysis will determine that the anonymous function returns to the let-binding of \( y \) in main upon completion, rather than to its caller. The analysis hence gives rise to the call graph in Fig. 1(c).

On a methodological level, we derive the analysis systematically by Cousot-Cousot-style abstract interpretation. The analysis approximates the reachable states of an existing abstract machine from the literature: the \( C_{EK} \) machine of Flanagan et al. [1993]. We obtain the analysis as the result of composing the collecting semantics induced by the abstract machine with a series of Galois connections that each specifies one aspect of the abstraction in the analysis.

We show how the abstract interpretation formulation lends itself to a lock-step equivalence proof between our analysis and a previously derived CPS-based CFA. More precisely, we define a relation between the abstract domains of the analyses that is a simulation between the two, reducing the proof to a fixpoint induction over the abstract interpretations.
To sum up, the main contributions of this article are:

- An abstract interpretation-derivation of a CFA for a higher-order functional language from a well-known operational semantics,
- a resulting CFA with reachability which computes both call and return control-flow,
- a proof of equivalence of the analysis of programs in direct style and the CPS analysis of their CPS counterparts,
- an equivalent constraint-based analysis extracted from the above.

1.1 Related work

We separate the discussion of related analyses in two: direct-style analyses and analyses based on CPS.

**Direct-style CFA** has a long research history. Jones [1981] initially developed methods for approximating the control flow of lambda terms. Since then Sestoft [1989] conceived the related closure analysis. Palsberg [1995] simplified the analysis and formulated an equivalent constraint-based analysis. At the same time Heintze [1994] developed a related set-based analysis formulated in terms of set constraints. For a detailed account of related work, we refer to a recent survey of the area [Midtgaard, 2007]. It is worth emphasizing that all of the above analyses focus on calls, in that they approximate the source lambdas being called at each call site. As such they do not directly determine return flow for programs in direct style.

**CPS-based CFA** was pioneered by Shivers [1988] who formulated control-flow analysis for Scheme. Since then several analyses have been formulated for CPS [Ayers, 1992, Ashley and Dybvig, 1998, MIGHT and Shivers, 2006]. In CPS all calls are tail calls, and even returns are encoded as calls to the current continuation. By determining “call flow” and hence the receiver functions of such continuation calls, a CPS-based CFA thereby determines return flow without additional effort.

**The impact of CPS transformation on static analyses** originates in binding-time analysis, for which the transformation is known to have a positive effect [Consel and Danvy, 1991, Damian and Danvy, 2003]. As to the impact of CPS transformation on CFA we separate the previous work on the subject in two:

1. results relating an analysis specialized to the source language to an analysis specialized to the target language (CPS), and
2. results relating the analysis of a program to the same analysis of the CPS transformed program.

Sabry and Felleisen [1994] designed and compared specialized analyses and hence falls into the first category as does the present paper. Damian and Danvy [2003] related the analysis of a program and its CPS counterpart for a standard flow-logic CFA (as well as for two binding-time analyses), and Palsberg and Wand [2003] related the analysis of a program and its CPS counterpart for a standard conditional constraint CFA. Hence the latter two fall into the second category.

We paraphrase the relevant theorems of Sabry and Felleisen [1994], of Damian and Danvy [2003], of Palsberg and Wand [2003], and of the present paper in order to underline the difference between the contributions (C refers to non-trivial, 0-CFA-like analyses defined in the cited papers, \( p \) ranges over direct-style programs, \( cps \) denotes CPS transformation, and \( \sim \) denotes analysis equivalence). Our formulations should not be read as a formal system, but only as a means for elucidating the difference between the contributions.

Sabry and Felleisen [1994]:

\[
\exists \text{analyses } C_1, C_2 : \exists p, C_1(p) \sim C_2(cps(p))
\]

Damian and Danvy [2003], Palsberg and Wand [2003]:

\[
\text{exists analysis } C : \forall p, C(p) \sim C(cps(p))
\]

Present paper, Theorem 5.1:

\[
\text{exists analyses } C_1, C_2 : \forall p, C_1(p) \sim C_2(cps(p))
\]

Our work relates to all of the above contributions. The disciplined derivation of specialized CPS and direct-style analyses results in comparable analyses, contrary to Sabry and Felleisen [1994]. Furthermore our equivalence proof extends the results of Damian and Danvy [2003] and Palsberg and Wand [2003] in that we relate both call flow, return flow, and reachability, contrary to their relating only the call flow of standard CFAs. In addition, the systematic abstract interpretation-based approach suggests a strategy for obtaining similar equivalence results for other CFAs derived in this fashion.

**Formulating CFA in the traditional abstract interpretation framework** was stated as an open problem by Nielsen and Nielson [1997]. It has been a recurring theme in the work of the present authors. In an earlier paper Spoto and Jensen [2003] investigated class analysis of object-oriented programs as a Galois connection-based abstraction of a trace semantics. In a recent article [Midtgaard and Jensen, 2008a], the authors systematically derived a CPS-based CFA from the collecting semantics of a stack-less machine. While investigating how to derive a corresponding direct-style analysis we discovered a mismatch between the computed return information.

As tail calls are identified syntactically, the additional information could also have been obtained by a subsequent analysis after a traditional direct-style CFA. However we view the need for such a subsequent analysis as a strong indication of a mismatch between the direct-style and CPS analysis formulations. Debrey and Proebsting [1997] have investigated such a “return analysis” for a first-order language with tail-call optimization. This paper builds a semantics-based CFA that determines such information, and for a higher-order language.

**The systematic design of constraint-based analyses** is a goal shared with the flow logic framework of Nielsen and Nielson [2002]. In flow logic an analysis specification can be systematically transformed into a constraint-based analysis. The present paper instead extracts a constraint-based analysis from an analysis developed in the original abstract interpretation framework.

The idea of CFA by control stack approximation, applies equally well to imperative or object-oriented programs, but it is beyond the scope of this paper to argue this point. Due to space limitations most calculations and proofs are also omitted. We refer the reader to the accompanying technical report [Midtggaard and Jensen, 2008b].

2. Language and semantics

Our source language is a simple call-by-value core language known as administrative normal form (ANF). The grammar of ANF terms is given in Fig. 2(a). Following Reynolds, the grammar distinguishes serious expressions, i.e., terms whose evaluation may diverge, from trivial expressions, i.e., terms without risk of divergence. Trivial expressions include constants, variables, and functions, and serious expressions include return, let-bindings, tail calls, and non-tail calls. Programs are serious expressions.

The analysis is calculated from a simple operational semantics in the form of an abstract machine. We use the environment-based \( C_{EK} \) abstract machine of Flanagan et al. [1993] given in Fig. 2 in which functional values are represented using closures, i.e., pairs of a lambda-expression and an environment. The environment component captures the (values of the) free variables of the lambda. Machine states are triples consisting of a serious expression, an
environment and a control stack. The control stack is composed of elements ("stack frames") of the form \([x, s, e]\) where \(x\) is the variable receiving the return value \(w\) of the current function call, and \(s\) is a serious expression whose evaluation in the environment \(e[x \mapsto w]\) represents the rest of the computation in that stack frame. The empty stack is represented by \(\text{stop}\). The machine has a helper function \(\mu\) for evaluation of trivial expressions. The machine is initialized with the input program, with an empty environment, and with an initial stack, that will bind the result of the program to a special variable \(x_r\) before halting. Evaluation follows by repeated application of the machine transitions.

3. Abstract interpretation basics

We assume some familiarity with the basic mathematical facts recalled in Appendix A. Canonical abstract interpretation approximates the collecting semantics of a transition system [Cousot, 1981]. A standard example of a collecting semantics is the reachable states of the C\(_d\)EK machine, expressed as the least fixed point \(\text{lpf} F\) of the following transition function.

\[
F : \wp(C \times \text{Env} \times K) \to \wp(C \times \text{Env} \times K)
\]

\[
F(S) = I_\emptyset \cup \{s \mid \exists s' \in S : s' \longrightarrow s\}
\]

where \(I_\emptyset = \{\langle p, \bullet, x_r, x_r, x_r \rangle : \text{stop}\}\).

First we formulate in Fig. 3(a) an equivalent helper function \(\mu_e\) extended to work on sets of environments.

**Lemma 4.1.** \(\forall t, e : \{\mu(t, e)\} = \mu_e(t, \{e\})\)

The equivalence of the two helper functions follow straightforwardly. This lemma enables us to express an equivalent collecting semantics based on \(\mu_e\), which appears in Fig. 3. The equivalence of \(F\) and \(F^e\) follows from the lemma and by unfolding the definitions.

The abstraction of the collecting semantics is staged in several steps. Figure 4 provides an overview. Intuitively, the analysis extracts three pieces of information from the set of reachable states.

1. An approximation of the set of reachable expressions.
2. A relation between expressions and control stacks that represents where the values of expressions are returned to.
3. An abstract environment mapping variables to the expressions that may be bound to that variable. This is standard in CFA and allows to determine which functions are called at a given call site.

Keeping an explicit set of reachable expressions is more precise than leaving it out, once we further approximate the expression-stack pairs. Alternatively the reachable expressions would be approximated by the expressions present in the expression-stack relation. However expressions may be in the expression-stack relation without ever being reached. An example hereof would be a diverging non-call.

To formalize this intuition, we first perform a Cartesian abstraction of the machine states, however keeping the relation between expressions and their corresponding control stacks. The second step in the approximation consists in closing the triples by a closure operator, to ensure that (a) any saved environment on the stack or nested within another environment is itself part of the environment.

4. Approximating the C\(_d\)EK collecting semantics

As our collecting semantics we consider the reachable states of the C\(_d\)EK machine, expressed as the least fixed point \(\text{lpf} F\) of the following transition function.

\[
F : \wp(C \times \text{Env} \times K) \to \wp(C \times \text{Env} \times K)
\]

\[
F(S) = I_\emptyset \cup \{s \mid \exists s' \in S : s' \longrightarrow s\}
\]

where \(I_\emptyset = \{\langle p, \bullet, x_r, x_r, x_r \rangle : \text{stop}\}\).

First we formulate in Fig. 3(a) an equivalent helper function \(\mu_e\) extended to work on sets of environments.

**Lemma 4.1.** \(\forall t, e : \{\mu(t, e)\} = \mu_e(t, \{e\})\)

The equivalence of the two helper functions follow straightforwardly. This lemma enables us to express an equivalent collecting semantics based on \(\mu_e\), which appears in Fig. 3. The equivalence of \(F\) and \(F^e\) follows from the lemma and by unfolding the definitions.

The abstraction of the collecting semantics is staged in several steps. Figure 4 provides an overview. Intuitively, the analysis extracts three pieces of information from the set of reachable states.

1. An approximation of the set of reachable expressions.
2. A relation between expressions and control stacks that represents where the values of expressions are returned to.
3. An abstract environment mapping variables to the expressions that may be bound to that variable. This is standard in CFA and allows to determine which functions are called at a given call site.

Keeping an explicit set of reachable expressions is more precise than leaving it out, once we further approximate the expression-stack pairs. Alternatively the reachable expressions would be approximated by the expressions present in the expression-stack relation. However expressions may be in the expression-stack relation without ever being reached. An example hereof would be a diverging non-call.

To formalize this intuition, we first perform a Cartesian abstraction of the machine states, however keeping the relation between expressions and their corresponding control stacks. The second step in the approximation consists in closing the triples by a closure operator, to ensure that (a) any saved environment on the stack or nested within another environment is itself part of the environment.
Finally as a third step we approximate stacks by their top element, above is defined formally as follows.

\[
\mu_c : T \times \rho(Env) \rightarrow \rho(Val)
\]

\[
\mu_c(c, E) = \{ c \}
\]

\[
\mu_c(x, E) = \{ w \mid \exists e \in E : w = e(x) \}
\]

\[
\mu_c(\text{fn } x \Rightarrow s, E) = \{ (\text{fn } x \Rightarrow s, e) \mid \exists e \in E \}
\]

(a) Helper function

\[
F^c : \rho(C \times Env \times K) \rightarrow \rho(C \times Env \times K)
\]

\[
F^c(S) = I_p
\]

\[
\bigcup_{(x, e, [x', w], k') \in S} \{ (s', s' [x \mapsto w], k') \}
\]

\[
\bigcup_{(let \ x := \text{fn } y \Rightarrow s, e) \in S} \{ (s, s' [x \mapsto w], e) \}
\]

\[
\bigcup_{\{x, y \in \text{Env}, s \in S\}} \{ (s', s' [y \mapsto w], [x, s, e] :: k) \}
\]

(b) Transition function

Figure 3: Collecting semantics

\[
\rho(C \times Env \times K) \quad \text{coll. sem.} \quad F^c
\]

\[
\alpha_c \bigg| \gamma_c
\]

\[
\rho(C) \times \rho(C \times K) \times \rho(Env) \quad - \quad F^c
\]

\[
\rho : 1
\]

\[
\rho(\rho(C) \times \rho(C \times K) \times \rho(Env)) \quad - \quad F^p
\]

\[
\alpha_c \bigg| \gamma_c
\]

\[
\rho(C) \times (C/\Rightarrow) \times Env \quad \text{0-CFA} \quad F^d
\]

Figure 3: Collecting semantics

4.2 A closure operator on machine states

For the final analysis, we are only interested in an abstraction of the information present in an expression-stack pair. More precisely, we aim at keeping track of the link between an expression and the top stack frame in effect during its evaluation, throwing away everything below. However, we need to make this information explicit for all expressions appearing on the control stack, i.e., for a pair \(\langle a, [x, s', e] :: k \rangle\) we also want to retain that \(s'\) will be evaluated with control stack \(k\). Similarly, environments can be stored on the stack or inside other environments and will have to be extracted. We achieve this by defining a suitable closure operator on these nested structures.

For environments, we adapt the definition of a constituent relation due to Milner and Tofte [1991] We say that each component \(x_i\) of a tuple \(\langle x_0, \ldots, x_n \rangle\) is a constituent of the tuple, written \(\langle x_0, \ldots, x_n \rangle \succ x_i\). For a partial function \(f = \langle x_0 \mapsto w_0, \ldots, x_n \mapsto w_n \rangle\), we say that each \(w_i\) is a constituent of the function, written \(f \succ w_i\). We write \(\succ^\ast\) for the reflexive, transitive closure of the constituent relation.

To deal with the control stack, we define an order on expression-stack pairs. Two pairs are ordered if (a) the stack component of the second is the tail of the first’s stack component, and (b) the expression component of the second, resides on the top stack frame of the first pair: \(\langle a, [x, s', e] :: k \rangle \succ \langle a', k' \rangle\). We write \(\succ^\ast\) for the reflexive, transitive closure of the expression-stack pair ordering.

Next, we consider an operator \(\rho\), defined in terms of the constituent relation and the expression-stack pair ordering. The operator \(\rho\) ensures that all constituent environments will themselves belong to the set of environments, and that any structurally smaller expression-stack pairs are also contained in the expression-stack relation.

Definition 4.1.

\[
\rho((C, F, E)) = \{ (a, k) \mid \exists (a', k') \in F : (a', k') \succ^\ast (a, k) \},
\]

\[
\{ e \mid \exists (a, k) \in F : (a, k) \succ^\ast e \land \exists e' \in E : e' \succ^\ast e \}
\]

We need to relate the expression-stack ordering to the constituent relation. By case analysis one can prove that \(\forall (a, k), (a', k') : (a, k) \succ (a', k') \implies k \succ k'\). By structural induction (on the stack component) it now follows that \(\forall (a, k), (a', k') : (a, k) \succ^\ast (a', k') \implies k \succ^\ast k'\). Based on these results we can verify that \(\rho\) is a closure operator and formulate an abstraction on the triples:

\[
\rho(C) \times \rho(C \times K) \times \rho(Env) \quad \frac{1}{\rho} \quad \rho(C) \times \rho(C \times K) \times \rho(Env)
\]

---

1 Milner and Tofte define the constituent relation for finite functions.
We use the notation $\sqcup_p$ for the join operation $\lambda X, \rho(\sqcup_p X)$ on the closure operator-induced complete lattice. First observe that in our case:

$$\sqcup_p X = \lambda X, \rho(\sqcup_p X) = \lambda X, \bigcup_i X_i = \bigcup_i$$

Based on the closure operator-based Galois connection, we can calculate a new intermediate transfer function $F^X$. The resulting transfer function appears in Fig. 6. This transfer function differs only minimally from the one in Fig. 5, in that (a) the signature has changed, (b) the set of initial states has been "closed" and now contains the structurally smaller pair $\langle x, \text{stop} \rangle$, and (c) the four indexed joins now each join "closed" triples in the image of the closure operator. By construction, the new transition function satisfies the following theorem.

**Theorem 4.2.** $\forall C, F, E : \rho \circ F^X \circ 1((C, F, E)) = F^0((C, F, E))$

### 4.3 Abstracting the expression-stack relation

Since stacks can grow unbounded (for non-tail recursive programs), we need to approximate the stack component and hereby the expression-stack relation. We first formulate a grammar of abstract stacks and an elementwise operator $\bowtie$:

$$\forall \langle C, F, E \rangle : \rho(\bowtie) = (C, F, E)$$

Notice how some expressions share the same return point (read: same stack): the expressions $\lambda x = t \in s$ and $\bar{s}$ share the same return point, and let $x = \text{stop} \in s$ and $\bar{s}$ share the same return point. In order to eliminate such redundancy we define an equivalence relation on serious expressions grouping together expressions sharing the same return point. We define the smallest equivalence relation $\equiv$ satisfying:

$$\lambda x = t \in s \equiv s$$
$$\lambda x = \text{stop} \in s \equiv s$$

Based hereon we define a second elementwise operator $\bowtie'$:

$$\rho(C \times K) \times \rho(\bowtie')}}$$

We can choose the outermost expression as a representative for each equivalence class by a linear top-down traversal of the input program.

**Pointwise coding of a relation [Cousot and Cousot, 1994]:** A relation can be isomorphically encoded as a set-valued function by a Galois connection:

$$\rho(A \times B) \sqsubseteq (A \mapsto \rho(B)) ; \sqsubseteq$$

and $\alpha_{\bowtie} : \lambda a. \{ b \mid \{ a, b \} \in r \} \quad \gamma_{\bowtie} (f) = \{ \{ a, b \} \mid b \in f(a) \}$

By composing the three above Galois connections we obtain our abstraction of the expression-stack relation:

$$\rho(C \times K) \xrightarrow{\alpha_{\bowtie}} C \equiv \rho(K^2)$$

where $\alpha_{\bowtie} = \alpha_{\bowtie} \circ \alpha_{\bowtie} \circ \alpha_{\bowtie} = \lambda F.[\bigcup \langle s, k \rangle, \rho_{\bowtie}(\bigcup \langle s, k \rangle)]$ and $\gamma_{\bowtie} = \gamma_{\bowtie} \circ \gamma_{\bowtie} \circ \gamma_{\bowtie}$. We can now prove a lemma relating the concrete and abstract expression-stack relations.

**Lemma 4.3.** Control stack and saved environments

Let $(C, F, E) \in \rho(C \times K) \times \rho(\bowtie)$ be given.

$$\langle s, \{ x, s', \bar{s} \} : k \rangle \in F \implies e \in E \land \{ \bar{s}', k \} \subseteq F$$

$\land \{ \{ x, s' \} \} \subseteq \alpha_{\bowtie}(F)(\{ s \})$

**Proof.** The first half follows from the assumptions. The second half follows from monotonicity of $\alpha_{\bowtie}$, and the definitions of $\alpha_{\bowtie}, \sqcup, \bowtie, \alpha_{\bowtie},$ and $\sqsubseteq$.

### 4.4 Abstracting environments

We also abstract values using an elementwise abstraction. Again we formulate a grammar of abstract values and an elementwise
Lemma 4.4. \( \forall t, E : \alpha_\Pi(\mu_\ell(t, E)) = \mu^2(t, \alpha_\Pi(E)) \)

The resulting helper function

\[
\mu^2(c, E^2) = \{c\}
\]

\[
\mu^2(x, E^2) = E^2(x)
\]

where we write \( E^2 \) as shorthand for \( Var \to \rho(Var) \). We shall need a lemma relating the two helper function definitions on closed environments.

Lemma 4.5. Helper function on closed environments (1)
Let \( (C, F, E) \in \rho(\rho(C) \times \rho(C \times K) \times \rho(Env)) \) be given.

\[
\{[\text{fx} \Rightarrow a, e]\} \subseteq \mu_\ell(t, E) \iff e \in E \land \{[\text{fx} \Rightarrow a]\} \subseteq \mu^2(t, \alpha_\Pi(E))
\]

The above lemma is easily extended to capture nested environments in all values returned by the helper function:

Lemma 4.6. Helper function on closed environments (2)
Let \( (C, F, E) \in \rho(\rho(C) \times \rho(C \times K) \times \rho(Env)) \) be given.

\[
\{w\} \subseteq \mu_\ell(t, E) \land w \Rightarrow^* e' \iff e' \in E
\]

4.6 Abstracting the machine states

We abstract the triplet of sets into abstract triples by a componentwise abstraction.

Componentwise abstraction [Cousot and Cousot, 1994]: Assuming a series of Galois connections: \( \rho(C_i) \xrightarrow{\gamma_i} A_i \) for \( i \in \{1, \ldots, n\} \), their componentwise composition induces a Galois connection on tuples:

\[
\begin{align*}
(\rho(C_1) \times \ldots \times \rho(C_n)) \times \gamma_{\\llcorner} & \xrightarrow{\gamma_{\\llcorner}} \gamma_{\\llcorner} (A_1 \times \ldots \times A_n) \\
\alpha_{\\llcorner}(X_1, \ldots, X_n) & = (\alpha_1(X_1), \ldots, \alpha_n(X_n)) \\
\gamma_{\\llcorner}(X_1, \ldots, X_n) & = (\gamma_1(X_1), \ldots, \gamma_n(X_n))
\end{align*}
\]

We write \( U_{\llcorner} \) and \( \llcorner \) for componentwise join and inclusion, respectively.

For the set of expressions \( \rho(C) \) we use the identity abstraction consisting of two identity functions. For the expression-stack
relation $\rho(C \times K)$ we use the expression-stack abstraction $\alpha_d$ developed in Section 4.3. For the set of environments $\rho(\text{Env})$ we use the environment abstraction $\alpha_i$ developed in Section 4.4.

Using the alternative “recipe” we can calculate the analysis by “pushing $\alpha_\gamma$'s” under the intermediate transition function: $\alpha_{\otimes}(F^3((C, F, E))) \subseteq F^1(C, \alpha_\gamma(F), \alpha_\gamma(E)))$ from which the final definition of $F^3$ can be read off. The resulting analysis appears in Fig. 7. The alert reader may have noticed that this final abstraction is not complete in that the above equation contains an inequality. Completeness is a desirable goal in an abstract interpretation but unfortunately it is not possible in general without refining the abstract domain [Giacobazzi et al., 2000]. Consider for example the addition operator over the standard sign-domain: $0 = \alpha(1 + (-1)) \nsubseteq \alpha(1) + \alpha(-1) = T$. As traditional [Cousot, 1999], we instead limit upward judgements to a minimum.

As a corollary of the construction, the analysis safely approximates the reachable states of the abstract machine.

**Corollary 4.1.** $\alpha_{\otimes} \circ \rho \circ \alpha_\gamma(F^3) \subseteq \text{lfp} F^3$

### 4.7 Characteristics of the analysis

First of all the analysis incorporates reachability: it computes an approximate set of reachable expressions and will only analyse those reachable program fragments. Reachability analyses have previously been discovered independently [Ayers, 1992, Palsberg and Schwartzbach, 1995, Gasser et al., 1997]. In our case they arise naturally from a projecting abstraction of a reachable states collecting semantics.

Second the formulation materializes monomorphism into two mappings: (a) one mapping merging all bindings to the same variable, and (b) one mapping merging all calling contexts of the same function. Both characterisitics are well known, but our presentation is novel in that it literally captures this phenomenon in two approximation functions.

Third the analysis handles returns inside-out (“callee-restore”), in that the called function restores control from the approximate control stack and propagates the obtained return values. This differs from the traditional presentations [Palsberg, 1995, Nielson et al., 1999] that handle returns outside-in (“caller-restore”) where the caller propagates the obtained return values from the body of the function to the call site (typically formulated as conditional constraints).

$$F^2: P \to \rho(C) \times (C/\to \to \rho(K^2)) \times \text{Env}^3 \to \rho(C) \times (C/\to \to \rho(K^2)) \times \text{Env}^3$$

$$F^2((C, F, E^2)) = (\langle p \rangle, \langle x, x_c \rangle, \langle x_c, \to \to \text{stop} \rangle, \lambda_\to, \emptyset)$$

$$\cup_\otimes \bigcup_{\{t\} \subseteq C} \langle \{s\}, F^2, E^2 \cup \{x \to \mu(t, E^2)\} \rangle$$

$$\cup_\otimes \bigcup_{\{t, t_1\} \subseteq C} \langle \{s\}, F^2, E^2 \cup \{x \to \mu(t, E^2)\} \rangle$$

$$\cup_\otimes \bigcup_{\{t, t_1\} \subseteq C} \langle \{s\}, F^2, E^2 \cup \{x \to \mu(t, E^2)\} \rangle$$

$$\cup_\otimes \bigcup_{\{t, t_1\} \subseteq C} \langle \{s\}, F^2, E^2 \cup \{x \to \mu(t, E^2)\} \rangle$$

**Figure 7:** The resulting analysis function

---

### 5. Analysis equivalence

In previous work [Midtgaard and Jensen, 2008a] we derived an initial CFA with reachability for a CPS language from the stack-less $CE$-machine [Flanagan et al., 1993]. In this section we show that the present ANF analysis achieves the same precision as obtained by first transforming a program into CPS and then using the CPS analysis. This is done by defining a relation that captures how the direct-style analysis and the CPS analysis operate in lock-step.

The grammar of CPS terms is given in Fig. 8. The grammar distinguishes variables in the original source program $x \in X$, from intermediate variables $\nu \in V$ and continuation variables $k \in K$. We assume the three classes are non-overlapping. Their union constitute the domain of CPS variables $\text{Var} = X \cup V \cup K$.

#### 5.1 CPS transformation and back again

In order to state the relation between the ANF and CPS analyses we first recall the relevant program transformations. The below presentation is based on Danvy [1991], Flanagan et al. [1993], and Sabry and Felleisen [1994].

The **CPS transformation** given in Fig. 9(a) is defined by two mutually recursive functions — one for serious and trivial expressions. A continuation variable $k$ is provided in the initial call to $\mathcal{F}$. A fresh $k$ is generated in $\mathcal{F}$’s lambda abstraction case. To ease the expression of the original, we choose $k$ unique to the serious expression $s \to k_s$. It follows that we only need one $k$ per lambda abstraction in the original program $+ \text{an additional } k$ in the initial case.

It is immediate from the definition of $\mathcal{F}$ that the CPS transformation of a let-binding $\lambda x = t$ in $s$ and the CPS transformation of its body $s$ share the same continuation identifier and similarly for non-tail calls. Hence we shall equate the two:

**Definition 5.1.** $k_s \equiv k_{s'}$ iff $s \equiv s'$

![Figure 8: BNF of CPS language](image-url)
The direct-style transformation given in Fig. 9(b) is defined by two mutually recursive functions over serious and trivial CPS expressions. We define the direct-style transformation of a program function \( f_k \Rightarrow e \) as the direct-style transformation of its body \( \mathcal{W}[e] \).

Transforming a program, a serious or trivial expression to CPS and back to direct style yields the original expression, which can be confirmed by (mutual) structural induction on trivial and serious expressions.

**Lemma 5.1.** \( \mathcal{D}[\mathcal{W}[p]] = p \land \mathcal{W}[\mathcal{F}_k[s]] = s \land \mathcal{D}[\mathcal{Y}[t]] = t \)

### 5.2 CPS analysis

We recall the CPS analysis of Midtgaard and Jensen [2008a] in Fig. 10. It is defined as the least fixed point of a program specific transformation \( \mathcal{F} : \mathcal{P} \to \mathcal{CProg} \)

\[ \mathcal{F}[p] = \mathcal{fn} k_p \Rightarrow \mathcal{F}_k[p] \]

We formally define a relation \( R \) between ANF and CPS.

\[ R[f_k \Rightarrow e] = \mathcal{W}[e] \]

\[ \mathcal{F} : \mathcal{P} \to \mathcal{CProg} \]

\[ \mathcal{F}[p] = \mathcal{fn} k_p \Rightarrow \mathcal{F}_k[p] \]

\[ \mathcal{W} : \mathcal{SExp} \to \mathcal{C} \]

\[ \mathcal{W}[k \ t] = \mathcal{P}[t] \]

\[ \mathcal{W}[\mathcal{fn} v \Rightarrow e] = \mathcal{fn} v \Rightarrow \mathcal{P}[t] \text{ in } \mathcal{W}[e] \]

\[ \mathcal{W}[t_0 t_1 \ k] = \mathcal{P}[t_0] \mathcal{P}[t_1] \]

\[ \mathcal{W}[t_0 t_1 (\mathcal{fn} v \Rightarrow e)] = \mathcal{fn} \mathcal{P}[t_0] \mathcal{P}[t_1] \text{ in } \mathcal{W}[e] \]

\[ \mathcal{Y} : \mathcal{TExp} \to T \]

\[ \mathcal{Y}[x] = x \]

\[ \mathcal{Y}[\mathcal{fn} x \Rightarrow s] = \mathcal{fn} \mathcal{Y}[x], \mathcal{Y}[s] \]

We are now in position to state our main theorem relating the ANF analysis to the CPS analysis. Intuitively the theorem relates:

- reachability in ANF to CPS reachability
- abstract stacks in ANF to CPS continuation closures
- abstract stack bottom in ANF to CPS initial continuation
- ANF closures to CPS function closures

**Theorem 5.1.** Let \( p \) be given. Let \( \langle C, F^1, E^1 \rangle = \text{lfp} F^1_p \) and \( \langle Q^2, R^2 \rangle = \text{lfp} T^2_p \). Then

\[ s \in C \iff \mathcal{F}_k[s] \in Q^2 \land \]

\[ [x, s'] \in F^2(s) \iff [\mathcal{fn} x \Rightarrow \mathcal{F}_k[s']] \in R^2(k_k) \land \]

\[ \text{stop} \in F^2(s) \iff \text{stop} \in R^2(k_k) \land \]

\[ [\mathcal{fn} x \Rightarrow s] \in E^2(y) \iff [\mathcal{fn} x, k_k \Rightarrow \mathcal{F}_k[s]] \in R^2(y) \]

For the purpose of the equivalence we equate the special variables \( x \) and \( v \), both naming the result of the computations. We prove the theorem by combining an implication in each direction with the identity from Lemma 5.1. We formulate both implication as relations and prove that both relations are preserved by the transfer functions.

### 5.4 ANF-CPS equivalence

We formally define a relation \( R^\text{ANF}_{\text{CPS}} \) that relates ANF analysis triples to CPS analysis pairs.

**Definition 5.2.** \( \langle C, F^1, E^1 \rangle \text{ RANF}_{\text{CPS}} \langle Q^2, R^2 \rangle \) if \( \forall s : \)

\[ s \in C \Rightarrow \mathcal{F}_k[s] \in Q^2 \land \]

\[ [x, s'] \in F^2(s) \Rightarrow [\mathcal{fn} x \Rightarrow \mathcal{F}_k[s']] \in R^2(k_k) \land \]

\[ \text{stop} \in F^2(s) \Rightarrow \text{stop} \in R^2(k_k) \land \]

\[ [\mathcal{fn} x \Rightarrow s] \in E^2(y) \Rightarrow [\mathcal{fn} x, k_k \Rightarrow \mathcal{F}_k[s]] \in R^2(y) \]

First we need a small lemma relating the ANF helper function to one of the CPS helper functions.

**Lemma 5.2.**

\[ [\mathcal{fn} x \Rightarrow s] \in \mu^2(t, E^2) \land \]

\[ \langle C, F^1, E^1 \rangle \text{ RANF}_{\text{CPS}} \langle Q^2, R^2 \rangle \]

\[ \Rightarrow [\mathcal{fn} x, k_k \Rightarrow \mathcal{F}_k[s]] \in \mu^2(\mathcal{Y}[t], R^2) \]
Again we formally define a relation now relating CPS analysis pairs to ANF analysis triples.

\[ T^2 : \text{CProg} \rightarrow \varphi(\text{SExp}) \times \text{Em}^2 \rightarrow \varphi(\text{SExp}) \times \text{Em}^2 \]

\[ T^2_{\text{fnx} \Rightarrow e}(\langle Q^\prime, R^\prime \rangle) = \langle \{ e \}, [k_r \mapsto \langle \text{stop} \rangle, k \mapsto \{ [\text{fn} v_r \Rightarrow k_r, v_r] \}] \rangle \cup \bigcup_{t, t_r \in C^Q} \langle \{ e' \}, R^1 \cup [x \mapsto \mu^1(t_1, R^1), k' \mapsto \mu^2(c, R^1)] \rangle \]

\[ \cup \bigcup_{t \in C^Q} \langle \{ e' \}, R^1 \cup [v \mapsto \mu^1(t, R^1)] \rangle \]

\[ \text{where } t_1 = t \, \text{and } k = k_r. \]

\[ \text{Proof. } \text{First we name the individual triples of the union in the function body of } F^1. \text{ We name the first triple of results as initial: } \langle C_l, F^{\prime}_l, E^{\prime}_l \rangle = \langle \{ p \}, [p \mapsto \{ x_r, x_s \}, x_r \mapsto \langle \text{stop} \rangle] \rangle. \text{ The results of the second, third, fourth, and fifth joined triples corresponding to return, binding, tail call, and non-tail call are named } \langle C_{\text{ret}}, F_{\text{ret}}, E_{\text{ret}} \rangle, \langle C_{\text{bind}}, F_{\text{bind}}, E_{\text{bind}} \rangle, \langle C_{\text{ic}}, F_{\text{ic}}, E_{\text{ic}} \rangle \text{ and } \langle C_{\text{nc}, \text{ic}}, F_{\text{nc}, \text{ic}}, E_{\text{nc}, \text{ic}} \rangle, \text{ respectively. Similarly we name the first result pair in the function body of the CPS analysis as initial: } \langle Q^\prime_1, R^\prime_1 \rangle = \langle \{ e \}, [k_r \mapsto \langle \text{stop} \rangle, k \mapsto \{ [\text{fn} v_r \Rightarrow k_r, v_r] \}] \rangle. \text{ The results of the second and third joined pair corresponding to call and return are named } \langle Q^\prime_{\text{call}}, R^\prime_{\text{call}} \rangle \text{ and } \langle Q^\prime_{\text{ret}, \text{ret}} \rangle, \text{ respectively.} \]

\[ \text{The proof proceeds by verifying five relations:} \]

1. \[ \langle C_l, F^{\prime}_l, E^{\prime}_l \rangle \rightarrow R^{\text{ANSF}}_{\text{CPS}} \langle Q^\prime_1, R^\prime_1 \rangle \]

2. \[ \langle C_{\text{ret}}, F_{\text{ret}}, E_{\text{ret}} \rangle \rightarrow R^{\text{ANSF}}_{\text{CPS}} \langle Q^\prime_{\text{ret}, \text{ret}} \rangle \]

3. \[ \langle C_{\text{bind}}, F_{\text{bind}}, E_{\text{bind}} \rangle \rightarrow R^{\text{ANSF}}_{\text{CPS}} \langle Q^\prime_{\text{ret}, \text{ret}} \rangle \]

4. \[ \langle C_{\text{ic}}, F_{\text{ic}}, E_{\text{ic}} \rangle \rightarrow R^{\text{ANSF}}_{\text{CPS}} \langle Q^\prime_{\text{call}, \text{call}} \rangle \]

5. \[ \langle C_{\text{nc}, \text{ic}}, F_{\text{nc}, \text{ic}}, E_{\text{nc}, \text{ic}} \rangle \rightarrow R^{\text{ANSF}}_{\text{CPS}} \langle Q^\prime_{\text{call}, \text{call}} \rangle \]

Realizing that the union of related triples and pairs we obtain the desired result.

After realizing that the bottom elements are related by the above relation, it follows by fixed point induction that their least fixed points (and hence the analyses) are related.

Corollary 5.1. \( \text{lfp} F^\prime_p \rightarrow R^{\text{ANSF}} \rightarrow \text{lfp} T^2_{\mathcal{P}} \)

5.5 CPS-ANF equivalence

Again we formally define a relation now relating CPS analysis pairs to ANF analysis triples.

Definition 5.3. \( (Q^\prime, R^\prime) \rightarrow R^{\text{CPS}}_{\text{ANF}} ((C, F^3, E^3) \) if \( e \in Q^\prime \rightarrow \exists e \in C \land \)

\[ \{ e \} \subseteq \text{lfp}(Q^\prime) \land \{ e \} \subseteq \text{lfp}(C) \land \]

\[ \{ e \} \subseteq \text{lfp}(F^3) \land \{ e \} \subseteq \text{lfp}(E^3) \]

We again need a helper lemma relating the helper functions.

Lemma 5.3. \( \{ e \} \subseteq \text{lfp}(Q^\prime) \rightarrow \exists e \in C \land \{ e \} \subseteq \text{lfp}(C) \land \)

\( \{ e \} \subseteq \text{lfp}(F^3) \land \{ e \} \subseteq \text{lfp}(E^3) \)

This relation is also preserved by the transfer functions.

Theorem 5.3. \( (Q^\prime, R^\prime) \rightarrow R^{\text{CPS}}_{\text{ANF}} ((C, F^3, E^3) \) if \( e \in Q^\prime \rightarrow \exists e \in C \land \)

\[ \{ e \} \subseteq \text{lfp}(Q^\prime) \land \{ e \} \subseteq \text{lfp}(C) \land \]

\( \{ e \} \subseteq \text{lfp}(F^3) \land \{ e \} \subseteq \text{lfp}(E^3) \)

This relation is also preserved by the transfer functions.

Corollary 5.2. \( \text{lfp} F^\prime_p \rightarrow R^{\text{ANSF}} \rightarrow \text{lfp} T^2_{\mathcal{P}} \)

6. Extracting constraints

The resulting analysis may appear complex at first glance. However we can express the analysis in the popular constraint formulation, extracted from the obtained definition. The formulation shown below is in terms of program-specific conditional constraints. Constraints have a (possibly empty) list of preconditions and a conclusion [Palsberg and Schwartzbach, 1995, Gasser et al., 1997]:

\[ \{ u_1 \} \subseteq \text{rhs}_1 \land \ldots \land \{ u_n \} \subseteq \text{rhs}_n \Rightarrow \text{lhs} \subseteq \text{rhs} \]

The constraints operate on the same three domains as the above analysis. Left-hand sides \( \text{lhs} \) can be of the form \( \{ u \}, F^3([u]) \), or \( E^3(x) \), right-hand sides \( \text{rhs} \) can be of the form \( C, F^3([u]) \), or \( E^3(x) \), and singleton elements \( u \) can be of the form \( a, c, [\text{fn} x \Rightarrow a] \), or \( [x, a] \). From Fig. 7 we directly read off the following constraints.
<table>
<thead>
<tr>
<th>i</th>
<th>ANF trace: $(C_i, F^i, E^i)$</th>
<th>CPS trace: $(Q^i, R^i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>${\text{let } f = \text{fn x } =&gt; x \text{ in let } a_2 = f \text{ cn1 in let } a_0 = f \text{ cn2 in } a_1}$</td>
<td>${(\text{fn } f =&gt; f \text{ ccn1}(f \text{ a1 } =&gt; f \text{ ccn2}(f \text{ a2 } =&gt; k_0 \text{ a0})))((\text{fn x, k_0 } =&gt; k_0 \text{ x}))}$</td>
</tr>
<tr>
<td>$\lambda_x.0$</td>
<td>$C_0 \cup {\text{let } a_2 = f \text{ cn1 in let } a_0 = f \text{ cn2 in } a_1}$</td>
<td>$Q_0^i \cup {f \text{ ccn1}(f \text{ a1 } =&gt; f \text{ ccn2}(f \text{ a2 } =&gt; k_0 \text{ a0}))}$</td>
</tr>
<tr>
<td>1</td>
<td>$F^1_0 \cup {x \mapsto [\text{fn x } =&gt; x]}$</td>
<td>$R^i_0 \cup {x \mapsto ((\text{fn x, k_0 } =&gt; k_0 \text{ x}))}$</td>
</tr>
<tr>
<td>2</td>
<td>$F^1_1 \cup {[x]_i \mapsto ([a_1, \text{let } a_0 = f \text{ cn2 in } a_0], [a_2, a_3])}$</td>
<td>$Q^i_1 \cup {k_0 \mapsto ([\text{fn a1 } =&gt; f \text{ ccn2}(\text{fn a2 } =&gt; k_0 \text{ a0})), [\text{fn a2 } =&gt; k_0 \text{ a0}])}$</td>
</tr>
<tr>
<td>$C_1 \cup {x}$</td>
<td>$R^i_1 \cup {a_1 \mapsto (\text{ccn1})}$</td>
<td>$x \mapsto ([\text{ccn1}])$</td>
</tr>
<tr>
<td>3</td>
<td>$F^1_2 \cup {a_1 \mapsto (\text{ccn1})}$</td>
<td>$Q^i_2$</td>
</tr>
<tr>
<td>4</td>
<td>$F^1_3 \cup {[x]_i \mapsto ([a_1, \text{let } a_2 = f \text{ cn2 in } a_2], [a_2, a_3])}$</td>
<td>$R^i_2 \cup {\text{ccn2}(f \text{ a2 } =&gt; k_0 \text{ a0})}$</td>
</tr>
<tr>
<td>$C_4 \cup {a_2}$</td>
<td>$R^i_2 \cup {a_0 \mapsto (\text{ccn1, ccn2})}$</td>
<td>$\text{ccn1, ccn2}$</td>
</tr>
<tr>
<td>5</td>
<td>$F^1_4 \cup {a_2 \mapsto (\text{ccn1, ccn2})}$</td>
<td>$Q^i_4 \cup {k_0, a_2}$</td>
</tr>
<tr>
<td>$C_5 \cup {x_i}$</td>
<td>$R^i_4 \cup {a_1 \mapsto (\text{ccn1, ccn2})}$</td>
<td>$a_2 \mapsto (\text{ccn1, ccn2})$</td>
</tr>
<tr>
<td>6</td>
<td>$F^1_5 \cup {x_i \mapsto (\text{ccn1, ccn2})}$</td>
<td>$Q^i_5 \cup {x, v_i}$</td>
</tr>
<tr>
<td>$C_6 \cup {x_i}$</td>
<td>$R^i_5 \cup {v_i \mapsto (\text{ccn1, ccn2})}$</td>
<td></td>
</tr>
</tbody>
</table>
the constraints is as precise as the information computed by the analysis. More formally:

**Theorem 6.1.** A solution to the CFA constraints of program p is a safe approximation of the least fixpoint of the analysis function \(F^2\) induced by \(p\). Furthermore, the least solution to the CFA constraints is equal to the least fixpoint of \(F^2\).

Implemented naively, a single constraint may take \(O(n)\) space alone. However by using pointers or by labelling each sub-expression and using the pointer/label instead of the sub-expression itself, a single constraint takes only constant space. By linearly determining a representative for each sub-expression, by generating \(O(n^2)\) constraints, linear post-processing, and iteratively solving them using a well-known algorithm [Palsberg and Schwartzbach, 1995, Nielson et al., 1999], we can compute the analysis in worst-case \(O(n^3)\) time.

The extracted constraints bear similarities to existing constraint-based analyses in the literature. Consider, e.g., calls \(t_0\ t_1\), which usually gives rise to two conditional constraints [Palsberg, 1995, Nielson et al., 1999]: (1) \([\{fn\ x \rightarrow s'\}] \subseteq \overline{C}(t_0) \Rightarrow \overline{C}(t_1) \subseteq \overline{E}(x)\) and (2) \([\{fn\ x \rightarrow s'\}] \subseteq \overline{C}(t_0) \Rightarrow \overline{C}(s') \subseteq \overline{C}(t_2 \ t_1)\). The first constraint resembles our third constraint for tail calls. The second “return constraint” differs in that it has a inside-out (or caller-restore) nature, i.e., propagation of return-flow from the function body is handled at the call site. The extracted reachability constraints are similar to Gasser et al. [1997] (modulo an isomorphic encoding \(\gamma(C) \equiv C \rightarrow \gamma(\{0\})\) of powersets).

### 7. Conclusion

We have presented a control-flow analysis determining interprocedural control-flow of both calls and returns for a direct-style language. Existing CFAs have focused on analysing which functions are called at a given call site. In contrast, the systematic derivation of our CFA has lead to an analysis that provides extra information about where a function returns to at no additional cost. In the presence of tail-call optimization, such information enables the creation of more precise call graphs.

The analysis was developed systematically using Galois connection-based abstract interpretation of a standard operational semantics for that language: the \(C/EK\) abstract machine of Flanagan et al. In addition to being more principled, such a formulation of the analysis is pedagogically pleasing since monomorphism of the analysis is made explicit through two Galois connections: one literally merges all bindings to the same variable and one merges all calling contexts of the same function.

The analysis has been shown to provide a result equivalent to what can be obtained by first CPS transforming the program and then running a control flow analysis derived from a CPS-based operational semantics. This extends previous results obtained by Damian and Danvy, and Palsberg and Wand. The close correspondence between the way that the analyses operate (as illustrated by the analysis trace in Table 1) leads us to conjecture that such equivalence results can be obtained for other CFAs derived using abstract interpretation.

The functional, derived by abstract interpretation, that defines the analysis may appear rather complex at first glance. As a final result, we have shown how to extract from the analysis an equivalent constraint-based formulation expressed in terms of the more familiar conditional constraints. Nevertheless, we stress that the derived functional can be used directly to implement the analysis. We have developed a prototype implementation of the resulting analysis in OCaml.\(^2\)

\(^2\)available at http://www.brics.dk/~jml/ABF-CFA/

The analysis has been developed for a minimalist functional language in order to be able to focus on the abstraction of the control structure induced by function calls and returns. An obvious extension is to enrich the language with numerical operators and study how our Galois connections interact with abstractions such as the interval or polyhedral abstraction of numerical entities.

The calculations involved in the derivation of a CFA are lengthy and would benefit enormously from some form of machine support. Certified abstract interpretation [Pichardie, 2005, Cachera et al., 2005] has so far focused on proving the correctness of the analysis inside a proof assistant by using the concretization (\(\gamma\)) component of the Galois connection to prove the correctness of an already defined analysis. Further work should investigate whether proof assistants such as Coq are suitable for conducting the kind of reasoning developed in this paper in a machine-checkable way.

## Acknowledgments

The authors thank Matthew Fluet, Amr Sabry, Mitchell Wand, Daniel Damian, Olivier Danvy, and the anonymous referees for comments on earlier versions. Part of this work was done with the support of the Carlsberg Foundation.

## References


P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In B. K. Rosen, editor, *Proc. of the Sixth Annual ACM Sym-


A. Underlying mathematical material

This section is based on known material [Cousot and Cousot, 1979, Cousot, 1981, Cousot and Cousot, 1992b, 1994, Davey and Priestley, 2002].

A complete lattice is a partially ordered set \( (C; \preceq, \bot, \top) \) (poset), such that the least upper bound \( \sqcup \) and the greatest lower bound \( \sqcap \) exists for every subset \( S \) of \( C \). \( \sqcap = \cap C \) denotes the infimum of \( C \) and \( \sqcup = \cup C \) denotes the supremum of \( C \). The set of total functions \( D \to C \), whose domain is a complete lattice \( C \), is itself a complete lattice \( \langle \mathcal{D} = \mathcal{D}_1 \cup \mathcal{T}, \sqsubseteq, \top, \bot \rangle \) under the pointwise ordering \( f \sqsubseteq g \iff \forall x. f(x) \sqsubseteq g(x) \), with bottom, top, join, and meet extended similarly. The powersets \( 2^S \) of a set \( S \) ordered by set inclusion is a complete lattice \( (2^S; \subseteq, \emptyset, \mathcal{P}(S)) \).

A Galois connection is a pair of functions \( \alpha, \gamma \) between two posets \( (C; \preceq, \bot, \top) \) and \( (A; \preceq, \bot, \top) \) such that for all \( a \in A \), \( \alpha(c) \leq a \iff c \in \gamma(a) \). Equivalently a Galois connection can be defined as a pair of functions satisfying (a) \( \alpha \) and \( \gamma \) are monotone, (b) \( \alpha \circ \gamma \) is reductive, and (c) \( \gamma \circ \alpha \) is extensive. Galois connections are typeset \( (C; \preceq, \bot, \top) \to (A; \preceq, \bot, \top) \). We omit the orderings when they are clear from the context. For a Galois connection between two complete lattices \( \alpha \) is a complete join-morphism (CJM) and \( \gamma \) is a complete meet morphism. The composition of two Galois connections \( (C; \preceq, \bot, \top) \to (B; \preceq, \bot, \top) \) and \( (B; \preceq, \bot, \top) \to (A; \preceq, \bot, \top) \) is itself a Galois connection \( (C; \preceq, \bot, \top) \to (A; \preceq, \bot, \top) \).

Galois connections in which \( \alpha \) is surjective (or equivalently \( \gamma \) is injective) are typeset \( (C; \preceq, \bot, \top) \to (A; \preceq, \bot, \top) \). Galois connections in which \( \gamma \) is surjective (or equivalently \( \alpha \) is injective) are typeset \( (C; \preceq, \bot, \top) \to (A; \preceq, \bot, \top) \). When both \( \alpha \) and \( \gamma \) are surjective, the two domains are isomorphic.

A(n upper) closure operator \( \rho \) is map \( \rho : S \to S \) on a poset \( \langle S; \preceq, \top, \bot \rangle \), that is (a) monotone: (for all \( s, s' \in S \). \( s \preceq s' \implies \rho(s) \preceq \rho(s') \)) (b) extensive (for all \( s \in S \). \( s \preceq \rho(s) \)), and (c) idempotent (for all \( s \in S \). \( \rho(s) = \rho(\rho(s)) \)). A closure operator \( \rho \) induces a Galois connection \( \langle S; \preceq, \bot, \top \rangle \to \langle (\rho(S); \preceq, \bot, \top) \rangle \), writing \( \rho(S) \) for \( \{ \rho(s) \mid s \in S \} \) and \( 1 \) for the identity function. Furthermore the image of a complete lattice \( (C; \preceq, \bot, \top) \) by an upper closure operator \( \rho \) is itself a complete lattice \( (\rho(C); \preceq, \bot, \top, \rho(\bot), \top, \rho(X), \top) \).