Hybrid Top-down and Bottom-up Interprocedural Analysis

Xin Zhang\(^1\) Ravi Mangal\(^1\) Mayur Naik\(^1\) Hongseok Yang\(^2\)

\(^1\) Georgia Institute of Technology \(^2\) Oxford University

Abstract

Interprocedural static analyses are broadly classified into top-down and bottom-up, depending upon how they compute, instantiate, and reuse procedure summaries. Both kinds of analyses are challenging to scale: top-down analyses are hindered by ineffective reuse of summaries whereas bottom-up analyses are hindered by inefficient computation and instantiation of summaries. This paper presents a hybrid approach SWIFT that combines top-down and bottom-up analyses in a manner that gains their benefits without suffering their drawbacks. SWIFT is general in that it is parameterized by the top-down and bottom-up analyses it combines. We show an instantiation of SWIFT on a type-state analysis and evaluate it on a suite of 12 Java programs of size 60-250 KLOC each. SWIFT outperforms both conventional approaches, finishing on all the programs while both of those approaches fail on the larger programs.

1. Introduction

Interprocedural static analyses are broadly classified into top-down and bottom-up. Top-down analyses start at root procedures of a program and proceed from callers to callees. Bottom-up analyses, on the other hand, begin from leaf procedures and proceed from callees to callers. For reasons of scalability and termination, both kinds of analyses compute and reuse summaries of analysis results over procedures, but they do so in fundamentally different ways.

Top-down analyses only analyze procedures under contexts in which they are called in a program. A key drawback of such analyses is that the summaries they compute tend to track details that are specific to individual calling contexts. These analyses thereby fail to sufficiently reuse summaries of a procedure across different calling contexts. This in turn causes a blow-up in the number of summaries and hinders the scalability of the analyses.

Bottom-up analyses analyze procedures under all contexts, not just those in which they are called in a program. These analyses have two key strengths: the summaries they compute are highly reusable and they are easier to parallelize. But these analyses also have drawbacks that stem from analyzing procedures in contexts that are unrealizable in a program: they either lose scalability due to the need to reason about too many cases, or they sacrifice precision by eliding needed distinctions between cases. Also, instantiating summaries computed by bottom-up analyses is usually expensive compared to top-down analyses.

It is thus evident that the performance of both top-down and bottom-up analyses depends crucially on how procedure summaries are computed, instantiated, and reused. Top-down analysis summaries are cheap to compute and instantiate but hard to reuse, whereas bottom-up analysis summaries are easy to reuse but expensive to compute and instantiate.

This paper proposes a new hybrid interprocedural analysis approach called SWIFT that synergistically combines top-down and bottom-up analyses. Our approach is based on two observations. First, multiple summaries of the top-down analysis for a procedure can be captured by a single summary of the bottom-up analysis for the procedure. Therefore, applying bottom-up summaries in the top-down analysis can greatly improve summary reuse. Second, although bottom-up analysis reasons about all possible cases over the unknown initial states of a procedure, only few of those cases may be encountered frequently during top-down analysis, or even be reachable from the root procedures of a program. Therefore, making the bottom-up analysis only analyze those cases that are encountered most frequently during top-down analysis can greatly reduce the cost of computing and instantiating bottom-up summaries.

We formalize SWIFT as a generic framework that is parametrized by the top-down and bottom-up analyses, and show how to instantiate it on a type-state analysis for object-oriented programs. This analysis is useful for checking a variety of program safety properties, features both may and must alias reasoning about pointers, and is challenging to scale to large programs. We implemented SWIFT for Java and evaluate it on the type-state analysis using 12 benchmark programs of size 60-250 KLOC each. SWIFT outperforms both conventional approaches in our experiments, achieving speedups up to 59X over the top-down approach and 118X over the bottom-up approach, and finishing successfully on all programs while both conventional approaches fail on the larger programs.

We summarize the main contributions of this paper:

1. We propose SWIFT, a new interprocedural analysis approach that synergistically combines top-down and bottom-up approaches. We formalize SWIFT as a generic framework and illustrate it on a realistic type-state analysis.
2. Central to SWIFT is a new kind of relational analysis that approximates input-output relationships of procedures without information about initial states, but avoids the common problem of generating too many cases by using a pruning operator to identify and drop infrequent cases during case splitting.
3. We present empirical results showing the effectiveness of SWIFT over both the top-down and bottom-up approaches for type-state analysis on a suite of real-world Java programs.

2. Overview

We illustrate SWIFT on a type-state analysis of an example program shown in Figure 1. The program creates three file objects and calls procedure \( \text{f} \) on each of them to open and close the file. Each file \( \text{f} \) can be in state \( \text{open} \), \( \text{closed} \), or \( \text{error} \) at any instant, and starts in state \( \text{closed} \). A call \( \text{f}.\text{open()} \) changes its state to \( \text{open} \) if it is \( \text{closed} \), and to \( \text{error} \) otherwise. Similarly, \( \text{f}.\text{close()} \) changes its state to \( \text{closed} \) if it is \( \text{open} \), and to \( \text{error} \) otherwise.

We use a type-state analysis by Fink et al. [11] which computes a set of abstract states at each program point to over-approximate the type-states of all objects. Each abstract state is of the form \((h, t, a, n)\) where \(h\) is an allocation site, \(t\) is the type-state in which an object created at that site might be in, and \(a\) and \(n\) are finite sets of program expressions with which that object is aliased (called \( \text{must} \)) and not aliased (called \( \text{must-not set} \)), respectively.

We next illustrate two common interprocedural approaches: top-down and bottom-up. Informally, we use top-down to mean \( \text{global} \) and \( \text{explicit} \) (or \( \text{tabulating} \)), and bottom-up to mean \( \text{compositional} \) and \( \text{symbolic} \) (or \( \text{functional} \)). Our formal meaning of these terms is given in Sections 3.1 and 3.2.
2.1 The Bottom-Up Approach

The bottom-up approach starts from root procedures and summarizes procedures as functions on abstract states. For our example, it starts from main, proceeds in the order of program execution, and computes summaries $T_1$ through $T_3$ for procedure foo, which are shown in Figure 1. Summaries $T_1$, $T_2$, and $T_3$ mean that an abstract state is a no-op when its argument $\theta$ is in the must set. In this case, the type-state analysis is able to perform a strong update, and establishes that the type-state remains closed after the calls to $f.open()$ and $f.close()$. Summaries $T_1$, $T_2$, $T_3$ share an analogous property that holds when $\theta$ definitely does not point to the abstract object $h$, (i.e., $\theta$ is in the must-not set). In this case, the analysis establishes that the type-state remains closed despite the calls to $f.open()$ and $f.close()$, since $h$ is different from $h$. However, these top-down summaries are specific to calling contexts, and fail to capture these two general properties. As a result, they are unlikely to be reused heavily. The only summary reused is $T_3$ at call site $pc_3$.

2.2 The Bottom-Up Approach

The bottom-up approach starts from leaf procedures and proceeds up along call chains. Like the top-down approach, it too computes summaries, but they differ in crucial ways. Top-down summaries consider only reachable incoming abstract states of procedures whereas bottom-up summaries cover all possible incoming abstract states. Also, caller-specific information is not present in bottom-up summaries. For example, the bottom-up approach computes summaries $B_1$ through $B_3$ for procedure foo, which are shown in Figure 1. These summaries represent four partial functions on abstract states, corresponding to four different cases of incoming abstract states of foo based on the kind of aliasing between argument $f$ and incoming abstract object $h$. Summary $B_3$ is applicable when $\theta$ in the incoming must-not set $n$. In this case, the incoming abstract state is simply returned. Summary $B_2$ is applicable when $f$ is in the incoming must set $a$. In this case, a strong update is performed, returning the incoming abstract state with the type-state updated to $(\iota_{close} \circ \iota_{open})(t)$, where

$\iota_{open} = \lambda t. if \ (t = closed) \ then \ opened \ else \ error$

$\iota_{close} = \lambda t. if \ (t = opened) \ then \ closed \ else \ error$

are type-state transformers associated with $open()$ and $close()$, respectively. The remaining two summaries $B_1$ and $B_4$ are applicable when $f$ is neither in the incoming must nor must-not set; this is possible as the must and must-not sets track only finite numbers of expressions. In this situation, the type-state analysis uses possibly less precise but still safe information from a may-alias analysis, denoted mayalias in summaries $B_3$ and $B_4$. If the may-alias analysis states that $f$ may-alias with $h$, then $B_3$ applies, and a weak update is performed, returning the error type-state. Otherwise, $B_4$ applies and the incoming abstract state is returned similar to $B_1$.

Procedure foo has only two statements yet there are already four cases represented in its bottom-up summaries. Note that this is despite the use of symbolic representations such as type-state transformers $\iota_{close} \circ \iota_{open}$ in $B_2$ instead of case-splitting on $f$. For real-world programs, the number of cases can grow exponentially with the number of commands, and hinder scalability.

2.3 Our Hybrid Approach: SWIFT

The above drawbacks of the top-down and the bottom-up approaches (namely, lack of generalization in top-down summaries and excessive case splitting in bottom-up summaries) motivate our hybrid approach SWIFT. SWIFT is parametrized by the top-down and the bottom-up versions of the given analysis, plus two thresholds $k$ and $\theta$ that control its overall performance. SWIFT triggers the bottom-up analysis on a procedure when the number of incoming abstract states of that procedure computed by the top-down analysis exceeds threshold $k$. Requiring sufficiently many incoming abstract states not only limits triggering the bottom-up analysis to procedures that are being re-analyzed the most often by the top-down analysis—and thus are likely suffering the most from lack of summary reuse and offer the greatest benefit of generalizing—but also helps the bottom-up analysis to determine the most common cases when it does case splitting, and track only those cases, unlike the original bottom-up analysis which tracks all cases. The threshold $\theta$ dictates the maximum number of such cases to track and thereby limit excessive case splitting.

We illustrate SWIFT using $k = 2$ and $\theta = 2$ on our example. SWIFT starts the top-down analysis of main in the usual order of program execution. Upon reaching program point $pc_1$ with abstract state $(h_1, closed, \{v_1\}, \emptyset)$, it checks whether any bottom-up summary is available for foo. Since there is none, it continues the top-down analysis, analyzes the body of foo with initial abstract state $(h_1, closed, \{f\}, \emptyset)$ and computes top-down summary $T_1$. The number of initial abstract states of foo is now one but not above the threshold ($k = 2$) needed to trigger the bottom-up analysis. So SWIFT continues with the top-down analysis, reaches program point $pc_2$ with abstract states $(h_2, closed, \{v_2\}, \emptyset)$ and $(h_1, closed, \{v_1\}, \{v_2\})$, proceeds to re-analyze foo in the corresponding new initial abstract states $(h_2, closed, \{f\}, \emptyset)$ and $(h_1, closed, \emptyset, \{f\})$ and computes top-down summaries $T_2$ and $T_3$, respectively. The number of initial abstract states of foo is now 3, which has exceeded our threshold $k = 2$. Hence, SWIFT triggers a bottom-up
analysis of foo. The bottom-up analysis starts analyzing foo with
\[ \lambda(h, t, a, n). \text{if (true) then } \{ h, t, a, n \} \]
which means the identity function on abstract states, and correctly
summarizes that the part of foo analyzed so far does not make any
state changes. The analysis then proceeds to transform the above
function according to the abstract semantics of each command in
foo, while avoiding case splitting by ignoring certain initial ab-
stract states of foo. When it analyzes the first command \( f \). open(\()\),
it transforms the identity function above to four cases, namely, \( B_1, B_3, \) and \( B_4 \) shown in Figure 1, plus
\[ \lambda(h, t, a, n). \text{if (f } \epsilon \text{ a) then } \{ h, t, a, n \} \]  \[ B_2' \]
\( B_2' \) differs from \( B_2 \) in Figure 1 only in skipping the application
of \( \text{close} \), since the second command \( f \). close(\()\) has not yet been
analyzed by the bottom-up analysis. At this point, the bottom-up
analysis inspects the three existing abstract states \( A_1, A_2, \) and \( A_3 \)
that have been recorded in the corresponding top-down summaries
\( T_1, T_2, \) and \( T_3, \) respectively, and determines that case \( B_2' \) is the
most common (applying to \( A_1 \) and \( A_2 \), case \( B_1 \) is the second-
most common (applying to \( A_3 \), and cases \( B_3 \) and \( B_4 \) are the least
common (applying to none of the existing abstract states). Since \( \theta = 2 \), it keeps the two most common cases \( B_2' \) and \( B_1 \), and prunes
other cases. \( B_3 \) and \( B_4 \). It then proceeds to analyze command \( f \). close(\()\) similarly to obtain the final bottom-up summaries of foo as
\[ \lambda(h, t, a, n). \text{if (f } \epsilon \text{ n) then } \{ h, t, a, n \} \]  \[ B_1 \]
\[ \lambda(h, t, a, n). \text{if (f } \epsilon \text{ a) then } \{ h, (\text{close } \circ \text{ open})(\text{t, a, n) \} } \]  \[ B_2' \]
Thus, while four cases \( B_1-B_4 \) existed in the original bottom-up
summaries of foo, these new summaries represent only two cases,
corresponding to the most common incoming abstract states of foo.

Once the bottom-up analysis is finished, SWIFT continues from
the statement following program point \( p_c \) in main, and reaches the
call to \( \text{foo} \) at \( p_c \) with three abstract states:
\[ \{ h_1, \text{closed, } \emptyset, \{ f \} \} \]  \[ A_3 \]
\[ \{ h_2, \text{closed, } \emptyset, \{ f \} \} \]  \[ A_4 \]
\[ \{ h_3, \text{closed, } \{ f \}, \emptyset \} \]  \[ A_5 \]

Since it had encountered \( A_1 \) at \( p_c \), it reuses top-down summary \( T_3 \)
and avoids re-analyzing foo, similar to a conventional top-down
analysis. But more significantly, SWIFT avoids re-analyzing foo
even for \( A_3 \) and \( A_5 \); of the bottom-up summaries \( B_1 \) and \( B_2 \) that it
computed for foo, \( B_1 \) applies to \( A_4 \), and \( B_2 \) applies to \( A_5 \).

In summary, for our example, SWIFT avoids creating top-down
summaries \( T_4 \) and \( T_5 \) that a conventional top-down analysis
computes, and it avoids creating bottom-up summaries \( B_3 \) and \( B_4 \) that
a conventional bottom-up analysis computes.

2.4 The Challenge of Pruning
Procedure \( \text{foo} \) has a single control-flow path which causes exactly
one of bottom-up summaries \( B_1-B_4 \) to apply to any incoming ab-
stract state \( A \). But in general, procedures have multiple control-flow
paths, which can cause multiple bottom-up summaries to apply to a
given state \( A \). Retaining some of these summaries while pruning
others, and reusing only the retained ones upon encountering state
\( A \), is unsound. We illustrate this with an alternate definition of \( \text{foo} \):
\[ \text{foo(File f, File g) \{ \}
\text{if (*) then } \{ \text{f.open(); f.close(); } \} \text{ else g.open(); } \}
\]

Its bottom-up analysis yields summaries \( B_1-B_4 \) for the true branch,
and four similar summaries for the false branch, which is
\[ \lambda(h, t, a, n). \text{if (g } \epsilon \text{ a) then } \{ h, \text{t.open(t, a, n) \}} \]  \[ B_3 \]

Suppose SWIFT prunes all of them except \( B_2 \) (case \( f \in a \)) and \( B_5 \)
(case \( g \in a \)), and then encounters two incoming abstract states:
\[ \langle h, \text{closed, } \{ f, g \}, \emptyset \rangle \]  \[ A_1 \]
\[ \langle h, \text{closed, } \{ g \} \} \]  \[ A_2 \]
Both \( B_2 \) and \( B_5 \) apply to \( A_1 \), yielding result \( \{ h, \text{closed, } \{ f, g \}, \emptyset \} \),
\[ \langle h, \text{opened, } \{ f, g \}, \emptyset \rangle \} \] as expected. In particular, none of the six
pruned cases apply to \( A_1 \), and therefore they have no effect on the
result. On the other hand, \( B_1 \) and \( B_3 \) apply to \( A_2 \). Since \( B_5 \) was pruned, applying \( B_3 \) alone will yield incorrect result
\[ \langle h, \text{opened, } \{ g \}, \{ f \} \rangle \}, \] as it omits state \( \langle h, \text{closed, } \{ g \}, \{ f \} \rangle \) produced by \( B_1 \), SWIFT guarantees correctness; specifically, we
prove that the hybrid approach it embodies is equivalent to a con-
ventional top-down approach (see Theorem 3.1). In the above sce-
nario, SWIFT re-analyzes foo for \( A_2 \), as a conventional top-down
approach would; only if both of \( B_1 \) and \( B_3 \) are retained does it
avoid re-analyzing, and reuses both of them. Thus, in either sce-
nario, SWIFT produces the correct result for \( A_2 \).

3. Formalism
This section presents SWIFT as a generic framework. Section 3.1
formulates the top-down analysis. Section 3.2 formulates the
bottom-up analysis. Section 3.3 describes conditions relating the
two analyses that SWIFT requires. Section 3.4 augments bottom-
up analysis with a pruning operator guided by top-down analysis.
Section 3.5 extends the formalism to (recursive) procedures.

3.1 Top-Down Analysis
Our formalism targets a language of commands \( C \):
\[ C :: c | C + C | C | C^* \]
It includes primitive commands, non-deterministic choice, sequen-
tial composition, and iteration. Section 3.5 adds procedure calls.

A top-down analysis \( A = (\Sigma, \text{trans}) \) is specified by:
1. a finite set \( \Sigma \) of abstract states, and
2. transfer functions \( \text{trans}(c) : \Sigma \rightarrow 2^\Sigma \) of primitive commands \( c \).

The abstract domain of the analysis is the powerset \( D = 2^\Sigma \) with the
subset order. The abstract semantics of the analysis is standard:
\[ (C)[\Sigma] : 2^\Sigma \rightarrow 2^\Sigma \]
\[ (c[\Sigma]) = \text{trans}(c)[\Sigma] \]
\[ (C_1 + C_2)[\Sigma] = (C_1)[\Sigma] \cup (C_2)[\Sigma] \]
\[ (C_1 ; C_2)[\Sigma] = (C_1)[(C_2)[\Sigma)] \]
\[ (C^*)[\Sigma] = \{ x | x = (\Sigma \cup C)[\Sigma] \} \]
where notation \( f^1 \) denotes lifting of function \( f : D_1 \times \ldots \times D_n \rightarrow 2^D \) to sets of input arguments, as follows: \( f^1(X_1, \ldots, X_n) = \bigcup \{ f(x_1, \ldots, x_n) \mid \forall x_i \in X_i \} \).

Example. We illustrate our formalism using the type-state anal-
ysis shown in Figure 2. This analysis computes a set of abstract
states (also called abstract objects) at each program point to over-
approximate the type-states of all objects. Each abstract state is of
the form \( (h, t, a) \) and represents that an object allocated at site \( h \)
may be in type-state \( t \) and is pointed to by at least variables \( a \)
(the must set). For clarity of exposition, this type-state analysis is
simpler than the full version in our experiments, in two respects:
first, it omits tracking the must-not set in each abstract state, unlike
the type-state analysis in Section 2; second, it restricts the must set
to only contain variables, whereas the implementation allows heap
access path expressions such as \( v.f \) and \( w.g.f \).

The transfer function of a primitive command \( c \) conservatively
updates the type-state and must set of each incoming abstract object
\( (h, t, a) \). The updated must set includes aliases newly generated by
Our bottom-up analysis uses a strong update on the incoming type-state: Domains: (method) $m \in M$ (allocation site) $h \in H$ (variable) $v \in V$ (access path set) $a \in A = 2^V$ (type state) $t \in T = \{\text{init}, \text{error}, \ldots\}$ (type-state function) $[m] \in I = I \to T$ (abstract states) $\sigma \in S = H \times T \times A$

Primitic Commands:

$e ::= v = \text{new} h \mid v = w \mid v.m()$

Transfer Functions:

$\text{trans}(v = \text{new} h)(t, a) = \{(h', t, a \notin \{v\})\}, (\text{init}, \{v\})$

$\text{trans}(v = w)(h, t, a) = \{(w \in a) \to \{(h', t, a \notin \{v\})\}\}$

$\text{trans}(v.m)(t, a) = \{(v \in a) \to \{(h, [m](t), a)\}\}$

$\text{trans}(e, a) = \{(v \in a) \to \{(h, [\text{error}], a)\}\}$

3.2 Bottom-Up Analysis

A bottom-up analysis $B = (\mathbb{R}, \text{id}^D, \gamma, \text{rtrans}, \text{rcomp})$ is specified by:

1. a domain of abstract relations $(\mathbb{R}, \text{id}^D, \gamma)$ where $\mathbb{R}$ is a finite set with an element $\text{id}^D$ and $\gamma$ is a function of type $\mathbb{R} \to 2^{\mathbb{R} \times \mathbb{R}}$, such that $\gamma(\text{id}^D) = \{(\sigma, \sigma) \mid \sigma \in S\}$;

2. transfer functions $\text{rtrans}(e) : \mathbb{R} \to 2^\mathbb{R}$ of primitive commands $e$;

3. an operator $\text{rcomp} : \mathbb{R} \times \mathbb{R} \to 2^\mathbb{R}$ to compose abstract relations.

Elements $r$ in $\mathbb{R}$ mean relations $\gamma(r)$ over abstract states in $S$. Hence, they are called abstract relations. We require a relation $\text{id}^D$ in $\mathbb{R}$ that denotes the identity relation on $S$. We denote the domain of a relation $r$ by $\text{dom}(r) = \{v \mid \exists \sigma' : (\sigma, \sigma') \in \gamma(r)\}$. The input to $\text{rtrans}(e)$ describes past state changes from the entry of the current procedure up to the primitive command $e$, and the function extends this description with the state change of $e$. The operator $\text{rcomp}$ allows composing two abstract relations, and is used to compute the effects of procedure calls; namely, when a procedure with summary $\{r_1, \ldots, r_n\}$ is called and an input relation to this call is $r$, the result of analyzing the call is $\bigcup_{i=1}^n \text{rcomp}(r, r_i)$.

Example. Our bottom-up type-state analysis is shown in Figure 3. It contains two types of abstract relations. The first type is $(\sigma, \phi)$, and it denotes a constant relation on abstract states that relates any $\sigma'$ satisfying $\phi$ to the given $\sigma$. The second type is $(t, a_0, a_1, \phi)$, and this means a relation that takes an abstract state $\sigma = (h, t, a)$ satisfying $\phi$ and updates its type-state to $u(t)$ and its must set to $(a \cap a_0) \cup a_1$. For instance, $(a \cap a_0) \cup a_1, \phi(\text{false}))$ denotes the relation that is defined only when the input must set contains $f$, and that produces as output the same must set but updates type-state $t$ to $t' = ((a \cap a_0) \cup a_1)(t)$ (e.g., if $t = \text{closed}$ then $t' = \text{closed}$, and if $t = \text{open}$ then $t' = \text{error}$). This is precisely the bottom-up summary $B_2$ of procedure $\text{foo}$ in the example in Section 2.

Domain of Abstract Relations:

$\phi \in \mathbb{Q}$

$\sigma = \{\sigma_0 \mid \phi \lor \phi \lor \text{have}(v) \lor \text{notHave}(v)\}$

Relation Composition:

$\text{rcomp}(r, r') = \{\sigma \mid \text{true} \lor \phi \lor \phi \lor \text{have}(v) \lor \text{notHave}(v)\}$

Here are the routines $\text{wp}$ and $r; r'$ defined as follows:

$\text{wp}(r, \text{true}) = \{\sigma \mid \phi \lor \phi \lor \text{have}(v) \lor \text{notHave}(v)\}$

$\text{wp}(r, \phi) = \{\sigma \mid \phi \lor \phi \lor \text{have}(v) \lor \text{notHave}(v)\}$

Next we describe transfer functions $\text{rtrans}$ of primitive commands. When the input abstract relation is $(\sigma, \phi), \text{rtrans}(c)$ simply updates the $\sigma$ part using trans from the top-down type-state analysis. When the input is $(t, a_0, a_1, \phi), \text{rtrans}(c)$ does not have such a uniform behavior—it changes each component of the input according to $\gamma(c)$. We explain this with $\text{rtrans}(c = w)$. Recall that trans$(v = w)(h, t, a)$ splits cases based on whether the must set $a$ contains $w$ or not. To implement this case split, $\text{rtrans}(v = w)$ views the input $(t, a_0, a_1, \phi)$ as a transformer on abstract states, and checks whether this transformer results in an abstract state with $w$ in its must set. The three cases in the definition of $\text{rtrans}(v = w)$ correspond to the three answers to this question: always, never and sometimes. In the first two cases, $\text{rtrans}(v = w)$ updates its input so that $v$ is included (first case) or excluded (second case) from the must set. In the third case, it generates two abstract relations that cover both possibilities of including and excluding $v$. 

---

1. Our bottom-up analysis uses $\text{id}^D$ as the initial abstract relation when analyzing procedures. See Section 3.5.
For all commands $c$, relations $r \in \mathbb{R}$, and states $\sigma, \sigma' \in S$:

$$\exists \sigma_0 \in \mathbb{R} : rtrans(c)(r) \land (\sigma, \sigma') \in \gamma(r)$$

[C1] For all $r, r' \in \mathbb{R}$ and $\sigma, \sigma' \in S$:

$$\exists \sigma_0 : (\sigma, \sigma_0) \in \gamma(r) \land (\sigma_0, \sigma') \in trans(c)(\sigma_0)$$

We now proceed to augment our bottom-up analysis with a pruning operator $\text{wp}$, which removes abstract relations $r$ that become void if we ignore abstract states in $\Sigma$ from the domain of $r$.

First, we define a pruning operator as a function $f : \mathbb{2}^2 \times \mathbb{2}^2 \rightarrow \mathbb{2}^2 \times \mathbb{2}^2$ such that for all $R, R' \subseteq \mathbb{R}$ and $\Sigma, \Sigma' \subseteq S$,

$$f(R, \Sigma) = (R', \Sigma') : (\Sigma \subseteq \Sigma' \land R' = \text{wp}(R, \Sigma'))$$

The purpose of a pruning operator $f$ is to filter out some abstract relations from its input $R$. When making this filtering decision, the operator also takes $\Sigma$, which contains abstract states that the bottom-up analysis has already decided to ignore. Given such an $R$ and $\Sigma$, the operator increases the set of ignored states to $\Sigma'$, and removes all abstract relations $r$ that do not relate any abstract states outside of $\Sigma'$ (i.e., $\text{dom}(r) \subseteq \Sigma'$).

SWIFT automatically constructs a pruning operator, denoted prune, by ranking abstract relations and choosing the top $\theta$ relations, where $\theta$ is a parameter to SWIFT. The ranking is based on the frequencies of incoming abstract states of the current procedure, which are encountered during top-down analysis performed by SWIFT. Formally, prune is built in four steps described next.

First, we assume a multi-set $M$ of incoming abstract states to a given command, which the top-down analysis has previously encountered while analyzing that command in a bigger context.

Second, we define a function rank : $\mathbb{R} \rightarrow \mathbb{N}$ that ranks abstract relations based on $M$ as follows:

$$\text{rank}(r) = \sum_{\sigma \in \text{dom}(r)} \# \text{ of copies of } \sigma \text{ in } M$$

Third, we define a function best : $\mathbb{2}^2 \rightarrow \mathbb{2}^2$ that chooses the top $\theta \geq 1$ abstract relations by their rank values as follows:

$$\text{best}_\theta(R) = \text{set of the top } \theta \text{ elements in } R \text{ according to rank}$$

Finally, we define the pruning operator prune as follows:

$$\text{prune}(R, \Sigma) = \text{let } R_0 = \text{best}_\theta(R) \text{ in let } \Sigma' = \Sigma \cup \bigcup_{r \in R \setminus R_0} \{ (\text{dom}(r)) \in (\text{excl}(R_0, \Sigma'), \Sigma') \}$$

The operator first chooses the top $\theta$ abstract relations from $R$, and forms a new set $R_0$ with these chosen relations. The next step is to increase $\Sigma$. The operator goes through every unchosen relation in $R$, computes its domain, and adds abstract states in the domain to $\Sigma$. The reason for performing this step is to find an appropriate restriction on the domains of $R$ and $R_0$ such that they have the same meaning under this restriction, although $R_0$ contains only selected few of $R$. The result of this iteration, $\Sigma'$, is such a restriction:

$$\gamma^1(R) \cap ((\Sigma \setminus \Sigma') \times S) = \gamma^1(R_0) \cap ((\Sigma \setminus \Sigma') \times S)$$

Note that once we decide to ignore abstract states in $\Sigma'$ from the domain of an abstract relation, some abstract relations in $R_0$ become redundant, because they do not relate any abstract states outside of $\Sigma'$. In the last step, the operator removes such redundant elements from $R_0$ using the operator $\text{excl}(-, \Sigma')$. The result of this further reduction and the set $\Sigma'$ become the output of the operator.

Example. We illustrate the prune operator on our type-state analysis using the example in Section 2. Suppose SWIFT has analyzed procedure $\text{foo}$ thrice using the top-down type-state analysis in incoming abstract states $A_1, A_2,$ and $A_3$, and suppose the bottom-up analysis it triggered has just finished analyzing command $t.\text{open}()$ in the body of $\text{foo}$. At this point, SWIFT has data:

$$M = \{(h_1, \text{closed}, \{ f \}), (h_2, \text{closed}, \{ f \}), (h_1, \text{closed}, \emptyset), \Sigma = \emptyset, R = \{ (\text{topen}, \emptyset, \emptyset, \text{have}(f)), (\text{at} \text{error}, \emptyset, \emptyset, \text{notHave}(f)) \}$$
If \( \theta = 1 \), the pruning operator will retain \( \{\text{wp}(\mathcal{V}, \emptyset, \theta, \text{have}(f))\} \) from \( R \), since two abstract states in \( M \) satisfy \( \text{have}(f) \) (namely, the first two listed in \( M \)) whereas only one satisfies \( \neg \text{have}(f) \). The result of the operator in this case will become:

\[
\Sigma' = \{ (h, t, a) \mid f \notin a \}, \quad R' = \{ \text{wp}(\mathcal{V}, \emptyset, \theta, \text{have}(f)) \}.
\]

**SWIFT** automatically augments the given bottom-up analysis with the prune operator to yield an analysis whose abstract domain is:

\[
\mathcal{D}_r = \{ (R, \Sigma) \in 2^\mathcal{V} \times 2^\Sigma \mid \forall r \in R. \text{dom}(r) \subseteq \Sigma \}.
\]

\[
(R, \Sigma) \subseteq (R', \Sigma') \iff \Sigma \subseteq \Sigma' \land \text{excl}(R, \Sigma) \subseteq R'.
\]

An element \((R, \Sigma)\) means a set of relations \( R \) on abstract states together with the set of ignored input abstract states \( \Sigma \). We require that every \( r \in R \) carries non-empty information when the input abstract states are restricted to \( S \setminus \Sigma \) (i.e., \( \text{dom}(r) \not\subseteq \Sigma \)). Our order \( \subseteq \) says that increasing the ignored set \( \Sigma \) or increasing the set of relations \( R \) makes \((R, \Sigma)\) bigger. It is a partial order with the following join operation \( \sqcup \) where \( \text{clean}(R, \Sigma, \Sigma) = (\text{excl}(R, \Sigma), \Sigma) \):

\[
\bigcup_{i \in I} (R_i, \Sigma_i) = \text{clean} \left( \bigcup_{i \in I} R_i, \bigcup_{i \in I} \Sigma_i \right).
\]

The semantics of the bottom-up analysis with pruning is as follows:

\[
[C]_\gamma^r : \mathcal{D}_r \to \mathcal{D}_r,
\]

\[
[C]_\gamma(r, \Sigma) = \text{prune}(\text{clean} r,\text{trans}(\gamma)^r (R, \Sigma)),
\]

\[
[C_1 ; C_2]_\gamma(r, \Sigma) = \text{prune}(C_1 \gamma^r (R, \Sigma) \cup C_2 \gamma^r (R, \Sigma))\]

\[
[C_1 ; C_2]_\gamma(r, \Sigma) = \text{prune}(C_1 \gamma^r (R, \Sigma)) \cup (C_2 \gamma^r (R, \Sigma)).
\]

\[
[C; \Sigma; R']_\gamma = \text{fix}(R; \Sigma).
\]

\[
\text{fix}(R; \Sigma)
\]

This sequence is increasing because \((R', \Sigma') \subseteq F(R', \Sigma')\) for every \((R', \Sigma')\), and the sequence has a stable element because the domain \( \mathcal{D}_r \) has finite height. Notice that whenever a new abstract relation \( r \) can be generated in the above semantics, prune is applied to filter \( r \) out unless it is considered one of common cases. The degree of filtering done by prune is the main knob of SWIFT for balancing performance against other factors such as the generality of computed abstract relations.

We now present our main theorem, which says that bottom-up analysis with pruning computes the same result as top-down analysis. It maps a program point \( p \) to a set of pairs \( (\sigma, \sigma') \), which represent state changes from the entry of the procedure containing \( p \) up to the procedure point \( p \). The first component \( \sigma \) is an incoming abstract state of the procedure containing \( p \), and the second \( \sigma' \) is an abstract state that arises at \( p \) when \( \sigma \) is the abstract state at the procedure entry. The top-down analysis works by generating new abstract states from pairs \((\sigma, \sigma') \in \mathcal{D}_r\) and propagating them to successors of \( p \). The set \( \mathcal{D}_r \) keeps a set of newly generated abstract states that should be handled by the top-down analysis subsequently. The remaining \( b \) is a table of procedure summaries computed by the bottom-up analysis. Note that \( b \) is a partial function. If \( b(u) \) is undefined, it means that the procedure \( f \) is not yet analyzed by the bottom-up analysis.

The algorithm repeatedly pops a \( w \in \text{workset} \) and processes it until \( \text{workset} \) becomes empty. Handling \( w \) normally means the update of \( \text{workset} \) and \( \mathcal{D}_r \) according to the top-down analysis. We
Algorithm 1: The SWIFT algorithm.

1: **INPUTS:** Initial abstract state \( \sigma_i \) and program \((G, \Gamma)\)
2: **OUTPUTS:** Analysis results \( td \) and \( bu \)
3: var workset, \( R_0, \Sigma_0, \Sigma, f, \sigma \)
4: \( td = \lambda pc. \theta, bu = \lambda f. undefined, workset = \{ \text{entry}_{\text{main}}, \sigma_i, \sigma_i \} \)
5: while \((\text{workset} \neq \emptyset)\) do
6: \( pop w \) from workset
7: if \((\text{command at} w \text{ is not a procedure call})\) then
8: \((td, \text{workset}) = \text{run}_{td}(G, w, td, \text{workset})\)
9: else
10: let \( f \) be the procedure invoked at \( w \)
11: let \( \sigma \) be the current abstract state in \( w \)
12: if \((\exists R_0, \Sigma_0 : \text{bu}(f) = (R_0, \Sigma_0) \land \sigma \not\in \Sigma_0)\) then
13: \( \Sigma = \{ (\sigma', \sigma) \mid \gamma(R_0) \}\)
14: \((td, \text{workset}) = \text{update}_{td}(\Sigma, w, td, \text{workset})\)
15: else
16: \((td, \text{workset}) = \text{run}_{td}(G, w, td, \text{workset})\)
17: if \((\# \text{ of input abstract states to} f \text{ in} td > \text{threshold} k)\) and \( \text{bu} \) is undefined for \( f \) then
18: \( \text{bu} = \text{run}_{bu}(\Gamma, \theta, f, \text{bu})\)
19: end if
20: end if
21: end if
22: end while

express this normal case in the algorithm by

\[(td, \text{workset}) := \text{run}_{td}(G, w, td, \text{workset})\]

where \( \text{run}_{td} \) is a standard tabulation-based computation [17] that we omit here. The exception to this normal case occurs when the command at the program point of \( w \) is a call to a procedure \( f \). In this case, the algorithm checks whether the bottom-up analysis has a summary for \( f \) that can be applied to the current abstract state \( \sigma \) of \( w \) (i.e., the third component of \( w \)). If the check passes, it uses \( \text{bu}(f) \) and computes the result \( \Sigma \) of analyzing \( f \) with \( \sigma \), and updates \((td, \text{workset})\) with \( \Sigma \) according to the top-down analysis (line 14). If the check fails, the algorithm resorts to the top-down analysis, and updates \((td, \text{workset})\). However, unlike the non-procedure call case, the handling of \( w \) does not stop here. Instead, it examines the possibility of running the bottom-up analysis on the body of \( f \). If the number of incoming abstract states of \( f \) in the top-down analysis exceeds the threshold \( k \), and the bottom-up analysis is not yet run on \( f \) and so \( \text{bu}(f) \) is undefined, then the algorithm runs the bottom-up analysis for all procedures \( F \) reachable from \( f \) via call chains, computes summaries for procedures in \( F \), and updates \( \text{bu} \) with these summaries. All these steps are expressed by a single instruction \( \text{bu} := \text{run}_{bu}(\Gamma, \theta, f, \text{bu}) \) in the algorithm (line 18), which gets expanded to the following pseudo-code:

\[
\text{run}_{bu}(\Gamma, \theta, f, \text{bu}) = \\
\text{let } F = \{ \text{procedures reachable from} f \} \text{ in} \\
\text{let } \text{bu}' = [\Gamma[\theta]]^w \text{ with } \theta \text{ used during pruning in} \\
\text{let } \gamma(g \in F) \text{ then } \text{bu}'(g) \text{ else } \text{bu}(g) \\
\]

where \([\Gamma[\theta]]^w\) denotes the run of the bottom-up analysis of Section 3.5 on procedures in \( F \).

We conclude by discussing two scenarios where the pruning operator could have difficulty in identifying common cases during the execution of \( \text{run}_{bu} \). Both scenarios could arise in theory but occurred rarely in our experiments. Assume a setting where the number of incoming abstract states to a procedure \( f \) has exceeded the threshold \( k \), and a procedure \( g \) is reachable from \( f \). In the first scenario, \( g \) has not been analyzed in the top-down analysis, although \( f \) was analyzed multiple times. Our pruning operator lacks data about \( g \) from the top-down analysis and so cannot steer the bottom-up analysis of \( g \) towards its common cases. Our implementation handles this by postponing executing \( run_{bu}(\Gamma, \theta, f, \text{bu}) \) until there is at least one incoming abstract state of \( g \). The second scenario is that \( g \) has been analyzed multiple times in the top-down analysis but most of these analyses do not originate from \( f \). In this scenario, our pruning operator uses the dominating incoming abstract states of \( g \) over the whole program, even though these may not be the dominating ones for \( g \)'s calling context from \( f \).

5. Discussion

Most existing interprocedural analyses either use the top-down approach or the bottom-up approach. This section discusses obligations that analysis developers using either of these approaches must satisfy in order to apply SWIFT for improving their scalability.

5.1 From Bottom-Up Analysis to SWIFT

Suppose a bottom-up analysis exists as specified in Section 3.2. To employ SWIFT, an analysis designer must supply a top-down analysis as specified in Section 3.1, and ensure that it satisfies condition C1 in Section 3.3 that relates the transfer functions for primitive commands trans and rtrans by the two analyses. (We discuss the remaining two conditions C2 and C3 momentarily.) Such a top-down analysis can be synthesized automatically from the bottom-up analysis:

\[
\text{trans}(c)(\sigma) = \{ (\sigma' \mid (\sigma, \sigma') \in \gamma(\text{rtrans}(c)(\sigma))) \}
\]

The only obligations for using SWIFT on an existing bottom-up analysis, then, are defining operators rcomp and wcomp of the bottom-up analysis in a manner that satisfies conditions C2 and C3, respectively. As we discussed in Section 3.3, discharging these conditions is not onerous, since they are stated over abstract semantics, not the concrete one. Also, the bottom-up analysis may already define these operators, as in the case of our type-state analysis.

5.2 From Top-Down Analysis to SWIFT

Suppose a top-down analysis exists as specified in Section 3.1. To make use of SWIFT, an analysis designer must supply a bottom-up analysis as specified in Section 3.2, and ensure that it satisfies conditions C1–C3. Unlike the opposite direction above, there is no general recipe to synthesize the bottom-up analysis automatically from the top-down analysis. Intuitively, the naïve synthesis approach, which defines

\[
r\text{trans}(c)(r) = \{ (\sigma_1, \sigma_3) \mid \exists \sigma_2 : (\sigma_1, \sigma_2) \in r \land \sigma_2 \in \text{trans}(c)(\sigma_2) \}
\]

does not generalize input-output relationships any more than the top-down analysis. Nevertheless, we have identified a general class of analyses for which we can automatically synthesize. We call these kill/gen analyses. The details of this synthesis are provided in Appendix B of the supplementary material. The intuition is that transfer functions of primitive commands for kill/gen analyses have a special simple form: they transform the input by using the meet and join with fixed abstract states, which are selected based on a transformer-specific case analysis on the input. These kill/gen analyses include both vector dataflow analyses as well as certain alias analyses (e.g., connection analysis [12]). Our type-state analysis is not an instance of kill/gen analysis, due to the transfer function of \( \text{v.m}() \), but its handling of the must sets re-uses our kill/gen recipe for synthesizing bottom-up analysis from top-down analysis.

6. Empirical Evaluation

This section presents an empirical evaluation of SWIFT. Section 6.1 describes our experimental setup. Section 6.2 compares SWIFT to conventional top-down and bottom-up approaches. Section 6.3
shows the effect of varying SWIFT’s thresholds \( k \) and \( \theta \). Throughout this section, we refer to the conventional top-down approach as TD and the conventional bottom-up approach as BU.

6.1 Experimental Setup

We implemented SWIFT for building hybrid interprocedural analyses for Java bytecode using the Chord program analysis platform [3]. The top-down part of the framework is based on the tabulation algorithm [17] while the bottom-up part is based on the relational analysis with pruning described in Section 3.

For concreteness, we built an interprocedural type-state analysis using SWIFT. Unlike the type-state analysis from Section 3, it allows tracking access path expressions formed using variables and fields, such as \( v.f \) and \( v.f.g \). By tracking more forms of access path expressions and handling field updates more precisely, the type-state analysis implemented is more precise but also more difficult to scale than the simplified one in Section 3.

We obtained the baseline TD and BU type analyses by switching off the bottom-up part and the top-down part, respectively, in SWIFT. Throughout this section, a top-down summary means a pair of input-output abstract states \((\sigma, \sigma')\) computed for a method by TD or the top-down part of SWIFT. A bottom-up summary is a pair \((r, \phi)\) computed for a method either by BU or the bottom-up part of SWIFT, such that \( r \) is an abstract relation and \( \phi \) the set of input abstract states to which it applies.

We compared SWIFT with TD and BU on 12 real-world Java programs shown in Table 1. The programs and type-state properties are from the Ashes Suite [1] and the DaCapo Suite [2]. All experiments were done using Oracle HotSpot JVM 1.6.0 on Linux machines with 3.0GHz processors and 16GB memory per JVM process.

6.2 Performance of SWIFT vs. Baseline Approaches

Table 2 shows the running time and the total number of top-down and bottom-up summaries computed by SWIFT and the baseline approaches on each benchmark. For SWIFT, we set the threshold on the number of top-down summaries to trigger bottom-up analysis to five (i.e., \( k = 5 \)) and limited to keeping a single case in the pruned bottom-up analysis (i.e., \( \theta = 1 \)), which we found optimal overall.

SWIFT successfully finished on all benchmarks and outperformed both TD and BU significantly on most benchmarks, while TD and BU only finished on a subset of the benchmarks.

SWIFT vs. TD. SWIFT significantly boosted the performance of the type-state analysis over TD, achieving speedups of 4X–59X for most benchmarks. Moreover, for the largest three benchmarks, SWIFT only took under seven minutes each, whereas TD ran out of memory. Besides running time, the table also shows the total number of top-down summaries computed by the two approaches. SWIFT avoided computing over 95% of the summaries computed by TD for most benchmarks.

Figure 5 shows the number of top-down summaries computed for each method by the two approaches. The Y-axis represents the number of summaries computed by TD and the X-axis represents the number of summaries computed by SWIFT. A point on the X-axis does not necessarily denote the same method for both approaches since they may differ in the sorted order. The graphs show that SWIFT greatly reduces the numbers of top-down summaries, keeping them close to the threshold \((k = 5)\) for most methods. It shows that the pruned bottom-up analysis successfully finds the dominating case.

We inspected the top-down summaries of some methods and found that, for most of the inspected methods, the identity function with a certain precondition was the dominating case.

SWIFT vs. BU. BU only finished on our two smallest benchmarks. Compared with TD, BU is much harder to scale due to the exponential case splitting and expensive summary instantiation, especially for an analysis like type-state analysis, which tracks non-trivial aliasing information. Even on these two benchmarks, SWIFT achieved speedups of 9X–118X over BU. Besides running time, Table 2 also shows the total number of bottom-up summaries computed in both approaches. SWIFT avoided computing 87% to 96% of the bottom-up summaries that BU computed.
6.3 Effect of Varying SWIFT Thresholds

We now evaluate the effect of varying thresholds $k$ and $\theta$ on the overall performance of SWIFT.

Effect of Varying $k$. Table 3 shows the total running time and the number of top-down summaries generated for one of our largest benchmarks avrora, using seven different values of $k$. The trend is similar for the other benchmarks. According to this table, $k = 50$ is optimal in terms of the running time while $k = 10$ is optimal in the number of top-down summaries generated.

If we fix the running time of bottom-up analysis, the performance of SWIFT can be approximated by the number of times the top-down analysis is performed on each method, which in turn can be captured by the number of top-down summaries generated. On one hand, setting $k$ too high generates too many top-down summaries before the bottom-up analysis is triggered on the method. As Table 3 shows, the numbers of top-down summaries generated for each method grow dramatically from $k = 10$ to $k = 500$. On the other hand, setting $k$ too low triggers the bottom-up analysis too early, resulting in failure to predict the dominating case in the top-down analysis. For example, using $k = 2$ and $k = 5$ generates more top-down summaries than using $k = 10$.

If we consider the running time of bottom-up analysis, there is a tradeoff between the time spent on running bottom-up analysis and the time saved by avoiding repeatedly running top-down analysis on the same method. Generally, bottom-up analysis is more expensive than the top-down analysis, even under our setting using pruning. The run using $k = 10$ thus consumes more time than that using $k = 50$ by running bottom-up analysis too frequently.

However, the run using $k = 50$ is faster than $k = 100$, as the time it spends on the top-down analysis compensates for the time spent on running the bottom-up analysis. The run using $k = 2$ not only invokes the bottom-up analysis too often but also the top-down analysis, due to its failure to predict the dominating case. It is thus even slower than the run using $k = 200$.

Effect of Varying $\theta$. Table 4 shows the effect of varying $\theta$, the maximum number of cases to be kept by the pruned bottom-up analysis. Using $\theta = 2$ reduced the number of top-down summaries computed by SWIFT, as expected, but on most benchmarks overall performance was worse since the overhead incurred in the bottom-up analysis offset the savings of applying bottom-up summaries in the top-down analysis. The only exception was the run on one of our largest benchmarks avrora, which received a slight boost in running time and a large drop in top-down summaries generated when increasing $\theta$ from 1 to 2. As shown in Table 3, using $k = 5$ triggers the bottom-up analysis too early, resulting in failure to predict the dominating case in the top-down analysis when just one case is tracked. Using $\theta = 2$ gives the bottom-up analysis additional budget and reduces the risk of pruning away the dominating case.

7. Related Work

Sharir and Pnueli [21] present the call-strings and functional approaches to interprocedural analysis. The call-strings approach is a particular kind of top-down approach in which procedure contexts are distinguished using call strings. They present two variants of the functional approach: one that uses a symbolic representation of summaries, which may be viewed as a bottom-up approach, and another that uses an explicit representation, which may be viewed as a top-down approach where procedure contexts are abstract states as opposed to call strings. They provide an iterative fixpoint algorithm for the functional approach variant that uses an explicit representation, but it may use exponential space. Reps et al. [17] identify a representation for the class of IFDS dataflow analysis problems that takes quadratic space and can be computed in cubic time.

Our work differs from the above works in the following ways. First, even when there is a compact representation of procedure summaries with polynomial guarantee (e.g., in the IFDS setting), our approach aims at empirically out-performing this guarantee. Second, our approach does not require a compact representation of
procedure summaries. For instance, a summary of our bottom-up type-state analysis is a set of tuples, whose size can be exponential in the number of program variables. The above works do not attempt to avoid such blowup, whereas ours provides a recipe for doing so, via the pruning operator and the interaction between the top-down and bottom-up versions of the analysis.

Jeannet et al. [15] propose an analysis to generate relational summaries for shape properties in three-valued logic. Yorsh et al. [24] present a logic to relate reachable heap patterns between procedure inputs and outputs. These works involve relational analyses, but they do not focus on controlling the amount of case splitting in a bottom-up relational analysis, as we do with a pruning operator. For instance, Jeannet et al.’s relational shape analysis works top-down, and computes summaries for given incoming abstract states, unlike our bottom-up summaries that can be applied to unseen states. The issue of case splitting does not arise in their setting.

Bottom-up analyses have been studied theoretically in [9, 14], but are less popular in practice than top-down analyses, because of the challenges in designing and implementing them efficiently. Notable exceptions are analyses about pointer and heap reasoning, such as those for may-alias information [13, 16, 20, 22], must-alias information [7, 10] and shape properties [6, 13], where the analyses typically use symbolic abstract domains.

In contrast, top-down analysis [8, 17, 21] is much better understood, and generic implementations are available in analysis frameworks such as Chord, Soot, and Wala. Various approaches have been proposed to scale top-down analyses. Rinetzky et al. [18, 19] improve summary reuse in heap reasoning by separating the part of the heap that can be locally changed by the procedure from the rest of the heap. Yorsh et al. [25] generalize top-down summaries by replacing explicit summaries with symbolic representations, thereby increasing reuse without losing precision. Ball et al. [5] generalize highly reusable summaries by encoding the transfer functions using BDDs. Our work provides a new technique to scale top-down analysis by tightly integrating it with a bottom-up counterpart.

Others have hinted at the existence of dominating cases in bottom-up analyses. Rinetzky et al. [18, 19] assume that a dereferenced heap cell at a program point $pc$ of a procedure $f$ is usually not aliased with any of the previously accessed cells in the same procedure, unless $f$ creates such an aliasing explicitly before reaching $pc$. The analysis, then, focuses on initial states to procedures that are considered common based on this assumption, and thereby avoids excessive case splitting. Bottom-up alias analyses [23] likewise assume non-aliasing between procedure arguments. These assumptions are not robust since they conjec- ture a property of common initial states to procedures without actually seeing any of them. Our hybrid analysis suggests a way to overcome this issue by collecting samples from the top-down analysis and identifying common cases based on these samples.

An orthogonal approach for scaling interprocedural analysis is parallelization. Bottom-up analyses are easy to parallelize—indepen- dent procedures can be analyzed in parallel—and recent work also addresses parallelizing top-down analyses [4]. A possible way to parallelize our hybrid approach is to modify it such that whenever a bottom-up summary is to be computed, it spawns a new thread to do this bottom-up analysis, and itself continues the top-down analysis. Developing this idea further and exploring other parallelizing strategies (such as [4]) is future work.

8. Conclusion

We proposed a new approach to scale interprocedural analysis by synergistically combining the top-down and bottom-up approaches. We formalized our approach in a generic framework and showed its effectiveness on a realistic type-state analysis. Our approach holds promise in contrast or complementation with existing techniques to scale interprocedural analysis, including those that use domain knowledge to increase summary reuse in top-down approaches, and those that use sophisticated symbolic techniques to efficiently compute and instantiate summaries in bottom-up approaches.

References

A. Proof of Theorem 3.1

In this appendix, we provide the proof of Theorem 3.1:

**Theorem 3.1 (Coincidence)** For all $\Sigma, \Sigma', R'$, if

$$([C]^{\dagger}(\{id^2\}, \emptyset) = (R', \Sigma')) \land (\Sigma \cap \Sigma' = \emptyset),$$

we have that for every $\sigma'$ in $\Sigma$, $\sigma' \in [C]^{\dagger}(\Sigma) \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma^1(R')$.

Our proof strategy is to define an intermediate abstract semantics working on $2^k$, and to relate both non-relational and relational semantics with this intermediate one. Our theorem will follow from these relationships.

A.1 Intermediate Abstract Semantics

The intermediate abstract semantics uses the domain $2^k$ with the subset order, and has the following abstract semantics:

$$[C]^{\dagger} : 2^k \to 2^k$$
$$[c]^{\dagger}(R) = rtrans(c)^{\dagger}(R)$$
$$[C_1 + C_2]^{\dagger}(R) = [C_1]^{\dagger}(R) \cup [C_2]^{\dagger}(R)$$
$$[C_1; C_2]^{\dagger}(R) = [C_2]^{\dagger}([C_1]^{\dagger}(R))$$
$$[C]^{\dagger}(R) = lfix(lam(R))\downarrow [C]^{\dagger}(R').$$

Although this semantics reuses $R$ and $rtrans$ from the relational analysis, it does not prune any abstract relations, and it uses the standard subset order and defines the abstract meaning of $C^*$ using the standard least fixpoint operator $lfix$.

**Theorem A.1.** For all commands $C$, sets $\Sigma$ of abstract states in $S$ and abstract states $\sigma'$,

$$\sigma' \in [C]^{\dagger}(\Sigma) \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma^1([C]^{\dagger}(\{id^2\})).$$

**Proof.** For all $R$ and $\Sigma$, we define

$$apply(R, \Sigma) = \{\sigma' \mid \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma^1(R)\}.$$

The theorem can be paraphrased to the following equation:

$$[C]^{\dagger}(\Sigma) = apply([C]^{\dagger}(\{id^2\}), \Sigma).$$

We prove the following slightly stronger property than this paraphrase of the theorem:

**Correspondence Property:** For all commands $C$, sets of abstract states $\Sigma$, and sets of abstract relations $R$,

$$[C]^{\dagger}(apply(R, \Sigma)) = apply([C]^{\dagger}(R), \Sigma).$$

By instantiating $R$ with $\{id^2\}$, we can derive the theorem from this property.

Our proof of the correspondence property uses the induction on the structure of $C$. The case of primitive commands follows from our requirement on $rtrans$. We handle the remaining cases separately. To do so, choose $R, \Sigma$.

The case $C = C_1; C_2$ is proved as follows:

$$[C_1; C_2]^{\dagger}(apply(R, \Sigma)) = [C_2]^{\dagger}([C_1]^{\dagger}(apply(R, \Sigma)))$$
$$= [C_2]^{\dagger}(apply([C_1]^{\dagger}(R), \Sigma))$$
$$= apply([C_2]^{\dagger}([C_1]^{\dagger}(R)), \Sigma)$$
$$= apply([C_1; C_2]^{\dagger}(R), \Sigma).$$

The first and last equalities just use the definitions of $[C_1; C_2]^{\dagger}$ and $[C_1; C_2]^{\dagger}$. The second and third equalities hold because of the induction hypothesis on $C_1$ and $C_2$.

The next case is $C = C_1 + C_2$, which we prove below:

$$[C_1 + C_2]^{\dagger}(apply(R, \Sigma))$$
$$= ([C_1]^{\dagger}(apply(R, \Sigma)) \cup [C_2]^{\dagger}(apply(R, \Sigma))$$
$$= apply([C_1]^{\dagger}(R), \Sigma) \cup apply([C_2]^{\dagger}(R), \Sigma)$$
$$= apply([C_1]^{\dagger}(R) \cup [C_2]^{\dagger}(R), \Sigma)$$
$$= apply([C_1 + C_2]^{\dagger}(R), \Sigma).$$

The first and last equalities are just the unrolling and rolling of the defining clauses in the two semantics. The second equality holds because of the induction hypothesis. The third equality holds because apply($\cdot$, $\Sigma$) preserves the union operation.

The remaining case is $C = C_1^\dagger$. Let $F$ and $G$ be functions defined by:

$$F = \lambda \Sigma'. (apply(R, \Sigma) \cup [C_1]^{\dagger}(\Sigma')),$$
$$G = \lambda R'. R \cup [C_1]^{\dagger}(R').$$

And let $\mathcal{R}$ be the following relation between sets of abstract states and those of abstract relations:

$$(\Sigma', R') \in \mathcal{R} \iff apply(R', \Sigma) = \Sigma'.$$

Then,

$$[C_1^\dagger](apply(R, \Sigma)) = lfix F \land [C_1^\dagger](R) = lfix G.$$

It is easy to show that $(\emptyset, \emptyset) \in \mathcal{R}$, and for all families $\{(R_i, \Sigma_i)\}_{i \in I}$,

$$(\forall i \in I. (R_i, \Sigma_i) \in \mathcal{R}) \Rightarrow (\bigcup_{i \in I} R_i, \bigcup_{i \in I} \Sigma_i) \in \mathcal{R}.$$

In other words, $\mathcal{R}$ preserves arbitrary union. Hence, to prove this case of $C = C_1^\dagger$, it is sufficient to show that

$$(\Sigma', R') \in \mathcal{R} \Rightarrow (F(\Sigma'), G(R')) \in \mathcal{R},$$

(1)

because this implies

$$(lfix F, lfix G) = (\bigcup_{n \in \mathbb{N}} F^n(\emptyset), \bigcup_{n \in \mathbb{N}} G^n(\emptyset)) \in \mathcal{R}$$

and unpacking the definition of $\mathcal{R}$ here gives the correspondence. Finally, we discharge the final proof obligation, i.e., the implication in (1):

$$(\Sigma', R') \in \mathcal{R}$$
$$\Rightarrow (([C_1]^{\dagger}(\Sigma'), [C_1^\dagger](R')) \in \mathcal{R}$$
$$\Rightarrow ((apply(R, \Sigma), R) \in \mathcal{R}) \land \(([C_1]^{\dagger}(\Sigma'), [C_1^\dagger](R')) \in \mathcal{R}$$
$$\Rightarrow (apply(R, \Sigma) \cup [C_1]^{\dagger}(\Sigma'), R \cup [C_1^\dagger](R')) \in \mathcal{R}$$
$$\Rightarrow (F(\Sigma'), G(R')) \in \mathcal{R}.$$

The first implication follows from the induction hypothesis, the second holds because $apply(R, \Sigma)$ and $R$ are related by $\mathcal{R}$, and the third equality uses the fact that $\mathcal{R}$ preserves the union. □

A.2 Relationship between Intermediate Abstract Semantics and Relational Analysis

We prove that the relational analysis computes the same results as the intermediate abstract semantics, as long as we filter out some abstract relations as indicated by the theorem below:

**Lemma A.2.** For all primitive commands $c$, and sets of abstract relations $R$, and those of abstract states $\Sigma$,

$$excl(rtrans(c)^{\dagger}(excl(R, \Sigma)), \Sigma) = excl(rtrans(c)^{\dagger}(R), \Sigma).$$

**Proof.** By the definition of $excl$, we have that

$$excl(R, \Sigma) \subseteq R.$$
Since both $\text{rtrans}(c)^\dagger(-)$ and $\text{excl}(-, \Sigma)$ are monotone with respect to the subset order, the LHS of the equation in this lemma should be included in the RHS of the equation. It remains to show the other inclusion. Pick $r \in \text{rtrans}(c)^\dagger(R, \Sigma)$. Then,
\[
\text{dom}(r) \not\subseteq \Sigma \wedge (\exists r' \in R : r \in \text{rtrans}(c)(r')).
\]

Let $r' \in R$ be the witness in the second conjunct. We will show
\[
\text{dom}(r') \not\subseteq \Sigma.
\]

This would imply $r' \in \text{excl}(R, \Sigma)$ and, hence, the desired membership of $r$ to the LHS of the equation in the lemma. Because of the first conjunct in (2), there exist $\sigma$ and $\sigma'$ such that
\[(\sigma, \sigma') \in \gamma(r) \wedge \sigma \not\in \Sigma.
\]

But $r \in \text{rtrans}(c)(r')$, so the requirement on $\text{rtrans}(c)$ gives
\[
\exists \sigma_0 : (\sigma, \sigma_0) \in \gamma(r') \wedge \sigma \in \text{trans}(c)(\sigma_0).
\]

Recall $\sigma \not\in \Sigma$. Thus, the first conjunct gives $\text{dom}(r') \not\subseteq \Sigma$. □

**Theorem A.3.** For every $R, R' \subseteq \mathbb{R}$ and $\Sigma, \Sigma' \subseteq \mathbb{S}$, if
\[
[[C]]^\circ \text{clean}(R, \Sigma) = (R', \Sigma')
\]
we have that $R' = \text{excl}([[C]]^\circ(R, \Sigma))$.

**Proof.** We prove the theorem by induction on the structure of $C$. Pick $R, R', \Sigma, \Sigma'$ such that
\[(R', \Sigma') = [[[C]]^\circ \text{clean}(R, \Sigma)).
\]

We first prove the base case that $C$ is a primitive command $c$:

\[
(R', \Sigma') = [[[c]]^\circ \text{clean}(R, \Sigma)
\]

\[
\Rightarrow (R', \Sigma') = \text{prune}(\text{rtrans}(c)^\dagger(\text{excl}(R, \Sigma), \Sigma))
\]

\[
\Rightarrow (R', \Sigma') = \text{prune}(\text{rtrans}(c)^\dagger(R, \Sigma), \Sigma)
\]

\[
\Rightarrow (R', \Sigma') = \text{prune}(\text{excl}(\text{rtrans}(c)^\dagger(R, \Sigma), \Sigma'))
\]

\[
\Rightarrow R' = \text{excl}(\text{rtrans}(c)^\dagger(R, \Sigma), \Sigma')
\]

\[
\Rightarrow R' = \text{excl}([[C]]^\circ(R, \Sigma), \Sigma')
\]

The first and third and sixth implications are just the unpacking and packing of the definitions of clean, $[[C]]^\circ$, and $[[C]]^\dagger$. The second holds because of Lemma A.2, the fourth follows from the conditions used for defining the pruning operator, and the fifth implication follows from the subset relationship $\Sigma \subseteq \Sigma'$.

The next case is that $C = C_1 + C_2$. For $i \in \{1, 2\}$, let
\[
(R'_i, \Sigma'_i) = ([[[C_i]]^\circ \text{clean}(R, \Sigma)) \wedge R''_i = [C_i]^\circ(R).
\]

Then, by the induction hypothesis, we have that for all $i \in \{1, 2\}$,
\[
R'_i = \text{excl}(R''_i, \Sigma'_i).
\]

Using this equality, we prove the case as follows:

\[
(R', \Sigma') = [[[C_1 + C_2]]^\circ \text{clean}(R, \Sigma)
\]

\[
\Rightarrow (R', \Sigma') = \text{prune}([[[C_1]]^\circ \text{clean}(R, \Sigma)) \cup [[[C_2]]^\circ \text{clean}(R, \Sigma))
\]

\[
\Rightarrow (R', \Sigma') = \text{prune}(\text{excl}(R'_1 \cup R'_2, \Sigma'_1 \cup \Sigma'_2), \Sigma_1 \cup \Sigma_2)
\]

\[
\Rightarrow R' = \text{excl}(\text{excl}(R'_1 \cup R'_2, \Sigma'_1 \cup \Sigma'_2), \Sigma')
\]

\[
\Rightarrow R' = \text{excl}(R'_1 \cup R'_2, \Sigma')
\]

\[
\Rightarrow R' = \text{excl}([[C_1 + C_2]]^\circ(R, \Sigma))
\]

The first and second implications are the unrolling of the definitions of $[[C_1 + C_2]]^\circ$ and the join operation, the third follows from the defining condition for the pruning operator, the fourth and sixth implications hold because $\Sigma'_i$ is a subset of $\Sigma'$, and the last holds because of the definition of $[[C_i + C_2]]^\circ$. The only remaining step is the fifth implication, and it uses the equality in (4) above.

The third case is that $C = C_1; C_2$. Let $(R''_i, \Sigma'_i)$ be $([[[C_i]]^\circ \text{clean}(R, \Sigma)$). We prove the case as follows:

\[
(R', \Sigma') = (C_1; C_2)^\circ \text{clean}(R, \Sigma)
\]

\[
\Rightarrow (R', \Sigma') = [[[C_1]]^\circ \text{clean}(R, \Sigma))
\]

\[
\Rightarrow (R', \Sigma') = [[[[C_1]]^\circ \text{clean}(R, \Sigma))
\]

\[
\Rightarrow (R', \Sigma') = [[[[C_1]]^\circ \text{clean}(R, \Sigma))
\]

\[
\Rightarrow (R', \Sigma') = ([[C_2]]^\circ \text{clean}([[[C_1]]^\circ \text{clean}(R, \Sigma)), \Sigma'))
\]

\[
\Rightarrow (R', \Sigma') = [[[C_2]]^\circ \text{clean}(R, \Sigma))
\]

\[
\Rightarrow R' = \text{excl}([[C_2]]^\circ(R', \Sigma'))
\]

\[
\Rightarrow R' = \text{excl}([[C_1; C_2]]^\circ(R, \Sigma)
\]

The first, second, fourth and sixth implications follow from the definitions of $[[C_1; C_2]]^\circ$, $(R'_1, \Sigma'_1)$, and $[[[C_1; C_2]]^\circ$. The third and fifth implications use induction hypothesis on $C_1$ and $C_2$, respectively.

**Theorem A.3.** Let $F(R_0, \Sigma_0) = \text{prune}(R_0, \Sigma_0) \cup [[C]]^\circ(R_0, \Sigma_0))$,

$G(R_0) = R_0 \cup [[C]]^\circ(R_0))$.

Also, define two sequences: for every $n \geq 0$,

\[
(R'_n, \Sigma'_n) = F^n(\text{clean}(R, \Sigma))
\]

\[
(R''_n, \Sigma''_n) = G^n(R).
\]

Then, there exists $m \geq 0$ such that

\[
[[C]]^\circ(\text{clean}(R, \Sigma)) = (R''_n, \Sigma''_n).
\]

Hence, it is sufficient to prove that for every $n \geq 0$,

\[
R'_n = \text{excl}(R''_n, \Sigma''_n).
\]

We do this by induction on $n$. The case of $n = 0$ is immediate. To prove the inductive case, we assume that the equality in (5) holds for $n$, and let

\[
(R_n, \Sigma_n) = [[C]]^\circ(R'_n, \Sigma'_n).
\]

We prove the inductive case as follows:

\[
(R_{n+1}, \Sigma_{n+1}) = \text{prune}(R'_n, \Sigma'_n) \cup [[C]]^\circ(R''_n, \Sigma''_n)
\]

\[
\Rightarrow (R_{n+1}, \Sigma_{n+1}) = \text{prune}(R'_n, \Sigma'_n) \cup (R''_n, \Sigma''_n)
\]

\[
\Rightarrow (R_{n+1}, \Sigma_{n+1}) = \text{prune}(R'_n \cup R''_n, \Sigma'_n \cup \Sigma''_n)
\]

\[
\Rightarrow R_{n+1} = \text{excl}(R'_n \cup R''_n, \Sigma'_n \cup \Sigma''_n)
\]

\[
\Rightarrow R_{n+1} = \text{excl}(R'_n, \Sigma'_n) \cup \text{excl}(R''_n, \Sigma''_n)
\]

\[
\Rightarrow R_{n+1} = [[[[C_1]]^\circ(R''_n, \Sigma''_n) \cup \text{excl}(R, \Sigma_{n+1})
\]

\[
\Rightarrow R_{n+1} = \text{excl}(R'_n \cup R''_n, \Sigma'_n \cup \Sigma''_n)
\]

\[
\Rightarrow R_{n+1} = \text{excl}(R'_n, \Sigma'_n) \cup \text{excl}(R''_n, \Sigma''_n)
\]

\[
\Rightarrow R_{n+1} = \text{excl}(R'_n \cup R''_n, \Sigma'_n \cup \Sigma''_n)
\]

\[
\Rightarrow R_{n+1} = \text{excl}(R'_n \cup R''_n, \Sigma'_n \cup \Sigma''_n)
\]

The first, second and third implications use the definitions of $(R_n, \Sigma_n)$, the join and the clean operation, respectively. The fourth uses the defining condition for the pruning operator and the subset relationship $\Sigma'_n \cup \Sigma_{n+1} \subseteq \Sigma_{n+1}$. The fifth implication holds because of the induction hypothesis, and the sixth is based on the subset relationship between $\Sigma_n$ and $\Sigma_{n+1}$. The seventh implication holds because

\[
\text{clean}(R, \Sigma) = (R'_0, \Sigma_0) \subseteq (R'_{n+1}, \Sigma'_{n+1}).
\]
The eighth uses the distributivity of \( \text{excl}(\_, \Sigma'_{n+1}) \) over union, and the ninth is the packing of the definition of \( R''_n \). The last implication holds because

\[ R''_n = \text{excl}(R''_n, \Sigma''_{n+1}) \subseteq R''_n \subseteq R''_{n+1}. \]

### A.3 Theorem 3.1 as a Corollary of Theorems A.1 and A.3

We will now prove Theorem 3.1 using Theorems A.1 and A.3. Consider \( \Sigma, \Sigma', R' \) such that

\[ (\{C\}'(\{\{d'\}\}, \emptyset) = (R', \Sigma') \wedge (\Sigma \cap \Sigma' = \emptyset). \]

We should prove that for every \( \sigma' \) in \( S \),

\[ \sigma' \in \{C\}'(\Sigma) \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma'(R'). \]

We disprove this proof step as follows:

\[ \sigma' \in \{C\}'(\Sigma) \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma'(\{C\}'(\{d'\}))) \]

\[ \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma'(\text{excl}(\{C\}'(\{d'\}), \Sigma'))) \]

\[ \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma'(R'). \]

The first equivalence follows from Theorem A.1, and the second holds because \( \Sigma \) and \( \Sigma' \) do not overlap and the source abstract state \( \sigma \) in the pair \( (\sigma, \sigma') \) is in \( \Sigma \). The last equivalence is valid because of Theorem A.3.

### B. Kill-Gen Analysis

In this appendix, we explain how to synthesize a bottom-up analysis from the top-down analysis, for a limited but useful class of analyses with transfer functions of a specific form, namely, so-called “kill/gen” dataflow analyses.

#### B.1 Top-Down Analysis

Our construction applies to a particular kind of top-down analysis \( (S, \text{trans}) \), where transfer functions of primitive commands have a simple form. To describe this form formally, we assume two domains associated with the analysis \( (S, \text{trans}) \).

1. A finite distributive lattice \( (\Delta, \bot, T, U, \top) \) with two operations:

\[ \emptyset, \oplus : S \times \Delta \rightarrow S. \]

Intuitively, elements of \( \Delta \) represent deltas on abstract states, i.e., changes to be made to abstract states. The \( \ominus \) operation incorporates such changes by taking intersection, and \( \oplus \) does the same by taking the union. We require that these operations satisfy the conditions below: for all \( \sigma \in S \) and \( \delta, \delta' \in \Delta \),

\[ (\sigma \ominus d) \oplus d' = \sigma \ominus (d \cap d') \]

\[ (\sigma \ominus d) \oplus d' = \sigma \ominus (d \cup d') \]

\[ (\sigma \ominus d) \ominus d' = (\sigma \ominus d') \oplus (d \cap d'). \]

The first two conditions say that \( \ominus \) and \( \oplus \) are the right monoid actions with respect to \( T \) and \( \bot \), respectively. The last condition expresses a form of distributivity of \( \ominus \) over \( \ominus \).

2. A collection \( \mathcal{A} \) of unary predicates on \( S \), i.e., functions of type \( S \rightarrow \{\text{true}, \text{false}\} \).

We require that \( \mathcal{A} \) contain the always-true predicate \( \phi_{\text{true}} \), and be closed under conjunction: for all \( \phi_1, \phi_2 \in \mathcal{A} \), there exists \( \phi \in \mathcal{A} \) such that

\[ \forall \sigma \in S \cdot (\phi(\sigma) = \text{true} \iff \phi_1(\sigma) \land \phi_2(\sigma) = \text{true}). \]

We write \( \phi(\sigma) = \text{true} \) instead of \( \phi(\sigma) \), true, when the omission can be easily recognized.

#### DEFN B.1. A function \( f \) from \( S \) to \( 2^S \) is simple iff

\[ f(\sigma) = \{\sigma_i | \phi_i(\sigma) \wedge i \in I\} \cup \{\sigma \ominus \delta_i \ominus \delta_j | \phi_j(\sigma) \wedge j \in J\}. \]

Here, \( I, J \) are fixed finite sets of indices, \( \sigma_i \) are abstract state, \( \delta_i, \delta_j \) are elements from \( \Delta \), and \( \phi_i, \phi_j \) are predicates in \( \mathcal{A} \).

#### DEFN B.2. The set \( \mathcal{A} \) of predicates is wp-closed iff

\[ \forall \delta, \delta' \in \Delta . \forall \sigma \in \mathcal{A} \cdot (\lambda \sigma . \phi((\sigma \ominus \delta) \ominus \delta')) \in \mathcal{A}. \]

#### DEFN B.3. The analysis \( (S, \text{trans}) \) is simple when \( \text{trans}(c) \) is simple for every primitive command \( c \).

#### LEMMA B.4. If \( (S, \text{trans}) \) is simple and \( \mathcal{A} \) is wp-closed, then \( \lambda \sigma . [C]\{\sigma\} \) is simple for every primitive command \( C \).

#### Proof. We prove the lemma by induction on the structure of \( C \).

When \( C \) is a primitive command \( c \), we have the desired weak input dependency by the assumption that the analysis has weak input dependency.

The next case is that \( C = C_1 : C_2 \). Let \( f = \lambda \sigma . [C_1]\{\sigma\} \) and \( g = \lambda \sigma . [C_2]\{\sigma\} \). By induction hypothesis, there exist

\[ I, J, K, \sigma, \delta_i, \delta_j, \epsilon_k, \epsilon'_k, \sigma_i, \sigma_k, \phi_i, \phi_j, \psi_k, \psi'_k \]

such that

\[ f(\sigma) = \{\sigma_i | \phi_i(\sigma) \wedge i \in I\} \cup \{\sigma \ominus \delta_i \ominus \delta_j | \phi_j(\sigma) \wedge j \in J\}. \]

Then, \([C_1 ; C_2]\{\sigma\} = \bigcup \{g(\sigma') \mid \sigma' \in f(\sigma)\} \). Since \([C_1 ; C_2] \)

 preserves set union, it can be expressed as follows:

\[ [C_1 ; C_2]\{\sigma\} = \]

\[ \{\sigma_k | \phi_k(\sigma) \wedge k \in K \} \cup \]

\[ \{\sigma_k \ominus \psi_k(\sigma) \wedge k \in K \} \cup \{\sigma \ominus \epsilon_i \ominus \epsilon'_i | \phi_i(\sigma) \wedge \psi_i(\sigma) \wedge (i, l) \in I \} \cup \]

\[ \{\sigma \ominus \delta_i \ominus \delta_j | \epsilon_i \ominus \epsilon'_i \wedge (j, l) \in J \} \]

Since \( \mathcal{A} \) is wp-closed and

\[ \{\sigma \ominus \delta_i \ominus \delta_j | \epsilon_i \ominus \epsilon'_i \} = \{\sigma \ominus (\delta_i \cap \delta_j) \ominus (\delta'_i \cap \epsilon_i \cup \epsilon'_i) \}

 the above expression \([C_1 ; C_2]\{\sigma\} \)

 is simple.

We move on to the case that \( C = C_1 + C_2 \). Let \( f = \lambda \sigma . [C_1] \{\sigma\} \) and \( g = \lambda \sigma . [C_2] \{\sigma\} \). By induction hypothesis, there are

\[ I, J, K, \sigma, \delta_i, \delta_j, \epsilon_k, \epsilon'_k, \sigma_i, \sigma_k, \phi_i, \phi_j, \psi_k, \psi'_k \]

such that

\[ f(\sigma) = \{\sigma_i | \phi_i(\sigma) \wedge i \in I\} \cup \{\sigma \ominus \delta_i \ominus \delta_j | \phi_j(\sigma) \wedge j \in J\}. \]

Then, \([C_1 + C_2]\{\sigma\} = \]

\[ \{\sigma_i | \phi_i(\sigma) \wedge i \in I\} \cup \{\sigma_k | \psi_k(\sigma) \wedge k \in K \} \cup \{\sigma \ominus \epsilon_i \ominus \epsilon'_i | \phi_i(\sigma) \wedge (i, l) \in I \} \cup \]

\[ \{\sigma \ominus \delta_i \ominus \delta_j | \phi_j(\sigma) \wedge (j, l) \in J \} \cup \{\sigma \ominus \epsilon_i \ominus \epsilon'_i | \phi_i(\sigma) \wedge (i, l) \in I \}. \]

Using the entities in the above expressions, we represent \([C_1 + C_2] \)

 as follows:

\[ [C_1 + C_2]\{\sigma\} = \]

\[ \{\sigma_i | \phi_i(\sigma) \wedge i \in I\} \cup \{\sigma_k | \psi_k(\sigma) \wedge k \in K \} \cup \]

\[ \{\sigma \ominus \delta_i \ominus \delta_j | \phi_j(\sigma) \wedge j \in J\} \cup \]

\[ \{\sigma \ominus \epsilon_i \ominus \epsilon'_i | \phi_i(\sigma) \wedge (i, l) \in I \}. \]

Hence, \( \lambda \sigma . [C_1 + C_2] \{\sigma\} \)

 is simple.

The remaining case is that \( C = C_1^+ \). Define a function \( F \):

\[ F(T) = \lambda \Sigma. \Sigma \cup ([C_1] \circ T)(\Sigma). \]
where $T$ is a monotone function on $2^S$ preserving set union and such $T$’s are ordered pointwise. It is well-known that

$$\llbracket T \rrbracket = \text{fix } F.$$

Call a function $T : 2^S \rightarrow 2^S$ simple if $T$ preserves set union and $\lambda \sigma. T(\{\sigma\})$ is simple. Then, the reasoning similar to the one for the preceding case above, we can show that $F$ preserves simplicity. Also, the set of simple functions on $2^S$ is closed under the join operation, which can be proved as in the case of nondeterministic choice. From these two results follows that the least fixpoint of $F$ is also simple. □

B.2 Bottom-Up Analysis

The main feature of the top-down analysis described above is that the transfer function of each primitive command has a particular form. This feature allows us to construct an equivalent bottom-up analysis that treats the incoming abstract state symbolically. Suppose we are given a top-down analysis $(\mathcal{S}, \mathcal{T}, \Delta, \bigcirc, \ominus, \ominus, \land, \land, \lor, \lor, \land, \land, \lor, \lor, \land, \land, \lor, \lor, \land, \land)$

We build a corresponding bottom-up analysis $(\mathcal{R}, \mathcal{R}, \mathcal{I}, \mathcal{I}, \mathcal{I}, \mathcal{I}, \mathcal{I}, \mathcal{I})$, apply as follows:

1. We define a set $T$:

$$T = \Delta \times \Delta.$$

Elements $t = (\delta, \delta')$ in $T$ describe transformers for abstract states. We use $\gamma$ to explain the meaning formally:

$$\gamma : T \rightarrow (\mathcal{S} \rightarrow \mathcal{S}) \quad \gamma(\delta, \delta')(\sigma) = (\sigma \ominus \delta) \odot \delta'.$$

2. Using $T$, we construct the domain $\mathcal{R}$ of abstract relations

$$\mathcal{R} = (\mathcal{S} \cup T) \times \mathcal{A}.$$

Then, we define the function apply, which provides the formal meaning to these abstract relations in terms of nondeterministic relations on $\mathcal{S}$:

$$\text{apply}(t, \phi, \sigma) = \{\sigma | \sigma(\sigma)\},$$

$$\text{apply}(t, \phi, \sigma) = \{\gamma(t)(\sigma) | \gamma(\sigma)\}.$$

3. We use the following element in $\mathcal{R}$ as the abstract identity relation:

$$\mathcal{I}^2 = ((T, \Delta), \mathcal{I}, \text{true}).$$

This meets the requirement for $\mathcal{I}^2$:

$$\text{apply}(\mathcal{I}^2, \sigma) = \{\sigma | \sigma(\sigma)\} = \{\sigma\}.$$

4. Finally, we specify a transfer function for each primitive command $c$:

$$\text{rtrans}(c) : \mathcal{R} \rightarrow 2^\mathcal{R}.$$

Let the transfer function for $c$ in the top-down analysis have the following shape:

$$\text{trans}(c)(\sigma) = \{\sigma | \sigma(\sigma) \land i \in I\}$$

$$\cup \{\sigma(\sigma) \land j \in J\}.$$

The corresponding transfer function $\text{rtrans}(c)$ is given as follows:

$$\text{rtrans}(c)(\sigma, \phi)) = \{\sigma | \sigma(\sigma) \land i \in I\}$$

$$\cup \{\sigma(\sigma) \land j \in J\}.$$

The corresponding transfer function $\text{rtrans}(c)$ is given as follows:

$$\text{rtrans}(c)(\sigma, \phi)) = \{\sigma | \sigma(\sigma) \land i \in I\}$$

$$\cup \{\sigma(\sigma) \land j \in J\}.$$

The corresponding transfer function $\text{rtrans}(c)$ is given as follows:

$$\text{rtrans}(c)(\sigma, \phi)) = \{\sigma | \sigma(\sigma) \land i \in I\}$$

$$\cup \{\sigma(\sigma) \land j \in J\}.$$

The corresponding transfer function $\text{rtrans}(c)$ is given as follows:

$$\text{rtrans}(c)(\sigma, \phi)) = \{\sigma | \sigma(\sigma) \land i \in I\}$$

$$\cup \{\sigma(\sigma) \land j \in J\}.$$

The corresponding transfer function $\text{rtrans}(c)$ is given as follows:

$$\text{rtrans}(c)(\sigma, \phi)) = \{\sigma | \sigma(\sigma) \land i \in I\}$$

$$\cup \{\sigma(\sigma) \land j \in J\}.$$