Hybrid Top-down and Bottom-up Interprocedural Analysis

Xin Zhang\textsuperscript{1} Ravi Mangal\textsuperscript{1} Mayur Naik\textsuperscript{1} Hongseok Yang\textsuperscript{2}
\textsuperscript{1} Georgia Institute of Technology \textsuperscript{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 \textsc{Swift} that combines top-down and bottom-up analyses in a manner that gains their benefits without suffering their drawbacks. \textsc{Swift} is general in that it is parameterized by the top-down and bottom-up analyses it combines. We show an instantiation of \textsc{Swift} on a type-state analysis and evaluate it on a suite of 12 Java programs of size 60-250 KLOC each. \textsc{Swift} outperforms both conventional approaches, finishing on all the programs while both of those approaches fail on the larger programs.

Categories and Subject Descriptors D.2.4 [SOFTWARE ENGINEERING]: Software/Program Verification

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 \textsc{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 \textsc{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 \textsc{Swift} for Java and evaluate it on the type-state analysis using 12 benchmark programs of size 60-250 KLOC each. \textsc{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 \textsc{Swift}, a new interprocedural analysis approach that synergistically combines top-down and bottom-up approaches. We formalize \textsc{Swift} as a generic framework and illustrate it on a realistic type-state analysis.
2. Central to \textsc{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 \textsc{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 \textsc{Swift} on a type-state analysis of an example program shown in Figure 1. The program creates three file objects and calls procedure \texttt{f\_foo} on each of them to open and close the file. Each file \texttt{f} can be in state \texttt{opened}, \texttt{closed}, or \texttt{error} at any instant, and starts in state \texttt{closed}. A call \texttt{f\_open()} changes its state to \texttt{opened} if it is \texttt{closed}, and to \texttt{error} otherwise. Similarly, \texttt{f\_close()} changes its state to \texttt{closed} if it is \texttt{opened}, and to \texttt{error} otherwise.
**Figure 1:** Example illustrating top-down and bottom-up approaches to interprocedural type-state analysis.

The top-down approach starts with 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 `T1` through `T5` for procedure `foo`, which are shown in Figure 1. Summaries `T1`, `T2`, and `T5` mean that an incoming abstract state `h1, closed, {f}, θ` is transformed to itself by `foo`, whereas summaries `T3` and `T4` mean the same for an incoming abstract state `h1, closed, θ, {f}`. Summaries `T1`, `T2`, and `T1` share the property that the effect of `foo` on the incoming abstract state is a no-op when its argument `f` definitely points to the abstract object `h1` (i.e., `f` 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 `T3` and `T4` share an analogous property that holds when `f` definitely does not point to the abstract object `h1` (i.e., `f` 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 `h1` is different from `f`. However, these five 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 `T3` at call site `pc1`.

### 2.1 The Top-Down Approach

The top-down 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 `T1` through `T5` for procedure `foo`, which are shown in Figure 1. Summaries `T1`, `T2`, and `T5` mean that an incoming abstract state `h1, closed, {f}, θ` is transformed to itself by `foo`, whereas summaries `T3` and `T4` mean the same for an incoming abstract state `h1, closed, θ, {f}`. Summaries `T1`, `T2`, and `T1` share the property that the effect of `foo` on the incoming abstract state is a no-op when its argument `f` definitely points to the abstract object `h1` (i.e., `f` 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 `T3` and `T4` share an analogous property that holds when `f` definitely does not point to the abstract object `h1` (i.e., `f` 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 `h1` is different from `f`. However, these five 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 `T3` at call site `pc1`.

### 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 `B0` through `B5` 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 `B1` is applicable when `f` is in the incoming must set `n`. In this case, the incoming abstract state is simply returned. Summary `B2` 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 `h1, closed, {f}, θ`.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Top-Down Approach</th>
<th>Bottom-Up Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>main()</code></td>
<td><code>{ v1 = new File(); // h1 }</code></td>
<td><code>{ v1 = new File(); // h1 }</code></td>
</tr>
<tr>
<td>pc1: <code>foo(v1);</code></td>
<td>`{ h1, closed, {f}, θ } → ({ h1, closed, {f}, θ }</td>
<td>`{ h1, closed, {f}, θ } → ({ h1, closed, {f}, θ }</td>
</tr>
<tr>
<td>pc2: <code>foo(v2);</code></td>
<td>`{ h2, closed, {f}, θ } → ({ h2, closed, {f}, θ }</td>
<td>`{ h2, closed, {f}, θ } → ({ h2, closed, {f}, θ }</td>
</tr>
<tr>
<td>pc3: <code>foo(v3);</code></td>
<td>`{ h3, closed, {f}, θ } → ({ h3, closed, {f}, θ }</td>
<td>`{ h3, closed, {f}, θ } → ({ h3, closed, {f}, θ }</td>
</tr>
</tbody>
</table>

We use a type-state analysis by Fink et al. [8] 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 `must set`) and not aliased (called `must-not set`), respectively.

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

### 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 `θ` 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 `θ` dictates the maximum number of such cases to track and thereby limit excessive case splitting.

We illustrate SWIFT using `k = 2` and `θ = 2` on our example. SWIFT starts the top-down analysis of `main` in the usual order of program execution. Upon reaching program point `pc1`, with abstract state `{ h1, closed, {v1}, θ }`, 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 `{ h1, closed, {f}, θ }` and computes bottom-up summary `T1`. 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 \( (h_2, \text{closed}, \{f_v\}, \emptyset) \) and \( (h_1, \text{closed}, \{v_1\}, \{v_2\}) \), proceeds to re-analyze \( foo \) in the corresponding new abstract states

\[
(h_2, \text{closed}, \{f\}, \emptyset) \quad [A_2]
\]

\[
(h_1, \text{closed}, \emptyset, \{f\}) \quad [A_3]
\]

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 simplifies 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 abstract states of \( foo \). When it analyzes the first command \( f. \text{open}() \), it transforms the identity function above to four cases, namely, \( B_1 \), \( B_3 \), and \( B_4 \) shown in Figure 1, plus

\[
\lambda(h, t, a, n), \text{if } (f \in a) \text{ then } \{(h, \text{topos}(t), a, n)\} \quad [B_2']
\]

\( B_2' \) differs from \( B_2 \) in Figure 1 only in skipping the application of \( t.\text{close}() \), since the second command \( f. \text{close}() \) 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 \( B_1 \) and \( B_3 \), and prunes cases \( B_2 \) and \( B_4 \). It then proceeds to analyze command \( f. \text{close}() \) similarly to obtain the final bottom-up summaries of \( foo \) as

\[
\lambda(h, t, a, n), \text{if } (f \in n) \text{ then } \{(h, t, a, n)\} \quad [B_1]
\]

\[
\lambda(h, t, a, n), \text{if } (f \in a) \text{ then } \{(h, (t.\text{close} \circ \text{topos})(t), a, n)\} \quad [B_2]
\]

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 \( pc_2 \) in main, and reaches the call to \( foo \) at \( pc_3 \) with three abstract states:

\[
(h_3, \text{closed}, \emptyset, \{f\}) \quad [A_3]
\]

\[
(h_2, \text{closed}, \emptyset, \{f\}) \quad [A_3]
\]

\[
(h_3, \text{closed}, \{f\}, \emptyset) \quad [A_5]
\]

Since it had encountered \( A_3 \) at \( pc_2 \), 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 \( A_3 \), 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 \( foo \) has a single control-flow path which causes exactly one of bottom-up summaries \( B_1–B_4 \) to apply to any incoming abstract 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 \( foo \):

\[
\text{foo(File } f, \text{ File } g) \{\text{ if } (* \{f. \text{open}(); f. \text{close}(); } \text{ else } g. \text{open}(); \}
\]

Its bottom-up analysis yields summaries \( B_1–B_4 \) for the true branch, and four similar summaries for the false branch, one of which is

\[
\lambda(h, t, a, n), \text{if } (g \in a) \text{ then } \{(h, \text{topos}(t), a, n)\} \quad [B_3]
\]

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:

\[
\langle h, \text{closed}, \{f, g\}, \emptyset \rangle \quad [A_1]
\]

\[
\langle h, \text{closed}, \emptyset, \{f\} \rangle \quad [A_2]
\]

Both \( B_2 \) and \( B_5 \) apply to \( A_1 \), yielding result \( \langle h, \text{closed}, \{f, g\}, \emptyset, \langle h, \text{open}, \{g\}, \emptyset \rangle \rangle \) 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 \( B_1 \) was pruned, applying \( B_3 \) alone will yield incorrect result \( \langle h, \text{open}, \{g\}, \emptyset \rangle \rangle \).

Thus, in either scenario, 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 \( C \):

\[
C ::= c \mid C + C \mid C; C \mid C^+\]

It includes primitive commands, non-deterministic choice, sequential composition, and iteration. Section 3.5 adds procedure calls.

A top-down analysis \( \mathcal{A} = (\Sigma, \text{trans}) \) 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 \( \mathbb{P} = 2^\Sigma \) with the subset order. The abstract semantics of the analysis is standard:

\[
[C] : 2^\Sigma \rightarrow 2^\Sigma
\]

\[
[c](\Sigma) = \text{trans}(c)^\dagger(\Sigma)
\]

\[
[c_1 + c_2](\Sigma) = [c_1](\Sigma) \cup [c_2](\Sigma)
\]

\[
[c_1; c_2](\Sigma) = [c_2](\Sigma) + [c_1](\Sigma)
\]

\[
([C^+](\Sigma) = \text{fix} (\lambda \Sigma'. \Sigma \cup [C](\Sigma'))\).
\]

where notation \( f^1 \) denotes lifting of function \( f : D_1 \times \ldots \times D_n \rightarrow 2^\Sigma \) to sets of input arguments, as follows: \( f^1(x_1, \ldots, x_n) = \bigcup \{f(x_1, \ldots, x_n) \mid \forall i, x_i \in X_i\} \).

Example. We illustrate our formalism using the type-state analysis shown in Figure 2. This analysis computes a set of abstract states (also called abstract objects) at each program point to overapproximate 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 in \( a \).
Domains:
(method) \( m \in M \)
(variable) \( v \in V \)
(access path set) \( a \in A = 2^V \)
(type state) \( t \in T = \{ \text{init, error, ...} \} \)
(type-state function) \( \gamma \in \mathbb{N} \to T \)
(abstraction states) \( \sigma \in S = \mathbb{N} \times T \times A \)

Primitve Commands:
\( c ::= v = \text{new} \ h \mid v = w \mid v.m() \)

Transfer Functions:
\[
\begin{align*}
\text{trans}(v = \text{new} \ h)(t, a) &= \{(h, t, \text{a}, \{v\}, \text{h', init, } \{v\})\} \\
\text{trans}(v = w)(t, a) &= \{(h, t, a, \{v\})\} \\
\text{trans}(v.m)(t, a) &= \{\{(h, m(t), a)\}\}
\end{align*}
\]

Figure 2: Top-down type-state analysis.

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 \( c \) and those in \( a \) that survive the state change of \( c \). For instance, \( \text{trans}(v = w)(t, a) \) removes \( v \) from \( a \) when \( w \) is not in \( a \).

3.2 Bottom-Up Analysis

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

1. a domain of abstract relations \((\mathbb{R}, \text{id}^2, \gamma)\) where \( \mathbb{R} \) is a finite set with an element \( \text{id}^2 \) and \( \gamma \) is a function of type \( \mathbb{R} \to 2^{V \times V} \) such that \( \gamma(\text{id}^2) = \{(\sigma, \sigma) \mid \sigma \in S\} \)
2. transfer functions \( rtrans(c) : \mathbb{R} \to 2^R \)
3. an operator \( rcomp : \mathbb{R} \times \mathbb{R} \to 2^R \) 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 \( \text{id}^2 \) in \( \mathbb{R} \) that denotes the identity relation on \( S \).\(^1\) We denote the domain of a relation \( r \) by \( \text{dom}(r) = \{(\sigma, \sigma') \in \gamma(r)\} \). The input to \( rtrans(c) \) describes past state changes from the entry of the current procedure up to the primitive command \( c \), and the function extends this description with the state change of \( c \). The operator \( rcomp \) allows composing two abstract relations, and is used to compute the effects of procedure calls; namely, when a procedure with summary \( \{r_1, ..., r_n\} \) is called and an input relation to this call is \( r \), the result of analyzing the call is \( \bigcup_{r_i} rcomp(r, r_i) \).

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 \((\text{<t, a, } \phi)\), and this means a relation that takes an abstract state \( \sigma = (h, t, a) \)

\(^1\) Our bottom-up analysis uses \( \text{id}^2 \) as the initial abstract relation when analyzing procedures. See Section 3.5.
For all commands $c$, relations $r \in R$, and states $s, s' \in S$:

$$(3\sigma_0 : r_0 \in \text{trans}(c)(r) \land (\sigma', r') \in \gamma(r_0)) \iff (3\sigma_0 : (\sigma, s_0) \in \gamma(r) \land \sigma' \in \text{trans}(c)(\sigma_0))$$

For all $r_1, r_2 \in R$ and $s, s' \in S$:

$$(\sigma, s') \in \gamma^1(\text{rcomp}(r_1, r_2)) \iff 3\sigma_0 : (\sigma, s_0) \in \gamma(r_1) \land (\sigma, s_0) \in \gamma(r_2)$$

For all $r \in R$ and $s \in S$ and $\Sigma \in 2^S$:

$$\sigma \in \text{wp}(r, \Sigma) \iff (\forall \sigma' : (\sigma, s') \in \gamma(r) \Rightarrow \sigma' \in \Sigma)$$

Conditions required by our SWIFT framework:

- Checks whether this transformer results in an abstract state with $w$ in its must set. The three cases in the definition of $\text{trans}(v = w)$ correspond to the three answers to this question: always, never and sometimes. In the first two cases, $\text{trans}(v = w)$ 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 $v$.

- The remaining part is the composition operator $\text{rcomp}(r, r')$. One difficulty for composing relations $r$ and $r'$ symbolically is that the precondition $\phi$ of $r'$ is not a property of initial states of the composed relation, but that of intermediate states. Hence, we need to compute the weakest precondition of $\phi'$ with respect to the first relation $r$. Our $\text{rcomp}$ operator calls the routine $\text{wp}(r, \phi')$ to do this computation, and constructs a new precondition by conjoining the precondition $\phi$ of the first relation $r$ with the result of this call. Computing the other state-termination part of the result of $\text{rcomp}(r, r')$ is relatively easier, and follows from the semantics of $\gamma(r)$ and $\gamma(r')$.

### 3.3 Conditions of SWIFT Framework

SWIFT allows combining a top-down analysis $A$ and a bottom-up analysis $B$ as specified in the preceding subsections. Since it is a generic framework, however, SWIFT lets users decide the relative degrees of these two analyses in the resulting hybrid analysis, by means of thresholds $\delta$ and $\theta$. SWIFT has to guarantee the correctness and equivalence of the resulting analyses for all choices of these thresholds. For this purpose, SWIFT requires three conditions

- Condition $C1$ requires trans and trrans—the transfer functions of the top-down and bottom-up analyses for primitive commands—to be equally precise. Our top-down and bottom-up type-state analyses satisfy this condition. In Section 5, we discuss ways to avoid manually specifying both trans and trrans, by automatically synthesizing one from the other while satisfying this condition.

- Condition $C2$ requires the operator rcomp : $R \times R \rightarrow 2^S$ to accurately model the composition of relations $\gamma(r_1)$ and $\gamma(r_2)$. Note that $\gamma(r_i)$ is a relation over abstract states, not concrete states, which makes it easier to discharge the condition. Besides, the bottom-up analysis might define rcomp in a manner that already satisfies this condition. The rcomp operator for our type-state analysis in Figure 3 illustrates both of these aspects.

- Condition $C3$ requires an operator wp : $R \times 2^S \rightarrow 2^S$ to compute the weakest precondition of an abstract relation over a given set of abstract states. SWIFT uses this operator to adjust bottom-up summaries of called procedures. Those summaries involve preconditions on incoming abstract states to the callee, and need to be recast as preconditions to the caller. The wp operator satisfies this need. Designing wp is relatively simple, because it computes a weakest precondition on abstract relations in $R$, not on relations over concrete states. Besides, this operator might already be defined as part of the bottom-up analysis. Both of these observations hold for the wp operator in Figure 3 for our type-state analysis.

In summary, the conditions required by SWIFT are not onerous, and may even already hold for the analyses to be combined.

### 3.4 Pruning and Coincidence

We now proceed to augment our bottom-up analysis with a pruning operator and show that it coincides with the top-down analysis. We first define an operator $\text{excl} : 2^S \times 2^S \rightarrow 2^S$ as follows:

$$\text{excl}(R, \Sigma) = \{ r \in R \mid \text{dom}(r) \not\subseteq \Sigma \}$$

which removes abstract relations $r$ that become void if we ignore abstract states in $\Sigma$ from the domain of $r$.

We then define a pruning operator as a function $f : 2^S \times 2^S \rightarrow 2^S \times 2^S$ such that for all $R, R', \Sigma, \Sigma' \subseteq S$,

$$f(R, \Sigma) = (R', \Sigma') \iff (\Sigma \subseteq \Sigma' \land R' = \text{excl}(R, \Sigma'))$$

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., $\text{dom}(r) \not\subseteq \Sigma'$).

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$\theta : 2^S \rightarrow 2^S$ that chooses the top $\theta \geq 1$ abstract relations by their rank values as follows:

$$\text{best}_\theta(R) = \{ r \mid \text{rank}(r) \geq \theta \}$$

Finally, we define the pruning operator prune as follows:

$$\text{prune}(R, \Sigma) = \{ r \mid \text{rank}(r) \geq \theta \} \text{ in } \{ r \mid \Sigma' \subseteq \Sigma \cup \{ \text{dom}(r) \mid r \in R \} \} \text{ in } \{ r \mid \Sigma' \subseteq \Sigma \} \text{ in } \{ r \mid \Sigma' \subseteq \Sigma \}$$

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 $R_0$ 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:

$$\gamma^1(R) \cap (\Sigma' \cup \Sigma) = \gamma^1(R_0) \cap (\Sigma' \cup \Sigma)$$

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 $\text{excl}(\Sigma, \Sigma')$. 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 $foo$ 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 \( f.\ open() \) in the body of \( \text{foo} \). At this point, \( \textit{SWIFT} \) has data:

\[
M = \{(h_1, \text{closed}, \{ f \}), (h_2, \text{closed}, \{ f \}), (h_1, \text{closed}, \emptyset), \Sigma = \emptyset, R = \{(\textit{topen}, \text{V}, \emptyset, \text{have}(f)), (\text{Xerror}, \text{V}, \emptyset, \text{notHave}(f))\}.
\]

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

\[
\Sigma' = \{(h, t, a) \mid f \not\in \alpha\}, \quad R' = \{(\textit{topen}, \text{V}, \emptyset, \text{have}(f))\}.
\]

\( \textit{SWIFT} \) automatically augments the given bottom-up analysis with the prune operator to yield an analysis whose abstract domain is

\[
\mathcal{D}_v = \{(R, \Sigma) \in 2^V \times 2^V \mid \forall r \in R. \text{dom}(r) \not\subseteq \Sigma\}
\]

\((R, \Sigma) \subseteq (R', \Sigma') \iff \Sigma \subseteq \Sigma' \land \text{exc}(R, \Sigma') \subseteq R'\)

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 \( \Sigma' \subseteq \Sigma \) (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 \( \cup \) where \( \text{clean}(R, \Sigma) = (\text{exc}(R, \Sigma), \Sigma) \):

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

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

\[
\mathcal{C}'' : \mathcal{D}_v \rightarrow \mathcal{D}_v
\]

\[
\mathcal{C}''((R, \Sigma)) = (\text{prune} \circ \text{clean})(\text{rtrans}(\epsilon))(R, \Sigma)
\]

\[
\mathcal{C}_1', \mathcal{C}_2' : (R, \Sigma) \rightarrow \mathcal{C}''((R, \Sigma))
\]

\[
\mathcal{C}''((R, \Sigma)) = \text{fix}^{(R, \Sigma)} F
\]

where \( F(R', \Sigma') = \text{prune}((R', \Sigma') \cup [\mathcal{C}''((R, \Sigma))]') \).

\( \text{fix}^{(R, \Sigma)} F \) gives the stable element of the increasing sequence:

\[
(R', \Sigma'), F(R', \Sigma'), F^2(R', \Sigma'), F^3(R', \Sigma'), \ldots
\]

This sequence is increasing because \((R', \Sigma') \subseteq F(R', \Sigma'), \ldots \) and the sequence has a stable element because the domain \( \mathcal{D}_v \) 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 \( \textit{SWIFT} \) 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, provided the set of incoming abstract states does not include any abstract state that the bottom-up analysis ignores. The proof is given in Appendix A.

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

\[
([C]'')((\text{id}^2), \emptyset) = (R', \Sigma) \wedge (\Sigma \cap \Sigma' = \emptyset),
\]

we have that for every \( \sigma' \in R' \),

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

### 3.5 Extension for Procedures

To handle procedures that are potentially mutually recursive, we extend the formalism we have so far, as follows.

---

2 A stable element of a sequence \( \{x_n\}_{n \geq 0} \) is \( x_n \) such that \( x_n = x_{n+1} \).
procedure summaries computed by the bottom-up analysis. Note that
bu is a partial function. If bu(f) is undefined, it means that the
procedure f is not yet analyzed by the bottom-up analysis.

Algorithm 1: The SWIFT algorithm.

1: INPUTS: Initial abstract state σ₀ and program (G, Γ)
2: OUTPUTS: Analysis results td and bu
3: var workset, R₀, Σ₀, Σ, f, σ
4: td = λpcθ, bu = λf, undef, workset = \{(entry_main, σ₁, σ₂)\}
5: while (workset ≠ ∅) do
6: pop w from workset
7: if (command at w is not a procedure call) then
8: (td, workset) = run_td(G, w, td, workset)
9: else
10: let f be the procedure invoked at w
11: let σ be the current abstract state in w
12: if (∃w₀, Σ₀ : bu(f) = (R₀, Σ₀) ∧ σ ∉ Σ₀) then
13: Σ = \{σ' | (σ, σ') ∈ γ(G₀)\}
14: (td, workset) = update_td(Σ, w, td, workset)
15: else
16: (td, workset) = run_td(G, w, td, workset)
17: if (# of input abstract states to f in td > threshold k
and bu is undefined for f) then
18: bu = run_bal(Γ, θ, f, bu)
19: end if
20: end if
21: end if
22: end while

The algorithm repeatedly pops a w ∈ workset and processes it
until workset becomes empty. Handling w normally means the
update of workset and td according to the top-down analysis. We
express this normal case in the algorithm by

(td, workset) := run_td(G, w, td, workset)

where run_td is a standard tabulation-based computation [14] 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 σ of
w (i.e., the third component of w). If the check passes, it uses bu(f)
and computes the result Σ of analyzing f with σ, and updates
(td, workset) with Σ according to the top-down analysis (line 14).
If the check fails, the algorithm resorts to the top-down analysis,
and updates (td, 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 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
bu with these summaries. All these steps are expressed by a single
instruction bu := run_bal(Γ, θ, f, bu) in the algorithm (line 18),
which gets expanded to the following pseudo-code:

run_bal(Γ, θ, f, bu) =
let F = \{procedures reachable from f\} in
let bu' = [Γ][f]' with θ used during pruning in
λg. if (g ∈ F) then bu'(g) else bu(g)

where [Γ][f]' 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 run_bal. Both scenarios could arise in theory but oc-
curred rarely in our experiments. Assume a setting where the num-
ber of incoming abstract states to a procedure f has exceeded
the threshold k, and a procedure g is reachable from f. In the first sce-
nario, 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 issue by postponing executing run_bal(Γ, θ, f, bu) un-
til 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 ab-
stract 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 obliga-
tions 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:

\[
\text{trans}(c)(σ) = \{σ' | (σ, σ') ∈ \gamma(r\text{trans}(c)(\text{id}^2))\}
\]

The only obligations for using SWIFT on an existing bottom-up
analysis, then, are defining operators rcomp and wp 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

\[
\text{rtrans}(c)(r) = \{(σ₁, σ₃) | \exists σ₂ : (σ₁, σ₂) ∈ r ∧ \exists σ₃ ∈ \text{trans}(c)(σ₂)\}
\]

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. 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 bitvector
dataflow analyses as well as certain alias analyses (e.g., connection
analysis [9]). Our type-state analysis is not an instance of kill/gen
analysis, due to the transfer function of v.vn(), but its handling of
the must sets re-uses our kill/gen recipe for synthesizing bottom-up
analysis from top-down analysis.
### Empirical Evaluation

This section empirically evaluates SWIFT. Section 6.1 describes our experiment setup. Section 6.2 compares SWIFT to conventional top-down and bottom-up approaches, called TD and BU, respectively. Section 6.3 shows the effect of varying thresholds $k$ and $\theta$.

#### 6.1 Experimental Setup

We implemented SWIFT for building hybrid interprocedural analyses for Java bytecode using the Chord program analysis platform. The top-down part of the framework is based on the tabulation algorithm [14] 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 (upto two), 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-state 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 and the DaCapo Suite. 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 TD and SWIFT for three different benchmarks. The X-axis represents indices of methods sorted by the number of summaries. The Y-axis, which uses log scale, represents the number of summaries.

#### 6.3 Effect of Varying SWIFT Thresholds

**Effect of Varying $k$**. Table 3 shows the total running time and the number of top-down summaries generated for one of our largest
Table 2: Running time and total number of summaries computed by SWIFT and the baseline approaches TD and BU. Experiments that timed out either ran out of memory or failed to terminate in 24 hours.

<table>
<thead>
<tr>
<th>benchmarks</th>
<th>running time (m=min., s=sec.)</th>
<th># summaries (k=thousands)</th>
</tr>
</thead>
<tbody>
<tr>
<td>javasrc-p</td>
<td>4m44s</td>
<td>3.36s</td>
</tr>
<tr>
<td>hede</td>
<td>2m37s</td>
<td>3.36s</td>
</tr>
<tr>
<td>lusearch</td>
<td>3m53s</td>
<td>3.36s</td>
</tr>
<tr>
<td>kawa-c</td>
<td>2352s</td>
<td>3.36s</td>
</tr>
<tr>
<td>avorra</td>
<td>timeout</td>
<td>3.36s</td>
</tr>
<tr>
<td>rhino-a</td>
<td>timeout</td>
<td>3.36s</td>
</tr>
<tr>
<td>sablcc-c</td>
<td>timeout</td>
<td>3.36s</td>
</tr>
</tbody>
</table>

Table 3: Running time and total number of top-down summaries computed by SWIFT using different $k$ on avorra with $\theta=1$.

<table>
<thead>
<tr>
<th>$k$</th>
<th>running time (m=min., s=sec.)</th>
<th># summaries (in thousands)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2m44s</td>
<td>372</td>
</tr>
<tr>
<td>5</td>
<td>5m35s</td>
<td>91</td>
</tr>
<tr>
<td>10</td>
<td>4m59s</td>
<td>68</td>
</tr>
<tr>
<td>50</td>
<td>2m37s</td>
<td>280</td>
</tr>
<tr>
<td>100</td>
<td>4m95s</td>
<td>543</td>
</tr>
<tr>
<td>200</td>
<td>2m7s</td>
<td>1,150</td>
</tr>
<tr>
<td>500</td>
<td>4m49s</td>
<td>2,663</td>
</tr>
</tbody>
</table>

Table 4: Running time and total number of top-down summaries computed by SWIFT using different $\theta$ on avorra with $k=5$.

<table>
<thead>
<tr>
<th>$\theta$</th>
<th>running time (m=min., s=sec.)</th>
<th># summaries (in thousands)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5m18s</td>
<td>3.5</td>
</tr>
<tr>
<td>2</td>
<td>5m18s</td>
<td>3.5</td>
</tr>
<tr>
<td>3</td>
<td>5m18s</td>
<td>3.5</td>
</tr>
</tbody>
</table>

7. Related Work
Sharir and Pnueli [19] 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. [14] identify a representation for the class of IFDS dataflow analysis problems that takes quadratic space and can be computed in cubic time. Sagiv et al. [17] generalize the IFDS problem into IDE problem, which takes quadratic space and can be computed in cubic time, if there exists efficient representations for the transfer functions.

Our work differs from the above works as follows. First, even when there is a compact representation of procedure summaries with polynomial guarantee, our approach aims at empirically outperforming this guarantee. Second, we do not require a compact representation of transfer functions or 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 we provide a recipe for it, via the pruning operator and the interaction between the top-down and bottom-up versions.

Jeannet et al. [12] propose an analysis to generate relational summaries for shape properties in three-valued logic. Yorsh et al. [22] 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 [6, 11], 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 [10, 13, 18, 20], must-alias information [4, 7] and shape properties [3, 10], where the analyses typically use symbolic abstract domains.

In contrast, top-down analysis [5, 14, 19] 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. Rinetzkly et al. [15, 16] 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. [23] generalize top-down summaries by replacing explicit summaries with symbolic representations, thereby increasing reuse without losing precision. Ball et al. [2] 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. The shape analysis of Calcagno et al. [3] assumes that a dereferenced heap cell at a program point pe 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 pe. 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 [21] likewise assume non-aliasing between procedure arguments. These assumptions are not robust since they conjecture 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—indeed procedures can be analyzed in parallel—and recent work also addresses parallelizing top-down analyses [1]. 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 [1]) 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.

Acknowledgements We thank the referees for useful feedback. This work was supported by DARPA under agreement #FA8750-12-2-0020, NSF award #1253867, and EPSRC. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright thereon.

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 
$$([C]^{\uparrow}(\{id^2\}, 0) = (R', \Sigma') \land (\Sigma \cap \Sigma' = \emptyset),$$
we have that for every $\sigma'$ in $\Sigma$,
$$\sigma' \in [C]^{\uparrow}(\Sigma) \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma(R').$$

Our proof strategy is to define an intermediate abstract semantics working on $2^R$, 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 $2^R$ with the subset order, and has the following abstract semantics:

$$[C]^{\uparrow} : 2^R \rightarrow 2^R$$

$$[c]^{\uparrow}(R) = rtrans(c)^{\uparrow}(R)$$

$$[C_1 + C_2]^{\uparrow}(R) = [C_1]^{\uparrow}(R) \cup [C_2]^{\uparrow}(R)$$

$$[C_1; C_2]^{\uparrow}(R) = [C_2]^{\uparrow}([C_1]^{\uparrow}(R))$$

$$[C]^{\uparrow}_0(R) = \fix (\lambda R. \Sigma \cup [C]^{\uparrow}_0(R')).$$

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 $\fix$.

**Theorem A.1.** For all commands $C$, sets $\Sigma$ of abstract states in $S$ and abstract states $\sigma'$,
$$\sigma' \in [C]^{\uparrow}(\Sigma) \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma([C]^{\uparrow}(\{id^2\})).$$

**Proof.** For all $R$ and $\Sigma$, we define
$$\text{apply}(R, \Sigma) = \{\sigma' | \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma(R')\}.$$ 

The theorem can be paraphrased to the following equation:

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

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 $R$,
$$[C]^{\uparrow}(R, \Sigma) = \text{apply}([C]^{\uparrow}_0(R), \Sigma).$$

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 $R$ and $\Sigma$.

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

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

$$= [C_1]^{\uparrow}(\text{apply}([C_1]^{\uparrow}(R), \Sigma))$$

$$= \text{apply}([C_1]^{\uparrow}(\text{apply}([C_1]^{\uparrow}(R), \Sigma)))$$

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

The first and last equalities just use the definitions of $[C_1; C_2]^{\uparrow}$ and $[C_1]^{\uparrow}(\{id^2\})$. 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:

$$[C_1 + C_2]^{\uparrow}(\text{apply}(R, \Sigma))$$

$$= [C_1]^{\uparrow}(\text{apply}(R, \Sigma)) \cup [C_2]^{\uparrow}(\text{apply}(R, \Sigma))$$

$$= \text{apply}([C_1]^{\uparrow}(R), \Sigma) \cup \text{apply}([C_2]^{\uparrow}(R), \Sigma)$$

$$= \text{apply}([C_1]^{\uparrow}(R) \cup [C_2]^{\uparrow}(R), \Sigma)$$

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

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 $C = C_1^*$. Let $F$ and $G$ be functions defined by:

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

$$G = \lambda R'. R \cup [C_1]^{\uparrow}(R').$$

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

$$([\Sigma', R']) \in R \iff \text{apply}(R', \Sigma) = \Sigma'.$$

Then,

$$[[C]^{\uparrow}_0(\text{apply}(R, \Sigma))] = \fix F \land \text{apply}((\Sigma), [C]^{\uparrow}_0(R')).$$

It is easy to show that $(\emptyset, \emptyset) \in R$, and for all families $((\Sigma_i), \Sigma_i) \in \I$,

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

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

$$(\Sigma', R') \in R \Rightarrow (F(\Sigma'), G(R')) \in R, \quad (1)$$

because this implies

$$(\fix F, \fix G) = \left(\bigcup_{n \in \N} F^n(\emptyset), \bigcup_{n \in \N} G^n(\emptyset)\right) \in R$$

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

$$(\Sigma', R') \in R \Rightarrow \left(\left([C_1]^{\uparrow}_0(\Sigma'), [C_1]^{\uparrow}_0(R')\right) \in R \land \left(\text{apply}(R, \Sigma), R \cup [C_1]^{\uparrow}_0(R') \in R \land \left(\text{apply}(R, \Sigma), R \cup [C_1]^{\uparrow}_0(R') \in R \Rightarrow (F(\Sigma'), G(R')) \in R.\right)\right)\right)$$

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

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

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

$$\text{excl}(R, \Sigma) \subseteq R.$$
Since both $\text{rtrans}(c)^\dag (-)$ 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 $r \in \text{excl}(\text{rtrans}(c)^\dag(R), \Sigma)$. Then,

$$(\text{dom}(r) \not\subseteq \Sigma) \land (\exists r' \in R : r \in \text{rtrans}(c)(r')).$$ (2)

Let $r' \in R$ be the witness in the second conjunct. We will show

$$\text{dom}(r') \not\subseteq \Sigma.$$ (3)

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

$$(\sigma, \sigma') \in \gamma(r) \land \sigma \not\in \Sigma.$$ But $r \in \text{rtrans}(c)(r')$, so the requirement on $\text{rtrans}(c)$ gives

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

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

**Theorem A.3.** For every $R$, $R', \Sigma, \Sigma' \subseteq S$, if

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

we have that $R' = \text{excl}([C]^o(R), \Sigma')$.

**Proof.** We prove the theorem by induction on the structure of $C$. Pick $R, R', \Sigma, \Sigma'$ such that

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

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

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

We then prove the case where $\Sigma \subseteq \Sigma'$.

The first, third and sixth implications are just the unpacking and packing of the definitions of $[C]^o$ and $[C]^o$. 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

$$(R_i', \Sigma_i') = ([C_i]^o \circ \text{clean})(R_i, \Sigma).$$

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:

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

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

$$\Rightarrow (R', \Sigma') = \text{prune}(\text{excl}(R_1' \cup R_2', \Sigma_1' \cup \Sigma_2', \Sigma_1' \cup \Sigma_2'))$$

$$\Rightarrow R' = \text{excl}(\text{excl}(R_1' \cup R_2', \Sigma_1' \cup \Sigma_2', \Sigma_1' \cup \Sigma_2'))$$

$$\Rightarrow R' = \text{excl}(R_1' \cup R_2', \Sigma_1' \cup \Sigma_2')$$

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

The first and second implications are the unrolling of the definitions of $[C_1 + C_2]^o$ 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 $[C_1 + C_2]^o$. 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 $([C_i]^o \circ \text{clean})(R, \Sigma)$. We prove the case as follows:

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

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

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

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

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

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

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

The first, second, fourth and sixth implications follow from the definitions of $[C_1 C_2]^o$, $(R_i', \Sigma_i')$, clean and $[C_1 C_2]^o$. The third and fifth implications use induction hypothesis on $C_1$ and $C_2$, respectively.

The remaining case is that $C = \Sigma^o$. Let

$$F(R_0, \Sigma_0) = \text{prune}(R_0, \Sigma_0) \cup [C]^o(R_0, \Sigma_0),$$

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

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

$$(R_n, \Sigma_n) = F^n(\text{clean}(R, \Sigma)),$$  
$$R_n = G^n(R).$$

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

$$[C]^o(\text{clean}(R, \Sigma)) = (R_m, \Sigma_m),$$  
$$[C]^o(R) = R_m.$$  

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

$$R_n = \text{excl}(R_n, \Sigma_n).$$ (5)

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

$$R_n, \Sigma_n) = ([C]^o(R_n, \Sigma_n)).$$

We prove the inductive case as follows:

$$(R_{n+1}, \Sigma_{n+1}) = \text{prune}(R_n, \Sigma_n \cup [C]^o(R_n, \Sigma_n))$$

$$\Rightarrow (R_{n+1}, \Sigma_{n+1}) = \text{prune}(R_n, \Sigma_n \cup R_n, \Sigma_n)$$

$$\Rightarrow (R_{n+1}, \Sigma_{n+1}) = \text{prune}(R_n, \Sigma_n \cup R_n, \Sigma_n)$$

$$\Rightarrow (R_{n+1}, \Sigma_{n+1}) = \text{prune}(\text{excl}(R_n, R_n, \Sigma_n) \cup \Sigma_n)$$

$$\Rightarrow R_{n+1} = \text{excl}(R_n, R_n, \Sigma_n)$$

$$\Rightarrow R_{n+1} = \text{excl}(R_n, R_n, \Sigma_n)$$

$$\Rightarrow R_{n+1} = \text{excl}(R_n, R_n, \Sigma_n)$$

$$\Rightarrow R_{n+1} = \text{excl}(R_n, R_n, \Sigma_n)$$

$$\Rightarrow R_{n+1} = \text{excl}(R_n, R_n, \Sigma_n)$$

$$\Rightarrow R_{n+1} = \text{excl}(R_n, R_n, \Sigma_n)$$

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 $\Sigma_n \subseteq \Sigma_{n+1}$. 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 excl(-, Σ') over union, and the ninth is the packing of the definition of R''
. The last implication holds because
\( R'' = \text{excl}(R'', \Sigma') \subseteq R'' \subseteq R'' \).

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
\( (C''(\{\{d'\}\}), \emptyset) = (R', \Sigma') \land (\Sigma \land \Sigma' = \emptyset) \).

We should prove that for every \( \sigma' \) in \( \Sigma \),
\( \sigma' \in \Sigma''(\Sigma) \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma(R') \).

We disprove this proof follows as:
\( \sigma' \in \Sigma''(\Sigma) \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma(\Sigma''(\{d'\})) \)
\( \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma(\text{excl}(\Sigma''(\{d'\})) \land \Sigma) \)
\( \iff \exists \sigma \in \Sigma : (\sigma, \sigma') \in \gamma(R') \).

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 \((\Delta, \perp, T, \lor, \land)\) with two operations:
\( \land \), \( \lor : \Delta \times \Delta \rightarrow \Delta \).

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

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

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

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

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

DEFN B.1. A function \( f \) from \( S \) to \( 2^S \) is simple
\( f(\sigma) = \{\sigma_i \mid \phi_i(\sigma) \land i \in I\} \cup \{\sigma \land \delta_j \mid \phi_j(\sigma) \land j \in J\} \).

Here, \( I, J \) are fixed finite sets of indices, \( \sigma_i \) is an abstract state, \( \delta_j \) is an element from \( \Delta \), and \( \phi_i, \phi_j \) are predicates in \( \Phi \).

DEFN B.2. The set \( \Phi \) of predicates is \textit{wp-closed}
\( \forall \delta, \delta' \in \Delta : \forall \phi \in \Phi : (\lambda \sigma. \phi((\sigma \land \delta) \lor (\sigma \land \delta'))) \in \Phi \).

DEFN B.3. The analysis \((S, \text{trans})\) is simple when \text{trans}(c) 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 \( C = C_1 \lor C_2 \). Let \( f = \lambda \sigma. [C_1][(\sigma)] \) and \( g = \lambda \sigma. [C_2][(\sigma)] \). By induction hypothesis, there exist
\( I, J, K, L, \delta_1, \delta_1', \delta_2, \delta_2', \sigma_1, \sigma_1', \phi_1, \phi_1', \psi_1, \psi_1', \)
such that
\( f(\sigma) = \{\sigma_i \mid \phi_i(\sigma) \land i \in I\} \cup \{\sigma \land \delta_j \mid \phi_j(\sigma) \land j \in J\} \)
\( g(\sigma) = \{\sigma_k' \mid \phi_k(\sigma) \land k \in K\} \cup \{\sigma \land \epsilon_l \mid \phi_l(\sigma) \land l \in L\} \).

Then, \([C_1 \lor C_2][(\sigma)] = U(\{g(\sigma') \mid \sigma' \in f(\sigma)\}) \).

Since \([C_1 \lor C_2] \) preserves set union, it can be expressed as follows:
\( [C_1 \lor C_2][(\sigma)] = \)
\( \{\sigma_k' \mid \phi_k(\sigma) \land (k, \epsilon) \in I \times K\} \cup \{\sigma \land \epsilon_l \mid \phi_l(\sigma) \land (\epsilon, \delta) \in I \times L\} \cup \{\sigma \land \delta_j \mid \phi_j(\sigma) \land (\delta, \epsilon) \in J \}
\( \lambda \sigma. [C_1][(\sigma)] \cup \{\phi_i(\sigma) \land (i, \epsilon) \in I \} \cup \{\phi_j(\sigma) \land (j, \delta) \in J\} \cup \lambda \sigma. [C_2][(\sigma)] \).

Since \( \Phi \) is \textit{wp-closed} and
\( ((\sigma \land \delta) \lor (\sigma \land \delta')) \lor (\sigma \land (\delta \lor \delta')) \)
\( ((\sigma \land \delta) \lor (\sigma \land \delta')) \lor (\sigma \land (\delta \lor \delta')) \)
the above expression \([C_1 \lor C_2][(\sigma)] \) shows that \( \lambda \sigma. [C_1 \lor C_2][(\sigma)] \) is simple.

We move on to the case that \( C = C_1 \lor C_2 \). Let \( f = \lambda \sigma. [C_1][(\sigma)] \) and \( g = \lambda \sigma. [C_2][(\sigma)] \). By induction hypothesis, there are
\( I, J, K, L, \delta_1, \delta_1', \delta_2, \delta_2', \sigma_1, \sigma_1', \phi_1, \phi_1', \psi_1, \psi_1', \)
such that
\( f(\sigma) = \{\sigma_i \mid \phi_i(\sigma) \land i \in I\} \cup \{\sigma \land \delta_j \mid \phi_j(\sigma) \land j \in J\} \)
\( g(\sigma) = \{\sigma_k' \mid \phi_k(\sigma) \land k \in K\} \cup \{\sigma \land \epsilon_l \mid \phi_l(\sigma) \land l \in L\} \).

Using the entities in the above expressions, we represent \([C_1 \lor C_2] \) as follows:
\( [C_1 \lor C_2][(\sigma)] = \)
\( \{\sigma_i \mid \phi_i(\sigma) \land i \in I\} \cup \{\sigma_k' \mid \phi_k(\sigma) \land k \in K\} \cup \{\sigma \land \epsilon_l \mid \phi_l(\sigma) \land (\epsilon, \delta) \in J\}
\( \lambda \sigma. [C_1][(\sigma)] \cup \{\phi_i(\sigma) \land (i, \epsilon) \in I \} \cup \{\phi_j(\sigma) \land (j, \delta) \in J\} \cup \lambda \sigma. [C_2][(\sigma)] \).

Hence, \( \lambda \sigma. [C_1 \lor C_2][(\sigma)] \) is simple.

The remaining case is that \( C = C_1 \lor C_2 \). Define a function \( F \):
\( F(T) = \lambda \sigma. \Sigma \lor \sigma \lor \{[C_1 \lor C_2][(\sigma)]\} \).


where $T$ is a monotone map on $2^S$ preserving the set union and such $T$'s are ordered pointwise. It is well-known that

$$[[C]] = \text{fix} F.$$  

Call a function $T : 2^S \to 2^S$ simple if $T$ preserves set union and $\lambda \sigma. T(\{\sigma\})$ is simple. Then, the reasoning by similar to the one for the sequencing 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, it 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 $(S, \text{trans}, \Delta, \otimes, \oplus, A)$. We build a corresponding bottom-up analysis $(R, \text{rtrans}, \text{id}^\ast, \text{apply})$ 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:

$$\gamma : T \to (S \to S) \quad \gamma(\delta, \delta')(\sigma) = (\sigma \otimes \delta) \oplus \delta'.$$

2. Using $T$, we construct the domain $R$ of abstract relations

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

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

$$\text{apply}((\sigma_0, \phi), \sigma) = \{\sigma_0 \mid \phi(\sigma)\},$$

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

3. We use the following element in $R$ as the abstract identity relation:

$$\text{id}^\ast = ((T, \bot), \text{true}).$$

This meets the requirement for $\text{id}^\ast$:

$$\text{apply}(\text{id}^\ast, \sigma) = \{(\sigma \otimes T) \oplus \bot \mid \phi_{\text{true}}(\sigma)\} = \{\sigma\}.$$

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

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

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

$$\text{trans}(c)(\sigma) = \{\sigma_i \mid \phi_i(\sigma) \land i \in I\}$$

$$\cup \{(\sigma \otimes \delta_j) \oplus \delta'_j \mid \phi_j'(\sigma) \land j \in J\}.$$  

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

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

$$\cup \{((\sigma \otimes \delta_j) \oplus \delta'_j, \phi_j'(\sigma) \land j \in J\}.$$  

$$\text{rtrans}(c)((\delta, \delta'), \phi) =$$

$$\{\sigma_i, \psi \land \psi \mid i \in I \land \lambda \sigma. \psi_i((\sigma \otimes \delta) \oplus \delta')\}$$

$$\cup \{((\delta \sqcap (\delta' \sqcap \delta) \sqcup \delta'_j), \psi \land \psi \mid j \in J \land \lambda \sigma. \psi_j'((\sigma \otimes \delta) \oplus \delta')\}. $$

Lemma B.5. For all primitive commands $c$, sets of abstract states $\Sigma$, and sets of abstract relations $R$,

$$\text{trans}(c)^\dagger(\text{apply}^\dagger(R, \Sigma)) = \text{apply}^\dagger(\text{rtrans}(c)^\dagger(R, \Sigma)).$$

**Proof.** Pick a primitive command $c$. It suffices to prove that for all abstract states $\sigma$ and abstract relations $r$.

$$\text{trans}(c)^\dagger(\text{apply}(r, \sigma)) = \text{apply}^\dagger(\text{rtrans}(c)(r, \{\sigma\})).$$

Assume that the transfer function for $c$ have the following form:

$$\text{trans}(c)(\sigma) = \{\sigma_i, \mid \phi_i(\sigma) \land i \in I\}$$

$$\cup \{(\sigma \otimes \delta_j) \oplus \delta'_j, \phi_j'(\sigma) \land j \in J\}.$$  

Then, by the definition of $\text{rtrans}(c)$,

$$\text{rtrans}(c)((\delta, \delta'), \phi) =$$

$$\{\{\sigma, \lambda \sigma. \phi_i((\sigma \otimes \delta) \oplus \delta') \land \phi(\sigma) \mid i \in I\}$$

$$\cup \{((\delta \sqcap \delta_j, \delta' \sqcap \delta_j \sqcup \delta'_j), \lambda \sigma. \phi_j'((\sigma \otimes \delta) \oplus \delta_j') \land \phi(\sigma) \mid j \in J\}.$$  

First, we consider the case that $r$ is in (6) is a pair $(\sigma', \sigma') \in S \times A$, and prove the lemma as follows:

$$\text{trans}(c)^\dagger(\text{apply}(\sigma', \phi')) =$$

$$\{\sigma_i, \mid \phi_i(\sigma') \land i \in I\}$$

$$\cup \{((\sigma \otimes \delta_j) \oplus \delta'_j, \phi_j'(\sigma') \land j \in J\}.$$  

The first and the third equalities hold because of the definition of apply. The second equality is just the unrolling of the definition of $\text{trans}(c)$. The last equality uses both the preservation of union by apply$^\dagger$ and the definition of $\text{rtrans}(c)$.

Next, we handle the other case that $r$ is $(\delta, \delta')$:

$$\text{trans}(c)^\dagger(\text{apply}(\delta, \delta'), \phi') =$$

$$\{\sigma_i, \mid \phi_i(\delta) \land i \in I\}$$

$$\cup \{((\sigma \otimes \delta_j) \oplus \delta'_j, \phi_j'(\delta) \land j \in J\}.$$  

The first and fourth equalities hold because of the definition of apply, and the second equality unfolds the definition of $\text{trans}(c)^\dagger$. The third equality uses the properties assumed for the $\otimes$ and $\oplus$ operators. The fifth equality holds because of the preservation of the set union by apply$^\dagger$ and the definition of $\text{rtrans}(c)$. □