Failure-Directed Program Trimming

Kostas Ferles
The University of Texas at Austin, USA
kferles@cs.utexas.edu

Maria Christakis
University of Kent, UK
M.Christakis@kent.ac.uk

Valentin Wüstholz
The University of Texas at Austin, USA
valentin@cs.utexas.edu

Isil Dillig
The University of Texas at Austin, USA
isil@cs.utexas.edu

ABSTRACT
This paper describes a new program simplification technique called program trimming that aims to improve the scalability and precision of safety checking tools. Given a program \( P \), program trimming generates a new program \( P' \) such that \( P \) and \( P' \) are equi-safe (i.e., \( P' \) has a bug if and only if \( P \) has a bug), but \( P' \) has fewer execution paths than \( P \). Since many program analyzers are sensitive to the number of execution paths, program trimming has the potential to improve the effectiveness of safety checking tools.

In addition to introducing the concept of program trimming, this paper also presents a lightweight static analysis that can be used as a pre-processing step to remove program paths while retaining equi-safety. We have implemented the proposed technique in a tool called TRIMMER and evaluate it in the context of two program analysis techniques, namely abstract interpretation and dynamic symbolic execution. Our experiments show that program trimming significantly improves the effectiveness of both techniques.

CCS CONCEPTS
• Software and its engineering → Formal methods;

KEYWORDS
Condition inference, abstract interpretation, dynamic symbolic execution

ACM Reference format:
https://doi.org/10.1145/3106237.3106249

1 INTRODUCTION
Due to its potential to dramatically simplify programs with respect to a certain criterion (e.g., the value of a program variable at a given location), program slicing [86] has been the focus of decades of research in the program analysis community [85]. In addition to being useful for program understanding, slicing also has the potential to improve the scalability of bug-finding and verification tools by removing irrelevant code snippets with respect to some property of interest. Yet, despite this potential, relatively few bug-finding and verification tools use slicing as a pre-processing step.

In this paper, we argue that existing notions of a “program slice” do not adequately capture the kinds of program simplification that are beneficial to safety checking tools. Instead, we propose a new semantic program simplification technique called program trimming, which removes program paths that are irrelevant to the safety property of interest. Given a program \( P \), program trimming generates a simplified program \( P' \) such that \( P' \) violates a safety property if and only if the original program \( P \) does (i.e., \( P \) and \( P' \) are equi-safe). However, \( P' \) has the advantage of containing fewer execution paths than \( P \). Since the scalability and precision of many program analyzers depend on the number of program paths, program trimming can have a positive impact on many kinds of program analyses, particularly those that are not property directed.

To illustrate the difference between the standard notion of program slicing and our proposed notion of program trimming, consider the following very simple program, where \( \star \) indicates a non-deterministic value (e.g., user input):

\[
\begin{align*}
  x := \star; & \quad y := \star; \\
  \text{if } (y > 0) \{ & \quad \text{while } (x < 10) \{ x := x + y; \}; \} \\
  \text{else} & \quad \{ x := x - 1; \}; \\
  \text{assert} & \quad x > 0; \\
\end{align*}
\]

Suppose that our goal is to prove the assertion; so, we are interested in the value of \( x \) at line 4. Now, every single statement in this program is relevant to determining the value of \( x \); hence, there is nothing that can be removed using program slicing. However, observe that the then branch of the if statement is actually irrelevant to the assertion. Since this part of the program can never result in a program state where the value of \( x \) is less than 10, lines 2 and 3 can be simplified without affecting whether or not the assertion can fail. Hence, for the purposes of safety checking, the above program is equivalent to the following much simpler trimmed program \( P' \):

\[
\begin{align*}
  x := \star; & \quad y := \star; \\
  \text{assume} & \quad y <= 0; \\
  x := & \quad x - 1; \\
  \text{assert} & \quad x > 0; \\
\end{align*}
\]

Observe that \( P' \) contains far fewer paths compared to the original program \( P \). In fact, while \( P \) contains infinitely many execution paths, the trimmed program \( P' \) contains only two, one through the successful and one through the failing branch of the assertion.
Consequently, program analyzers that eagerly explore all program paths, such as bounded model checkers [14, 28] and symbolic execution engines [66], can greatly benefit from program trimming in terms of scalability. Furthermore, since many static analyzers (e.g., abstract interpreters [31]) typically lose precision at join points of the control flow graph, program trimming can improve their precision by removing paths that are irrelevant to a safety property.

Motivated by these observations, this paper introduces the notion of failure-directed program trimming and presents a lightweight algorithm to remove execution paths in a way that guarantees equi-safety. The key idea underlying our approach is to statically infer safety conditions, which are sufficient conditions for correctness and can be computed in a lightweight way. Our technique then negates these safety conditions to obtain trimming conditions, which are necessary conditions for the program to fail. The trimming conditions are used to instrument the program with assumptions such that program paths that violate an assumption are pruned.

Program trimming is meant as a lightweight but effective pre-processing step for program analyzers that check safety. We have implemented our proposed trimming algorithm in a tool called TRIMMER and used it to pre-process hundreds of programs, most of which are taken from the software verification competition (SV-COMP) [11]. We have also evaluated the impact of trimming in the context of two widely-used program analysis techniques, namely abstract interpretation [31] and dynamic symbolic execution [18, 51]. Our experiments with CRAB [49, 50] (an abstract interpreter) show that program trimming can considerably improve the precision of static analyzers. Furthermore, our experiments with KLEE [17] (a dynamic symbolic execution tool) show that program trimming allows the dynamic symbolic execution engine to find more bugs and verify more programs within a given resource limit.

Figure 1: Running example illustrating program trimming.

To summarize, this paper makes the following key contributions:

- We introduce the notion of program trimming as a new kind of program simplification technique.
- We propose an effective and lightweight inference engine for computing safety conditions.
- We describe a modular technique for instrumenting the program with trimming conditions.
- We demonstrate empirically that program trimming has a significant positive impact on the effectiveness of program analyzers.

2 GUIDED TOUR

The running example, shown in Figure 1, is written in C extended with assume and assert statements. Note that the example is intentionally quite artificial to illustrate the main ideas behind our technique. Procedure main assigns a non-deterministic integer value to variable m and computes its factorial using the recursive fact procedure. The (light and dark) gray boxes are discussed below and should be ignored for now. We examine two variations of this example: one for dynamic symbolic execution (DSE) engines and another for abstract interpreters (AI).

Motivation #1: scalability. First, let us ignore the assertion on line 7 and only consider the one on line 15. Clearly, this assertion cannot fail unless m is equal to 123. Observe that procedure main contains infinitely many execution paths because the number of recursive calls to fact can become very expensive (especially in the presence of loops or recursion), making such an approach unsuitable as a pre-processing step for program analyzers that already check safety. Instead, we use lightweight techniques to infer safety conditions that describe a subset of the safe executions in the program. That is, the safety conditions inferred by our approach can be stronger than necessary, but they are still useful for ruling out many program paths that “obviously” cannot violate a safety property.

In contrast to a safety condition, a trimming condition at a given program point reflects a necessary condition for the rest of the program execution to fail. Since a necessary condition for a property Q can be obtained using the negation of a sufficient condition for Q, we can compute a valid trimming condition for a program point π as the negation of the safety condition at π. Thus, our approach trims the program by instrumenting it with assumptions of the form π(ϕ), where ϕ is the negation of the safety condition for that program point. Since condition π(ϕ) is, by construction, necessary for the program to fail, the trimmed program preserves the safety of the original program. Moreover, since execution terminates as soon as we encounter an assumption violation, instrumenting the program with trimming conditions prunes program paths in a semantic way.

Program trimming on this example. Revisiting our running example from Figure 1, the safety condition right after line 14 is

```c
m != 123 || f == 0; // DSE
```

Since procedure fact called at line 14 neither
contains any assertions nor modifies the value of \( n \), a valid safety condition right before line 14 is \( n \neq 1 = 123 \). Indeed, in executions that reach line 14 and satisfy this safety condition, the assertion does not fail. We can now obtain a sound trimming condition by negating the safety condition. This allows us to instrument the program with the \( \text{assume} \) statement shown in the dark gray box of line 13. Any execution that does not satisfy this condition is correct and is effectively removed by the \( \text{assume} \) statement in a way that preserves safety. As a result, a dynamic symbolic execution tool running on the instrumented program will only explore the single execution path containing the bug and will not waste any resources on provably correct paths. Observe that a bounded model checker would similarly benefit from this kind of instrumentation.

**Motivation #2: precision.** To see how our approach might improve the precision of program analysis, let us ignore the assertion on line 15 and only consider the one on line 7. Since \( n = \emptyset \) implies \( r = 1 \) on line 7, this assertion can clearly never fail. However, an abstract interpreter, like Crab, using intervals [31] cannot prove this assertion due to the inherent imprecision of the underlying abstract domain. In particular, the abstract interpreter knows that \( n \) is non-negative at the point of the assertion but has no information about \( r \) (i.e., its abstract state is \( \top \)). Hence, it does not have sufficient information to discharge the assertion at line 7.

Suppose, however, that our technique can infer the safety condition \( n = \emptyset \) on line 3. Using this condition, we can now instrument this line with the trimming condition \( n \neq \emptyset \), which corresponds to the assumption in the light gray box. If we run the same abstract interpreter on the instrumented program, it now knows that \( n \) is strictly greater than \( \emptyset \) and can therefore prove the assertion even though it is using the same interval abstract domain. Hence, as this example illustrates, program trimming can also be useful for improving the precision of static analyzers in verification tasks.

### 3 PROGRAM TRIMMING

In this section, we formally present the key insight behind failure-directed program trimming using a simple imperative language in the style of IMP [87], augmented with \( \text{assert} \) and \( \text{assume} \) statements. This lays the foundation for understanding the safety condition inference, which is described in the next section and is defined for a more expressive language. Here, we present the semantics of the IMP language using big-step operational semantics, specifically using judgments of the form \( \langle \sigma, s \rangle \Downarrow \sigma' \) where:

- \( s \) is a program statement,
- \( \sigma, \sigma' \) are valuations mapping program variables to values,
- \( \varphi \in \{ \bot, \top, \checkmark \} \) indicates whether an assertion violation occurred (\( \bot \)), an assumption was violated (\( \varnothing \)), or neither assertion nor assumption violations were encountered (denoted \( \checkmark \)).

We assume that the program terminates as soon as an assertion or assumption violation is encountered. We also ignore non-determinism to simplify the presentation.

**Definition 3.1. (Failing execution)** We say that an execution of \( s \) under \( \sigma \) is failing iff \( \langle s, \sigma \rangle \Downarrow \sigma' \), and successful otherwise.

In other words, a failing execution exhibits an assertion violation. Executions with \( \text{assumption} \) violations also terminate immediately but are not considered failing.

**Definition 3.2. (Equi-safety)** We say that two programs \( s, s' \) are equi-safe iff, for all valuations \( \sigma \), we have:

\[
\langle s, \sigma \rangle \Downarrow \sigma' \iff \langle s', \sigma \rangle \Downarrow \sigma'
\]

In other words, two programs are equi-safe if they exhibit the same set of failing executions starting from the same state \( \sigma \). Thus, program \( s' \) has a bug if and only if \( s \) has a bug.

As mentioned in Section 1, the goal of program trimming is to obtain a program \( s' \) that (a) is equi-safe to \( s \) and (b) can terminate early in successful executions of \( s \):

**Definition 3.3. (Trimmed program)** A program \( s' \) is a trimmed version of \( s \) iff, \( s, s' \) are equi-safe and

\[
\begin{align*}
(1) & \quad \langle s, \sigma \rangle \Downarrow \sigma' \implies \langle s', \sigma \rangle \Downarrow \sigma' \\
(2) & \quad \langle s, \sigma \rangle \Downarrow \sigma' \implies \langle s', \sigma \rangle \Downarrow \sigma''
\end{align*}
\]

Here, the first condition says that the trimmed program \( s' \) either exhibits the same successful execution as the original program or terminates early with an assumption violation. The second condition says that, if the original program terminates with an assumption violation, then the trimmed program also violates an assumption but can terminate in a different state \( \sigma'' \). In the latter case, we allow the trimmed program to end in a different state \( \sigma'' \) than the original program because the assumption violation could occur earlier in the trimmed program. Intuitively, from a program analysis perspective, we can think of trimming as a program simplification technique that prunes execution paths that are guaranteed not to result in an assertion violation.

Observe that program trimming preserves all terminating executions of program \( s \). In other words, if \( s \) terminates under valuation \( \sigma \), then the trimmed version \( s' \) is also guaranteed to terminate. However, program trimming does not give any guarantees about non-terminating executions. Hence, even though this technique is suitable as a pre-processing technique for safety checking, it does not necessarily need to preserve liveness properties. For example, non-terminating executions of \( s \) can become terminating in \( s' \).

The definition of program trimming presented above does not impose any syntactic restrictions on the trimmed program. For instance, it allows program trimming to add and remove arbitrary statements as long as the resulting program satisfies the properties of Definition 3.3. However, in practice, it is desirable to make some syntactic restrictions on how trimming can be performed. In this paper, we perform program trimming by adding assumptions to the original program rather than removing statements. Even though this transformation does not “simplify” the program from a program understanding point of view, it is very useful to subsequent program analyzers because the introduction of \( \text{assume} \) statements prunes program paths in a semantic way.

### 4 STATIC ANALYSIS FOR TRIMMING

As mentioned in Section 1, our trimming algorithm consists of two phases, where we infer safety conditions using a lightweight static analysis in the first phase and instrument the program with trimming conditions in the next phase. In this section, we describe the safety condition inference.
Program $\mathcal{P}$ ::= $\mathbf{prc}$

Procedure $\mathbf{prc}$ ::= $\mathbf{proc}$ $\mathbf{prc}(<\mathit{in}>): e_{\text{out}}$ \{ $\mathbf{s}$ \}

Statement $\mathbf{s}$ ::= $\mathbf{s;}s_2$ | $\mathbf{v} := e$ | $\mathbf{v} := \mathbf{call} \; \mathbf{prc}(\mathbf{e})$
| $\mathbf{assert} \; p \; \mathbf{assume} \; p$
| $\mathbf{if} \; (\ast) \; \{s_1\} \; \mathbf{else} \; \{s_2\}$

Expression $e$ ::= $v | c | e_1 \oplus e_2$ (where $\oplus \in \{+,-,\times\}$)
| $p_1 \land p_2 | p_1 \lor p_2 | \neg p$

Predicate $p$ ::= $e_1 \land e_2$ (where $\land \in \{<,=,\leq\})$

\begin{figure*}[h]
\centering
\includegraphics[width=\textwidth]{figure3.png}
\caption{Programming language used for formalization. The notation $\mathbf{s}$ denotes a sequence $s_1, \ldots, s_n$.}
\end{figure*}

\subsection{Programming Language}

In order to precisely describe our trimming algorithm, we first introduce a small, but realistic, call-by-value imperative language with pointers and procedure calls. As shown in Figure 2, a program in this language consists of one or more procedure definitions. Statements include sequencing, assignments, heap reads and writes, memory allocation, procedure calls, assertions, assumptions, and conditionals. Since loops can be expressed as tail-recursive procedures, we do not introduce an additional loop construct. Also, observe that we only allow conditionals with non-deterministic predicates, denoted $\ast$. However, a conditional of the form $\mathbf{if} \; (p) \; \{s_1\} \; \mathbf{else} \; \{s_2\}$ can be expressed as follows in this language:

$$\mathbf{if} \; (\ast) \; \{\mathbf{assume} \; p; s_1\} \; \mathbf{else} \; \{\mathbf{assume} \; \neg p; s_2\}$$

Since the language is quite standard, we do not present its operational semantics in detail. However, as explained in Section 3, we assume that the execution of a program terminates as soon as we encounter an assertion or assumption violation (i.e., the predicate evaluates to false). As in Section 3, we use the term failing execution to indicate a program run with an assertion violation.

\subsection{Safety Condition Inference}

Recall from Section 1, that a safety condition at a given program point $\pi$ is a sufficient condition for any execution starting at $\pi$ to be error free. More precisely, a safety condition for a (terminating) statement $s$ is a formula $v$ such that $v \Rightarrow \mathsf{wp}(s, \mathit{true})$, where $\mathsf{wp}(s, \phi)$ denotes the weakest precondition of $s$ with respect to postcondition $\phi$ [37]. While the most precise safety condition is $\mathsf{wp}(s, \mathit{true})$, our analysis intentionally infers stronger safety conditions so that trimming can be used as a pre-processing technique for safety checkers.

Our safety condition inference engine is formalized using the rules shown in Figure 3. Our formalization makes use of an oracle $\Lambda$ for resolving queries about pointer aliasing and procedure side effects. For instance, this oracle can be implemented using a scalable pointer analysis, such as the Data Structure Analysis (DSA) method of Lattner et al. [69]. In the rest of this section, we assume that the oracle for resolving aliasing queries is flow-insensitive.

Figure 3 includes two types of inference rules, one for statements and one for procedures. Both forms of judgments utilize a summary environment $\mathcal{Y}$ that maps each procedure $\mathbf{prc}$ to its corresponding safety condition (or "summary"). Since our language contains recursive procedures, we would, in general, need to perform a fixed-point computation to obtain sound and precise summaries. However, because our analysis initializes summaries conservatively, the analysis can terminate at any point to produce sound results.

With the exception of rule (10), all rules in Figure 3 derive judgments of the form $\Lambda, \mathcal{Y}, \Phi + s : \Phi'$. The meaning of this judgment is that, using environments $\Lambda$ and $\mathcal{Y}$, it is provable that $(\Phi')s(\Phi)$ is a valid Hoare triple (i.e., $\Phi' \Rightarrow \mathsf{wp}(s, \phi)$ if $s$ terminates). Similarly to the computation of standard weakest preconditions [37], our analysis propagates safety conditions backward but sacrifices precision to improve scalability. Next, we only focus on those rules where our inference engine differs from standard precondition computation.

\begin{figure*}[h]
\centering
\includegraphics[width=\textwidth]{figure3.png}
\caption{Inference rules for computing safety conditions.}
\end{figure*}

\textbf{Heap reads and writes.} An innovation underlying our safety condition inference is the handling of the heap. Given a store operation $+v := e$, this statement can modify the value of all expressions $x$, where $x$ is an alias of $v$. Hence, a sound way to model the heap is to rewrite $+v := e$ as

$$+v := e; \mathbf{if} \; ((v = v_1) \; \ast \; v_1 := e; \ldots; \mathbf{if} \; ((v = v_k) \; \ast \; v_k := e;$$

where $v_1, \ldots, v_k$ are potential aliases of $v$. Effectively, this strategy accounts for the "side effects" of statement $+v := e$ to other heap
locations by explicitly introducing additional statements. These statements are of the form \( i f (v = u_i) \ast v := e \), i.e., if \( v \) and \( u_i \) are indeed aliases, then change the value of expression \( \ast v := e \).

While the strategy outlined above is sound, it unfortunately conflicts with our goal of computing safety conditions using lightweight analysis. In particular, since we use a coarse, but scalable alias analysis, most pointers have a large number of possible aliases in practice. Hence, introducing a linear number of conditionals causes a huge blow-up in the size of the safety conditions computed by our technique. To prevent this blow-up, our inference engine computes a safety precondition that is stronger than necessary by using the following conservative \( \text{store} \) operation.

**Definition 4.1. (Memory location)** We represent memory locations using terms that belong to the following grammar:

\[
\text{Memory location } a := v \mid \text{drf}(a)
\]

Here, \( v \) represents any program variable, and \( \text{drf} \) is an uninterpreted function representing the dereference of a memory location.

To define our conservative store operation, we make use of a function \( \text{aliases}(v, \Lambda) \) that uses oracle \( \Lambda \) to retrieve all memory locations \( a \) that may alias \( v \).

**Definition 4.2. (Store operation)** Let \( \text{derefs}(\Phi) \) denote all \( a' \) for which a sub-term \( \text{drf}(a') \) occurs in formula \( \Phi \). Then,

\[
\text{store}(\text{drf}(a), e, \Lambda, \Phi) := \Phi(e/\text{drf}(a)) \land \bigwedge_{a_i \in \text{aliases}(\Lambda)} a_i \neq a
\]

where \( \Lambda \models \text{aliases}(\lambda, \Lambda) \cap \text{derefs}(\Phi) \).

In other words, we compute the precondition for statement \( \ast v := e \) as though the store operation was a regular assignment, but we also “assert” that \( v \) is distinct from every memory location \( a_i \) that can potentially alias \( v \). To see why this is correct, observe that \( \Phi(e/\text{drf}(v)) \) gives the weakest precondition of \( \ast v := e \) when \( v \) does not have any aliases. If \( v \) does have aliases that are relevant to the safety condition, then the conjunction \( \bigwedge_{a_i \in \Lambda} a_i \neq v \) evaluates to \( \text{false} \), meaning that we can never guarantee the safety of the program. Thus, \( \text{store}(\text{drf}(v), e, \Lambda, \Phi) \) logically implies \( \text{wp}(\ast v := e, \Phi) \).

**Example 4.3.** Consider the following code snippet:

```plaintext
if (x) { assume x = y; a := 3; }
else { assume x ≠ y; y := 3; }
* x := a; t := * y;
assert t = 3;
```

Right before the heap write \( \ast x := a \), our analysis infers the safety condition \( \text{drf}(y) = 3 \land x ≠ y \). Before the heap write \( \ast y := 3 \), the safety condition is \( x ≠ y \), which causes the condition before the assumption \( x ≠ y \) to be \( \text{true} \). This means that executions through the else branch are verified and may be trimmed because \( x \) and \( y \) are not aliases for these executions.

**Interprocedural analysis.** We now turn our attention to the handling of procedure calls. As mentioned earlier, we perform interprocedural analysis in a modular way, computing summaries for each procedure. Specifically, a summary \( \Upsilon(f) \) for procedure \( f \) is a sufficient condition for any execution of \( f \) to be error free.

With this intuition in mind, let us consider rule (6) for analyzing procedure calls of the form \( v := \text{call prc(}\bar{e}\text{)} \). Suppose that \( \bar{a} \) is the set of memory locations modified by the callee \( \text{prc} \) but expressed in terms of the memory locations in the \text{caller}. Then, similarly to other modular interprocedural analyses \([8, 9]\), we conservatively model the effect of the statement \( v := \text{call prc(}\bar{e}\text{)} \) as follows:

\[
\text{assert summary(prc)};
\text{havoc } v \text{; havoc } \bar{a};
\]

Here, \( \text{havoc } \alpha \) denotes a statement that assigns an unknown value to memory location \( \alpha \). Hence, our treatment of procedure calls asserts that the safety condition for \( \text{prc} \) holds before the call and that the values of all memory locations modified in \( \text{prc} \) are “destroyed”.

While our general approach is similar to prior techniques on modular analysis \([8, 9]\), there are some subtleties in our context to which we would like to draw the reader’s attention. First, since our procedure summaries (i.e., safety conditions) are not provided by the user, but instead inferred by our algorithm (see rule (10)), we must be conservative about how summaries are “initialized”. In particular, because our analysis aims to be lightweight, we do not want to perform an expensive fixed-point computation in the presence of recursive procedures. Therefore, we use the following \( \text{summary} \) function to yield a conservative summary for each procedure.

**Definition 4.4. (Procedure summary)** Let \( \text{hasAsrts}(f) \) be a predicate that yields \( \text{true} \) iff procedure \( f \) or any of its (transitive) callees contain an assertion. Then,

\[
\text{summary}(f, \Upsilon, \bar{v}) = \begin{cases}
\Upsilon(f)[v/\bar{v}] & \text{if } f \in \text{dom}(\Upsilon) \\
\text{false} & \text{if hasAsrts}(f) \\
\text{true} & \text{otherwise}
\end{cases}
\]

In other words, if procedure \( f \) is in the domain of \( \Upsilon \) (meaning that it has previously been analyzed), we use the safety condition given by \( \Upsilon(f) \), substituting formulas by the actuals. However, if \( f \) has not yet been analyzed, we then use the conservative summary \( \text{false} \) if \( f \) or any of its callees have assertions, and \( \text{true} \) otherwise. Observe that, if \( f \) is not part of a strongly connected component (SCC) in the call graph, we can always obtain the precise summary for \( f \) by analyzing the program bottom-up. However, if \( f \) is part of an SCC, we can still soundly analyze the callee by using the conservative summaries given by \( \text{summary}(f, \Upsilon, \bar{v}) \).

The other subtlety about our interprocedural analysis is the particular way in which havocing is performed. Since the callee may modify heap locations accessible in the caller, we define a \( \text{havoc} \) operation that uses the \text{store} function from earlier to conservatively deal with memory locations.

**Definition 4.5. (Havoc operation)**

\[
\text{havoc(drfs}(a), \Lambda, \Phi) := \forall v_{\text{new}}. \text{store}(\text{drf}(a), v_{\text{new}}, \Lambda, \Phi)
\]

where \( v_{\text{new}} \notin \text{freeVars}(\Phi) \)

\[
\text{havoc(} \bar{\Upsilon}, \Lambda, \Phi) := \text{havoc(tail}(\bar{\Upsilon}), \Lambda, \text{havoc(head}(\bar{\Upsilon}), \Lambda, \Phi))
\]

Observe that the above definition differs from the standard way this operation is typically defined \([8]\). In particular, given a scalar variable \( v \), the assignment \( v := \ast \), and its postcondition \( \Phi \), the standard way to compute a conservative precondition for the assignment is \( \forall v. \Phi (i.e., \Phi \) must hold for any value of \( v \). Note that an alternative way of computing the precondition is \( \forall x. \Phi[x/v] \), where \( x \) is not a free variable in \( \Phi \). In the context of scalars, these two definitions are essentially identical, but the latter view allows
We instrument the program with the statement \( \text{assume} \) instrumentation we could add to callers to callees in a separate pass. However, this latter strategy may seem counter-intuitive. However, because one

\textbf{Theorem 4.6.} Suppose that \( \Lambda, \Psi \models s : \Phi' \), and assume that \( \Lambda \) provides sound information about aliasing and procedure side effects. Then, under the condition that \( s \) terminates and that the summaries provided by \( \Psi \) are sound, we have \( \Phi' \Rightarrow \wp(s, \Psi) \).}

\section{5 PROGRAM INSTRUMENTATION}

In the previous section, we discussed how to infer safety conditions for each program point. Recall that program trimming annotates the code with \textit{trimming conditions}, which are necessary conditions for failure. Here, we describe how we instrument the program with suitable assumptions that preserve safety of the original program.

\textbf{Intraprocedural instrumentation.} First, let us ignore procedure calls and consider instrumenting a single procedure in isolation. Specifically, consider a procedure with body \( s_1; \ldots; s_n \) and let:

\[ \Lambda, \Psi, \text{true} \vdash s_1; \ldots; s_n : \Phi \]

We instrument the program with the statement \( \text{assume} \) right before statement \( s_j \) if \( s_j \) complies with the instrumentation strategy specified by the user (see Section 6). Note that we do not instrument at every single instruction because subsequent safety checkers must also analyze the assumptions, which adds overhead to their analysis.

\textbf{Theorem 5.1.} Suppose that our technique adds a statement \( \text{assume} \) \( \Phi \) before \( s_1; \ldots; s_n \). Then, \( \Phi \) is a necessary condition for \( s_1; \ldots; s_n \) to have an assertion violation.

\textbf{Interprocedural instrumentation.} One of the key challenges in performing program instrumentation is how to handle procedure calls. In particular, we cannot simply annotate a procedure \( f \) using the safety conditions computed for \( f \). The following example illustrates why such a strategy would be unsafe.

\textbf{Example 5.2.} Consider procedures foo, bar, and baz:

\begin{verbatim}
proc foo(x) {x := 2;
proc bar(a) {x := malloc(a);foo(x);assert a < 100;
proc baz(b) {x := malloc(b);foo(x);assert b > 10;

Here, the safety condition for procedure foo is just \textit{true} since foo does not contain assertions or have callees with assertions. However, observe that we cannot simply instrument foo with \textit{assume false} because there are assertions after the call to foo in bar and baz. One possible solution to this challenge is to only instrument the main method, which would be very ineffective. Another possible strategy might be to propagate safety conditions top-down from callers to callees in a separate pass. However, this latter strategy also has some drawbacks. For instance, in this example, variables \( a \) and \( b \) are not in scope in foo; hence, there is no meaningful instrumentation we could add to foo short of assume \textit{true}, which is the same as having no instrumentation at all.

We solve this challenge by performing a program transformation inspired by previous work [54, 67]. The key idea underlying this transformation is to create, for each procedure \( prc \), a new procedure

\[ prc' \] that can never fail. In particular, we create \( prc' \) by (a) changing all assertions \( \text{assert} \phi \) in \( prc \) to \( \text{assume} \phi \), and (b) replacing all calls to \( f \) (including recursive ones) with \( f' \). Now, given a call site of \( prc \), \( v := \text{call} \ prc'(\bar{e}) \), we replace it with the following conditional:

\[ \text{if} \ (\star) \ (v := \text{call} \ prc'(\bar{e});)
\]

This transformation is semantics preserving since it is merely a case analysis: Either \( prc \) succeeds, in which case it is safe to replace the call to \( prc \) with \( prc' \), or it fails, in which case we can call original \( prc \) but add \textit{assume false} afterward since \( prc \) has failed. The following example illustrates this transformation.

\textbf{Example 5.3.} Consider the following procedures:

\begin{verbatim}
proc foo(x,y) {assert x > 0;bar(y);)
proc bar(z) {assert z > 0;
proc main(x,y) {foo(x,y);

Our transformation yields the following new program:

\begin{verbatim}
proc foo'(x,y) {assume x > 0;bar'(y);}
proc foo(x,y) {
   assert x > 0;
   if (\star) {bar'(y);}
   else {bar(y);assume false;}
}
proc bar'(z) {assume z > 0;
proc bar(z) {assume z > 0;
proc main(x,y) {
   if (\star) {foo'(x,y);}
   else {foo(x,y);assume false;}
}

The main advantage of this transformation is that it allows us to perform program instrumentation in a modular and conceptually simple way. In particular, we do not need to instrument the "safe" version \( prc' \) of a procedure \( prc \) since \( prc' \) never fails. On the other hand, it is safe to instrument \( prc \) with the negation of the local safety conditions since every call site of \( prc \) is followed by the statement \textit{assume false} (i.e., execution terminates immediately after the call).

\textbf{Example 5.4.} Consider the following procedures foo and bar:

\begin{verbatim}
proc foo(x) {assert x > 10;
proc bar(a,x) {foo(x);assert a < 100;

Our instrumentation yields the following new program:

\begin{verbatim}
proc foo'(x) {assume x > 10;}
proc foo(x) {assume x \leq 10;assert x > 10;}
proc bar(a,x) {
   assume a \geq 100 \lor x \leq 10;
   if (\star) {foo'(x);}
   else {foo(x);assume false;}
   assert a < 100;
}

\textbf{Discussion.} The reader may notice that our program transformation introduces additional branches that did not exist in the original program. Since the goal of program trimming is to reduce the number of execution paths while retaining equi-safety, this transformation may seem counter-intuitive. However, because one

---

1This paper’s extended version [46] includes proofs or proof sketches for all theorems.
of the branches is always followed by assume false, our transformation does not lead to a blow-up in the number of paths and allows us to perform the instrumentation modularly.

6 IMPLEMENTATION

We have implemented our program trimming algorithm as a tool called TRIMMER, meant as a lightweight pre-processor for program analyzers that check safety. Our implementation is based on the LLVM infrastructure [68] and performs instrumentation at the LLVM bit-code level. Hence, TRIMMER can be conveniently integrated into any safety checking tool that is built on top of the LLVM infrastructure and is capable of analyzing assume statements.

Recall from Section 4 that TRIMMER’s safety inference engine requires alias and side effect information to soundly analyze heap stores and procedure calls. For this purpose, TRIMMER leverages LLVM’s DSA pointer analysis [69], a highly-scalable, summary-based, flow-insensitive analysis.

Since TRIMMER can be useful to a variety of program analysis tools (including both static and dynamic analyzers), TRIMMER can be customized in different ways depending on the assumptions made by subsequent safety checkers. In what follows, we describe the different configurations that TRIMMER provides.

Reasoning about integer arithmetic. TRIMMER provides the option of treating integral-type expressions either as mathematical (unbounded) or fixed-width integers. Since some safety checkers ignore integer over- and under-flows but others do not, TRIMMER supports both encodings.2 Analyzers treating values as mathematical integers can therefore use the configuration of TRIMMER that also makes this same unsound assumption.

Eliminating quantifiers. Recall from Section 4 that the safety conditions generated by our inference engine contain universal quantifiers. Hence, when negating the safety conditions, the resulting trimming conditions contain existentially-quantified variables. TRIMMER provides two alternatives for eliminating quantifiers. First, TRIMMER can remove quantifiers using Z3’s quantifier elimination (QE) capabilities [36] after simplifying and pre-processing the formula. Second, TRIMMER also allows replacing quantified variables by calls to non-deterministic functions. Since quantified variables at the formula level correspond to program variables with unknown values, this strategy has the same effect as quantifier elimination.

Bounding the instrumentation. After TRIMMER instruments the program with trimming conditions, subsequent safety checkers need to analyze the assumptions. Hence, the number of additional assume statements as well as the size of the predicates can affect the running time of program analyzers. For this reason, TRIMMER allows users to customize where to add assumptions in the code. For example, sensible strategies include adding instrumentation right before loops and procedure calls, or before every conditional.

In a similar vein, TRIMMER also provides different options for bounding the size of the formulas used in assume statements. For example, the user can bound the number of conjuncts in the formula to be at most $k$, where $k$ is a value chosen by the user. This strategy is sound because TRIMMER guarantees that the “simplified” formulas are weaker than the original trimming conditions.

7 EXPERIMENTS

To evaluate the effectiveness of program trimming, we have used TRIMMER to pre-process hundreds of programs by instrumenting them with assume statements. Since these assumptions are not useful on their own, we evaluate the effect of program trimming in the context of two different LLVM-based program analyzers for safety checking. In particular, we use CRAB, an abstract interpreter that supports several abstract domains, and KLEE, a widely-used dynamic symbolic execution engine.

We ran our experiments on 439 programs3, most of which (92%) are taken from the software verification competition (SV-COMP) benchmarks, which have clearly defined outcomes and are handled by numerous tools. Since the errors in many of the buggy programs in this benchmark set are very shallow4, we also augment these benchmarks with additional buggy programs, either taken from other sources or obtained by injecting deeper bugs into safe SV-COMP benchmarks. The benchmarks taken from SV-COMP span a broad range of categories, including ControlFlow, Loops, Recursive, and ArrayReach, but exclude categories that are not handled by KLEE or CRAB, e.g., BitVectorsReach, Concurrency.

In what follows, we describe the effects of program trimming on the results of CRAB and KLEE. We ran all of our experiments on an Intel Xeon CPU E5-2640 v3 @ 2.60GHz machine with 132 GB of memory running the Ubuntu 14.04.1 operating system. We used the latest available version of CRAB and the latest version of KLEE that was compatible with LLVM 3.6, which CRAB requires.

7.1 Impact of Program Trimming on CRAB

To demonstrate that program trimming increases precision across a range of abstract domains, we compare the performance of CRAB (with and without trimming) on three different domains with varying levels of precision:

- **Int** denotes the (non-relational) interval domain [31], which infers invariants of the form $c_1 \leq x \leq c_2$;
- **Zones** is the (relational) zones abstract domain [77], which infers difference constraints of the form $x - y \leq c$;
- **RTZ** is CRAB’s most precise (native) abstract domain and corresponds to the reduced product of disjunctive intervals (i.e., disjunctions of constraints of the form $c_1 \leq x \leq c_2$) [45] and the zones abstract domains.

As mentioned in Section 6, TRIMMER can be customized using a variety of different configurations. To understand the precision vs. performance trade-off, we evaluate CRAB using the configurations of TRIMMER shown in Table 1. Here, the column labeled MC indicates the maximum number of conjuncts used in an assume statement. The third column labeled QE indicates whether we use quantifier elimination or whether we model quantified variables using calls to non-deterministic functions (recall Section 6). Finally, the columns labeled L/P and C denote the instrumentation strategy.

In configurations where there is a checkmark under L/P, we add

---

2For the fixed-width integer encoding, TRIMMER strengthens safety conditions by requiring that there are no integer over- or under-flows. Specifically, TRIMMER utilizes arithmetic operations in the LLVM instruction set that return both the result of the operation and a flag indicating whether an over-flow occurred. Note that TRIMMER does not use bit-vectors for encoding fixed-width integers.

3Available at: https://mariachris.github.io/FSE2017/benchmarks.zip

4For example, in the existing SV-COMP benchmarks, KLEE can find the bug with a very low resource limit for 85% of the buggy programs.
Table 1: Overview of trimming configurations (incl. total number of added \texttt{assume} statements and time for pre-processing all benchmarks in the two right-most columns).

<table>
<thead>
<tr>
<th>Configuration</th>
<th>MC</th>
<th>QE</th>
<th>L/P</th>
<th>C</th>
<th>A</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{Trim_B}</td>
<td>4</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>143</td>
<td>5.31</td>
</tr>
<tr>
<td>\texttt{Trim_B}</td>
<td>4</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>1638</td>
<td>4.97</td>
</tr>
<tr>
<td>\texttt{Trim_ND+B}</td>
<td>4</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>2801</td>
<td>7.34</td>
</tr>
<tr>
<td>\texttt{Trim_L}</td>
<td>∞</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>156</td>
<td>6.05</td>
</tr>
<tr>
<td>\texttt{Trim_ND}</td>
<td>∞</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>1735</td>
<td>5.74</td>
</tr>
<tr>
<td>\texttt{Trim_ND}</td>
<td>∞</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>2852</td>
<td>8.62</td>
</tr>
</tbody>
</table>

The results of our evaluation are summarized in Table 2. As we can see from this table, all configurations of program trimming improve the precision of \texttt{Crab}, and these improvements range from \(23\%\) to \(54\%\). For instance, for the interval domain, the most precise configuration of \texttt{Trimmer} allows the verification of 68 benchmarks instead of only 49 when using \texttt{Crab} without trimming.

Another observation based on Table 2 is the precision vs. performance trade-offs between different configurations of \texttt{Trimmer}. Versions of \texttt{Crab} that use \texttt{Trimmer} with \texttt{QE} seem to be faster and more precise than those configurations of \texttt{Trimmer} without \texttt{QE}. In particular, the version of \texttt{Trimmer} with \texttt{QE} performs better because there are fewer variables for the abstract domain to track. We also conjecture that \texttt{Trimmer} using \texttt{QE} is more precise because the abstract domain can introduce imprecision when reasoning about logical connectives. For instance, consider the formula \(\exists x (x = 1 \land x \neq 1)\), which is logically equivalent to \texttt{false}, so \texttt{Trimmer} with \texttt{QE} would instrument the code with \texttt{assume false}. However, if we do not use \texttt{QE}, we would instrument the code as follows:

\[
\texttt{x := nondet(); assume } x = 1 \land x \neq 1;
\]

When reasoning about the \texttt{assume} statement, an abstract interpreter using the interval domain takes the meet of the intervals \([1, 1]\) and \(\top\), which yields \([1, 1]\). Hence, using \texttt{Trimmer} without \texttt{QE}, \texttt{Crab} cannot prove that the subsequent code is unreachable.

Summary: Table 2 shows that trimming significantly improves the precision of an abstract interpreter with reasonable overhead. Our cheapest trimming configuration (\texttt{Trim\_B + Int}) proves 21\% more programs safe than the most expensive configuration of \texttt{Crab} without trimming (\texttt{RTZ}) in less than 70\% of the time.

7.2 Impact of Program Trimming on \texttt{Klee}

In our second experiment, we evaluate the impact of program trimming on \texttt{Klee}, a state-of-the-art dynamic symbolic execution tool. We use a subset\(^3\) of the variants of \texttt{Trimmer} (see Table 1) and evaluate trimming on \texttt{Klee} with three search strategies: breadth-first search (BFS), depth-first search (DFS), and random search (R).

Since programs usually have infinitely many execution paths, it is necessary to enforce some resource bounds when running \texttt{Klee}. In particular, we run \texttt{Klee} with a timeout of 300 seconds and a limit of 64 on the number of forks (i.e., symbolic branches).

The results of our evaluation are presented in Table 3. Here, the column labeled \texttt{Safe} shows the number of programs for which \texttt{Klee} explores all execution paths without reporting any errors or warnings.\(^6\) Hence, these programs can be considered verified. The second column, labeled \texttt{Unsafe}, shows the number of programs reported as buggy by each variant of \texttt{Klee}. In this context, a bug corresponds to an explicit assertion violation in the program. Next, the third column, labeled \texttt{Time}, shows the total running time of each \texttt{Klee} variant on all benchmarks.

As shown in Table 3, program trimming increases the number of programs that can be proved safe by 16–18\%. Furthermore, program trimming allows \texttt{Klee} to find up to 30\% more bugs within the given resource limit. In addition, \texttt{Klee} with program trimming needs to explore significantly fewer paths (up to 38\%) and reaches the resource bound on significantly fewer programs. Finally, observe that the overall running time of \texttt{Klee} decreases by up to 30\%.

\(^3\)In particular, since \texttt{Klee}’s analysis is already path-sensitive we do not consider variants that instrument before conditionals here.

\(^6\)By warning, we mean any internal \texttt{Klee} warning that designates an incompleteness in \texttt{Klee}’s execution (e.g., solver timeouts and concretizing symbolic values).
Table 3: Summary of comparison with Klee. Since Klee treats integers in a sound way, we also use the variant of Trimmer that reasons about integer over- and under-flows.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Safe</th>
<th>Unsafe</th>
<th>Paths</th>
<th>Timeout</th>
<th>Max-Forks</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Klee_EFS</td>
<td>126 (+0%)</td>
<td>118 (+0%)</td>
<td>9231 (+0%)</td>
<td>73 (+0%)</td>
<td>73 (+0%)</td>
<td>21679</td>
</tr>
<tr>
<td>Trim_L + Klee_EFS</td>
<td>146 (+16%)</td>
<td>145 (+23%)</td>
<td>5978 (+35%)</td>
<td>52 (-40%)</td>
<td>46 (-51%)</td>
<td>15558</td>
</tr>
<tr>
<td>Trim_L + Klee_EFS</td>
<td>146 (+16%)</td>
<td>153 (+30%)</td>
<td>5678 (+38%)</td>
<td>50 (-32%)</td>
<td>40 (-45%)</td>
<td>15264</td>
</tr>
<tr>
<td>Trim_L + Klee_EFS</td>
<td>146 (+16%)</td>
<td>124 (+25%)</td>
<td>6939 (-31%)</td>
<td>72 (-21%)</td>
<td>48 (-36%)</td>
<td>20797</td>
</tr>
<tr>
<td>Trim_L + Klee_EFS</td>
<td>146 (+16%)</td>
<td>129 (+30%)</td>
<td>6695 (-33%)</td>
<td>72 (-21%)</td>
<td>43 (-43%)</td>
<td>21164</td>
</tr>
<tr>
<td>Trim_L + Klee_EFS</td>
<td>146 (+16%)</td>
<td>121 (+0%)</td>
<td>9227 (+0%)</td>
<td>71 (+0%)</td>
<td>72 (+0%)</td>
<td>21077</td>
</tr>
<tr>
<td>Trim_L + Klee_EFS</td>
<td>149 (+18%)</td>
<td>146 (-21%)</td>
<td>5967 (-35%)</td>
<td>49 (-31%)</td>
<td>44 (-39%)</td>
<td>14844</td>
</tr>
<tr>
<td>Trim_L + Klee_EFS</td>
<td>149 (+18%)</td>
<td>152 (+26%)</td>
<td>5699 (-38%)</td>
<td>48 (-32%)</td>
<td>40 (-44%)</td>
<td>14850</td>
</tr>
</tbody>
</table>

Figure 4 compares the number of benchmarks solved by the original version of Klee (using BFS) with its variants using program trimming. Specifically, the x-axis shows how many benchmarks were solved (i.e., identified as safe or unsafe) by each variant (sorted by running time), and the y-axis shows the corresponding running time per benchmark. For instance, we can see that Trim_L + Klee_EFS solves 246 benchmarks within less than one second each, whereas the original version of Klee only solves 203 benchmarks.

Summary: Overall, the results shown in Table 3 and Figure 4 demonstrate that program trimming significantly improves the effectiveness and performance of a mature, state-of-the-art symbolic execution tool. In particular, program trimming allows Klee to find more bugs and prove more programs correct within a given resource limit independently of its search strategy.

7.3 Threats to Validity

We identified these threats to the validity of our experiments:

- **Sample size**: We used 439 programs, most of which, however, are taken from the SV-COMP benchmarks, a widely-used and established set of verification tasks.
- **Safety checkers**: We evaluate our technique using two safety checkers, which, however, are mature and representative of two program analysis techniques.
- **Trimming configurations**: We only presented experiments using a selection of the different configurations that Trimmer provides (see Section 6). However, all of these configurations are orthogonal to each other, and we evaluated a large variety of them to demonstrate the benefits of our technique.

8 RELATED WORK

The ideas in this paper are related to a long line of previous work on program transformations and safety precondition inference.

- **Program slicing**: One of the most well-known program simplification techniques is program slicing, which removes program statements that are not relevant to some criterion of interest (e.g., value of a variable at some program point) [1, 15, 83, 86]. A program slice can be computed either statically or dynamically and includes both forward and backward variants. Program trimming differs from traditional program slicing in two ways: first, trimming focuses on removing execution paths as opposed to statements; second, it is meant as a pre-processing technique for safety checkers rather than a transformation to aid program understanding. In particular, a typical slicing tool may not produce compilable and runnable code that could be consumed by subsequent safety checkers.

More semantic variants of program slicing have also been considered in later work [5, 20, 30, 47, 55, 65]. For instance, Jhala and Majumdar propose path slicing to improve the scalability of software model checkers [65]. In particular, path slicing eliminates all operations that are irrelevant toward the reachability of the target location in a given program path. Unlike program trimming, path slicing is not used as a pre-processing step and works on a single program path that corresponds to a counterexample trace.

Prior work has also considered how to slice the program with respect to a predicate [20, 30, 47, 55]. Such techniques can be useful for program understanding, for example, when the user only wants to see statements that affect a given condition (e.g., the predicate of a conditional). In contrast, program trimming is not meant as a program understanding technique and removes program paths that are irrelevant for a given safety property. Furthermore, the trimmed program is not meant for human consumption, as it semantically prunes program paths through the insertion of assume statements.

Slicing has been used before invoking a program analyzer [22, 23, 44, 56, 63, 64, 76]. A key difference with these approaches is that the result of trimming is valid code, which compiles and runs, instead of an abstract representation, such as a control flow graph or model.

- **Pre-processing for program analyzers**: In the same spirit as this paper, prior work has also used program transformations to improve the precision or scalability of program analyzers [24, 26, 27, 54, 67, 84, 88]. For instance, a transformation for faster goal-directed search [67] moves all assertions to a single main procedure with the goal of speeding up analysis. Another program transformation
called loop splitting aims to improve the precision of program analyzers by turning multi-phase loops into a sequence of single-phase loops [84]. However, neither of these techniques instrument the program with assumptions to guide safety checking tools.

Recent techniques rely on the verification results of a full-fledged analyzer, such as an abstract interpreter or a model checker, to guide automatic test case generation tools [24, 26, 34, 35] or other static analyzers [13, 25, 27, 88], some even using slicing as an intermediate step [34]. In contrast, program trimming is more lightweight by not relying on previous analyzers and, thus, can be used as a pre-processing step for any safety checker.

Precondition inference. The use of precondition inference dates back to the dawn of program verification [37]. Most verification techniques infer a sufficient condition for program safety and prove the correctness of the program by showing the validity of this condition [8, 10, 21, 37, 48, 59–61, 78]. In this work, we do not aim to infer the weakest possible safety precondition; instead, we use lightweight, modular static analysis to infer a sufficient condition for safety. Furthermore, we use safety conditions to prune program paths rather than to verify the program.

Program trimming hinges on the observation that the negation of a sufficient condition for property $P$ yields a necessary condition for the negation of $P$. Prior program analysis techniques also exploit the same observation [39–41, 90]. For this reason, this duality has been used to perform modular path-sensitive analysis [39] and strong updates on elements of unbounded data structures [40, 41].

While most program analysis techniques focus on the inference of sufficient preconditions to guarantee safety, some techniques also infer necessary preconditions [32, 33, 73, 74, 79]. For example, Verification Modulo Versions (VMV) infers both necessary and sufficient conditions and utilizes previous versions of the program to reduce the number of warnings reported by verifiers [74]. Similarly, necessary conditions are inferred to repair the program in such a way that the repair does not remove any “good” traces [73]. Finally, the techniques described by Cousot et al. infer necessary preconditions, which are used to improve the effectiveness of the Code Contracts abstract interpreter [32, 33, 45].

Abductive reasoning. There has been significant work on program analysis using abductive reasoning, which looks for a sufficient condition that implies a desired goal [3, 19, 38, 42, 43, 71, 91]. Our analysis for computing safety conditions can be viewed as a form of abductive reasoning in that we generate sufficient conditions that are stronger than necessary for ensuring safety. However, we perform this kind of reasoning in a very lightweight way without calling an SMT solver or invoking a logical decision procedure.

Modular interprocedural analysis. The safety condition inference we have proposed in this paper is modular in the sense that it analyzes each procedure independently of its callers. There are many previous techniques for performing modular (summary-based) analysis [2, 19, 39, 81, 89]. Our technique differs from these approaches in several ways: First, our procedure summaries only contain safety preconditions, but not post-conditions, as we handle procedure side effects in a very conservative way. Second, we do not perform fixed-point computations and achieve soundness by initializing summaries to false. Finally, we use summary-based analysis for program transformation rather than verification.

Property-directed program analysis. There is a significant body of work that aims to make program analyzers property directed. Many of these techniques, such as BLAST [12, 57, 58], SLAM [4, 6, 7], and YOGI [52, 80] rely on counterexample-guided abstraction refinement (CEGAR) [29] to iteratively refine an analysis based on counterexample traces. Another example of a property-directed analysis is the IC3/PDR algorithm [16, 62], which iteratively performs forward and backward analysis for bounded program executions to decide reachability queries. Although abstract interpretation is traditionally not property directed, there is recent work [82] on adapting and rephrasing IC3/PDR in the framework of abstract interpretation. In contrast, we propose a general pre-processing technique to make any eager program analysis property directed.

Path-exploration strategies. Most symbolic execution and testing techniques utilize different strategies to explore the possible execution paths of a program. For example, there are strategies that prioritize “deeper paths” (in depth-first search), “less-traveled paths” [72], “number of new instructions covered” (in breadth-first search), “distance from a target line” [75], or “paths specified by the programmer” [83]. In the context of symbolic execution, program trimming can be viewed as a search strategy that prunes safe paths and steers exploration toward paths that are more likely to contain bugs. However, as shown in our experiments, our technique is beneficial independently of a particular search strategy.

9 CONCLUSION

In this paper, we have proposed program trimming, a program simplification technique that aims to reduce the number of execution paths while preserving safety. Program trimming can allow any safety checker to be goal directed by pruning execution paths that cannot possibly result in an assertion violation. Furthermore, because our proposed trimming algorithm is very lightweight, it can be used as an effective pre-processing tool for many program analyzers. As shown by our evaluation, program trimming allows an abstract interpreter, namely Crab, to verify 21% more programs while cutting running time by 30%. Trimming also allows Klee, a dynamic symbolic execution engine, to find more bugs and verify more programs within a given resource limit.

In future work, we plan to investigate the impact of program trimming on other kinds of program analyzers, such as bounded model checkers. We also plan to investigate alternative program trimming algorithms and strategies.

ACKNOWLEDGMENTS

We would like to thank Cristian Cadar and Martin Nowack for their help with Klee. We would also like to thank the main developer of Crab, Jorge Navas, for his help with Crab and for his positive feedback on the usefulness of program trimming. We are grateful to Microsoft for partly funding the first three authors and to the anonymous reviewers for their constructive feedback. This work is supported by AFRL Award FA8750-15-2-0096 and NSF Award #1453386. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.