Compositional Safety Verification with Max-SMT

Marc Brockschmidt *, Daniel Larraz †, Albert Oliveras †, Enric Rodríguez-Carbonell † and Albert Rubio †

*Microsoft Research, Cambridge
†Universitat Politècnica de Catalunya

Abstract—We present an automated compositional program verification technique for safety properties based on conditional inductive invariants. For a given program part (e.g., a single loop) and a postcondition $\varphi$, we show how to, using a Max-SMT solver, an inductive invariant together with a precondition can be synthesized so that the precondition ensures the validity of the invariant and that the invariant implies $\varphi$. From this, we build a bottom-up program verification framework that propagates preconditions of small program parts as postconditions for preceding program parts. The method recovers from failures to prove the validity of a precondition, using the obtained intermediate results to restrict the search space for further proof attempts.

As only small program parts need to be handled at a time, our method is scalable and distributable. The derived conditions can be viewed as implicit contracts between different parts of the program, and thus enable an incremental program analysis.

I. INTRODUCTION

To have impact on everyday software development, a verification engine needs to be able to process the millions of lines of code often encountered in mature software projects. At the same time, the analysis should be repeated every time developers commit a change, and should report feedback in the course of minutes, so that fixes can be applied promptly. Consequently, a central theme in recent research on automated program verification has been scalability. As a natural solution to this problem, compositional program analyses [1]–[3] have been proposed. They analyze program parts (semi-)independently and then combine the results to obtain a whole-program proof.

For this, a compositional analysis has to predict likely intermediate assertions that allow us to break whole-program reasoning into many instances of local reasoning. This strategy simplifies the individual reasoning steps and allows distributing the analysis [4]. The disadvantage of compositional analyses has traditionally been their precision: local analyses must blindly choose the intermediate assertions. While in some domains (e.g., heap) some heuristics have been found [2], effective strategies for guessing and/or refining useful intermediate assertions or summaries in arithmetic domains remains an open problem.

In this paper we introduce a new method for predicting and refining intermediate arithmetic assertions for compositional reasoning about sequential programs. A key component in our approach is Max-SMT solving. Max-SMT solvers can deal with hard and soft constraints, where hard constraints are mandatory, and soft constraints are those that we would like to hold, but are not required to. Hard constraints express what is needed for the soundness of our analysis, while soft ones favor the solutions that are more useful for our technique. More precisely, we use Max-SMT to iteratively infer conditional inductive invariants $^1$, which prove the validity of a property, given that a precondition holds. Hence, if the precondition holds, the program is proved safe. Otherwise, thanks to a novel program transformation technique we call narrowing $^2$, we exploit the failing conditional invariants to focus on what is missing in the safety proof of the program. Then new conditional invariants are sought, and the process is repeated until the safety proof is finally completed. Based on this, we introduce a new bottom-up program analysis procedure that infers conditional invariants in a goal-directed manner, starting from a property that we wish to prove for the program. Our approach makes distributing analysis tasks as simple as in other bottom-up analyses, but also enjoys the precision of CEGAR-based provers.

II. ILLUSTRATION OF THE METHOD

In this section, we illustrate the core concepts of our approach by using some small examples. We will give the formal definition of the used methods in Sect. IV.

We handle programs by considering one strongly connected component (SCC) $C$ of the control-flow graph at a time, together with the sequential parts of the program leading to $C$, either from initial states or other SCCs.

Instead of program invariants, for each SCC we synthesize conditional inductive invariants. These are inductive properties such that they may not always hold whenever the SCC is reached, but once they hold, then they are always satisfied.

a) Conditional Inductive Invariants:

As an example, consider the program snippet in Fig. 1, where we do not assume any knowledge about the rest of the program. To prove the assertion, we need an inductive property $Q$ for the loop such that $Q$ together with the negation of the loop condition $i > 0$ implies the assertion. Using our constraint-solving based method CondSafe (cf. Sect. IV-A), we find $Q_1 = x + 5 \cdot i \geq 0$. The property $Q_1$ can be seen as a precondition at the loop entry for the validity of the assertion.

1This concept was previously introduced with the name “quasi-invariant” in [5] in the different context of proving program non-termination.

2This narrowing is inspired by the narrowing in term rewrite systems, and is unrelated to the notion with the same name used in abstract interpretation.
b) Combining Conditional Inductive Invariants: Once we have found a conditional inductive invariant for an SCC, we use the generated preconditions as postconditions for its preceding SCCs in the program.

As an example, assume that the loop from Fig. 1 is directly preceded by the loop in Fig. 2. We now use the precondition $Q_1$ we obtained earlier as input to our conditional invariant synthesis method, similarly to the assertion in Fig. 1. Thus, we now look for an inductive property $Q_2$ that, together with the loop condition, implies the negation of the conditional $\neg(j > 0)$, implies $Q_1$. In this case we obtain the conditional invariant $Q_2 = j \geq 0 \land x + 5 \cdot (i + j) \geq 0$ for the loop. As with $Q_1$, now we can see $Q_2$ as a precondition at the loop entry, and propagate $Q_2$ up to the preceding SCCs in the program.

c) Recovering from Failures: When we cannot prove that a precondition always holds, we try to recover and find an alternative precondition. In this process, we make use of the results obtained so far, and narrow the program using our intermediate results. As an example, consider the loop in Fig. 3.

We again apply our method CondSafe to find a conditional invariant for this loop which, together with the loop condition, implies the assertion in the loop body. As it can only synthesize conjunctions of linear inequalities, it produces the conditional invariant $Q_3 = x > y$ for the loop. However, assume that the precondition $Q_3$ could not be proven to always hold in the context of our example. In that case, we use the obtained information to narrow the program and look for another precondition.

Intuitively, our program narrowing reflects that states represented by the conditional invariant found earlier are already proven to be safe. Hence, we only need to consider states for which the negation of the conditional invariant holds, i.e., we can add its negation as an assumption to the program. In our example, this yields the modified version of Fig. 3 displayed in Fig. 4. Another call to CondSafe then yields the conditional invariant $Q_3' = x < y$ for the loop. This means that we can ensure the validity of the assertion before the conditional statement we satisfy that $\neg((x > y) \Rightarrow x < y)$, or equivalently, $x \neq y$. In general, this narrowing allows us to find (some) disjunctive invariants.

III. Preliminaries

1) SAT, Max-SAT, and Max-SMT: Let $P$ be a fixed set of propositional variables. For $p \in P$, $p$ and $\neg p$ are literals. A clause is a disjunction of literals $l_1 \lor \cdots \lor l_n$. A (CNF) propositional formula is a conjunction of clauses $C_1 \land \cdots \land C_m$. The problem of propositional satisfiability (SAT) is to determine whether a propositional formula is satisfiable. An extension of SAT is satisfiability modulo theories (SMT) [6], where satisfiability of a formula with literals from a given background theory is checked. We will use the theories of quantifier-free (non-)linear arithmetic, where literals are inequalities of linear (resp. polynomial) arithmetic expressions.

Another extension of SAT is Max-SAT [6], which generalizes SAT to finding an assignment such that the number of satisfied clauses in a given formula $F$ is maximized. Finally, Max-SMT combines Max-SAT and SMT. A (weighted partial) Max-SMT problem is a formula of the form $H_1 \land \cdots \land H_n \land [S_1, \omega_1] \land \cdots \land [S_m, \omega_m]$, where the hard clauses $H_i$ and the soft clauses $S_j$ (with weight $\omega_j$) are disjunctions of literals over a background theory, and the aim is to find a model of the hard clauses that maximizes the sum of the weights of the satisfied soft clauses.

2) Programs and States: We make heavy use of the program structure and hence represent programs as graphs. For this, we fix a set of (integer) program variables $V = \{v_1, \ldots, v_n\}$ and denote by $F(V)$ the formulas consisting of conjunctions of linear inequalities over the variables $V$. Let $L$ be the set of program locations, which contains a canonical start location $l_0$. Program transitions $T$ are tuples $(\ell, \tau, \ell')$, where $\ell$ and $\ell' \in L$ represent the pre- and post-location respectively, and $\tau \in F(V) \cup V'$ describes its transition relation. Here $V' = \{v'_1, \ldots, v'_n\}$ are the post-variables, i.e., the values of the variables after the transition. A transition is initial if its source location is $l_0$. A program is a set of transitions. We view a program $P = (L, T)$ as a directed graph (the control-flow graph, CFG), in which edges are the transitions $T$ and nodes are the locations $L$.

A state $s = (l, v)$ consists of a location $l \in L$ and a valuation $v : V \to \mathbb{Z}$. A state $(l, v)$ is initial if $l = l_0$. We denote an evaluation step with transition $t = (\ell, \tau, \ell')$ by $(l, v) \xrightarrow{t} (l', v')$, where the valuations $v, v'$ satisfy the formula $\tau$ of $t$. We use $\rightarrow_P$ if we do not care about the executed transition, and $\rightarrow^*_P$ to denote the transitive-reflexive closure of $\rightarrow_P$. We say that a state $s$ is reachable if there exists an initial state $s_0$ such that $s_0 \rightarrow^*_P s$.

3) Safety and Invariants: An assertion $(\ell, \varphi)$ is a pair of a transition $t \in T$ and a formula $\varphi \in F(V)$. A program $P$ is safe for the assertion $(\ell, \varphi)$ if for every evaluation $(l_0, v_0) \xrightarrow{t_0 \cdots t_n} (l, v)$, we have $v \models \varphi$. Note that proving that a formula $\varphi$ always holds at a location $l$ can be handled in this setting by adding an extra location $l^*$ and an extra transition $t^* = (l, \text{true}, l^*)$ and checking safety for $(l^*, \varphi)$.

We call a map $I : L \to F(V)$ a program invariant (or often just invariant) if for all reachable states $(l, v)$, we have $v \models I(l)$. An important class of program invariants are inductive invariants. An invariant $I$ is inductive if the following conditions hold:

Initiation:  
\[ I(l_0) \models I(l_0) \]

Consequence:  
\[ (l, \tau, l') \in P : I(l) \land \tau \models I(l') \]

Footnotes:
3For $\varphi \in F(V)$, $\varphi' \in F(V')$ is the version of $\varphi$ using primed variables.

4Since we label transitions only with conjunctions of linear inequalities, disjunctive conditions are represented using several transitions with the same pre- and post-location. Thus, $P$ is actually a multigraph.

5Here, $\rightarrow^*_P \circ \rightarrow_1$ denotes arbitrary program evaluations that end with an evaluation step using $t$. 
4) Constraint Solving for Verification: Inductive invariants can be generated using a constraint-based approach [7], [8]. The idea is to consider templates for candidate invariant properties, such as (conjunctions of) linear inequalities. These templates contain both the program variables $V$ as well as template variables $V_T$, whose values have to be determined to ensure the required properties. To this end, the conditions on inductive invariants are expressed by means of constraints of the form $\exists V_T \cdot \forall V \ldots$. Any solution to these constraints then yields an invariant. In the case of linear arithmetic, Farkas’ Lemma [9] is often used to handle the quantifier alternation in the generated constraints. Intuitively, it allows one to transform $\exists V$ problems encountered in invariant synthesis into $\exists V_T$ problems. In the general case, an SMT problem over non-linear arithmetic is obtained, for which effective SMT solvers exist [10], [11].

By assigning weights to the different conditions, invariant generation can be cast as an optimization problem in the Max-SMT framework [5], [12].

IV. PROVING SAFETY

Most automated techniques for proving program safety iteratively construct inductive program invariants as over-approximations of the reachable state space. Starting from the known set of initial states, a process to discover more reachable states and refine the approximation is iterated, until it finally reaches a fixed point (i.e., the invariant is inductive) and is strong enough to imply program safety. However, this requires taking the whole program into account, which is sometimes infeasible or undesirable in practice.

In contrast to this, our method starts with the known unsafe states, and iteratively constructs an under-approximation of the set of safe states, with the goal of showing that all initial states are contained in that set. For this, we introduce the notion of conditional safety. Intuitively, when proving that a program is $(t, \varphi)$-conditionally safe for the assertion $(t, \varphi)$ we consider evaluations starting after a $\gamma_\ell (t, \bar{v})$ step, where $\bar{v}$ satisfies $\varphi$, instead of evaluations starting at an initial state. In particular, a program that is $(t_0, \top)$-conditionally safe for $(t, \varphi)$ for all initial transitions $t_0$ is (unconditionally) safe for $(t, \varphi)$.

**Definition 1** (Conditional safety). Let $P$ be a program, $t, \bar{t}$ transitions and $\varphi, \bar{\varphi} \in F(V)$. The program $P$ is $(t, \bar{t})$-conditionally safe for the assertion $(t, \varphi)$ if for any evaluation that contains $\gamma_\ell (t, \bar{v}) \rightarrow_{P} (t, \bar{v}) \rightarrow_{\varphi} (t, \bar{v})$, we have $\bar{v} \models \bar{\varphi}$ implies that $v \models \varphi$.

Conditional safety is “transitive” in the sense that if a set of transitions $E = \{t_1, \ldots, t_m\}$ dominates $t$, and for all $i = 1, \ldots, m$ we have $P$ is $(t_i, \bar{\varphi}_i)$-conditionally safe for $(t, \varphi)$ and $P$ is safe for $(t_i, \bar{\varphi}_i)$, then $P$ is also safe for $(t, \varphi)$. In what follows we exploit this observation to prove program safety by means of conditional safety.

A program component $C$ of a program $P$ is an SCC of the control-flow graph, and its entry transitions (or entries)

<table>
<thead>
<tr>
<th>while $i &gt; 0$ do</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x := x + 5$;</td>
</tr>
<tr>
<td>$i := i - 1$;</td>
</tr>
<tr>
<td>$\land x' = x$</td>
</tr>
<tr>
<td>$\land i' = i - 1$</td>
</tr>
</tbody>
</table>

$E_C$ are those transitions $t = (\ell, \tau, \ell')$ such that $t \notin C$ but $\ell'$ appears in $C$. By considering each component as a single node, we can obtain from $P$ a DAG of SCCs, whose edges are the entry transitions. Our technique analyzes components independently, and communicates the results of these analyses to other components along entry transitions.

Given a component $C$ and an assertion $(t, \varphi)$ such that $t \notin C$ but the source node of $t$ appears in $C$, we call $t$ an exit transition of $C$. For such exit transitions, we compute a sufficient condition $\psi_i$ for each entry transition $t \in E_C$ such that $C \cup \{t\}$ is $(t, \psi_i)$-conditionally safe for $(t, \varphi)$. Then we continue reasoning backwards following the DAG and try to prove that $P$ is safe for each $(t, \psi_i)$. If we succeed, following the argument above we will have proved $P$ safe for $(t, \varphi)$.

In the following, we first discuss how to prove conditional safety of single program components in Sect. IV-A, and then present the algorithm that combines these local analyses to construct a global safety proof in Sect. IV-B.

A. Synthesizing Local Conditions

Here we restrict ourselves to a program component $C$ and its entry transitions $E_C$, and assume we are given an assertion $(t_{\text{exit}}, \psi)$, where $t_{\text{exit}} = (\ell_{\text{exit}}, \bar{v}_{\text{exit}}, \ell_{\text{exit}})$ is an exit transition of $C$ (i.e., $t_{\text{exit}} \notin C$ and $\ell_{\text{exit}}$ appears in $C$). We show how a precondition $(t, \psi)$ for $(t_{\text{exit}}, \psi)$ can be obtained for each $t \in E_C$. Here we only consider the case of $\varphi$ being a single clause (i.e., a disjunction of literals); if $\varphi$ is in CNF, each conjunct is handled separately. The preconditions on the exit transitions will be determined by a conditional inductive invariant, which like a standard invariant is inductive, but not necessarily initiated in all program runs. Indeed, this initialization condition is what we will extract as precondition and propagate backwards to preceding program components in the DAG.

**Definition 2** (Conditional Inductive Invariant). We say a map $Q : L \rightarrow F(V)$ is a conditional (inductive) invariant for a program (component) $P$ if for all $(\ell, v) \rightarrow_{P} (t', \bar{v}')$, we have $v \models Q(\ell)$ implies $\bar{v}' \models Q(t')$.

Conditional invariants are convenient tools to express conditions for safety proving, allowing reasoning in the style of “if the condition for $Q$ holds, then the assertion $(t, \varphi)$ holds”.

**Example 1.** Consider the program snippet in Fig. 5. A conditional inductive invariant supporting safety of this program part is $Q_2(\ell_1) \equiv x + 5 \cdot i \geq 50$, $Q_2(\ell_2) \equiv x \geq 50$. In fact, any conditional invariant $Q_m(\ell_1) \equiv x + m \cdot i \geq 50$ with $0 \leq m \leq 5$...
would be a conditional inductive invariant that, together with the negation of the loop condition $i \leq 0$, implies $x \geq 50$.

We use a Max-SMT-based constraint-solving approach to generate conditional inductive invariants. Unlike in [5], to use information about the initialization of variables before a program component, we take into account the entry transitions $E_C$. The precondition for each entry transition is the conditional invariant that has been synthesized at its target location.

To find conditional invariants, we construct a constraint system. For each location $i \in C$ we create a template $I_{t,k}(V) \equiv \bigwedge_{1 \leq j \leq k} I_{t,j,k}(V)$ which is a conjunction of $k$ linear inequations of the form $I_{t,j,k}(V) \equiv t_{i,j} + \sum_{v \in V} t_{i,j,n}.v \leq 0$, where the $t_{i,j}$ are fresh variables from the set of template variables $V_T$. We then transform the conditions for a conditional invariant proving safety for the assertion $(t_{\text{exit}}, \varphi)$ to the constraints in Fig. 6. Here, e.g., $I_{t',k}$ refers to the variant of $I_{t,k}$ using primed versions of the program variables $V$, but unprimed template variables $V_T$.

In the overall constraint system, we mark the Conjunctions and Safety constraints as hard requirements. Thus, any solution to these constraints is a conditional inductive invariant implying our assertion. However, as we mark the Initiation constraints as soft, the found conditional invariants may depend on preconditions not implied by the direct context of the considered component. On the other hand, the Max-SMT solver prefers solutions that require fewer preconditions. Overall, we create the following Max-SMT formula

$$F_k \overset{df}{=} \bigwedge_{t \in C} \big( t_{i,j,k} \land \bigwedge_{t \in E_C, 1 \leq j \leq k} (t_{i,j,k} \lor \neg p_{i,j,k}) \land S_k \land \bigwedge_{t \in E_C, 1 \leq j \leq k} [p_{i,j,k}, \omega_j] \big)$$

where the $p_{i,j,k}$ are propositional variables which are true if the Initiation condition $I_{t,j,k}$ is satisfied, and $\omega_j$ is the corresponding weight.\footnote{We use $F_k$ in our procedure CondSafe in Alg. 1.}

Algorithm 1 Proc. CondSafe computing conditional invariant

Input: component $C$, entry transitions $E_C$, assertion $(t_{\text{exit}}, \varphi)$ such that $t_{\text{exit}}$ is an exit transition of $C$ and $\varphi$ is a clause

Output: None $|$ $Q$, where $Q$ maps locations in $C$ to conjunctions of inequations

1: $k \leftarrow 1$
2: repeat
3: construct formula $F_k$ from $C$, $E_C$ and $(t_{\text{exit}}, \varphi)$
4: $\sigma \leftarrow$ Max-SMT-solver($F_k$)
5: if $\sigma$ is a model then
6: $Q \leftarrow \{ \ell \mapsto \sigma(I_{t,k}) \mid \ell \text{ in } C \}$ return $Q$
7: $k \leftarrow k + 1$
8: until $k > \text{MAX_CONJUNCTS}$ return None

In CondSafe, we iteratively try “larger” templates of more conjuncts of linear inequations until we either give up (in our implementation, MAX_CONJUNCTS is 3) or finally find a conditional invariant. Note, however, that here we are only trying to prove safety for one clause at a time, which reduces the number of required conjuncts as compared to dealing with a whole CNF in a single step. If the Max-SMT solver is able to find a model for $F_k$, then we instantiate our invariant templates $I_{t,k}$ with the values found for the template variables in the model $\sigma$, obtaining a conditional invariant $Q$. When we obtain a result, for every entry transition $t = (\ell, \tau, t') \in E_C$ the conditional invariant $Q(t')$ is a precondition that implies safety for the assertion $(t_{\text{exit}}, \varphi)$. The following theorem states the correctness of this procedure.

Theorem 1. Let $C$ be a component, $E_C$ its entry transitions, and $(t_{\text{exit}}, \varphi)$ an assertion $t_{\text{exit}}$ an exit transition of $C$ and $\varphi$ a clause. If the procedure call CondSafe$(C, E_C, (t_{\text{exit}}, \varphi))$ returns $Q \neq \text{None}$, then $Q$ is a conditional inductive invariant for $C$ and $\varphi$ is a clause.

Proof. All proofs can be found in Appendix A. \hfill \Box

B. Propagating Local Conditions

In this section, we explain how to use the local procedure CondSafe to prove safety of a full program. To this end we now consider the full DAG of program components. As outlined above, the idea is to start from the assertion provided by the user, call the procedure CondSafe to obtain preconditions for the entry transitions of the corresponding component, and then use these preconditions as assertions for preceding components, continuing recursively. If eventually for each initial transition the transition relation implies the corresponding preconditions, then safety has been proven. If we fail to prove safety for certain assertions, we backtrack, trying further possible preconditions and conditional invariants.

The key to the precision of our approach is our treatment of failed proof attempts. When the procedure CondSafe finds a conditional invariant $Q$ for $C$, but proving $(t, Q(t'))$ as a postcondition of the preceding component fails for some $t = (\ell, \tau, t') \in E_C$, we use $Q$ to narrow our program representation and filter out evaluations that are already known to be safe.

As outlined above, in our proof process we treat each clause of the conjunction $Q(t')$ separately, and pass each one as its own assertion to preceding program components, allowing for a fine-grained program-narrowing technique. By construction of $Q$, evaluations that satisfy all literals of $Q(t')$ after executing $t = (\ell, \tau, t') \in E_C$ are safe. Thus, among the evaluations that use $t$, we only need to consider those where at least one literal in $Q(t')$ does not hold. Hence, we narrow each entry transition by conjoining it with the negation of the conjunction of all literals for which we could not prove safety (see line 13 in Alg. 2). Note that if there is more than one literal in this conjunction, then the negation is a disjunction, which in our program model implies splitting transitions.

We can narrow program components similarly. For a transition $t = (\ell, \tau, t') \in C$, we know that if either $Q(\ell)$ or $Q(t')'$ holds in an evaluation passing through $t$, the program
Algorithm 2 Procedure CheckSafe for proving a program safe for an assertion

Input: Program $\mathcal{P}$, a component $C$, entries $\mathcal{E}_C$, assertion $(t_{exit}, \varphi)$ s.t. $t_{exit}$ is an exit transition of $C$ and $\varphi$ a clause

Output: Safe | Maybe

1: Let $(t_{exit}, \tau, t'_{exit}) = t_{exit}$
2: if $(\tau \Rightarrow \varphi')$ then return Safe
3: else if $t_{exit} = \ell_0$ then return Maybe
4: $Q \leftarrow \text{CondSafe}(C, \mathcal{E}_C, (t_{exit}, \varphi))$
5: if $Q = \text{None}$ then return Maybe
6: for all $t = (\ell, \tau, t') \in \mathcal{E}_C$, $L \in Q(t')$ do
7: $\tilde{C} \leftarrow \text{component}(\ell, \mathcal{P})$
8: $\mathcal{E}_C \leftarrow \text{entries}(\tilde{C}, \mathcal{P})$
9: $\text{res}[t, L] \leftarrow \text{CheckSafe}(\mathcal{P}, \tilde{C}, \mathcal{E}_C, (t, L))$
10: if $\forall t = (\ell, \tau, t') \in \mathcal{E}_C$, $L \in Q(t')$. $\text{res}[t, L] = \text{Safe}$ then
11: return Safe
12: else
13: $\tilde{C} \leftarrow \{ (\ell, \tau \land \neg(\bigwedge_{L \in Q(t')} L'), t') \mid t = (\ell, \tau, t') \in \mathcal{E}_C \}$
14: $\tilde{C} \leftarrow \{ (\ell, \tau \land \neg(\neg(\bigwedge_{L \in Q(t')} L') \land \neg Q(t), t') \mid t = (\ell, \tau, t') \in \mathcal{E}_C \}$
15: return CheckSafe($\mathcal{P}, \tilde{C}, (t_{exit}, \varphi)$)

is safe. Thus, we narrow the program by replacing $\tau$ by $\tau \land \neg Q(\ell) \land \neg Q(\ell)'$ (see line 14 in Algo. 2).

This narrowing allows us to generate disjunctive conditional invariants, where each result of CondSafe is one disjunct. Note that not all disjunctive invariants can be discovered like this, as each intermediate result needs to be inductive using the disjuncts found so far. However, this is the pattern observed in phase-change algorithms [13].

Our overall safety proving procedure CheckSafe is shown in Algo. 2. The helper procedures component and entries are used to find the program component for a given location and the entry transitions for a component. The result of CheckSafe is either Maybe when the proof failed, or Safe if it succeeded. In the latter case, we have managed to create a chain of conditional invariants that imply that $(t_{exit}, \varphi)$ always holds.

Theorem 2. Let $\mathcal{P}$ be a program, $C$ a component and $\mathcal{E}_C$ its entries. Given an assertion $(t_{exit}, \varphi)$ such that $t_{exit}$ is an exit transition of $C$ and $\varphi$ is a clause, if CheckSafe($\mathcal{P}, \tilde{C}, \mathcal{E}_C, (t_{exit}, \varphi)$) = Safe, then $\mathcal{P}$ is safe for $(t_{exit}, \varphi)$.

Example 2. We demonstrate CheckSafe on the program displayed in Fig. 7, called $\mathcal{P}$ in the following, which is an extended version of the example from Fig. 3.

We want to prove the assertion $(t_5, x \neq y)$. Hence we make a first call CheckSafe($\mathcal{P}, \{t_3\}, \{t_4\}, (t_5, x \neq y)$): the non-trivial SCC containing $t_2$ is $\{t_1\}$ and its entry transitions are $\{t_3\}$. Hence, we call CondSafe($\{t_4\}, \{t_3\}, (t_5, x \neq y)$) and the resulting conditional invariant for $t_2$ is either $x < y$ or $y < x$. Let us assume it is $y < x$. In the next step, we propagate this to the predecessor SCC $\{t_2\}$, and call CheckSafe($\mathcal{P}, \{t_2\}, \{t_1\}, (t_3, y < x)$).

In turn, this leads to calling CondSafe($\{t_2\}, \{t_1\}, (t_3, y < x)$) to our synthesis subprocedure. No conditional invariant supporting this assertion can be found, and hence None is returned by CondSafe, and consequently Maybe is returned by CheckSafe. Hence, we return to the original SCC $\{t_4\}$ and its entry $\{t_3\}$, and then by narrowing we obtain two new transitions:

$t'_4 = (t_2, x' = x + 1 \land y' = y + 1 \land (y < x), t_2)$,
$t'_3 = (t_1, x < 0 \land x' = x \land y' = y \land (y < x), t_2)$

Using these, we call CheckSafe($\mathcal{P}, \{t'_3\}, \{t'_4\}, (t_5, x \neq y)$). The next call to CondSafe then yields the conditional invariant $x < y$ at $t_2$, which is in turn propagated backwards with the call CheckSafe($\mathcal{P}, \{t_2\}, \{t_1\}, (t'_4, x < y)$). This then yields a conditional invariant $x < y$ at $t_1$, which is finally propagated back in the call CheckSafe($\mathcal{P}, \{\}, \{t_1, x < y\}$), which directly returns Safe.

C. Improving Performance

The basic method CheckSafe can be extended in several ways to improve performance. We now present a number of techniques that are useful to reduce the runtime of the algorithm and distribute the required work. Note that none of these techniques influences the precision of the overall framework.

a) Using conditional invariants to disable transitions: When proving an assertion, it is often necessary to find invariants that show the unfeasibility of some transition, which allows disabling it. In our framework, the required invariants can be conditional as well. Therefore, CheckSafe must be called recursively to prove that the conditional invariant is indeed invariant. In our implementation, we generate constraints such that every solution provides conditional invariants either implying the postcondition or disabling some transition. By
imposing different weights, we make the Max-SMT solver prefer solutions that imply the postcondition.

b) Handling unsuccessful proof attempts: One important aspect is that the presented algorithm does not learn facts about the reachable state space, and so duplicates work when assertions appear several times. To alleviate this for unsuccessful recursive invocations of CheckSafe, we introduce a simple memoization technique to avoid repeating such calls. So when CheckSafe(P, C, E, (t, ϕ)) = Maybe, we store this result, and use it for all later calls of CheckSafe(P, C, E, (t, ϕ)). This strategy is valid as the return value Maybe indicates that our method cannot prove the assertion (t, ϕ) at all, meaning that later proof attempts will fail as well. In our implementation, this memoization of unsuccessful attempts is local to the initial call to CheckSafe. The rationale is that, when proving unrelated properties, it is likely that few calls are shared and that the book-keeping does not pay off.

c) Handling successful proof attempts: When a recursive call yields a successful result, we can strengthen the program with the proven invariant. Remember that CheckSafe(P, C, E, (t, ϕ)) = Safe means that whenever the transition t is used in any evaluation, ϕ holds in the succeeding state. Thus, we can add this knowledge explicitly and change the transition in the original program. In practice, this strengthening is applied only if the first call to CheckSafe was successful, i.e., no narrowing was applied. The reason is that, if the transition relation of t was obtained through repeated narrowing, in general one needs to split transitions, and it is not correct to just add ϕ′ to t. Namely, assume that t₀ = (ℓ, τ₀, ℓ′) is the original (unnarowed version of) a transition t = (ℓ, τ, ℓ′) ∈ E. As t is an entry transition of C, we have τ = τ₀ ∧ ¬ψ₁ ∧ . . . ∧ ¬ψₘ by construction, where ψᵢ is the additional constraint we added in the i-th narrowing of component entries. Thus what we proved is that ψ₁ ∨ . . . ∨ ψₘ ∨ ϕ′ always holds after using transition t₀. So we should replace t₀ in the program with a transition labeled with τ₀ ∧ (ψ₁ ∨ . . . ∨ ψₘ ∨ ϕ′). As we cannot handle disjunctions natively, this implies replacing t₀ by m + 1 new transitions.

Note that this program modification approach, unlike memoization, makes the gained information available to the Max-SMT solver when searching for a conditional invariant. A similar strategy can be used to strengthen the transitions in the considered component C.

d) Parallelizing & distributing the analysis: Our analysis can easily be parallelized. We have implemented this at two stages. First, at the level of the procedure CondSafe, we try at the same time different numbers of template conjuncts (lines 3-6 in Alg. 1), which requires calling several instances of the solver simultaneously. Secondly, at a higher level, the recursive calls of CheckSafe (line 9 in Alg. 2) are parallelized. Note that, since narrowing and the “learning” optimizations described above are considered only locally, they can be handled as asynchronous updates to the program kept in each worker, and do not require synchronization operations. Hence, distributing the analysis onto several worker processes, in the style of Bolt [4], would be possible as well.

Other directions for parallelization, which have not been implemented yet, are to return different conditional invariants in parallel when the Max-SMT problem in procedure CondSafe has several solutions. Moreover, based on experimental observations that successful safety proofs have a short successful path in the tree of proof attempts, we are also interested in exploring a look-ahead strategy: after calling CondSafe in CheckSafe, we could make recursive calls of CheckSafe on some processes while others are already applying narrowing.

e) Iterative proving: Finally, one could store the conditional invariants generated during a successful proof, which are hence invariants, so that they can be re-used in later runs. E.g., if a single component is modified, one can reprocess it and compute a new precondition that ensures its postcondition. If this precondition is implied by the previously computed invariant, the program is safe and nothing else needs to be done. Otherwise, one can proceed with the preceding components, and produce respective new preconditions in a recursive way. Only when proving safety with the previously computed invariants in this way fails, the whole program needs to be reprocessed again. This technique has not been implemented yet, as our prototype is still in a preliminary state.

V. RELATED WORK

Safety proving is an active area of research. In the recent past, techniques based on variations of counterexample guided abstraction refinement have dominated [14]–[23]. These methods prove safety by repeatedly unfolding the program relation using a symbolic representation of program states, starting in the initial states. This process generates an over-approximation of the set of reachable states, where the coarseness of the approximation is a consequence of the used symbolic representation. Whenever a state in the over-approximation violates the safety condition, either a true counterexample was found and is reported, or the approximation is refined (using techniques such as predicate abstraction [24] or Craig interpolation [25]). When further unwinding does not change the symbolic representation, all reachable states have been found and the procedure terminates. This can be understood as a “top-down” approach (starting from the initial states), whereas our method is “bottom-up” (starting from assertions).

Techniques based on Abstract Interpretation [26] have had substantial success in the industrial setting. There, an abstract interpreter is instantiated by an abstract domain whose elements are used to over-approximate sets of program states. The interpreter then evaluates the program on the chosen abstract domain, discovering reachable states. A widening operator, combining two given over-approximations to a more general one representing both, is employed to guarantee termination of the analysis when handling loops.

“Bottom-up” safety proving with preconditions found by abduction has been investigated in [27]. This work is closest to ours in its overall approach, but uses fundamentally different techniques to find preconditions. Instead of applying Max-SMT, the approach uses an abduction engine based on maximal universal subsets and quantifier elimination in Presburger
were performed on an Intel i5 2.6 GHz CPU with 8 Gb of memory. The time limit is 300 seconds. The benchmarks and our tool can be found at http://www.cs.upc.edu/~albert/VeryMax.html.

VII. Conclusion

We have presented a novel approach to compositional safety verification. Our main contribution is a proof framework that refines intermediate results produced by a Max-SMT-based precondition synthesis procedure. In contrast to most earlier work, we proceed bottom-up to compute summaries of code that are guaranteed to be relevant for the proof.

We plan to further extend VeryMax to cover more program features and include standard optimizations (e.g., slicing and constraint propagation with simple abstract domains). It currently handles procedure calls by inlining, and does not support recursive functions yet. We plan to deal with such cases similarly to loops, by introducing templates for function pre/postconditions.

In the future, we are interested in experimenting with alternative precondition synthesis methods (e.g., abduction-based ones). We also want to combine our method with a Max-SMT-based termination proving method [12] and extend it to existential properties such as reachability and non-termination [5]. We expect to combine all of these techniques in an alternating procedure [1] that tries to prove properties at the same time as their duals, and which uses partial proofs to narrow the state space that remains to be considered. Eventually,
these methods could be combined to verify arbitrary temporal properties. In another direction, we want to consider more expressive theories to model program features such as arrays or the heap.

REFERENCES


We will show that our narrowing preserves unsafe evaluations. With which are (modulo renaming) also discussed in [8].

CheckSafe Then, as the recursive call of via induction over the length of evaluations. Assume that there and our induction hypothesis, we know that the program prove that our program narrowing is indeed correct. Assume this then implies that the program is safe for \( (l_{m-1}, v_m) \) is safe for \( (l_m, v_m) \) and \( v_n \) \( \not\in \varphi \).

Proof of Thm. 1. We prove the proposition by induction over the number \( u \) of recursive calls of CheckSafe.

In the base case \( u = 0 \), we have that \( \tau_{\text{exit}} \Rightarrow \varphi' \), i.e., the condition to prove is always a consequence of using the transition \( t_{\text{exit}} \), and the claim trivially holds.

Let now \( u > 0 \), and we assume that the proposition has been shown for all calls of CheckSafe that return \( \text{Safe} \) and need at most \( u - 1 \) recursive calls of CheckSafe.

We now consider a program evaluation

\[
(\ell_0, v_0) \to t_{\text{exit}} \to t_{m-1} (\ell_m, v_m) \to t_m \to t_n (\ell_n, v_n)
\]

with \( t_{m-1} \in E_C \) and \( t_n = t_{\text{exit}} \).

First, we consider the case that CheckSafe returns \( \text{Safe} \) in line 11, where all preconditions are satisfied for all entry transitions. By the condition \( \forall L \in Q(l_m) \hspace{1em} \text{res}[t_{m-1}, L] = \text{Safe} \) and our induction hypothesis, we know that the program is safe for \( (l_{m-1}, Q(l_m)) \). By construction of \( Q \) and Thm. 1, this then implies that the program is safe for \( (t_{\text{exit}}, \varphi) \).

The second case is returning the result of CheckSafe on the narrowed program in lines 19 and 20. For this, we need to prove that our program narrowing is indeed correct. Assume now that the considered evaluation is unsafe, i.e., that \( v_n \not\in \varphi \).

We will show that our narrowing preserves unsafe evaluations. Then, as the recursive call of CheckSafe (with recursion depth \( u - 1 \)) is correct by our induction hypothesis, we can conclude that \( \text{Safe} \) is only returned if there are no unsafe evaluations.

We first consider the narrowing \( \hat{C} \). By our induction hypothesis, we know that \( v_m \models (t_{m-1}, t_{\text{exit}}) = \text{Safe} \) holds. Now assume that the narrowed version of \( t_{m-1} \) is not enabled anymore because of the added condition. Then \( v_m \not\models \neg(t_{m-1}, t_{\text{exit}}) \models \text{Maybe} \) holds, and thus \( v_m \models Q(t_m) \). But then, our evaluation is safe (by the same argument as in the proof of Thm. 1), contradicting our assumption that the considered evaluation is unsafe. Thus, unsafe evaluations are not broken by our narrowing of entry transitions.

Similarly, we now consider the narrowing \( \hat{C} \). We consider an evaluation step \( (\ell_w, v_w) \to t_w (\ell_{w+1}, v_{w+1}) \) with \( t_w \in \hat{C} \). If the narrowed version \( t_w \in \hat{C} \) of \( t_w \) cannot be used, then either \( v_w \models Q(t_w) \) or \( v_{w+1} \models Q(t_{w+1}) \), and again, by an argument similar to the proof of Thm. 1, this contradicts the assumption that our evaluation is unsafe. Thus, unsafe evaluations are preserved by narrowing of the program component.

\( \square \)