

Precondition Inference via Partitioning of Initial States

Bishoksan Kaffle¹, Graeme Gange², Peter Schachte¹,
Harald Søndergaard¹, and Peter J. Stuckey²

¹ The University of Melbourne

² Monash university

Abstract. Precondition inference is a non-trivial task with several applications in program analysis and verification. We present a novel iterative method for automatically deriving sufficient preconditions for safety and unsafety of programs which introduces a new dimension of modularity. Each iteration maintains over-approximations of the set of *safe* and *unsafe initial* states. Then we repeatedly use the current abstractions to partition the program’s *initial* states into those known to be safe, known to be unsafe and unknown, and construct a revised program focusing on those initial states that are not yet known to be safe or unsafe. An experimental evaluation of the method on a set of software verification benchmarks shows that it can solve problems which are not solvable using previous methods.

1 Introduction

Precondition analysis infers conditions (on the initial states of a program) that establish runtime properties of interest. For example, a *sufficient* precondition for safety is a set of initial states, each of which is guaranteed to be safe with respect to given safety properties (assertions). Preconditions have several important applications and shed light on the following questions: (i) which inputs ensure safe program execution? (program analysis); (ii) which inputs can or cannot cause an error? (program debugging); (iii) what are the valid inputs for a program? (program understanding); and (iv) which library functions need to be modified to ensure valid outputs? (program specialisation).

However, the problem is undecidable in general, hence approaches to finding preconditions use approximations. Preconditions derived by over-approximations are usually too weak, while under-approximations are usually too strong to be useful in practice. Unfortunately, for reasons of computability, we cannot hope to obtain an exact (optimal) precondition (though such preconditions enable their re-use, for example, under different calling contexts), so we must instead look for a (weaker) precondition that is useful. This work builds upon the transformation-guided framework of Kaffle et al. [23]. Additionally, we model the set of safe terminating states so that we can iteratively refine the approximations of the set of safe states as well (as in [23]). We also partition initial states guided by the over-approximations of the safe and unsafe states to derive more precise sufficient

<pre> int main(int a, int b) { while (a ≥ 1) { a = a - 1; b = b - 1; } assert (b ≥ 0); } </pre>	<pre> c₁. init(A, B). c₂. wh(A, B) ← init(A, B). c₃. wh(A, B) ← A₀ ≥ 1, A = A₀ - 1, B = B₀ - 1, wh(A₀, B₀). c₄. unsafe ← A < 1, B < 0, wh(A, B). c₅. safe ← A < 1, B ≥ 0, wh(A, B). </pre>
----------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Fig. 1: Running example: (left) original program, (right) translation to CHCs

preconditions, and in some cases precise necessary and sufficient preconditions (optimal).

We use constrained Horn clauses (CHCs) to encode the computation of C programs. CHCs can conveniently be used to represent big- and small-step semantics, transition systems, imperative programs and other models of computation. The use of CHCs allows decoupling programming language syntax and semantics from the analysis. We use two special predicates, **safe** and **unsafe** respectively to encode the set of safe and the set of unsafe (error) states. A safe state is reached in all paths without error (return statements are encoded by **safe** predicate). The predicate **init** encodes the set of initial states. We assume that the users specify all the states of interest by an appropriate construct provided by the language (for example, *assert(c)*, *return ⟨n⟩* of the C language). States not specified by the user (for example, *buffer-overflow*, *floating point exceptions*) are not taken into account while generating CHCs. Hence the correctness of the preconditions depends on the user specified set of states.

Running example. Before formally presenting our approach, we illustrate the main steps via the example program in Figure 1. The left side shows a C program fragment, and the right its CHC representation, encoding the reachable states of the computation. Program variables in C are represented by logical variables (Prolog style capital letters) in CHC. The clause c_1 specifies the initial states of the program via the predicate *init* which is always reachable. Similarly, the clauses c_2 and c_3 encode the reachability of the *while* loop via the predicate *wh*. c_2 states that the loop is reachable if *init* is reachable while c_3 states that the loop is reachable if it is already in the loop and the loop guard is satisfied (recursive case). The first three clauses on the right define the behaviour of the program in Figure 1 (left) and the last two clauses represent the properties of the program. The clause c_4 states that an “unsafe” state is reached if $B < 0$ after exiting the loop whereas the clause c_5 states that the program terminates gracefully if $B \geq 0$. Note that the semantics of *assert(c)* is *if(c) SKIP else ERROR*. CHCs can be obtained from an imperative program using various approaches [27,14,16,10]. Henceforth whenever we refer to a program, we refer to its CHC representation.

Observe that the assertion is violated if the initial conditions on a and b entail $(b < 0 \wedge a \leq 0) \vee (a \geq 1 \wedge a > b)$, and the program terminates gracefully if $(b \geq 0 \wedge a \leq 0) \vee (a \geq 1 \wedge b \geq a)$. Automatic derivation of these preconditions is challenging for the following reasons: (i) the desired result is a disjunction of

linear constraints—so we need a domain that can express disjunctions; (ii) information has to be propagated forwards and backwards because we lose information on b and a in the forward and in the backward direction respectively; (iii) we need to reason simultaneously about the safe and unsafe states; one cannot simply be obtained by complementing the other. Existing methods [18,2,26,25,23] cannot infer the desired preconditions.

Let φ_s^N and φ_u^N represent the over-approximations of safe and unsafe initial states, that is, necessary preconditions (NPs) for safety and unsafety, respectively. From the program in Figure 1, we get $\varphi_s^N = \varphi_u^N = \text{true}$ (the set of initial states). Thus the sufficient preconditions (SPs) for: (i) safety $\varphi_s^S = \varphi_s^N \wedge \neg\varphi_u^N$ and (ii) unsafety $\varphi_u^S = \varphi_u^N \wedge \neg\varphi_s^N$ are both *false*. These SPs, although valid, are uninteresting. So, we transform the program with respect to the predicates **safe** and **unsafe** using CHC transformations described in Section 3 (with the aim of strengthening NPs) and derive $\varphi_s^N \equiv (B \geq 0 \wedge A \leq 0) \vee (A \geq 1 \wedge B \geq 0) \equiv B \geq 0$ and $\varphi_u^N \equiv (B < 0 \wedge A \leq 0) \vee A \geq 1 \equiv B \leq 0 \vee A \geq 1$ from the resulting programs. The SPs from this iteration are $\varphi_s^S \equiv B \geq 0 \wedge A \leq 0$ and $\varphi_u^S \equiv B < 0$. These NPs are more precise than the one obtained in the previous step. However further refinement is possible since the NPs for safety and unsafety overlap, that is, $\varphi_s^N \wedge \varphi_u^N = B \geq 0 \wedge A \geq 1$ is *satisfiable*. Since the formulae $\varphi_s^N \wedge \neg\varphi_u^N$ and $\varphi_u^N \wedge \neg\varphi_s^N$ are already proven to be *safe* and *unsafe* initial states respectively, we can focus our attention on $\varphi_s^N \wedge \varphi_u^N$, which is yet to be classified as *safe* or *unsafe*. To perform further classification, we constrain the initial states of the program in Figure 1 to $B \geq 0 \wedge A \geq 1$ and restart the analysis by specialising the programs with respect to **safe** and **unsafe**. As a result, we derive $\varphi_s^N \equiv (B \geq A \wedge A \geq 1)$ and $\varphi_u^N \equiv (B \geq 0 \wedge A > B)$ as NPs. Since $\varphi_s^N \wedge \varphi_u^N \equiv \text{false}$, the preconditions are optimal (they are both sufficient and necessary for the validity of assertions) and the algorithm terminates. The final SPs are given (as the disjunction of SPs over the iterations) as follows (after simplifications):

$$\varphi_s^S \equiv (B \geq 0 \wedge A \leq 0) \vee (B \geq A \wedge A \geq 1). \quad \varphi_u^S \equiv B < 0 \vee (B \geq 0 \wedge A > B).$$

The key contributions of the paper are as follows.

- We extend the transformation-guided framework of Kafle et al. [23] which can now be used to derive SPs not only for safety but also for unsafety using over-approximation techniques. This is enabled by the encoding of the *safe* set of states together with the *unsafe* set of states and their simultaneous over-approximations. It also allows detecting optimality as well as controlling precision of the derived preconditions. In addition, it allows us to derive precondition for non-termination.
- We partition the initial states of the program (guided by over-approximations) into those known to be safe, known to be unsafe, and whose safety are unknown. This enables us to reason incrementally on the new partition that is yet to be proven safe or unsafe. The precondition for the original program can then be derived by composing preconditions of each partitions.

Paper outline. After preliminaries in Section 2, we describe preconditions, CHC transformations and their relationships in Section 3. Section 4 presents our algorithm for precondition inference, and Section 5 is an account of experimental evaluation. Section 6 places the work in context and Section 7 concludes.

2 Preliminaries

An atomic formula (simply *atom*), is a formula $p(\mathbf{x})$ where p is a predicate symbol and \mathbf{x} a tuple of arguments. A constrained Horn clause (CHC) is a first-order formula written as $p_0(\mathbf{x}_0) \leftarrow \varphi, p_1(\mathbf{x}_1), \dots, p_k(\mathbf{x}_k)$ following Constraint Logic Programming (CLP) standard, where φ is a finite conjunction of quantifier-free *constraints* on variables \mathbf{x}_i with respect to some constraint theory \mathbb{T} , $p_i(\mathbf{x}_i)$ are atoms and $p_0(\mathbf{x}_0)$ and $\varphi, p_1(\mathbf{x}_1), \dots, p_k(\mathbf{x}_k)$ are respectively called the *head* and the *body* of the clause.

In textual form, we use Prolog-like syntax and typewriter font, with capital letters for variable names and linear arithmetic constraints. A *constrained fact* is a clause of the form $p_0(\mathbf{x}_0) \leftarrow \varphi$, where $\varphi \in \mathbb{T}$. A clause of the form $\text{unsafe} \leftarrow \dots$ is called an *integrity constraint* where the predicate `unsafe` is always interpreted as *false*. A set of CHCs is usually called a program.

CHC semantics. The semantics of CHCs is derived from the semantics of predicate logic. An *interpretation* assigns to each predicate a relation over the domain of the constraint theory \mathbb{T} . An interpretation that satisfies each clause in the set is called a model of a set of CHCs. Note that the set of CHCs without any *integrity constraint* always has a model (an interpretation that assigns *true* to each atom on the head of a clause). When modelling safety properties of systems using CHCs, we also refer to CHCs as being *safe* or *unsafe* when they have a model, or do not have a model, respectively. We assume that the theory \mathbb{T} is equipped with a decision procedure and a projection operator, and that it is closed under negation. We use notation $\varphi|_V$ to represent the constraint formula φ projected onto variables V .

Definition 1 (AND-tree or derivation tree, adapted from [13]). *An AND-tree for a set of CHCs is a labelled tree whose nodes are labelled as follows.*

1. *each non-leaf node corresponds to a clause (with variables suitably renamed) of the form $A \leftarrow \varphi, A_1, \dots, A_k$ and is labelled by an atom A, φ , and has children labelled by A_1, \dots, A_k ,*
2. *each leaf node corresponds to a clause of the form $A \leftarrow \varphi$ (with variables suitably renamed) and is labelled by an atom A and φ , and*

Given a derivation tree t , $\text{constr}(t)$ represents the conjunction of its constraints. The tree t is *feasible* if and only if $\text{constr}(t)$ is satisfiable over \mathbb{T} .

Definition 2 (Initial clauses and nodes). *Let P be a set of CHCs, with a distinguished predicate p^I in P which we call the initial predicate. The constrained facts $\{(p^I(\mathbf{x}) \leftarrow \theta) \mid (p^I(\mathbf{x}) \leftarrow \theta) \in P \text{ and } \theta \in \mathbb{T}\}$ are called the initial*

clauses of P . Let t be an AND-tree for P . A node labelled by $p^I(\mathbf{x}) \leftarrow \theta$ is an initial node of t . We extend the term “initial predicate” and use the symbol p^I to refer also to renamed versions of the initial predicate that arise during clause transformations.

3 Preconditions and CHC transformations

We limit our attention to the sets of clauses for which every derivation tree for **safe** and **unsafe** (whether feasible or infeasible) has at least one initial node.

Definition 3 (Transforming CHCs by replacing initial states). Let P be a set of CHCs and φ be a constraint over \mathbb{T} . Let P' be the set of clauses obtained from P by replacing the initial clauses $\{(p^I(\mathbf{x}) \leftarrow \theta_i) \mid 1 \leq i \leq k\}$ by $\{(p^I(\mathbf{x}) \leftarrow \varphi)\}$. This operation is denoted by $\text{init_replace}(P, \varphi)$.

Definition 4 (NP and SP for safety). Let P be a set of CHCs and φ be a constraint over \mathbb{T} . Then

- φ is an NP for safety of P ($\varphi_s^N(P)$) if $P \vdash_{\mathbb{T}} \text{safe}$ entails $\text{init_replace}(P, \varphi) \vdash_{\mathbb{T}} \text{safe}$. In other words, φ (possibly true) is an over-approximation of the set of initial states of P that can reach **safe**.
- φ is an SP for safety of P ($\varphi_s^S(P)$) if $\text{init_replace}(P, \varphi) \not\vdash_{\mathbb{T}} \text{unsafe}$. In other words, φ (possibly false) represents an under-approximation of the set of initial states of P that cannot reach **unsafe**.

Thus an SP for safety is a constraint that is sufficient to block derivations of **unsafe** (given that we assume clauses for which p^I is essential for any derivation of **unsafe**). However in practice, we would like to consider SP for safety as a constraint that is sufficient to allow derivations of **safe** and block derivations of **unsafe**. Analogously, we can define both NP ($\varphi_u^N(P)$) and SP ($\varphi_u^S(P)$) for unsafety. In the following, we show how an NP and an SP can be derived from a set of clauses.

Lemma 1 (NP extracted from clauses). Let P be a set of clauses encoding reachable states of a program. Then the formula $\varphi_s^N(P) = \bigvee \{\theta \mid (p^I(\mathbf{x}) \leftarrow \theta) \in P\}$ is an NP for safety.

Proof (sketch). Let $P' = \text{init_replace}(P, \varphi_s^N(P))$. To show: $P \vdash_{\mathbb{T}} \text{safe}$ entails $P' \vdash_{\mathbb{T}} \text{safe}$.

Let $P \vdash_{\mathbb{T}} \text{safe}$. Then there exists a derivation tree t rooted at **safe** such that $\text{constr}(t)$ is satisfiable in \mathbb{T} . From our assumption, t uses some initial nodes at its leaves. Since all constraints from initial nodes of P are in $\varphi_s^N(P)$ and are used in constructing initial clauses of P' , t is a feasible derivation of P' as well. Then we have $P' \vdash_{\mathbb{T}} \text{safe}$. \square

An NP for unsafety can be obtained analogously. Given NPs, we can compute *sufficient preconditions* for safety and unsafety as follows. $\varphi_s^S(P) = \varphi_s^N(P) \wedge$

$\neg\varphi_u^N(P)$ and similarly $\varphi_u^S(P) = \varphi_u^N(P) \wedge \neg\varphi_s^N(P)$. A precondition is *optimal* if $\varphi_s^N(P) \wedge \varphi_u^N(P)$ is *unsatisfiable*. Then we have $\varphi_s^S(P) = \varphi_s^N(P)$, that is, the necessary and the sufficient conditions are the same for the validity of the assertion. Next, we show how a given set of SPs can be combined to derive a new SPs for a program.

Proposition 1 (Composing Preconditions). *Let $\varphi_1, \varphi_2, \dots$ be a (possibly infinite) set of formulas such that each φ_i is an SP for (un)safety of P . Then their disjunction $\bigvee_i \varphi_i$ is also an SP for (un)safety of P .*

Proof (sketch). Consider the case for safety, that is, each φ_i ($i = 1, 2, \dots$) is an SP for safety of P . Let $P'_i = \text{init_replace}(P, \varphi_i)$. For each φ_i , we have $P'_i \not\vdash_{\mathbb{T}} \text{unsafe}$. That is, *unsafe* is not derivable from any of P'_i . Let $P' = \text{init_replace}(P, \bigvee_i \varphi_i)$. The initial clauses of P' are the union of all the initial clauses of each P'_i while the rest of the clauses are the same. From our assumption, any derivation of *unsafe* need to use at least one of the initial clauses, our hypothesis under this condition ensures that such a derivation either does not exist or is infeasible. Then obviously, *unsafe* is not derivable from P' . The proof for unsafety can be done analogously. \square

Next, we present a special kind of under-approximation of CHCs by restricting their initial states which is useful in partitioning the set of CHCs. We say a set of CHCs P' is an under-approximation of P if for an atom A , we have $P' \vdash_{\mathbb{T}} A$ entails $P \vdash_{\mathbb{T}} A$ (the reverse is not necessarily true).

Definition 5 (Under-approximating CHCs by restricting initial states). *Let P be a set of CHCs and φ be a constraint over \mathbb{T} . Let P' be the set of clauses obtained from P by replacing the initial clauses $\{(p^I(\mathbf{x}) \leftarrow \theta_i) \mid 1 \leq i \leq k\}$ by $\{(p^I(\mathbf{x}) \leftarrow \theta_i \wedge \varphi) \mid 1 \leq i \leq k\}$. This operation is denoted by $\text{u_approximate}(P, \varphi)$.*

Proposition 2. *Let P be a set of CHCs, φ be any constraint over \mathbb{T} and $P' = \text{u_approximate}(P, \varphi)$. Then P' is an under-approximation of P .*

Proof (sketch). This is obvious since P' is initial clauses restricted version of P . \square

Note that $\text{u_approximate}(P, \varphi)$ only restricts the initial clauses of P while keeping others intact. Then Definition 4 implies that an SP of $\text{u_approximate}(P, \varphi)$ is also an SP of P . Formally,

Proposition 3. *Let P be a set of CHCs, φ be any constraint over \mathbb{T} and $P' = \text{u_approximate}(P, \varphi)$. Let ψ be an SP for (un)safety of P' then ψ is also a SP for (un)safety of P .*

Proof (sketch). Consider the case for safety. Let ψ be an SP for safety of P' . Since P and P' differ only in the set of initial clauses, both the constructions $\text{init_replace}(P, \varphi)$ and $\text{init_replace}(P', \varphi)$ yield the same set of clauses. So ψ is an SP for safety of P as well. The proof for the case of unsafety can be done analogously. \square

<pre> unsafe ← B < 0, A ≤ 0, wh_2(A, B). wh_2(A, B) ← B < 0, A ≤ 0, init_2(A, B). wh_2(A, B) ← B < 0, A = 0, C = 1, B - D = -1, wh_1(C, D). wh_1(A, B) ← A ≥ 1, init_1(A, B). wh_1(A, B) ← A ≥ 1, A - C = -1, B - D = -1, wh_1(C, D). init_1(A, B) ← A ≥ 1. init_2(A, B) ← A ≤ 0, B ≥ 0. </pre>	<pre> safe ← B ≥ 0, A ≤ 0, wh_2(A, B). wh_2(A, B) ← B ≥ 0, A ≤ 0, init_2(A, B). wh_2(A, B) ← B ≥ 0, A = 0, C = 1, B - D = -1, wh_1(C, D). wh_1(A, B) ← A ≥ 1, B ≥ 0, init_1(A, B). wh_1(A, B) ← B ≥ 0, A ≥ 1, A - C = -1, B - D = -1, wh_1(C, D). init_1(A, B) ← A ≥ 1, B ≥ 0. init_2(A, B) ← B ≥ 0, A ≤ 0. </pre>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Fig. 2: Partially evaluated programs: wrt **unsafe** (left) and wrt **safe** (right).

We now present some CHC transformations, taken from the literature on CLP and Horn clause verification. These are well known transformations and we refer to [23] for details.

Partial Evaluation (PE). Partial evaluation [20] with respect to a goal specialises a program for the given goal; preserving only those derivations that are relevant for deriving the goal. PE algorithm we apply here [12,23] produces a polyvariant specialisation, that is, a finite number of versions of each predicate, which is essential for deriving disjunctive information.

The result of applying PE to the example program in Figure 1 with respect to **unsafe** and **safe** is shown in Figure 2. The algorithm is a bit involved, so we do not provide details here and ask the readers to refer to [23]. However a key point to note is that due to polyvariant specialisation the predicates *init* and *wh* are split, leading to a more precise approximations as shown below. But all the feasible derivations of **safe** and **unsafe** are preserved. We derive the following NPs from these programs:

$$\begin{aligned}\varphi_s^N &\equiv (B \geq 0 \wedge A \leq 0) \vee (A \geq 1 \wedge B \geq 0) \equiv B \geq 0. \\ \varphi_u^N &\equiv (B < 0 \wedge A \leq 0) \vee A \geq 1 \equiv B < 0 \vee A \geq 1.\end{aligned}$$

Constraint Specialisation (CS) [21]. CS strengthens constraints in the clauses, while preserving derivations of a given atom (goal). The transformation prunes those paths that are not relevant for deriving the given atom. Next we explain the transformation with an example.

Figure 3 (left) shows an example program and Figure 3 (right) its constraint specialised version preserving the derivation of **unsafe**. The strengthened constraints are obtained by recursively propagating $B \geq A$ top-down from the goal **unsafe** and $A = 1, B = 1$ bottom-up from the constrained fact. An invariant $A \geq B, B \geq 0$ for the recursive predicate $p(A, B)$ in derivations of **unsafe** is computed and conjoined to each call to p in the clauses (underlined in the clauses in Figure 4 (right)).

The result of applying CS to the program in Figure 2 (left) with respect to **unsafe** and Figure 2 (right) with respect to **safe** is shown in Figure 4. Then we derive the following NPs: $\varphi_s^N \equiv (B \geq 0 \wedge A \leq 0) \vee (A \geq 1 \wedge B \geq A)$ and $\varphi_u^N \equiv$

$\begin{aligned} &\text{unsafe} \leftarrow B > A, p(A, B). \\ &p(A + B, B + 1) \leftarrow p(A, B). \\ &p(A, B) \leftarrow A = 1, B = 0. \end{aligned}$	$\begin{aligned} &\text{unsafe} \leftarrow B > A, \underline{B \geq 0}, \underline{A \geq B}, p(A, B). \\ &p(A + B, B + 1) \leftarrow \underline{B \geq 0}, \underline{A \geq B}, p(A, B). \\ &p(A, B) \leftarrow A = 1, B = 0, \underline{B \geq 0}, \underline{A \geq B}. \end{aligned}$
--------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Fig. 3: Example program (left) and its constraint specialised version preserving the derivation of `unsafe` (right).

$(B < 0 \wedge A \leq 0) \vee (A \geq 1 \wedge A > B)$. Since $\varphi_s^N \wedge \varphi_u^N$ is *unsatisfiable*, these preconditions are optimal.

Trace Elimination (TE). TE is a program transformation that eliminates an AND-tree of P from P while preserving the rest of its AND-trees. We illustrate the transformation via the program in Figure 5. The program on the right is the result of eliminating the AND-tree $c_1 - c_3$ from the program on the left. Note that the elimination has caused splitting of the predicate p so that the same AND-tree is no longer possible to construct while the rest of the AND-trees are preserved. In summary, the method consists of representing the program and the trace as finite tree automata, removing the trace using automata difference construction and reconstructing a program from the result as detailed in [22].

$\begin{aligned} &c_1. \text{unsafe} \leftarrow B > A, p(A, B). \\ &c_2. p(A + B, B + 1) \leftarrow p(A, B). \\ &c_3. p(A, B) \leftarrow A = 1, B = 0. \end{aligned}$	$\begin{aligned} &\text{unsafe} \leftarrow B > A, p_1(A, B). \\ &p_1(A + B, B + 1) \leftarrow p(A, B). \\ &p(A + B, B + 1) \leftarrow p(A, B). \\ &p(A, B) \leftarrow A = 1, B = 0. \end{aligned}$
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Fig. 5: A program (left) and its version after removing the trace $c_1 - c_3$ (right).

TE is a useful transformation since it can act as a refinement or problem decomposition as we shall see later. Furthermore, the splitting of the predicates can help derive disjunctive information. While the elimination of infeasible trees does not have any effect on preconditions, extra care must be taken while eliminating feasible ones. Lemma 2 allows us to derive a safe precondition in this case. To be consistent with the rest of the transformations, we can define TE which takes a program P and an atom A and searches for a derivation of P rooted at A and eliminates it if any.

$\begin{aligned} &\text{unsafe} \leftarrow B \leq 0, A < 0, \text{wh_2}(B, A). \\ &\text{wh_2}(A, B) \leftarrow B < 0, A \leq 0, \text{init_2}(A, B). \\ &\text{wh_2}(A, B) \leftarrow B < 0, A = 0, C = 1, \\ &\quad B - D = -1, \text{wh_1}(C, D). \\ &\text{wh_1}(A, B) \leftarrow A > B, A \geq 1, \text{init_1}(A, B). \\ &\text{wh_1}(A, B) \leftarrow A > B, A \geq 1, A - C = -1, \\ &\quad B - D = -1, \text{wh_1}(C, D). \\ &\text{init_1}(A, B) \leftarrow A > B, A \geq 1. \\ &\text{init_2}(A, B) \leftarrow B < 0, A \leq 0. \end{aligned}$	$\begin{aligned} &\text{safe} \leftarrow B \geq 0, A \leq 0, \text{wh_2}(A, B). \\ &\text{wh_2}(A, B) \leftarrow B \geq 0, A \leq 0, \text{init_2}(A, B). \\ &\text{wh_2}(A, B) \leftarrow B \geq 0, A = 0, C = 1, \\ &\quad B - D = -1, \text{wh_1}(C, D). \\ &\text{wh_1}(A, B) \leftarrow A \geq 1, B \geq A, \text{init_1}(A, B). \\ &\text{wh_1}(A, B) \leftarrow B \geq 0, A \geq 1, A - C = -1, \\ &\quad B - D = -1, \text{wh_1}(C, D). \\ &\text{init_1}(A, B) \leftarrow A \geq 1, B \geq A. \\ &\text{init_2}(A, B) \leftarrow B \geq 0, A \leq 0. \end{aligned}$
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Fig. 4: Constraint specialised programs: wrt `unsafe` (left) and wrt `safe` (right)

Definition 6 (θ_t). Let P be a set of CHCs and t be a feasible AND-tree from P for (un)safe. Let $p^I(\mathbf{x})$ be the atom label of an initial node of t then $\theta_t = \text{constr}(t)|_{\mathbf{x}}$.

In other words, θ_t is basically the result of eliminating all variables but \mathbf{x} from $\text{constr}(t)$. Note that θ_t is necessary condition for t to be feasible.

Lemma 2 ([23]). Let P' be the result of eliminating a feasible AND-tree t for safe (unsafe) from P . Then $\varphi_s^N(P) = \varphi_s^N(P') \vee \theta_t$ ($\varphi_u^N(P) = \varphi_u^N(P') \vee \theta_t$), where θ_t is a constraint extracted from t (Def. 6).

Transformations such as PE, CS and TE (which removes *infeasible* trees) not only preserve the goal but also the initial clauses. This allows us to construct a sequence of clauses P_0, P_1, \dots, P_m where $P = P_0$ and each element of the sequence is more specialised than its predecessor with respect to derivations of safe (unsafe). As a consequence, the NPs are more precise. We write $P \Rightarrow_A P'$ when P' is a goal-preserving transformation of P with respect to an atom A , that is, $P \models A$ iff $P' \models A$. TE (eliminating *feasible* trees) is a little different which does not preserve the goal. We abuse the notation and write $P \Rightarrow_{t_A} P'$ for transformation of P by eliminating a feasible tree rooted at A , yielding P' . Lemma 2 shows that soundness is ensured in this case.

Let us now wrap these transformations and their combinations. Let tr and tr-seq be any functions satisfying the following:

$$\text{tr}_A \langle P, \varphi \rangle = \begin{cases} \langle P', \varphi \rangle & \text{where } P \Rightarrow_A P' \\ \text{or} \\ \langle P', \varphi' \rangle & \text{where } P \Rightarrow_{t_A} P' \text{ and } \varphi' = \varphi \vee \theta_{t_A} \text{ (Def. 6)} \end{cases}$$

$$\text{tr-seq}_A \langle P, \varphi, n \rangle = \text{tr}_A^n \langle P, \varphi \rangle \text{ for } n \geq 1$$

where $f^1 = f$ and $f^n = f^{n-1} \circ f$.

tr-seq allows us to combine the above transformations in any order and Proposition 4 allows us to derive more precise preconditions from the combination.

Proposition 4 (Adapted from Proposition 2 of [23]). Let P be a set of CHCs and $n \geq 1$. Let $\langle P_s, \varphi_s \rangle = \text{tr-seq}_{\text{safe}} \langle P, \text{false}, n \rangle$. Then $\models_{\mathbb{T}} (\varphi_s^N(P_s) \vee \varphi_s) \rightarrow \varphi_s^N(P)$. Similarly, if $\langle P_u, \varphi_u \rangle = \text{tr-seq}_{\text{unsafe}} \langle P, \text{false}, n \rangle$, then $\models_{\mathbb{T}} (\varphi_u^N(P_u) \vee \varphi_u) \rightarrow \varphi_u^N(P)$.

4 An algorithm for precondition inference

Given a set of CHC transformations and their relationships with the preconditions, we now state the algorithm for computing SPs for safety and unsafety in Algorithm 1.

The algorithm takes a set of CHCs as input (with special predicates encoding the sets of safe and unsafe states) and a positive number n representing the length of a sequence of transformations and returns a pair of SPs for safety and unsafety.

Algorithm 1 Algorithm for inferring sufficient preconditions

```

1: Input: A set of CHCs  $P$  with clauses for safe and unsafe and the length of the
   sequence of transformations  $n$ .
2: Output: Sufficient precondition for safety and unsafety wrt safe and unsafe.
3: Initialisation:  $\varphi_s^S \leftarrow false$ ;  $\varphi_u^S \leftarrow false$ ;  $P_s \leftarrow P$ ;  $P_u \leftarrow P$ ;
4:  $\varphi_{old} \leftarrow \varphi_s^N(P)$  (Definition 1);
5: while true do
6:    $\langle P_s, \theta_s \rangle \leftarrow \text{tr-seq}_{\text{safe}}(P_s, false, n)$ ;  $\langle P_u, \theta_u \rangle \leftarrow \text{tr-seq}_{\text{unsafe}}(P_u, false, n)$ ;
    $\varphi_s \leftarrow \varphi_s^N(P_s) \vee \theta_s$   $\varphi_u \leftarrow \varphi_u^N(P_u) \vee \theta_u$ 
7:    $\varphi_{new} \leftarrow \varphi_s \wedge \varphi_u$ 
8:   if  $\varphi_{new} \equiv false$  (optimal condition reached) then
9:      $\varphi_s^S \leftarrow \varphi_s^S \vee \varphi_s$   $\varphi_u^S \leftarrow \varphi_u^S \vee \varphi_u$ 
10:    return  $\langle \varphi_s^S, \varphi_u^S \rangle$ 
11:   else if  $\varphi_{old} \rightarrow \varphi_{new}$  (approximation does not get stronger) then
12:      $\varphi_s^S \leftarrow \varphi_s^S \vee (\varphi_s \wedge \neg \varphi_u)$   $\varphi_u^S \leftarrow \varphi_u^S \vee (\varphi_u \wedge \neg \varphi_s)$ 
13:    return  $\langle \varphi_s^S, \varphi_u^S \rangle$ 
14:   else (refine clauses via under-approximation using Def. 5)
15:      $\varphi_{old} \leftarrow \varphi_{new}$ 
16:      $\varphi_s^S \leftarrow \varphi_s^S \vee (\varphi_s \wedge \neg \varphi_u)$ ;  $\varphi_u^S \leftarrow \varphi_u^S \vee (\varphi_u \wedge \neg \varphi_s)$ ;
        $P_s \leftarrow \text{u\_approximate}(P_s, \varphi_{new})$   $P_u \leftarrow \text{u\_approximate}(P_u, \varphi_{new})$ 

```

The SPs φ_s^S and φ_u^S are initialised to *false*. The algorithm aims to weaken these SPs as much as possible. φ_{old} keeps track of the set of initial states that are yet to be proven safe or unsafe and is initialised to the set of initial states of P . P_s and P_u keep track of the transformations of P with respect to **safe** and **unsafe** respectively, and also their under-approximations.

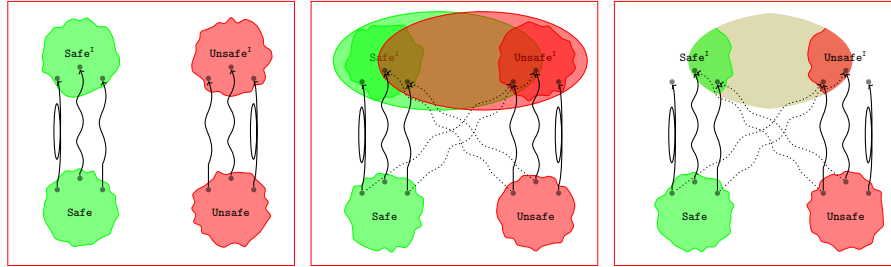


Fig. 6: Precondition inference: Reality (left), Initial approximations (middle), One step refinement of approximations using Algorithm 1 (right). We discard the regions classified as definitely safe or unsafe considering only the intersection.

The progress of Algorithm 1 is depicted in Figure 6. The leftmost panel reflects the reality, that is, it depicts the set of concrete safe and unsafe states along with the set of initial states leading to them. The set of safe states and the set of initial states leading to them are respectively marked as **Safe** and **Safe^I** and are drawn on the left side of each panel. Similarly, the set of unsafe

states and the set of initial states leading to them are respectively marked as **Unsafe** and **Unsafe**^I and are shown on the right side of each panel. Given a program together with the description of the sets of interest (safe and unsafe states), the precondition analysis infers a set of initial states that leads to these sets of interest. Due to approximations, it discovers over-approximations of the initial sets of states. These over-approximations are depicted as ellipses in the middle panel with the corresponding colours for safe and unsafe initial states. These approximations may intersect. As a consequence, there are some witness traces from the left ellipse to **Unsafe** (shown by dotted arrows) and vice versa. The algorithm aims to reduce these ellipses progressively towards the optimal condition, where the left ellipse leads to the set of safe states and the right one to the set of unsafe states (that is, these ellipses do not overlap anymore). A single step of refinement is illustrated in the rightmost panel.

In the algorithm, the following operations are carried out in an iterative manner and possibly in parallel (within the *while* loop). The instructions on two sides of the boxes can be executed in parallel. One or more of the transformation of P_s and P_u with respect to **safe** and **unsafe** respectively are carried out and the NPs are extracted from the resulting programs (*line 6*). The algorithm terminates and returns an SP if the conjunction of these NPs is unsatisfiable (*line 10, optimal*) or it is not stronger (in the sense of implication of formulas) than φ_{old} (*line 13*). Otherwise, the algorithm iterates with the new under-approximations obtained by restricting their initial states with the conjunction (*line 16*). Note that the conjunction needs to be converted to DNF before applying Definition 5, which may blow up the number of resulting clauses (only the initial ones).

Simulating the algorithm on the example program. We denote the program in Figure 1 by P . Initially, $\varphi_{old} = \text{true}$, the initial state of P . First, we choose to apply PE to P with respect to **safe** and **unsafe** respectively (call it the iteration 0 of the algorithm). The resulting set of CHCs are shown in Figure 2 along with the derived NPs. Since the conjunction of φ_s^N and φ_u^N , that is, $B \geq 0 \wedge A \geq 1$, is *satisfiable*, the preconditions are not optimal. But the conjunction is stronger than φ_{old} (conjunction of previous approximations), so the algorithm progresses to refinement (*line 14-16*). Before under-approximating the programs, we update the SPs from this iteration as:

$$\begin{aligned}\varphi_s^S &\equiv \text{false} \vee (B \geq 0 \wedge \neg(B < 0 \vee A \geq 1)) \equiv B \geq 0 \wedge A \leq 0. \\ \varphi_u^S &\equiv \text{false} \vee ((B < 0 \vee A \geq 1) \wedge \neg B \geq 0) \equiv B < 0.\end{aligned}$$

The results of under-approximating the programs in Figure 2 by $B \geq 0 \wedge A \geq 1$ following Definition 5 are trivial and are not shown here. In the next iteration (iteration 1), we apply CS with respect to **safe** and **unsafe** respectively to the under-approximations, obtaining the clauses shown in Figure 7. Then the NPs are: $\varphi_s^N \equiv (B \geq A \wedge A \geq 1)$ and $\varphi_u^N \equiv (B \geq 0 \wedge A > B)$. Since $\varphi_s^N \wedge \varphi_u^N \equiv \text{false}$, the preconditions are optimal and the algorithm terminates. The final SPs are given as the disjunction of SPs over the iterations as follows: $\varphi_s^S \equiv (B \geq 0 \wedge A \leq 0) \vee (B \geq A \wedge A \geq 1)$ and $\varphi_u^S \equiv B < 0 \vee (B \geq 0 \wedge A > B)$.

<pre> unsafe ← A < 0, B = 0, wh_2(B, A). wh_2(A, B) ← B < 0, A = 0, C = 1, B - D = -1, wh_1(C, D). wh_1(A, B) ← A > B, B ≥ 0, A ≥ 1, init(A, B). wh_1(A, B) ← A > B, A ≥ 1, A - C = -1, B - D = -1, wh_1(C, D). init(A, B) ← A > B, B ≥ 0. </pre>	<pre> safe ← A ≥ 0, B = 0, wh_2(B, A). wh_2(A, B) ← B ≥ 0, A = 0, C = 1, B - D = -1, wh_1(C, D). wh_1(A, B) ← B ≥ A, A ≥ 1, init(A, B). wh_1(A, B) ← B ≥ A, A - C = -1, A ≥ 1, B - D = -1, wh_1(C, D). init(A, B) ← B ≥ A, A ≥ 1. </pre>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Fig. 7: Constraint specialised programs: wrt **unsafe** (left) and wrt **safe** (right)

If instead we apply the sequence CS , PE to the original program, we get $\varphi_s^N \equiv (B \geq 0 \wedge A \leq 0) \vee (A \geq 1 \wedge B \geq A)$, $\varphi_u^N \equiv (B < 0 \wedge A \leq 0) \vee (A \geq 1 \wedge A > B)$ as *optimal* preconditions. This suggests that a sequence of transformations can potentially avoid the costly DNF conversion (needed during refinement) after each transformation. Therefore, in our experiments, we apply the sequence of transformations PE followed by CS followed by TE , rather than a single one. The rationale behind this particular sequences is that CS is most effective when performed after PE , which propagates constraints and introduces new versions of predicates. Trace elimination helps decompose the problem as well as splitting predicates, which induces a split in the resulting programs.

In each iteration of the loop, the algorithm either explores a strictly smaller set of initial states that have not yet been classified as safe or unsafe or, terminates. This property is formalised in Proposition 5.

Proposition 5 (Progress and Termination of Algorithm 1). *At each iteration of the while loop, Algorithm 1 either progresses (considers a smaller set of states that is yet to be proven safe or unsafe) or terminates.*

Proof (sketch). At each iteration, the algorithm maintains a constraint formula (representing the initial set of states that is yet to be classified as safe or unsafe). The algorithm can exit if the formula in the current iteration is the formula *false* (line 8-10), or is equivalent to the formula in the previous iteration (line 11-13). In other case, the current formula is stronger (representing a smaller set of initial states, treating constraint formula as a set) than that in the previous iteration, so it recurses (line 14-16). This means the set that is yet to be proven safe or unsafe gets smaller. In this sense, the algorithm makes progress.

Proposition 4 establishes the correctness of the combination of transformations, Proposition 3 ensures that the precondition of an under-approximation of CHCs is also that of the original and Proposition 1 allows us to combine preconditions derived in each iterations. All these propositions together ensure the soundness of Algorithm 1, which is formally stated as follows.

Theorem 1 (Soundness of Algorithm 1). *Let P be a set of CHCs annotated with the predicates **safe** (indicating a set of safe terminating states) and **unsafe** (indicating a set of unsafe states). If Algorithm 1 returns a tuple $\langle S, U \rangle$, then S and U are the SPs for safety and unsafety of P , respectively, with respect to the predicates **safe** and **unsafe**.*

Proof (sketch). In each iteration the algorithm essentially computes over approximations of the set of *safe* and *unsafe* states using the sequence of transformations. Proposition 4 establishes the correctness of the sequence. Then it computes the under-approximations of the original program with the sets of states that are yet to be classified as *safe* or *unsafe* while accumulating those states (preconditions) that are known to be *safe* and known to be *unsafe*. The under-approximations are fed to the next iteration. Proposition 3 ensures that the precondition of an under-approximation of CHCs is also that of the original. Proposition 1 ensures that the preconditions accumulated (disjunctively) in each iteration are the preconditions for the original program. These arguments together ensures the soundness of the algorithm. \square

Limitations of our method and non-termination. The SPs derived by our method may include non-terminating inputs, that neither lead to safe nor unsafe. Popeea and Chin [28] treat such inputs as *unsafe* whereas Seghir and Schrammel [30] ignore them, as do we. However, the modelling of safe and unsafe terminating states and their over-approximations allow us to reason about a limited form of non-termination as suggested by Popeea and Chin [28]. That is, any input state that is neither in the over-approximation of safe nor unsafe is non-terminating (again assuming that we model all the terminating safe and unsafe states).

We illustrate this with the example in Figure 8. This program does not terminate if $a \in [0, 10]$. We derive $\varphi_s^N = a \geq 11$ and $\varphi_u^N = a < 0$ as NPs. Thus the condition satisfying $\neg(\varphi_s^N \vee \varphi_u^N)$, that is, $\neg(a \geq 11 \vee a < 0) \equiv a \in [0, 10]$ is a precondition for non-termination (which happens to be precise in this case). It is obtained as our method’s side-effect and we leave the primary analysis of non-termination for future work.

```
void main(int a) {
  while (a ≥ 0) {
    if (a ≤ 9)  a++;
    else if (a == 10)
      a = 5;
    else return;
  }
  assert (false);
}
```

Fig. 8: Non-termination

5 Experimental evaluation

We implemented Algorithm 1 (a sequential version) in the tool PI-HORN (Precondition Inferer for Horn clauses), which is available from <https://github.com/bishoksan/PI-Horn>. Given 3 different program transformations, the implementation fixes the length of the sequence to 3. The order of their application is PE followed by CS followed by TE. The tool is written in Ciao Prolog [17] and makes use of the Parma Polyhedra Library (PPL) [1] and Yices2 SMT solver [11]. The input to our tool is a set of CHCs; with *safe*, *unsafe* and *init* as distinguished predicates (for technical reasons). It outputs a pair of SPs for safety and unsafety. The derived SPs are classified as: (i) *optimal*: the precondition is both necessary and sufficient (exact); (ii) *(un)safe-non-trivial*: the SP for (un)safety is different from *false* (but not *optimal*) and (iii) *(un)safe-trivial*: the SP for (un)safety is *false*.

Benchmarks and experimental settings. We tested our approach with 261 integer programs (available from <https://github.com/bishoksan/PI-Horn/tree/master/benchmarks>) collected from the following sources which we think could be the good candidates. (i) 150 programs from the loop (69) and recursive (81) categories of SV-COMP’18 [4]; (ii) 83 programs from the DAGGER [15] and TRACER tools [19] and (iii) 28 programs from the literature on precondition inference and backwards analysis [2,25,26,3,5]. Unfortunately, we could not include all the benchmarks used by Kaffle et al. [23] since some of their C sources were not available, but only their CHCs representations modelling only the *unsafe* terminating states. Benchmark set (i) is designed for software verification competitions while (ii) and (iii) are designed to demonstrate the strength of some specific tools and techniques. We adapt these programs written in C for precondition inference in the following way. They are first translated to CHCs by specialising an interpreter of C written in Prolog using the tool VeriMap [9]. The specialisation approach was described by De Angelis et al. [10], and models only the states leading to an “error” state by the predicate *unsafe*. The current translation also models *return* statements and the initial states of programs by two special predicates *safe* and *init* respectively (again using VeriMap), which allows us to reason about the safe terminating states and the initial states respectively. Given a sequence of initial state variables x_1, \dots, x_n and the corresponding initial clause $\text{init}(x_1, \dots, x_n) \leftarrow \varphi(x_1, \dots, x_n)$ obtained by the translation, we replace $\varphi(x_1, x_2, \dots, x_n)$ by *true* obtaining the clause $\text{init}(x_1, x_2, \dots, x_n) \leftarrow \text{true}$. The replacement allows the analysis to infer preconditions in terms of these variables starting from an unrestricted set of *initial* states.

Unfortunately, we could not compare our tool against the recent works of Seghir et al. [29,30] and that of Bakhirkin et al. [2], the first due to some issues with the tool (discovered together with the authors), and the second due to the lack of a tool automating their approach (confirmed by the authors via email). But we do compare to the work of Kaffle et al. [23] (represented in the table as WP-RAHFT). Although some of the components used in our tools are the same, a direct comparison is difficult due to different outcomes. That tool, for example, cannot detect optimality and does not attempt to do so, unlike ours. Therefore, it is hard to compare the quality of the generated preconditions.

Experiments have been carried on a MacBook Pro, running OS X 10.11 in 16GB Memory and 2.7 GHz Intel Core i5 processor.

Experimental Results. Table 1 presents the results. The columns respectively show *iter* (# of refinement iterations (*line 14-16*)), *opt* (# of programs with optimal preconditions), *ntS* (*Sw*) (# of programs with non-trivial SPs for safety excluding optimal cases, and, in parentheses, the difference with trivial SPs for unsafety), *ntU* (*Uw*) (same, but for unsafety), *ntSU* (# of programs with non-trivial SPs for both safety and unsafety), *tSU* (# of programs with trivial SPs for both safety and unsafety), *total/iter* (# of programs with non-trivial plus optimal SP per iteration), WP-RAHFT *total/iter* (# of programs with non-trivial SP per iteration for WP-RAHFT). For example, the entry 9 (7) in column 3 indicates that there were 9 non-trivial SPs for safety, of which 7 had trivial SPs

iter	opt	ntS (Sw)	ntU (Uw)	ntSU	tSU	total/iter	WP-RAHFT total/iter
0	58	0 (0)	0 (0)	0	0	58	197
1	87	9 (7)	5 (3)	2	20	99	20
2	21	20 (15)	7 (2)	5	0	43	0
3	5	6 (3)	3 (0)	3	0	11	0
4	2	3 (1)	2 (0)	2	0	5	0
5	2	0 (0)	0 (0)	0	0	2	1
6	1	0 (0)	0 (0)	0	0	1	0
#total	176	38 (26)	17 (5)	12	20	219	218

Table 1: Experimental results on 261 programs, with a timeout of 300 seconds.

for unsafety. Each row contains the number of instances for which the algorithm terminated after the given number of iterations.

The results show our tool is able to generate non-trivial preconditions for 83% of the programs while timing out for 9%. The average time taken (ignoring timeouts) per each instance is 5.94 seconds. Optimal preconditions are inferred for 67% of the programs whereas for 8% the tool fails to infer any meaningful preconditions. A meaningful SP for safety or unsafety ($\neq false$) apart from optimal ones is inferred for 16% of the problems (columns 3rd and 4th). Preprocessing using partial evaluation and constraint specialisation, as well as refinement by removing program traces and restarting the analysis from unresolved initial states, increases the precision of the analysis for the following reasons. On the one hand, partial evaluation brings polyvariant specialisation by creating several versions of the predicates, which the abstract interpreter in constraint specialisation can take advantage of. On the other hand, the refinement helps limit the set of initial states to explore and/or reduces the number of paths to explore. Note that the tool infers optimal preconditions for 58 programs due to preprocessing alone, which is indicated by the result along the row *iteration* 0 in the table, whereas it infers optimal preconditions for 99 programs after the first refinement. However, it should be noted that the refinement also hinders the performance of the analysis by increasing the size of the resulting programs. This explains why we solve fewer and fewer problems after iteration 2. The number of programs with non-trivial SPs are almost the same for both the tools (219 vs. 218), but they differ in the quality (such as optimality) of the generated SPs. The refinement in our approach allows us to derive optimal or non-trivial preconditions for more programs, but in case of WP-RAHFT it does not yield any better results after the first refinement iteration (note though that the derived preconditions may be more general). The average time taken (ignoring the timeouts) by WP-RAHFT per each instance is 5.59 (first *iteration*) and 8.34 (sixth *iteration*) seconds. The first one is bit lower and the second is bit higher than in our approach. The reason for this difference is that WP-RAHFT does not know when to stop refining since the termination criterion, the maximum number of iterations, is rather weak. Another possible reason is that at each iteration an under-approximation of the original program is analysed by our tool as opposed to WP-RAHFT, which can

be easier. Though the refinement may help derive a weaker SP, it also consumes more time.

6 Related work

Given a wide range of applications, there are a handful of techniques in the literature dealing with precondition inference. We classify them as follows.

Abstract interpretation: Over-approximation techniques (forward and backwards abstract interpretations or their combination [6,7,3]) inherently derive NPs and complementation allows deriving SPs at the cost of precision (due to approximation of the complement). In order to minimise the loss, we need to find either a (pseudo) complemented domain [24] or an alternative to complementation that is less aggressive. Along these lines, Howe et al. [18] utilise the pseudo-complemented domain *Pos* to infer SPs whereas Bakhirkin et al. [2] exchange an abstract complement operation for abstract logical subtraction. In contrast to these lines of work, we neither assume an abstract domain to be complemented nor apply complementation of an abstract element during abstract interpretation. Instead our method applies to any abstract domain, and the complementation is carried out as a separate process outside the abstract domain, storing the result as a formula without any loss of precision.

Little work has been done that inherently computes SPs without complementation. The notable exception is the work of Miné [25], which designs all required purpose-built backward transfer functions for intervals, octagons and convex polyhedra domains. The downside is that the purpose-built operations, including widening, can be rather intricate and require substantial implementation effort. Moy [26] employs weakest-precondition reasoning and forward abstract interpretation to attempt to generalise conditions at loop heads to infer SPs. The derived conditions offer limited use except for a theorem prover. As opposed to these works, our method makes use of standard tools and techniques offering simplicity and ease of implementation. Furthermore, our results can be consumed by other tools in the area of program analysis and verification. Though formulated in the context of software verification, the dual-analysis approach of Poppea and Chin [28] uses over-approximations as in our approach to concurrently infer NPs for safety and unsafety of each method (and program), from which SPs can be derived. However, in contrast to our approach, no refinement of the derived preconditions takes place.

Program transformation: The forward and backward iterative specialisation approach of De Angelis et al. [8] designed to verify program properties can be used for deriving preconditions, as in our approach. The transformation approach uses constraint generalisation method instead of abstract interpretation and can be adjusted to refine preconditions.

Counterexample-guided abstraction refinement (CEGAR): Seghir et al. [29,30] use a CEGAR approach to derive *exact* necessary and sufficient preconditions for safety. Like us, they model safe and unsafe states of a program

and refine their approximations until they are disjoint. Their algorithm may diverge due to (i) the lack of a suitable generalisation of the counterexamples (an inherent limitation of CEGAR) and (ii) the termination condition (disjointness) that is too hard to achieve for realistic programs (due to undecidability). We, on the other hand, use abstract interpretation and program transformation, so each step of the algorithm terminates and a sound precondition can be derived from the resulting programs. In addition, optimality is not the end goal for us and it is obtained as a by-product of precision refinement.

The work of Kafle et al. [23] is orthogonal to all of the above; it combines a range of established tools and techniques such as abstract interpretation, CEGAR and program transformations in a profitable way. The iterative nature of their approach allows them to derive more precise preconditions for safety on demand, however the termination criterion, the maximum number of iterations supplied by the user, is rather weak. The quality of the preconditions such as optimality cannot be checked using their approach. The current work offers several advantages over that approach. We model both safe and unsafe states of programs. This allows detecting optimality and also inferring NP and SP for both safety and unsafety. In addition, it allows reasoning about a limited form of non-termination and provides more refined termination criteria. Unlike many methods in the literature [29,30,2], our method can handle not only programs with procedures, but also recursive programs, in a uniform way.

7 Concluding remarks

We have presented an iterative method for automatically deriving sufficient preconditions for safety and unsafety of programs. It maintains over-approximations of the set of *safe* and *unsafe* initial states. At each iteration, only the set of states that are common to these over-approximations are considered, as those are yet to be classified as safe or unsafe. The method terminates when the common set of states is empty or the common set does not get smaller in successive iterations. Experimental results show that the method is able to generate optimal preconditions in 67% of the cases and also solves some problems which are otherwise unsolvable using only approximations of the unsafe states (as was done in previous work). Owing to over-approximation, the sufficient preconditions may include some non-terminating states, which hinders the derivation of optimal preconditions. In future work we intend to augment our method with non-termination analysis.

Acknowledgement We thank John Gallagher for comments on an earlier draft and many useful discussions which has led to many improvements. We thank Emanuele de Angelis for C to CHC translation, help with the tool VeriMAP, benchmarks and many stimulating discussions.

References

1. R. Bagnara, P. M. Hill, and E. Zaffanella. The Parma Polyhedra Library: Toward a complete set of numerical abstractions for the analysis and verification of hardware and software systems. *Sci. Comput. Program.*, 72(1-2):3-21, 2008.
2. A. Bakhirkin, J. Berdine, and N. Piterman. Backward analysis via over-approximate abstraction and under-approximate subtraction. In *Static Analysis*, volume 8723 of *LNCS*, pages 34-50. Springer, 2014.
3. A. Bakhirkin and D. Monniaux. Combining forward and backward abstract interpretation of Horn clauses. In *Static Analysis*, volume 10422 of *LNCS*, pages 23-45. Springer, 2017.
4. D. Beyer. Software verification with validation of results (report on SV-COMP 2017). In *Proc. TACAS 2017*, volume 10206 of *LNCS*, pages 331-349, 2017.
5. F. Cassez, P. G. Jensen, and K. G. Larsen. Refinement of trace abstraction for real-time programs. In *Reachability Problems*, volume 10506 of *LNCS*, pages 42-58. Springer, 2017.
6. P. Cousot and R. Cousot. Abstract interpretation and application to logic programs. *J. Log. Program.*, 13(2&3):103-179, 1992.
7. P. Cousot, R. Cousot, and F. Logozzo. Precondition inference from intermittent assertions and applications to contracts on collections. In *VMCAI 2011*, volume 6538 of *LNCS*, pages 150-168. Springer, 2011.
8. E. De Angelis, F. Fioravanti, A. Pettorossi, and M. Proietti. Program verification via iterated specialization. *Sci. Comput. Program.*, 95:149-175, 2014.
9. E. De Angelis, F. Fioravanti, A. Pettorossi, and M. Proietti. VeriMAP: A tool for verifying programs through transformations. In *TACAS 2014*, volume 8413 of *LNCS*, pages 568-574. Springer, 2014.
10. E. De Angelis, F. Fioravanti, A. Pettorossi, and M. Proietti. Semantics-based generation of verification conditions via program specialization. *Sci. Comput. Program.*, 147:78-108, 2017.
11. B. Dutertre. Yices 2.2. In *Proc. CAV 2014*, volume 8559 of *LNCS*, pages 737-744. Springer, 2014.
12. J. P. Gallagher. Specialisation of logic programs: A tutorial. In *PEPM 1993*, pages 88-98, 1993.
13. J. P. Gallagher and L. Lafave. Regular approximation of computation paths in logic and functional languages. In *Partial Evaluation*, volume 1110 of *LNCS*, pages 115-136. Springer, 1996.
14. S. Grebenshchikov, N. P. Lopes, C. Popeea, and A. Rybalchenko. Synthesizing software verifiers from proof rules. In *PLDI 2012*, pages 405-416. ACM, 2012.
15. B. S. Gulavani, S. Chakraborty, A. V. Nori, and S. K. Rajamani. Automatically refining abstract interpretations. In *TACAS 2008*, volume 4963 of *LNCS*, pages 443-458. Springer, 2008.
16. A. Gurfinkel, T. Kahsai, A. Komuravelli, and J. A. Navas. The SeaHorn verification framework. In *CAV 2015*, volume 9206 of *LNCS*, pages 343-361. Springer, 2015.
17. M. V. Hermenegildo, F. Bueno, M. Carro, et al. An overview of Ciao and its design philosophy. *Theory and Practice of Logic Programming*, 12(1-2):219-252, 2012.
18. J. M. Howe, A. King, and L. Lu. Analysing logic programs by reasoning backwards. In *Program Development in Computational Logic*, volume 3049 of *LNCS*, pages 152-188. Springer, 2004.
19. J. Jaffar, V. Murali, J. A. Navas, and A. E. Santosa. TRACER: A symbolic execution tool for verification. In *CAV 2012*, volume 7358 of *LNCS*, pages 758-766. Springer, 2012.

20. N. Jones, C. Gomard, and P. Sestoft. *Partial Evaluation and Automatic Software Generation*. Prentice Hall, 1993.
21. B. Kafle and J. P. Gallagher. Constraint specialisation in Horn clause verification. *Sci. Comput. Program.*, 137:125–140, 2017.
22. B. Kafle and J. P. Gallagher. Horn clause verification with convex polyhedral abstraction and tree automata-based refinement. *Computer Languages, Systems & Structures*, 47:2–18, 2017.
23. B. Kafle, J. P. Gallagher, G. Gange, et al. An iterative approach to precondition inference using constrained Horn clauses. *Theory and Practice of Logic Programming*, 18:553–570, 2018.
24. K. Marriott and H. Søndergaard. Precise and efficient groundness analysis for logic programs. *ACM LOPLAS*, 2(1–4):181–196, 1993.
25. A. Miné. Inferring sufficient conditions with backward polyhedral under-approximations. *Electr. Notes Theor. Comput. Sci.*, 287:89–100, 2012.
26. Y. Moy. Sufficient preconditions for modular assertion checking. In *VMCAI 2008*, volume 4905 of *LNCS*, pages 188–202. Springer, 2008.
27. J. C. Peralta, J. P. Gallagher, and H. Sağlam. Analysis of imperative programs through analysis of constraint logic programs. In *Static Analysis*, volume 1503 of *LNCS*, pages 246–261, 1998.
28. C. Popeea and W. Chin. Dual analysis for proving safety and finding bugs. *Sci. Comput. Program.*, 78(4):390–411, 2013.
29. M. N. Seghir and D. Kroening. Counterexample-guided precondition inference. In *ESOP 2013*, volume 7792 of *LNCS*, pages 451–471. Springer, 2013.
30. M. N. Seghir and P. Schrammel. Necessary and sufficient preconditions via eager abstraction. In *APLAS 2014*, volume 8858 of *LNCS*, pages 236–254. Springer, 2014.