Research Note
RN/13/23

Proving nontermination via safety
January 18, 2014

Hong-Yi Chen  Byron Cook  Carsten Fuhs
Kaustubh Nimkar  Peter O’Hearn

Abstract

We show how the problem of nontermination proving can be reduced to a question of underapproximation search guided by a safety prover. This reduction leads to new nontermination proving implementation strategies based on existing tools for safety proving. Our preliminary implementation beats existing tools. Furthermore, our approach leads to easy support for programs with unbounded nondeterminism.
Abstract. We show how the problem of nontermination proving can be reduced to a question of underapproximation search guided by a safety prover. This reduction leads to new nontermination proving implementation strategies based on existing tools for safety proving. Our preliminary implementation beats existing tools. Furthermore, our approach leads to easy support for programs with unbounded nondeterminism.

1 Introduction

The problem of proving program nontermination represents an interesting complement to termination as, unlike safety, termination’s falsification cannot be witnessed by a finite trace. While the problem of proving termination has now been extensively studied, the search for reliable and scalable methods for proving nontermination remains open.

In this paper we develop a new method of proving nontermination based on a reduction to safety proving that leverages the power of existing tools. An iterative algorithm is developed which uses counterexamples to a fixed safety property to refine an underapproximation of a program. With our approach, existing safety provers can now be employed to prove nontermination of programs that previous techniques could not handle. Not only does the new approach perform better, it also leads to nontermination proving tools supporting programs with nondeterminism, for which previous tools had only little support.

Limitations. Our proposed nontermination procedure can only prove nontermination. On terminating programs the procedure is likely to diverge (although some heuristics are proposed which aim to avoid this). While our method could be extended to further programming language features (e.g. heap, recursion), in practice the supported features of an underlying safety prover determine applicability. Our implementation uses a safety prover for non-recursive programs with linear integer arithmetic commands.

Example. Before discussing our procedure in a formal setting, we begin with a simple example given to the right. In this program the command \(i := \text{nondet}()\) represents nondeterministic value introduction into the variable \(i\). The loop in this program


definition

```python
if (k ≥ 0)
    skip;
else
    i := -1;
while (i ≥ 0) {
    i := \text{nondet}();
}
i := 2;
```
is nonterminating when the program is invoked with appropriate inputs and when appropriate choices for nondet assignment are made. We are interested in automatically detecting this nontermination. The basis of our procedure is the search for an underapproximation of the original program that never terminates. As “never terminates” can be encoded as safety property (defined later as closed recurrence in Sect. 2), we can then iterate a safety prover together with a method of underapproximating based on counterexamples. We have to be careful, however, to find the right underapproximation in order to avoid unsoundness.

In order to find the desired underapproximation for our example, we introduce an assume statement at the beginning with the initial precondition true. We also place assume(true) statements after each use of nondet. We then put an assert(false) statement at points where the loop under consideration exits (thus encoding the “never terminates” property). See Fig. 1(a).

We can now use a safety checker to search for paths that violate this assertion. Any error path clearly cannot contribute towards the nontermination of the loop. After detecting such a path we calculate restrictions on the introduced assume statements such that the path is no longer feasible when the restriction is applied.

Initially as a first counterexample to safety, we might get the path \( k < 0, \ i := -1, \ i < 0 \), from a safety prover. We now want to determine from which states we can reach assert(false) and eliminate those states. Using a precondition computation similar to Calcagno et al. [6] we find the condition \( k < 0 \). The trick is to use the standard weakest precondition rule for assignments, but to use

\[
pre(assume(Q), P) \equiv P \land Q
\]

instead of the standard

\[
wp(assume(Q), P) \equiv Q \Rightarrow P.
\]

This way, we only consider executions that actually reach the error location. To rule out the states \( k < 0 \) we can add the negation (e.g. \( k \geq 0 \)) to the precondition assume statement. See Fig. 1(b).

In our procedure we try again to prove the assertion statement unreachable, using the program in Fig. 1(b). In this instance we might get the path \( k \geq 0, \ skip, i < 0 \), which again violates the assertion. For this path we would discover the precondition \( k \geq 0 \land i < 0 \), and to rule out these states we refine the precondition assume statement with “assume\( (k \geq 0 \land i \geq 0)\)”. See Fig. 1(c).

On this program our safety prover will again fail, perhaps resulting in the path \( k \geq 0, \ skip, i \geq 0, \ i := nondet() \), \( i < 0 \). Then our procedure would stop computing the precondition at the command \( i := nondet() \) (for reasons discussed later). Here we would learn that at the nondeterministic command the result must be \( i < 0 \) to violate the assertion, thus we would refine the assume statement just after the nondet with the negation of \( i < 0 \): “assume\( (i \geq 0)\)” See Fig. 1(d).

The program in Fig. 1(d) cannot violate the assertion, and thus we have hopefully computed the desired underapproximation to the transition relation needed in order to prove nontermination. However, for soundness, it is essential to ensure that the loop in Fig. 1(d) is still reachable, even after the successive restrictions to the state-space. We encode this condition as a safety problem. See Fig. 1(e). This time we add assert(false) before the loop and aim to prove that the assertion is violated. The existence of a path violating the assertion ensures that the loop in Fig. 1(d) is reachable. Here the assertion and thus the
assume(true);
if (k ≥ 0)
    skip;
else
    i := -1;

while (i ≥ 0) {
    i := nondet();
    assume(true);
}
assert(false);
i := 2;

assume(k ≥ 0);
if (k ≥ 0)
    skip;
else
    i := -1;

while (i ≥ 0) {
    i := nondet();
    assume(true);
}
assert(false);
i := 2;

assume(k ≥ 0 ∧ i ≥ 0);
if (k ≥ 0)
    skip;
else
    i := -1;

while (i ≥ 0) {
    i := nondet();
    assume(i ≥ 0);
}
assert(false);
i := 2;

assume(k ≥ 0 ∧ i ≥ 0);
if (k ≥ 0)
    skip;
else
    i := -1;

skip;
while (i ≥ 0) {
    i := nondet();
    assume(i ≥ 0);
}
assert(false);
i := 2;

assume(k ≥ 0 ∧ i ≥ 0);
assume(k ≥ 0);
if (k ≥ 0)
    skip;
else
    i := -1;

skip;
while (i ≥ 0) {
    i := nondet();
    assume(i ≥ 0);
}

Fig. 1. Original instrumented program (a) and its successive underapproximations (b), (c), (d). Reachability check for the loop (e), and nondeterminism-assume that must be checked for satisfiability (f).

loop are still reachable. The path violating the assertion is our desired path to the loop which we refer to as stem. Fig. 1(f) shows the stem and the loop.

Finally we need to ensure that the assume statement in Fig. 1(f) can always be satisfied with some i by any reachable state from the restricted pre-state. This is necessary: our underapproximations may accidentally have eliminated not only the paths to the loop’s exit location, but also all of the nonterminating paths inside the loop. Once this check succeeds we have proved nontermination.
2 Closed recurrence sets

In this section we define a new concept which is at the heart of our procedure, called closed recurrence. Closed recurrence extends the known concept of (open) recurrence [16] in a way that facilitates automation, e.g. via a safety prover.

Preliminaries. Let $S$ be the set of states. Given a transition relation $R \subseteq S \times S$, for a state $s$ with $R(s, s')$, we say that $s'$ is a successor of $s$ under $R$.

We will be considering programs $P$ with finitely many program locations $\mathbb{L}$ and a set of memory states $M$, so the program’s state space $S$ is given as $S = \mathbb{L} \times M$. For instance, for a program on $n$ integer variables, we have $M = \mathbb{Z}^n$, and a memory state amounts to a valuation of the program variables.

A program $P$ on locations $\mathbb{L}$ is represented via its control-flow graph (CFG) $(\mathbb{L}, \Delta, l_i, l_f, l_e)$. The program locations are the CFG’s nodes and $\Delta$ is a set of edges between locations labeled with commands. We designate special locations in $\mathbb{L}$: $l_i$ is the initial location, $l_f$ the final location, and $l_e$ the error location. Each $(l, T, l') \in \Delta$ is a directed edge from $l$ to $l'$ labeled with a command $T$. We write $R_T \subseteq M \times M$ for the relation on memory states induced by $T$ in the usual way.

We say that a memory state $s$ at node $l$ has a successor $s'$ along the edge $(l, T, l')$ iff $R_T(s, s')$ holds. A path $\pi$ in a CFG is a sequence of edges $(l_0, T_0, l_1) (l_1, T_1, l_2) \ldots (l_{n-1}, T_{n-1}, l_n)$. The composite transition relation $R_\pi$ of a path $\pi$ is the composition $R_{T_n} \circ R_{T_{n-1}} \circ \ldots \circ R_{T_1}$ of the individual relations. We also describe a path $\pi$ by the sequence of nodes it visits, e.g. $l_0 \rightarrow l_1 \rightarrow \ldots \rightarrow l_{n-1} \rightarrow l_n$.

Commands. We represent by $V$ the set of all program variables. A deterministic assignment statement is of the form $i := \text{exp}$ where $i \in V$ and $\text{exp}$ is an expression over program variables. A nondeterministic assignment statement is of the form $i := \text{nondet}(); \text{assume}(Q)$; where $i \in V$, \text{nondet}() is a nondeterministic choice and $Q$ is a boolean expression over $V$ representing the restriction that the \text{nondet}() choice must obey. Conditional statements are encoded using \text{assume} commands (from Nelson [22]): \text{assume}(Q), where $Q$ is a boolean expression over $V$. W.l.o.g. $l_i$ has 0 incoming and 1 outgoing edge, labeled with $\text{assume}(Q)$, where initially usually $Q \equiv \text{true}$. For readability, in our example CFGs we often write $Q$ for $\text{assume}(Q)$. Our algorithm will later strengthen $Q$ in the \text{assume}-statements.

We define the indegree of a node $l$ in a CFG to be the number of incoming edges to $l$. Similarly, the outdegree of a node $l$ in a CFG is the number of outgoing edges from $l$. A node $l \in \mathbb{L} \setminus \{l_i, l_f, l_e\}$ must be of one of the following types.

1. A deterministic assignment node: $l$ has outdegree exactly 1 and the outgoing edge is labeled with a deterministic assignment statement or $\text{skip}$. Any memory state $s$ at $l$ has a unique successor $s'$ along the edge.
2. A deterministic conditional node: $l$ has outdegree 2 with one edge labeled $\text{assume}(\varphi)$, the other edge labeled $\text{assume}(\neg \varphi)$. Any memory state $s$ at $l$ has a unique successor $s'$ along one edge and no successor along the other edge.
3. A nondeterministic assignment node: $l$ has outdegree exactly 1 and the outgoing edge is labeled with a nondeterministic assignment statement. A memory state $s$ at $l$ may have zero or more successors along the outgoing edge depending on the condition present in the $\text{assume}(Q)$ statement.
In our construction of a CFG, a lone statement \( \text{assume}(Q) \) from an input program is modeled by a deterministic conditional node, with one edge labeled \( \text{assume}(Q) \) and the other edge labeled \( \text{assume}(\neg Q) \) leading to the end location \( l_f \).

**Example.** Consider the CFG for our initial example given in Fig. 2. Here we have the initial location \( l_i = 0 \), the final location \( l_f = 7 \), and the error location \( l_e = 8 \). The nodes 2, 3 and 6 are deterministic assignment nodes, nodes 1 and 4 are deterministic conditional nodes, and node 5 is a nondeterministic assignment node.

**CFG loops.** Given a program with its CFG, a loop \( L \) in the CFG is a set of nodes s.t.
- There exists a path from any node of \( L \) to any other node of \( L \).
- (W.l.o.g.) we assume that there is only one node \( h \) of \( L \) s.t. there exists a node \( n \not\in L \) with an edge from \( n \) to \( h \). The node \( h \) is called the header node of \( L \).

The subgraph of CFG containing all nodes of \( L \) is called the loop body of \( L \). Header \( h \) of \( L \) is a deterministic conditional node with one edge that is part of the loop body, the guard edge of \( L \). The other edge of \( h \) goes to a node \( e \not\in L \). We call this edge the exit edge of \( L \) and \( e \) the exit location of \( L \).

**Example.** In Fig. 2, the only loop is \( L = \{4, 5\} \), and its header node \( h \) is 4. The exit location of \( L \) is 6.

Given a loop \( L \) in program \( P \), we define a loop path \( \pi_L \) as any finite path through \( L \)'s body of the form \( (l_0 = l_h) \rightarrow l_1 \rightarrow ... \rightarrow l_{n-1} \rightarrow (l_n = l_h) \), where \( l_h \) is the header node of \( L \) and \( \forall p. (0 < p < n) \rightarrow l_p \neq l_h \). We define the composite transition relation \( R_L \) of \( L \) as \( R_L(s, s') \iff \) there exists a loop path \( \pi \) s.t. \( R_\pi(s, s') \). Here \( R_L \) can be an infinite (or empty) set. The initial states \( I_L \) for \( R_L \) are the set of reachable states at the loop header before the loop is entered for the first time.

**Preconditions.** When computing preconditions of \( \text{assume} \) statements we borrow from Calcagno et al. [6]: \( \text{pre}(\text{assume}(Q), P) \triangleq P \land Q \), called the “assume as assert trick”. This lets us interpret \( \text{assume} \) statements (often from conditional branches) in a way that allows us to determine in a precondition the states from which an error location can be reached in a safety counterexample path. For assignment statements we will use the standard weakest precondition [12].

**Example.** Note that the weakest precondition of an assignment with nondeterminism is a little subtle. Let \( i := \text{nondet}(); \text{assume}(\text{true}) \); be the \( \text{nondet} \) statement under consideration. The weakest precondition for the postcondition \( i < j \) is **false** (equivalent to \( \forall i, i < j \)). However the weakest precondition for the postcondition \( i < j \lor k > 0 \) is \( k > 0 \).

languages like Java or C allow loops with additional exit edges also from locations other than the loop header, which are implemented by commands like \text{break} or \text{goto}.

We also support such more general loops, via a program transformation.
Recurrence sets. A relation \( R \) with initial states \( I \) is nonterminating iff there exists an infinite transition sequence \( s_0 \xrightarrow{R} s_1 \xrightarrow{R} s_2 \xrightarrow{R} \ldots \) with \( s_0 \in I \). Gupta et al. [16] characterize nontermination of a relation \( R \) by the existence of a recurrence set, viz. a nonempty set of states \( G \) such that for each \( s \in G \) there exists a transition to some \( s' \in G \). In particular, an infinite transition sequence \( s_0 \xrightarrow{R} s_1 \xrightarrow{R} s_2 \xrightarrow{R} \ldots \) itself gives rise to the recurrence set \( \{s_0, s_1, s_2, \ldots\} \). Here we extend the notion of a recurrence set to include initial states. A transition relation \( R \) with initial states \( I \) has an (open) recurrence set of states \( G(s) \) iff (1) and (2) hold. A transition relation \( R \) with initial states \( I \) is nonterminating iff it has a recurrence set of states.

A set \( G \) is a closed recurrence set for a transition relation \( R \) with initial states \( I \) iff the conditions (3)–(5) hold. In contrast to open recurrence sets, we now require a purely universal property: for each \( s \in G \) and for each of its successors \( s' \), also \( s' \) must be in the recurrence set (Condition (5)). So instead of requiring that we can stay in the recurrence set, we now demand that we must stay in the recurrence set. This now helps us to incorporate nondeterministic transition systems too.

Now what if a state \( s \) in our recurrence set \( G \) has no successor \( s' \) at all? Our alleged infinite transition sequence would reach a sudden halt, yet our universal formula would trivially hold. Thus, we impose that each \( s \in G \) has some successor \( s' \) (Condition (4)). But this existential statement need not mention that \( s' \) must be in \( G \) again—our previous universal statement already takes care of this.

Theorem 1 (Closed Recurrence Sets are Recurrence Sets). Let \( G \) be a closed recurrence set for \( R \) with initial states \( I \). Then \( G \) is also an (open) recurrence set for \( R \) with initial states \( I \).

The proofs for all theorems can be found in the Appendix.

**Underapproximation.** We call a transition relation \( R' \) with initial states \( I' \) an underapproximation of transition relation \( R \) with initial states \( I \) iff \( R' \subseteq R \), \( I' \subseteq I \). Then every nonterminating program contains a closed recurrence set as an underapproximation (i.e., together with underapproximation, closed recurrence sets characterize nontermination).

Theorem 2 (Open Recurrence Sets Always Contain Closed Recurrence Sets). There exists a recurrence set \( G \) for a transition relation \( R \) with initial states \( I \) iff there exist an underapproximation \( R' \) with initial states \( I' \) and \( G' \subseteq G \) such that \( G' \) is a closed recurrence set for \( R' \) with initial states \( I' \).

3 Algorithm

Our nontermination proving procedure **Prover** is detailed in Fig. 3. Its input is a program \( P \) given by its CFG, and a loop to be considered for nontermination. To prove nontermination of the entire program \( P \) we need to find only one nonterminating loop \( L \). This can be done in parallel. Alternatively, the procedure
Prover (CFG $P$, Loop $L$)

- $h :=$ header node of $L$
- $e :=$ exit node of $L$ in $P$

$P' := \text{UNDERAPPROXIMATE}(P, e)$

$L' :=$ refined loop $L$ in $P'$

if $\neg \text{REACHABLE}(P', h)$ then
  return Unknown, $\bot$

$\Pi := \{ \pi | \pi \text{ feasible path to } h \text{ in } P' \}$

for all $\pi \in \Pi$ do
  $P' := \pi' : L' // \text{ concatenation}$
  if \text{VALIDATE}(P') then
    return NonTerminating, $P'$
  fi
done
return Unknown, $\bot$

Underapproximate (CFG $P$, Node $e$)

- $\kappa := [ ]$

while $\text{REACHABLE}(P, e)$ do

  $\pi :=$ feasible path to $e$ in $P$

  $\kappa := \kappa : \pi$ (concatenation)

  $P := \text{REFINE}(P, \pi)$

  if the $n$ most recent paths in $\kappa$
    are repeating then
    $P := \text{STRENGTHEN}(P, \text{FIRST}(\kappa))$
  fi

done
return $P$

Refine (CFG $P$, Path $\pi$)

- $(l_0 T_0 l_1)(l_1 T_1 l_2) \ldots (l_{n-1} T_{n-1} l_n) := \pi$

Calculate WP $\psi_1, \psi_2 \ldots \psi_{n-1}$ along $\pi$

so $\{ \psi_1 \} T_1 \{ \psi_2 \} T_2 \ldots \{ \psi_{n-1} \} T_{n-1} \{ \text{true} \}$

are valid Hoare-triples.

Find $p$ s.t. $\psi_p \neq \text{false} \land \forall q < p. \psi_q = \text{false}$

$P := P | (\{ T_{p-1} \alpha \psi_p \} P)$

return $P$

Strengthen (CFG $P$, Path $\pi$)

- $(l_0 T_0 l_1)(l_1 T_1 l_2) \ldots (l_{n-1} T_{n-1} l_n) := \pi$

Calculate WP $\psi_1, \psi_2 \ldots \psi_{n-1}$ along $\pi$

so $\{ \psi_1 \} T_1 \{ \psi_2 \} T_2 \ldots \{ \psi_{n-1} \} T_{n-1} \{ \text{true} \}$

are valid Hoare-triples.

Find $p$ s.t. $\psi_p \neq \text{false} \land \forall q < p. \psi_q = \text{false}$

$W := \{ v | v \text{ gets updated in subpath} (l_p T_p l_{p+1}) \ldots (l_{n-1} T_{n-1} l_n) \}$

$\rho_p := \text{QE}(3W, \psi_p)$

$P := P | (\{ T_{p-1} \alpha \psi_p \} P)$

return $P$

Validate (CFG $P'$)

- $L' :=$ the outermost loop in $P'$

$M := \{ l | l \text{ is nondet assignment node in } L' \}$

for all $l \in M$ do

  Calculate invariant $\text{inv}_l$ at node $l$ in $P'$

  let nondet statement at $l$ be $v := \text{nondet}(); \text{assume}(\varphi)$;

  if $\text{inv}_l \Rightarrow \exists v. \varphi$ is not valid then
    return false
  fi

done
return true

**Fig. 3.** Algorithm Prover for underapproximation to synthesize a reachable nonterminating loop. To prove nontermination of $P$, Prover should be run on all loops $L$.

can be implemented sequentially, but then timeouts are advisable in Prover, as the procedure might diverge and cause another loop to not be considered.

The subprocedure Underapproximate performs the search for an underapproximation such that we can prove the loop is never exited. While the loop exit is still REACHABLE (a.k.a. “unsafe”), we use the subprocedure Refine to examine paths returned from an off-the-shelf safety prover. Here the notation $P | (T_i, \alpha \psi)$ denotes $P$ with an additional assume($\varphi$) added to the transition $T_i$. From the postcondition true (used to indicate success in reaching the loop exit), we use a backwards precondition analysis to find out which program states will inevitably end up in the loop exit. We continue this precondition calculation until either we have reached the beginning of the path or until just before we have reached a nondeterministic assignment that leads to the precondition false. We then negate this condition as our underapproximating refinement.
In some cases our refinement is too weak, leading to divergence. The difficulty is that in cases the same loop path will be considered repeatedly, but at each instance the loop will be unrolled for an additional iteration. To avoid this problem we impose a limit \( n \) for the number of paths that go along the same locations (possibly with more and more repetitions). We call such paths \textit{repeating}. If we reach this limit, we use the subprocedure \textsc{Strengthen} to strengthen the precondition, inspired by a heuristic by Cook and Koskinen [8]. Here we again calculate a precondition, but when we have found \( \psi_p \), we quantify out all the variables that are written to after \( \psi_p \) and apply quantifier elimination (QE) to get \( \rho_p \). We then refine with \( \neg \rho_p \). This leads to a more aggressive pruning of the transition relation. This heuristic can lead to additional incompleteness.

\textit{Example.} Consider the instrumented program to the right. Suppose we have initially \( \varphi \triangleq i \geq 0 \). We might get \( \text{cex}_1 : 0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 1 \rightarrow 6 \) as a first counterexample. The \textsc{Refine} procedure finds the weakest precondition \( k \geq 0 \land i = 0 \) at location 1. Adding its negation to \( \varphi \) and simplifying the formula gives us \( \varphi \triangleq (i \geq 0) \land (k < 0 \lor i \geq 1) \). Now we may get \( \text{cex}_2 : 0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 1 \rightarrow 6 \) as next counterexample, and \textsc{Refine} updates \( \varphi \triangleq (i \geq 0) \land (k < 0 \lor i \geq 1) \). Now we may get \( \text{cex}_3 : 0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 1 \rightarrow 6 \) as next counterexample. Note that \( \text{cex}_1, \text{cex}_2, \text{cex}_3 \) are repeating counterexamples and if we just use the \textsc{Refine} procedure, \textsc{Underapproximate} gets stuck in a sequence of infinite counterexamples. Now \textsc{Strengthen} identifies the repeating counterexamples, considers \( \text{cex}_1 \) and calculates the weakest precondition \( \psi_1 \triangleq k \geq 0 \land i = 0 \). It then existentially quantifies out variable \( i \) as it gets modified later along \( \text{cex}_1 \). We get \( \exists i. k \geq 0 \land i = 0 \), and quantifier elimination yields \( \rho_1 \triangleq k \geq 0 \). Clearly \( \psi_1 \) entails \( \rho_1 \). Adding \( \neg \rho_1 \) to \( \varphi \) and simplifying the formula we get \( \varphi \triangleq i \geq 0 \land k < 0 \). Now all repeating counterexamples are eliminated, the program is safe, and we have obtained a closed recurrence set witnessing nontermination of the original program.

In the \textsc{Underapproximate} procedure, once there are no further counterexamples to safety of \( P \), we know that in \( P \) the loop exit is not reachable. The procedure returns the final underapproximation (denoted by \( P' \)) that is safe.

When \textsc{Underapproximate} returns to \textsc{Prover}, we check if in \( P' \) the original loop \( L \) after refinements has a closed recurrence set. We refer to the refined loop as \( L' \). In order to check the existence of a closed recurrence set, we first need to ensure that \( L' \) is reachable in \( P' \) even after the refinements. We again pose this problem as a safety/reachability problem. This time we mark the header node of \( L' \) as an error location in \( P' \) and hope that \( P' \) is unsafe. If \( P' \) is safe then clearly we have failed to prove nontermination and we report the result as unknown. If \( P' \) is unsafe, then the counterexample to its safety is a path to the header of \( L' \). We enumerate all such paths to the header of \( L' \) in a set \( \Pi \) (generated lazily
in our implementation). For each such path $\pi \in \Pi$ we then create a simplified CFG $P'$ by concatenating $\pi$ to $L'$, thus eliminating other paths to $L'$.

At this point, we are sure that the header of $L'$ is reachable and there is no path that can reach the exit location of $L'$. However refinements in UNDERAPPROXIMATE may have restricted the nondet statements inside $L'$ by strengthening the assume statements associated with them. Thus a reachable state at the nondeterministic assignment node may not have a successor along its outgoing edge. This would bring our alleged infinite execution to a halt. The safety checker cannot detect this since then the path just gets blocked at this node, and the error location at the exit of $L'$ cannot be reached.

**Example.** Consider the instrumented program in Fig. 4. Suppose initially $\varphi \triangleq \text{true}$. The original program (without instrumentation) is clearly terminating. Our algorithm might give $\text{cex}_1: 0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 6 \rightarrow 1 \rightarrow 7$ as the first counterexample. The nondet statement at node 2 gets restricted by updating $\varphi \triangleq (j \leq 3 \lor i == 9)$. Now we might get $\text{cex}_2: 0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 6 \rightarrow 1 \rightarrow 7$ as the next counterexample. Our algorithm restricts the nondet statement at node 2 by updating $\varphi \triangleq (j \leq 3 \lor i == 9) \land (j \geq 4 \lor i == 11)$.

However now there are no further counterexamples, and the safety checker returns safe. The state $s \models i = 10$ at node 2 has no successor along the outgoing edge as there is no way to satisfy the condition $\varphi$ and the execution is halted, so it would be unsound to report the result as Nonterminating.

Note that at first it may appear that adding another outgoing edge to node 2 with $j := \text{nondet}(); \text{assume}(\neg \varphi)$; and marking the next node as an error node would help us catch the halted execution. However the problem is that this would discover again all of the previously eliminated counterexamples as well. Thus we need a special check by the VALIDATE procedure, which we describe next.

VALIDATE takes as input the final underapproximation $P'$. It first calculates a location invariant at every nondet. assignment node inside the outermost loop $L'$ in $P'$. Let $l$ be a nondet. assignment node with: $v := \text{nondet}(); \text{assume}(\varphi)$; Let $inv$ be a location invariant at $l$. VALIDATE then checks if (6) is valid. This formula checks if for all reachable states at $l$, a choice can be made for the nondet assignment obeying $\varphi$ (and thus Condition (4) holds). VALIDATE returns true iff (6) holds for all nondet statements in $L'$.

**Example.** Consider the program in Fig. 1(f). Using a standard invariant generator we calculate the invariant $i \geq 0$ before line 4. Substituting in (6) we get, $i \geq 0 \rightarrow \exists i'. i' \geq 0$. Clearly the formula is valid. Note that in most of the cases
even the weakest invariant true can be sufficient to prove validity of (6). In this example as well we can easily prove that true → ∃ i', i' ≥ 0 is valid.

Moreover, consider the program in Fig. 4. Suppose ϕ ≜ (j ≤ 3 ∨ i == 9) ∧ (j ≥ 4 ∨ i == 11). Using an invariant generator, we obtain the location invariant i = 10 at location 2. Then (6) becomes i = 10 → ∃ j. (j ≤ 3 ∨ i = 9) ∧ (j ≥ 4 ∨ i = 11). Clearly the formula is not valid. In this case Validate returns false.

If Validate returns true, we are sure that every reachable state at the nondeterministic assignment node in L' has a successor along the edge. At this point, we report nontermination and return the final underapproximation P' of P as a proof of nontermination for P: P' is a closed recurrence set.

Note that as invariants are overapproximations, we may report unknown in some cases even when the discovered underapproximation actually does have a closed recurrence set. However, the check is essential to retain soundness.

**Theorem 3 (Correctness of Prover for Nontermination).** Let P be a program and L a loop in P. Suppose Prover (P, L) = Nonterminating, P'. Then P is nonterminating.

### 4 Nested Loops

Our algorithm can handle nested loops easily. That is a part of the beauty of the reduction to safety, as existing safety provers (e.g. SLAM, IMPACT, etc.) handle nested loops with ease. Note that technically we only need to consider an outermost loop. Consider the instrumented program with nested loops to the right. Here the outer loop decreases the value of i 10 times and then it is the inner loop that is nonterminating. However, it suffices only to consider the outermost loop for safety as the assert(false) at the end of the outer loop is not reachable, but the head of the outer loop is reachable, so that we have proved nontermination.

**Tricky example.** We close with an example that partially explains the advantage seen for our tool over TNT (discussed in Sect. 5). Consider the program to the right (already shown with our algorithm’s instrumentation, initially with ϕ ≜ true). This program clearly does not terminate, yet TNT will fail to prove it. In fact, our implementation of TNT which follows the strategy discussed for enumerating lassos [16] diverges looking at larger and larger cyclic paths (i.e. straight-line code from a location back to that location). The difficulty here is that each cyclic path is well-founded. Consider e.g. this cyclic path from the head h of the outer loop back to h:

\[
k ≥ 0, \quad k := k + 1, \quad j := k, \quad j ≥ 1, \quad j := j - 1, \quad j < 1, \quad k ≥ 0
\]

This path is well-founded. In fact the path cannot be repeated. The root of the problem is the command sequence j ≥ 1, j := j - 1, j < 1, which tells us that j goes from exactly 1 to 0. Because j = 1 before entering the inner loop, we know
that \( k = 1 \), thus by the \( k := k + 1 \) command we know that \( k = 0 \) at the start of the loop’s execution. Thus the command sequence respects the following condition: \( k' > k \land k' \leq 1 \), and thus it is well-founded. Hence, the lasso-based tool TNT will never be able to prove nontermination of this program. The tool AProVE cannot prove such \textit{aperiodic} nontermination for nested loops either [5].

Our approach, however, does not fall victim to this problem. It will find the path: \( k < 0 \), resulting in \( \varphi \triangleq k \geq 0 \). As \texttt{assert(false)} is unreachable with this restriction (and the loop is still reachable), we have proved nontermination.

5 Related work

Automatic tools for proving nontermination of term rewriting systems include [14, 23]. However, while nontermination analysis for term rewriting considers the \textit{entire} state space as legitimate initial states for a (possibly infinite) evaluation sequence, our setting also factors in reachability from the initial states.

Static nontermination analysis has also been investigated for logic programs (\textit{e.g.} [24, 31]). Most related to our setting are techniques for constraint-logic programs (CLPs) [25]. Termination tools for CLPs (\textit{e.g.} [25]) can in cases be used to prove nontermination of imperative programs (\textit{e.g.} JULIA [26] can show nontermination for Java Bytecode programs if the abstraction to CLPs is exact, but gives no witness like a recurrence set to the user). The main difficulty for imperative programs is that typically overapproximating abstractions (in general unsound for nontermination) are used for converting languages like Java and C to CLPs.

TNT [16] uses a characterization of nontermination by recurrence sets. We build upon this notion and introduce closed recurrence sets in our formalization, as an intermediate concept during our nontermination proof search. In contrast to us, TNT is restricted to programs with \textit{periodic} “lasso-shaped” counterexamples to termination. We support unbounded nondeterminism in the program’s transition relation, whereas TNT is restricted to deterministic commands.

The tool \textsc{Invel} [30] analyzes nontermination of Java programs using a combination of theorem proving and invariant generation. However, \textsc{Invel} does not provide a witness for nontermination. Like Brockschmidt \textit{et al.} [5], we were unable to obtain a working version of \textsc{Invel}. Note that in the empirical evaluation by Brockschmidt \textit{et al.} [5], the AProVE tool (which we have compared against) subsumed \textsc{Invel} on \textsc{Invel}’s data set. Finally, \textsc{Invel} is only applicable to deterministic (integer) programs, yet our approach allows nondeterminism as well.

Atig \textit{et al.} [1] describe a technique for proving nontermination of multithreaded programs, via a reduction to nontermination reasoning for sequential programs. Our work complements Atig \textit{et al.}, as we provide improvements to the underlying sequential tools that future multithreaded tools can make use of.

The tool \textsc{TREx} [19] combines existing nontermination proving techniques with a \textsc{Terminator}-like [9] iterative procedure. Our new method should complement \textsc{TREx} nicely, as ours is more powerful than the underlying nontermination proving approach previously used [16].
AProVE [13] uses SMT to prove nontermination of Java programs [5]. First nontermination of a loop regardless of its context is shown, then reachability of this loop with suitable values. Drawbacks are that they require recurrence sets to be singletons (after program slicing) or the loop conditions to be invariants.

Gurfinkel et al. [18] present the CEGAR-based model checker Yasm which supports arbitrary CTL properties, such as $\text{EG } p \neq \text{END}$, denoting nontermination. Yasm implements a method of both under and over-approximating the input program. Unfortunately, together with the author of Yasm we were not able to get the tool working on our examples [17]. We suspect that our approach will be faster, as it uses current safety proving techniques, i.e. Impact [20] rather than SLAM-style technology [2]. This is a feature of our approach: any off-the-shelf software model checker can be turned into a nontermination prover.

Nontermination proving for finite-state systems is essentially a question of safety [3]. Nontermination and/or related temporal logics are also supported for more expressive systems, e.g. pushdown automata [28].

Recent work on CTL proving for programs uses an off-the-shelf nontermination prover [8]. We use a few steps when treating nondeterminism which look similar to the approach from [8]. The key difference is that our work provides a nontermination prover, whereas the previous work requires one off-the-shelf.

Gulwani et al. [15] (Claim 3), make a false claim that is similar to our own. Their claim is false, as a nondeterministic program can be constructed which represents a counterexample. Much of the subtlety in our approach comes from our method of dealing with nondeterminism.

6 Experiments

We have built a preliminary implementation of our approach within the tool T2 [10, 4] and conducted an empirical evaluation with it against these tools:

- TNT [16], the original TNT tool was not available, and thus we have reimplemented its constraint-based algorithm with Z3 [11] as SMT backend.
- AProVE [13], via the Java Bytecode frontend, using the SMT-based nontermination analysis by Brockschmidt et al. [5].
- JULIA [29], which implements an approach via a reduction to constraint logic programming described by Payet and Spoto [26].

As a benchmark set, we used a set of 492 benchmarks for termination analysis from a variety of applications also used in prior tool evaluations (e.g. Windows device drivers, the APACHE web server, the POSTGRESQL server, integer approximations of numerical programs from a book on numerical recipes [27], integer approximations of benchmarks from LLBMC [21] and other tool evaluations).5

Of these, 81 are known to be nonterminating and 254 terminating. For 157 examples, the termination status is unknown. These examples include a program whose termination would imply the Collatz conjecture, and the remaining examples are too large to render a manual analysis feasible. On average a CFG in

---

4 We will make our implementation available in the next source code release of T2.

5 Download: http://www0.cs.ucl.ac.uk/staff/C.Fuhs/safety-nontermination
Fig. 5. Evaluation success overview, showing the number of problems solved for each tool. Here (a) represents the results for known nonterminating examples, (b) is known terminating examples, (c) is (previously) unknown examples.

Unfortunately each tool requires a different machine configuration, and thus a direct comparison is difficult. Experiments with our procedure were performed on a dualcore Intel Core 2 Duo U9400 (1.4 GHz, 2 GB RAM, Windows 7). TNT was run on Intel Core i5-2520M (2.5 GHz, 8 GB RAM, Ubuntu Linux 12.04). We ran AProVE on Intel Core i7-950 (3.07 GHz, 6 GB RAM, Debian Linux 7.2). Note that the TNT-/AProVE-machines are significantly faster than the machine our new procedure was run on, thus we can make some adjusted comparison between the tools. For JULIA, an unknown cloud-based configuration was used. All tools were run with a timeout of 60s. When a tool returned early with no definite result, we display this in the plots using the special “NR” (no result) value.

We ran three sets of experiments: (a) all the examples previously known to be nonterminating, (b) all the examples previously known to be terminating, and (c) all the examples where no previous results are known. With (a) we assess the efficiency of the algorithm, (b) is used to demonstrate its soundness, and (c) checks if our algorithm scales well on relatively large and complicated examples. The results of the three sets of experiments are given in Fig. 5, which shows for each tool and for each set (a)–(c) the numbers of benchmarks with nontermination proofs (“Nonterm”), timeouts (“TO”), and no results (“No Res”). (Proofs of termination, found by AProVE and JULIA, are also listed as “No Res”.)

On the 89 deterministic instances of our benchmark set, our implementation proves nontermination of 33 examples, and TNT of 21 examples. We have also experimented with different values for the number of repeated paths before invoking STRENGTHEN. The results are reported in Fig. 6 (runtimes are for successful nontermination proofs).

Fig. 7 charts the difference in power and performance between our implementation and TNT in a scatter plot, in log scale. Here we have included all programs from (a)–(c). Each ‘x’-mark in the plot represents an example from the benchmark. The value of the x-axis plots the runtime of TNT and the y-axis value plots the runtime of our procedure on the same example. Points under the diagonal are in favor of our procedure. Thus, the more ‘x’-marks there are in the lower-righthand corner, the better our tool has performed.

Discussion. Figs. 5(a&c) demonstrate that our technique is overwhelmingly the most successful tool (Fig. 5(b) confirms simply that no tool has demonstrable
soundness bugs). The poor precision of AProVE & JULIA is mainly due to the non-deterministic updates originally present in many of the benchmarks and also introduced by the (automated) conversion of the benchmarks to Java (the two tools’ input syntax). This shows the lack of reliable support of nondeterminism in today’s nontermination tools.

The TNT algorithm requires outright that nondeterminism must not occur in the input. Our implementation of TNT softens this requirement slightly: parts of the program with nondet-assignments are allowed as long as they are not used during the synthesis of recurrence sets.

Finally, we observe in Fig. 6 that the STRENGTHEN procedure provides additional precision for our approach without harming performance.

7 Conclusion

We have introduced a new method of proving nontermination. The idea is to split the reasoning in two parts: a safety prover is used to prove that a loop in an underapproximation of the original program never terminates; meanwhile failed safety proofs are used to calculate the underapproximation. We have shown that nondeterminism can be easily handled in our framework while previous tools often fail. Furthermore, we have shown that our approach leads to performance improvements against previous tools where they are applicable.

Our technique is not restricted to linear integer arithmetic: Given suitable tools for safety proving and for precondition inference, in principle our approach is applicable to any program setting (note that the STRENGTHEN procedure is just an optimization). For future work, e.g. heap programs are a highly promising candidate for nontermination analysis via abduction tools for separation logic [6].

This technical report is an extended version of the conference paper [7].

Acknowledgments. We thank Marc Brockschmidt, Fabian Emmes, Florian Frohn and Fausto Spoto for help with the experiments and Tony Hoare, Jules Villard and the anonymous reviewers for insightful comments.

References

A Proofs

In this appendix we provide the proofs for all theorems introduced in our paper.

Theorem 1 (Closed Recurrence Sets are Recurrence Sets). Let $G$ be a closed recurrence set for $R$ with initial states $I$. Then $G$ is also an (open) recurrence set for $R$ with initial states $I$.

Proof. We only need to show Condition (2), which follows directly from Condition (4) and Condition (5). \qed

Theorem 2 (Open Recurrence Sets Always Contain Closed Recurrence Sets). There exists a recurrence set $G$ for a transition relation $R$ with initial states $I$ iff there exist an underapproximation $R'$ with initial states $I'$ and $G' \subseteq G$ such that $G'$ is a closed recurrence set for $R'$ with initial states $I'$.

Proof. "$\Rightarrow$": Any closed recurrence set $G'$ for some transition relation $R'$ with initial states $I'$ with $R' \subseteq R$ and $I' \subseteq I$ is also a recurrence set for the transition relation $R$ with initial states $I$. 

"$\Rightarrow$": Suppose $G$ is a recurrence set for the transition relation $R$ with initial states $I$. Thus there must exist an infinite $R$-path $\pi$ in $G$ with $\pi \equiv s_0 \xrightarrow{R} s_1 \xrightarrow{R} s_2 \xrightarrow{R} \ldots$ and $s_0 \in I$ such that \{s_i | i \geq 0\} $\subseteq$ $G$. We now set $G' = \{s_i | i \geq 0\}$, $I' = \{s_0\}$, and $R' = \{(s_i, s_{i+1}) | (s_i, s_{i+1}) \in \pi\}$. Thus, $I' \subseteq I$ and $R' \subseteq R$ hold by construction, making $R'$ with initial states $I'$ an underapproximation of $R$ with initial states $I$, and $G' \subseteq G$ is a closed recurrence set for $R'$ with initial states $I'$. \qed

For the proof of correctness of our method, we still need the following concepts and a lemma:

Let $M_P$ be the set of all memory states in $P$. Let $R_L' \subseteq M_P \times M_P$ be the composite transition relation of $L'$. Let $I_L'$ be the set of initial states for $L'$. Formally $I_L'$ is the strongest postcondition after execution of $\pi$.

Lemma 1 (Prover Finds Closed Recurrence Sets for Loops). Let $P$ be a program and $L$ a loop in $P$. Suppose PROVER $(P, L) = Nonterminating, P'$. Then the set of all reachable memory states at the loop header $h$ of $L'$ forms a closed recurrence set for the composite relation $R_L'$ with initial states $I_L'$.

Proof. Let $\Theta \subseteq M$ represent the set of all reachable memory states at the loop header $h$ of $L'$. We need to show Conditions (3), (4), and (5) for $\Theta$.

For Condition (3) for $\Theta$: As $L'$ is reachable via $\pi$ (because $\text{REACHABLE}(P', h)$ holds), we must have $\exists s. I_L'(s)$. We have $I_L' \subseteq \Theta$. Thus we have $\exists s. I_L'(s) \land \Theta(s)$. Thus we have Condition (3) for $\Theta$.

For Condition (4) for $\Theta$: Let $s$ such that $\Theta(s)$. We need to show that there exists some $s'$ such that $R_L'(s, s')$ holds. As finally the safety check in the UNDER-APPROXIMATE loop succeeds, we know that $s$ cannot have a successor along the
exit edge of \( L \). (Otherwise the error location would be reachable and the safety checker would catch it.) By construction of deterministic conditional nodes, the memory state \( s \) at \( h \) must have a successor along the guard edge of \( L' \).

Every reachable memory state at every deterministic conditional node of \( L \) must have a successor along one of its outgoing edges. Similarly, every reachable memory state at every deterministic assignment node of \( L \) must have a successor along its outgoing edge. As \text{VALIDATE} returns \text{true}, every reachable memory state at a nondeterministic assignment node in \( L' \) also has a successor along its outgoing edge. This ensures that there must be a loop path \( \pi \) from memory state \( s \) to a memory state \( s' \) at the loop header going through the loop body such that \( R_\pi(s,s') \). This ensures that \( R_{L'}(s,s') \). Thus we have Condition (4) for \( \Theta \).

For Condition (5) for \( \Theta \): Let \( s, s' \) such that \( \Theta(s) \wedge R_{L'}(s,s') \). Clearly \( s' \) is also a reachable memory state at the loop header of \( L' \) and the definition of \( \Theta \) implies \( \Theta(s') \). Thus we have Condition (5) for \( \Theta \). \( \square \)

Now we are ready for the proof of Thm. 3.

**Theorem 3 (Correctness of Prover for Nontermination).** Let \( P \) be a program and \( L \) a loop in \( P \). Suppose \( \text{PROVER} (P,L) = \text{Nonterminating}, P' \). Then \( P \) is nonterminating.

**Proof.** Let \( L' \) be the loop in \( P' \). Let \( \pi \) be the path to \( L' \) in \( P' \). Let \( L \) be the corresponding loop in \( P \) before the refinements.

Note that every refinement in \( \text{PROVER} \) either restricts the \text{assume} statement at the initial node \( l_i \) representing the precondition for \( P \) or restricts the \text{assume} statement associated with a nondeterministic assignment statement. Thus every edge \( (l, T, l') \) in \( P \) gets refined to the edge \( (l, T', l') \) such that \( R_T \subseteq R_{T'} \).

Now let \( s \) such that \( I_{L'}(s) \). Then we must have \( I_L(s) \), as the memory state \( s \) must be reachable at the header node of \( L \) in \( P \) as well. This gives \( I_{L'} \subseteq I_L \).

Let \( s, s' \) such that \( R_{L'}(s,s') \). We must have \( R_L(s,s') \). This gives \( R_{L'} \subseteq R_L \).

From Lemma 1 we have that the reachable memory states at the loop header of \( L' \) form a closed recurrence set for \( R_{L'} \) with initial memory states \( I_{L'} \). Now Thm. 2 implies the existence of a recurrence set for \( R_L \) with initial states \( I_L \). This proves that \( P \) is nonterminating. \( \square \)