Proving Termination of Imperative Programs Using Max-SMT

Daniel Larraz, Albert Oliveras, Enric Rodríguez-Carbonell, Albert Rubio
Universitat Politècnica de Catalunya, Barcelona, Spain

Abstract—We show how Max-SMT can be exploited in constraint-based program termination proving. Thanks to expressing the generation of a ranking function as a Max-SMT optimization problem where constraints are assigned different weights, quasi-ranking functions—functions that almost satisfy all conditions for ensuring well-foundedness—are produced in a lack of ranking functions. By means of trace partitioning, this allows our method to progress in the termination analysis where other approaches would get stuck. Moreover, Max-SMT makes it easy to combine the process of building the termination argument with the usually necessary task of generating supporting invariants. The method has been implemented in a prototype that has successfully been tested on a wide set of programs.

I. INTRODUCTION

Proving termination is necessary to ensure total correctness of programs. Still, termination bugs are difficult to trace and are hardly notified: as they do not arise as system failures but as unresponsive behavior, when faced to them users tend to restart their devices without reporting to software developers. Due to this, approaches for proving termination of imperative programs have regained an increasing interest in the last decade [1]–[4].

One of the major difficulties in these methods is that often supporting invariants are needed. E.g., in [5] linear invariants are exhaustively computed before termination analysis. In the same paper a heuristic approach is also presented, which only requires a light-weight invariant generator by restricting to single-variable ranking functions. Another solution is proposed in [6], where invariant generation is not performed eagerly but on demand. By formulating both invariant and ranking function synthesis as constraint problems, both can be solved simultaneously, so that only the necessary supporting invariants for the targeted ranking functions—namely, lexicographic linear ranking functions—need to be discovered.

Based on [5], [6], we present a Max-SMT constraint-based approach for proving termination. The crucial observation in our method is that, albeit our goal is to show that transitions cannot be executed infinitely by finding a ranking function or an invariant that disables them, if we only discover an invariant, or an invariant and a quasi-ranking function that almost fulfills all needed properties for well-foundedness, we have made some progress: either we can remove part of a transition and/or we have improved our knowledge on the behavior of the program. A natural way to implement this idea is by considering that some of the constraints are hard (the ones guaranteeing invariance) and others are soft (those guaranteeing well-foundedness) in a Max-SMT framework. Moreover, by giving different weights to the constraints we can set priorities and favor those invariants and (quasi-) ranking functions that lead to the furthest progress.

The technique has been implemented in our tool CppInv, which analyses programs with integer variables and linear expressions. Thanks to it, we have proved termination of a wide set of programs, which have been taken from the programming learning environment Jutge.org [7] and from benchmark suites in the literature [8].

A. Related Work.

As mentioned above, our method is based on [5]. Namely, we have borrowed the core argument for termination proofs, which is based on iteratively discarding those transitions that cannot be executed infinitely. However, we improve on the way supporting invariants are generated. While in [5] invariants are pre-computed in a process that is independent from the termination analysis and which turns out to be the bottleneck of the approach, we find lazily the invariants needed to ensure that ranking functions meet their requirements.

Our research also builds upon [6], where the constraint-based method [9] was first applied to termination. However, we extend this work in several aspects. First, in that approach only linear programs with unnested loops can be handled, while we can deal with arbitrary control structures. Moreover, in [6] the generation of their lexicographic ranking functions requires a higher-level loop that, before sending the constraint problem to the solver, determines the precedence of the transitions in the lexicographic order. On the other hand, in our approach this outer loop is not needed. Finally, thanks to assigning weights to the constraints, unlike [6] we do not need to stipulate the number of supporting invariants that will be needed a priori, and hence our constraint problems are simpler. Further, weights allow us to guide the solving engine in the search of appropriate ranking functions and invariants.

In [10], the lexicographic approach of [6] is extended so as to handle programs with complex control flow. However, their method still requires to search for the right ordering of the transitions in order to obtain a successful termination proof. Moreover, in this technique the procedures for synthesizing ranking functions and auxiliary invariants do not share enough information, while in our proposal these mechanisms are tightly coupled. Finally, in [8] a method closely related to ours is presented. Both approaches, which have been developed independently, go in the same direction of achieving a better cooperation between the invariant and the ranking function.
syntheses. Still, a significant difference is that we can exploit the quasi-ranking functions produced in the absence of ranking functions in order to progress in the termination analysis.

In addition to lexicographic ranking functions, there is a group of effective tools whose termination arguments are based on Ramsey’s Theorem and the notion of transition invariant [11]. Transition invariants are over-approximations of the transitive closure of the transition relation restricted to the reachable state space. The crucial observation is that a transition relation is called disjunctively well-founded, i.e., that is included in the union of well-founded relations, must be well-founded too. Hence, if one is able to find a transition invariant that is also disjunctively well-founded, the program must be terminating. In [12], this transition invariant is computed iteratively, starting from the empty relation, by discovering unranked paths of the program thanks to a reachability check, and using the approach in [3] for synthesizing new ranking functions for them. On the other hand, in [13] the generation of the disjunctively well-founded transition invariant is performed bottom-up from innermost loops by identifying invariant and transitive relations among a set of templates that are disjunctively well-founded by construction. Nested loops are then handled thanks to loop summarization. Our techniques can also be seen as producing a disjunctively well-founded transition invariant, being the difference with respect to the previous approaches in the way new unranked paths are identified and how a termination argument is generated for them.

Finally, a problem related to proving termination that has recently raised interest in the area is that of conditional termination: to synthesize automatically preconditions on the inputs that ensure program termination. In this context, in [13] the authors consider what they call potential ranking functions, which are functions over program states that are bounded but not necessarily decreasing. The quasi-ranking functions that we consider here are more general, as for instance functions that are increasing but not bounded are also included. In [16], the problem of conditional termination is also considered. The approach is based on disjunctively well-founded relations as in [12], but instead of identifying unranked program paths, thanks to a dual inclusion the authors partition the transition relation into those behaviors already proved to be terminating and those whose status is still unknown. In our work we also proceed by splitting the transition relation into a terminating part and an unknown part. However, in [16] this division is achieved by means of a fixpoint computation, while our approach is constraint-based.

II. PRELIMINARIES

A. SMT and Max-SMT

Let $P$ be a finite set of propositional variables. If $p \in P$, then $p$ and $\neg p$ are literals. The negation of a literal $l$, written $\neg l$, denotes $\neg p$ if $l$ is $p$, and $p$ if $l$ is $\neg p$. A clause is a disjunction of literals. A propositional formula is a conjunction of clauses. The problem of propositional satisfiability (abbreviated as SAT) consists in, given a formula, to determine whether or not it is satisfiable, i.e., if it has a model: an assignment of Boolean values to variables that satisfies the formula.

An extension of SAT is the satisfiability modulo theories (SMT) problem [17]: to decide the satisfiability of a given quantifier-free first-order formula with respect to a background theory. Here we will consider the theories of linear arithmetic (LA), where literals are linear inequalities, and the more general theory of non-linear arithmetic (NA), where literals are polynomial inequalities.

Another generalization of SAT is the Max-SAT problem [17]: it consists in, given a weighted formula $F$ where each clause $C_i$ has a weight $\omega_i$ (a positive number or infinity), to find the assignment such that the cost, i.e., the sum of the weights of the falsified clauses, is minimized. Clauses with infinite weight are called hard, while the rest are called soft. Equivalently, the problem can be seen as finding the model of the hard clauses such that the sum of the weights of the falsified soft clauses is minimized.

Finally, the problem of Max-SMT[18] merges Max-SAT and SMT, and is defined from SMT analogously to how Max-SAT is derived from SAT. Namely, the Max-SMT problem consists in, given a weighted formula, to find an assignment that minimizes the sum of the weights of the falsified clauses in the background theory.

B. Transition Systems, Invariants and Ranking Functions

Henceforth we will model imperative programs by means of transition systems. A transition system $S = (\mathcal{L}, \Theta, T)$ consists of a tuple of variables $\mathcal{V}$, a set of locations $\mathcal{L}$, a map $\Theta$ from locations to formulas characterizing the initial values of the variables, and a set of transitions $T$. Each transition $\tau \in T$ is a triple $(l, l', \rho)$, where $l, l' \in \mathcal{L}$ are the pre and post locations respectively, and $\rho$ is the transition relation: a formula over the program variables $\mathcal{V}$ and their primed versions $\mathcal{V}'$, which represent the values of the variables after the transition. See Fig. 1 for an example of a program together with a corresponding representation as a transition system.

From now on we assume that variables take integer values and programs are linear, i.e., the initial conditions $\Theta$ and transition relations $\rho$ are described as conjunctions of linear inequalities. Strict inequalities may be translated into non-strict ones thanks to the integer type of the variables.

```c
int main() {
    int x, y, z;
    \ell_1: while (y \geq 1) {
        x = x - 1;
        y = y + 1;
    }
    \ell_2: while (y < z) {
        x = x + 1;
        z = z - 1;
    }
    y = x + y;
}
```

Fig. 1. Program and its transition system.
A state is an assignment of a value to each of the variables in $\tau$. A configuration is a pair $(\ell, \sigma)$ consisting of a location $\ell$ and a state $\sigma$. A computation is a (possibly infinite) sequence of configurations $(\ell_0, \sigma_0), (\ell_1, \sigma_1), \ldots$ such that $\sigma_0 \models \Theta(\ell_0)$, and for each pair of consecutive configurations $(\ell_i, \sigma_i)$ and $(\ell_{i+1}, \sigma_{i+1})$, there exists a transition $\tau = (\ell_i, \ell_{i+1}, \rho) \in T$ such that $(\sigma_i, \sigma_{i+1}) \models \rho$. A configuration $(\ell, \sigma)$ is reachable if there exists a computation ending at $(\ell, \sigma)$. A transition system is said to be terminating if all its computations are finite. The problem that we target in this work is, given a transition system, to determine if it is terminating or not.

A transition $\tau = (\ell, \ell', \rho)$ is disabled if it can never be executed, i.e., if for all reachable configuration $(\ell, \sigma)$, there does not exist any $\sigma'$ such that $(\sigma, \sigma') \models \rho$. A transition $\tau$ is called finitely executable if in any computation, $\tau$ is only executed a finite number of times (in particular, if $\tau$ is disabled). Otherwise, i.e., if there exists a computation where $\tau$ is executed infinitely, we say that $\tau$ is infinitely executable.

An assertion is a first-order formula over $\tau^*$. An assertion $I$ is an invariant at location $\ell$ if for any reachable configuration $(\ell, \sigma)$, it holds that $\sigma \models I$. An invariant map $\mu$ assigns an invariant $\mu(\ell)$ to each of the locations $\ell$. An important class of invariant maps is that of inductive invariant maps:

Definition 1: An invariant map $\mu$ is said to be inductive if:

- [Initiation] For every location $\ell \in \mathcal{L}$: $\Theta(\ell) \models \mu(\ell)$
- [Consequence] For every transition $\tau = (\ell, \ell', \rho) \in T$: $\mu(\ell) \wedge \rho \models \mu(\ell')$

Invariants are fundamental when analyzing program termination. For instance, a transition $\tau = (\ell, \ell', \rho)$ is proved to be disabled if there is an invariant $\mu(\ell)$ at location $\ell$ such that $\mu(\ell) \wedge \rho$ is unsatisfiable. In general, if $\mu$ is an invariant map, then any transition $\tau = (\ell, \ell', \rho)$ can be safely strengthened by replacing the transition relation $\rho$ by $\mu(\ell) \wedge \rho$.

The basic idea of the approach we follow for proving program termination is to argue by contradiction that no transition is infinitely executable. First of all, no disabled transition can be infinitely executable trivially. Moreover, one just needs to focus on transitions joining locations in the same strongly connected component (SCC): if a transition is executed over and over again, then its pre and post locations must belong to the same SCC. So let us assume that one has found a ranking function for such a transition $\tau$, according to:

Definition 2: Let $\tau = (\ell, \ell', \rho)$ be a transition such that $\ell$ and $\ell'$ belong to the same SCC, denoted by $C$. A function $R : \mathcal{T} \rightarrow \mathbb{Z}$ is said to be a ranking function for $\tau$ if:

- [Boundedness] $\rho \models R \geq 0$
- [Strict Decrease] $\rho \models R > R'$
- [Non-increase] For every $\tau' = (\ell, \ell', \rho') \in \mathcal{T}$ such that $\ell, \ell' \in C$: $\rho' \models R \geq R'$

Note that boundedness and strict decrease only depend on $\tau$, while non-increase depends on all transitions in the SCC.

The key result is that if $\tau = (\ell, \ell', \rho)$ admits a ranking function $R$, then it is finitely executable. Indeed, first notice that if one can execute $\tau$ from a configuration $(\ell, \sigma)$ then $R(\sigma) \geq 0$, because of boundedness. Also, the value of $R$ at the states along any path contained in $C$ cannot increase, thanks to the non-increase property. Moreover, in any cycle contained in $C$ traversing $\tau$, the value of $R$ strictly decreases, due to the strict decrease property. Now, let us assume that there was a computation where $\tau$ was executed infinitely. Such a computation would eventually visit only locations in $C$. Because of the previous observations, by evaluating $R$ at the states at which $\tau$ is executed we could construct an infinitely decreasing sequence of non-negative integers, a contradiction.

Finitely executable transitions can be safely removed from the transition system as regards termination analysis. This in turn may break the SCC’s into smaller pieces. If by applying this reasoning recursively one can prove that all transitions are finitely executable, then the transition system is terminating.

C. Constraint-Based Program Analysis

Here we review the constraint-based program analysis approach [6, 9]. The idea is to consider a template for candidate invariant properties (respectively, ranking functions), e.g., linear inequalities (linear expressions). These templates involve both program variables as well as unknowns whose values have to be determined so as to ensure the required properties. To this end, the implications in Definition 1 (Definition 2) are expressed by means of constraints (hence the name of the approach) on the unknowns. If implications are encoded soundly, any solution to the constraints yields an invariant map (ranking function). Specifically, if linear arithmetic is the target language, this can be achieved with Farkas’ Lemma:

Theorem 1 (Farkas’ Lemma): Let $S$ be a system of linear inequalities $Ax + b \leq 0$ ($A \in \mathbb{R}^{m \times n}, b \in \mathbb{R}^m$) over real variables $x^T = (x_1, \ldots, x_n)$. When $S$ is satisfiable, it entails a linear inequality $c^T x + d \leq 0$ ($c \in \mathbb{R}^n, d \in \mathbb{R}$) iff there is $\lambda \in \mathbb{R}^m$ such that $\lambda \geq 0$, $c^T = \lambda^T A$ and $d \leq \lambda^T b$. Further, $S$ is unsatisfiable iff $1 \leq 0$ can be so derived.

For clarity, henceforth the following notation is used. Given a conjunction of linear inequalities $Ax + b \leq 0$ and a linear inequality $c^T x + d \leq 0$, where the coefficients $a_{ij}, b_i, c_j, d$ may be real numbers or unknowns, we denote by $Ax + b \leq 0 \perp c^T x + d \leq 0$ the set of constraints on the unknown coefficients and on fresh real unknowns $\lambda = (\lambda_1, \ldots, \lambda_m)$, consisting in $\lambda \geq 0$, $c^T = \lambda^T A$ and $d \leq \lambda^T b$.

III. Termination Analysis with Max-SMT

In this section we first describe a constraint-based method for termination analysis that uses SMT and identify some of its shortcomings (Sect. III-A). Then we show how Max-SMT can be used to overcome these limitations (Sect. III-B).

A. An SMT Approach to Proving Termination

Following the approach described in Sect. III-B [5], to show that a transition $\tau$ is finitely executable and thus discard it, one needs either a disability argument or a ranking function for it. To this end we construct a constraint system, i.e., an SMT formula, whose solutions correspond to either an invariant that proves disability, or a ranking function. Given an SCC, the constraint system, if satisfiable, will allow discarding (at least,
but possibly more than) one of the transitions in the SCC. By iterating this procedure until no cycles are left we will obtain a termination argument for the SCC.

To construct the constraint system, first of all we consider:
- for each location $\ell$, a linear invariant template $I_\ell(\tau) \equiv i_{\ell,0} + \sum v \in P i_{\ell,v} \cdot v \leq 0$, where $i_{\ell,0}$, $i_{\ell,v}$ are unknown;
- a linear ranking function template $R(\tau) \equiv r_0 + \sum v \in P r_v \cdot v$,
  where $r_0$, $r_v$ are unknown.

Recall that ranking functions are associated to transitions, not to locations. However, instead of introducing a template for each transition, we just have one single template, which, if the constraint system has a solution, will be a ranking function for a transition to be determined by the solver.

Similarly to [8], we take the following constraints from the definitions of inductive invariant and ranking function:

**Initiation:** For $\ell \in L$,
$$I_\ell \defeq \Theta(\ell) \vdash I_\ell$$

**Disability:** For $\tau = (\ell, \ell', r) \in T$:
$$D_\tau \defeq I_\ell \land \rho + 1 \leq 0$$

**Consecution:** For $\tau = (\ell, \ell', r) \in T$:
$$C_\tau \defeq I_\ell \land \rho \land \neg I_{\ell'}$$

**Boundedness:** For $\tau = (\ell, \ell', r) \in T$:
$$B_\tau \defeq I_\ell \land \rho \land R \geq 0$$

**Strict Decrease:** For $\tau = (\ell, \ell', r) \in T$:
$$S_\tau \defeq I_\ell \land \rho \land R > R'$$

**Non-increase:** For $\tau = (\ell, \ell', r) \in T$:
$$N_\tau \defeq I_\ell \land \rho \land R \geq R'$$

Let $L$ and $T$ be the sets of locations and transitions in the SCC in hand, respectively. Let also $P$ be the set of pending transitions, i.e., which have not been proved to be finitely executable yet. Then we build the next constraint system:
$$\bigwedge_{\ell \in L} I_\ell \land \bigwedge_{\tau \in T} (D_\tau \lor C_\tau) \land \bigvee_{\tau \in P} (D_\tau \lor (B_\tau \land S_\tau)) \land ((\bigwedge_{\tau \in P} N_\tau) \lor \bigvee_{\tau \in P} D_\tau).$$

The first two conjuncts guarantee that an invariant map is computed; the other two, that at least one of the pending transitions can be discarded. Notice that, if there is no disabled transition, we ask that all transitions in $P$ are non-increasing, but only that at least one transition in $P$ (the next to be removed) is both bounded and strict decreasing. Note also that for finding invariants one has to take into account all transitions in the SCC, even those that even have been proved to be finitely executable: otherwise some reachable states might not be covered, and the invariant generation would become unsound. Hence in our termination analysis we consider two transition systems: the original transition system for invariant synthesis, whose transitions are $T$ and which remains all the time the same; and the termination transition system, whose transitions are $P$, i.e., where transitions already shown to be finitely executable have been removed. This duplication is similar to the cooperation graph of [8].

However, this first approach is problematic when a ranking function needs several invariants. A possible solution is to add more templates iteratively, so that for example initially invariants consisting of a single linear inequality are tried, if unsuccessful then invariants consisting of a conjunction of two linear inequalities are tried, etc. But when proceeding in this way, all problems before the right number of invariants is found are unsatisfiable. This is wasteful, as no constructive information is retrieved from unsatisfiable constraint systems.

Another problem with this method for analyzing termination is that the kind of termination proofs it yields may be too restricted. More specifically, when one proves that a transition $\tau$ is finitely executable, then a single termination argument shows there is no computation where $\tau$ appears infinitely. Although this produces compact proofs, on the other hand sometimes there may not exist such a unique reason for termination, and it becomes necessary a more fine-grained examination. However, the approach as presented so far does not provide a natural way or guidance for refining the analysis.

**B. A Max-SMT Approach to Proving Termination**

The main contribution of our work is to show that the constraint system can be expressed in such a way that, even if it turns out to be unsatisfiable, some information useful for refining the termination analysis can be obtained. The key observation is that, even though our aim is to prove transitions to be finitely executable (by finding a ranking function or an invariant that disables them), if we just find an invariant, or an invariant and a quasi-ranking function that is close to fulfill all required conditions, we have progressed in our analysis.

The idea is to consider the constraints guaranteeing invariance as hard, so that any solution to the constraint system will satisfy them, while the rest are soft. Let us consider propositional variables $p_B$, $p_S$, and $p_N$, which intuitively represent if the conditions of boundedness, strict decrease and non-increase in the definition of ranking function are violated respectively, and corresponding weights $\omega_B$, $\omega_S$ and $\omega_N$. We consider now the next constraint system (where soft constraints are written $[\cdot, \omega]$, and hard ones as usual):
$$\bigwedge_{\ell \in L} I_\ell \land \bigwedge_{\tau \in T} (D_\tau \lor C_\tau) \land \bigvee_{\tau \in P} (D_\tau \lor (B_\tau \lor (S_\tau \lor p_B))) \land (\bigwedge_{\tau \in P} N_\tau) \lor \bigvee_{\tau \in P} D_\tau \lor (\neg p_B, \omega_B) \lor \neg p_S, \omega_S \lor \neg p_N, \omega_N.$$

Note that ranking functions have cost 0, and (if no transition is disabled) functions that fail in any of the conditions are penalized with the respective weight. Thus, the Max-SMT solver looks for the best solution and gets a ranking function if feasible; otherwise, the weights guide the search to get invariants and quasi-ranking functions that satisfy as many conditions as possible.

Hence this Max-SMT approach allows recovering information even from problems that would be unsatisfiable in the initial method. This information can be exploited to perform dynamic trace partitioning [19] as follows. Assume that the optimal solution to the above Max-SMT formula has been computed, and let us consider a transition $\tau \in P$ such that $D_\tau \lor (B_\tau \lor p_B) \lor (S_\tau \lor p_B)$ evaluates to true in the solution. Then we distinguish several cases depending on the properties satisfied by (and the computed function $R$):
- If $\tau$ is disabled then it can be removed.
- If $R$ is non-increasing and satisfies boundedness and strict decrease for $\tau$, then $\tau$ can be removed too: $R$ is a ranking function for it.
- If $R$ is non-increasing and satisfies boundedness for $\tau$ but not strict decrease, one can split $\tau$ in the termination
transition system into two new transitions: one where $R > R'$ is added to $\tau$, and another one where $R = R'$ is enforced. Then the new transition with $R > R'$ is automatically eliminated, as $R$ is a ranking function for it. Equivalently, this can be seen as adding $R = R'$ to $\tau$. Now, if the solver could not prove $R$ to be a true ranking function for $\tau$ because it was missing an invariant, this transformation will guide the solver to find that invariant so as to disable the transition with $R = R'$.

- If $R$ is non-increasing and satisfies strict decrease for $\tau$ but not boundedness, the same technique from above can be applied: it boils down to adding $R < 0$ to $\tau$.
- If $R$ is non-increasing but neither strict decrease nor boundedness are fulfilled for $\tau$, then $\tau$ can be split into two new transitions: one with $R < 0$, and another one with $R \geq 0 \land R = R'$.
- If $R$ does not satisfy the non-increase property, then it is rejected; however, the invariant map from the solution can be used to strengthen the transition relations for the following iterations of the termination analysis.

Note this analysis may be worth applying on other transitions $\tau$ in the termination transition system apart from those that make $D_\tau \lor (D_\tau \lor p_S) \land (S_\tau \lor p_S)$ true. E.g., if $R$ is a ranking function for a transition $\tau$ but fails to be so for another one $\tau'$ because strict decrease does not hold, then, according to the above discussion, $\tau'$ can be strengthened with $R = R'$.

On the other hand, working in this iterative way requires imposing additional constraints to avoid getting to a standoff. Namely, in the case where non-increase does not hold and so one would like to exploit the invariant, it is necessary to impose that the invariant is not redundant. More in detail, let us consider a fixed location $\ell$, and let $I_1^{(1)}, \ldots, I_2^{(k)}$ be the previously computed invariants at location $\ell$. Then $I_\ell$, the invariant to be generated at $\ell$, is redundant if it is implied by $I_1^{(1)}, \ldots, I_2^{(k)}$, i.e., if $\exists \ell \in L. E_\ell$ so we impose $p_{\ell} \rightarrow \neg \land_{\ell \in L} E_\ell$ to ensure that violating non-increase leads to non-redundant invariants. Conditions are added similarly to avoid redundant quasi-ranking functions.

Another advantage of this Max-SMT approach is that by using different weights we can express priorities over conditions. Since, as explained above, violating the property of non-increase invalidates the computed function $R$, it is convenient to make $\omega_S$ the largest weight. On the other hand, when non-increase and boundedness are fulfilled but not strict decrease an equality is added to the transition, whereas when non-increase and strict decrease are fulfilled but not boundedness just an inequality is added. As we prefer the former to the latter, in our implementation (see Sect. we set $\omega_S > \omega_B$.

A further improvement is the generation of termination implications. A termination implication at a location $\ell$ is an assertion $J(\Pi)$ such that any transition in the termination transition system that leads into $\ell$ implies it, i.e., it holds that $\rho \models J(\Pi)$, where $\rho$ is the relation of the transition. Thus, $J$ will eventually hold when $\ell$ is reached (although, unlike ordinary invariants, may not initially be true; see

\[ \Theta(\ell_1) \equiv \text{true} \quad \Theta(\ell_2) \equiv \text{false} \]

\[ \rho_{\ell_2}: \quad y \geq 1, \quad x' = x - 1, \quad y' = y, \quad z' = z \]

\[ \rho_{\ell_3}: \quad y < z, \quad x' = x + 1, \quad y' = y, \quad z' = z - 1 \]

\[ \rho_{\ell_4}: \quad y \geq z, \quad x' = x, \quad y' = x + y, \quad z' = z \]

\[ \rho_{\ell_5}: \quad y \geq 1, \quad y \geq z, \quad x' = x, \quad y' = x + y, \quad z' = z \]

![Fig. 2. Evolution of the termination transition system: initially (a) and after the first (b), second (c) and third (d) round.](image)

Example [1 below]. Hence, it can be propagated forward in the termination transition system to the transitions going out from $\ell$. To produce termination implications, for each location $\ell$ a new linear inequality template $J_{\ell}(\Pi)$ is introduced and the following constraint is imposed: $\land_{\ell_1(\ell, \ell'), \ell_2(\ell, \ell') \in P(\Pi)} (D_\ell \lor I_\ell \land \rho \models J_{\ell}(\Pi))$. Additional constraints are enforced to ensure that new termination implications are not redundant with the already computed invariants and termination implications.

\textbf{Example 1:} Let us show a termination analysis of the program in Fig. 1. In the first round, the solver finds the invariant $y \geq 1$ at $\ell_2$ and the ranking function $z$ for $\ell_2$. While $y \geq 1$ can be added to $\tau_1$ (resulting into a new transition $\tau_1'$), the ranking function allows eliminating $\tau_2$ from the termination transition system (see Fig. 2(b)).

In the second round, the solver cannot find a ranking function. However, thanks to the Max-SMT formulation, it can produce the quasi-ranking function $x$, which is non-increasing and strict decreasing for $\tau_1$, but not bounded. This quasi-ranking function can be used to split transition $\tau_1$ into two new transitions $\tau_{1,1}$ and $\tau_{1,2}$ as follows:

\[ \rho_{\tau_{1,1}}: \quad x \geq 0, \quad y \geq 1, \quad x' = x - 1, \quad y' = y, \quad z' = z \]

\[ \rho_{\tau_{1,2}}: \quad x < 0, \quad y \geq 1, \quad x' = x - 1, \quad y' = y, \quad z' = z \]

Then $\tau_{1,1}$ is immediately removed, since $x$ is a ranking function for it. The current termination transition system is given in Fig. 2(c).

In the third and final round, the termination implication $x < 0$ is generated at $\ell_2$, together with the ranking function $y$ for transition $\tau_2'$. Note that the termination implication is crucial to prove the strict decrease of $y$ for $\tau_2'$, and that the previously generated invariant $y \geq 1$ at $\ell_2$ is needed to ensure boundedness. Now $\tau_3'$ can be removed, which makes the graph acyclic (see Fig. 2(d)). This concludes the termination proof.
The method presented in Sect. III has been implemented in the tool CppInv. This section describes this implementation.

CppInv admits code written in C++ as well as in the language of T2 [10]. The system analyzes programs with integer variables, linear expressions and function calls. Variables of other data types, such as floating-point variables, are treated as unknown values. Function calls are handled with techniques similar to those in [20], although currently the returned value is ignored. Further, for recursive functions, after a function call we assign unknowns to all variables that can be modified in the call (i.e., global variables and variables passed by reference).

In the transformation from the source code to the internal transition system representation, CppInv attempts to reduce the number of locations by composing transitions. Still, this preprocessing may result in an exponential growth in the number of transitions. As our technique does not require minimized transition systems for soundness, the tool stops this location minimization if a threshold number of transitions is reached. Moreover, whenever a chain of locations connected by transitions that do not modify variables (see Fig. 3) is detected, CppInv does not attempt to eliminate the locations: since no variable is updated, in these transitions any function satisfies the non-increase condition, while no ranking function is possible. For this reason, when producing the constraints, these transitions are ignored as far as termination is concerned, and are only considered for the generation of invariants.

Once the input is represented as a transition system, the actual termination analysis starts. See function proved_TS_term:

```cpp
bool proved_TS_term(TermSys S) { // (C, <) = compute_SCCs_and_topologically_sort(S);
  for (C ∈ C by <) { // (L, T) = (locations(C), transitions(C));
    P = copy(T);
    for (ℓ ∈ L : ∃(ℓ, ℓ′, ρ) ∈ T with ℓ ∈ C < C) // (ℓ, τ(ℓ)) = Θ(ℓ) ∨ SPost(ρ);
      if (not proved_SCC_term(L, T, P)) return false; }
  return true; }
```

The SCC’s are computed and topologically sorted, and each SCC is processed according to ordering < (C, <) = compute_SCCs_and_topologically_sort(S). Processing an SCC involves first performing a copy of the transitions for keeping track of those not proven finitely executable yet. Then the initial conditions are updated with the strongest postconditions of the incoming transitions from previous SCC’s, where the strongest postcondition of a transition relation ρ(⃗{v}, ⃗{w}) is the assertion SPost(ρ(⃗{v}, ⃗{w})) = ∃⃗{w′} ρ(⃗{w}, ⃗{w′}). Finally the SCC is analyzed for termination. If it could not be proved terminating, the procedure stops. Otherwise the next SCC is dealt with.

The analysis of termination of SCC’s is orchestrated by the function proved_SCC_term:

```cpp
bool proved_SCC_term(SetLoc L, SetTrans T, SetTrans P) { // (dis_trans(L, T, P) or rank_fun(L, T, P) or term_impl(L, T, P))
  if (P == ∅) return true;
  if (T′ = transitions(C);
      if (T′ ≠ ∅ and not proved_SCC_term(L, T, T′)) return false; }
  return true;
}
```

It takes as arguments: a set of locations L and a set of transitions T, corresponding to an SCC of the transition system; and the termination transition system: a non-empty set P ⊆ T of transitions that still have to be proved finitely executable. As explained in Sect. II-B one may assume that the graph induced by P is strongly connected. The function returns true if all transitions in P can be proved finitely executable. We found out that, instead of directly solving the full constraint system introduced in Sect. III-B in practice it is preferable to proceed by phases. Each phase (functions dis_trans, rank_fun and term_impl) attempts to remove transitions from P by different means, and returns true if P has become empty or it is no longer strongly connected. In the former case, we are done. In the latter, the same procedure is recursively called. If after all phases P is non-empty, we report failure to prove termination.

In the first phase (function dis_trans), CppInv attempts to eliminate transitions with disability arguments by generating the appropriate invariants (neither ranking functions nor termination implications are considered at this point). This is achieved by solving the following Max-SMT formula: ∧ℓ∈L ∃ℓ′ ∧ τ ∈ T (Dτ ∨ Cτ) ∧ (∨τ∈T) (Dτ ∨ P0) ∧ ¬P0, ω ≥ 0 where P0 is a propositional variable meaning that no transition can be disabled, and ω is the corresponding weight. Transitions that are detected to be disabled (by means of a call to an SMT solver) are removed both from the original and the termination transition system. Invariants are used to strengthen the transition relations as described in Sect. II-B. The process is repeated while new transitions can be disabled.

```cpp
bool dis_trans(SetLoc L, SetTrans T, SetTrans P) { if (cont = true) {
  for (const) {
    τ = (ℓ, ℓ′, ρ) ∈ P
    (ρ is UNSAT) 
    (T, P) = (T − {τ}, P − {τ});
    if (P == ∅) return true;
    if (c ∈ L) break; // No solution to hard clauses
    for (c ∈ L, (ℓ, ℓ′, ρ) ∈ T) // Strengthen relation with invariant ρ = ρ ∧ I(ℓ);
      if (c == 0) cont = true; }
  return not is_strongly_connected(P); }
```

These phases have a time limit in our implementation although this is not made explicit in the pseudo-code shown below.

Constraints that avoid redundancy are not included for simplicity.
In the second phase (function \texttt{rank\_fun}), the system eliminates transitions by using ranking functions as arguments (termination implications are not considered at this point). If the computed function \( R \) satisfies the non-increase property, then each of the transitions \( \tau \) in the termination transition system is examined and either removed if \( R \) is a ranking function for \( \tau \), or split otherwise, as described in Sect. III-H.

\begin{verbatim}
bool rank_fun(Set_Loc L, Set_Trans T, Set_Trans P){
  while (true) {
    H = \bigwedge_{\ell \in L} \bigwedge_{r \in T} \bigvee_{p \in P} \big( (B_r \lor p_\ell) \land (S_r \lor p_\ell) \big) \land \bigwedge_{p \in P} (N_r \lor p_\ell)
    S = \big[ -p_\beta, \omega_\beta \big] \land \big[ -p_\omega, \omega_\omega \big] \land \big[ -p_\omega, \omega_\omega \big];
    (I, R, c) = solve(H \land S);
    if (c == \infty) return false; // No solution to hard clauses
    for (\ell \in L, (\ell, \ell', \rho) \in T) // Strengthen relation with invariant
      \rho = \rho \land I(\ell)
    for (\tau \in P)
      if (\rho is UNSAT) // \tau is disabled
        (T, P) = (T - \{ \tau \}, P - \{ \tau \});
      else if (non_increase(R))
        for (\tau \in P)
          if (bounded(\tau, R) and strict_decrease(\tau, R)) P = P - \{ \tau \};
          else split (\tau, R, P); // Splits \tau
    if (P == \emptyset or not strongly_connected(P)) return true; }
}
\end{verbatim}

The third and final phase (function \texttt{term\_impl}, not detailed here for lack of space) is very similar to the previous one, with the difference that termination implications are also included.

As regards the constraints, we restrain ourselves to invariants and ranking functions with integer coefficients, since this allows us to exploit efficient non-linear solving techniques [21]. Moreover, in order to perform integer reasoning, the following variation of Farkas’ Lemma, based on the Gomory-Chvátal cutting plane rule [22], is employed:

\textbf{Lemma 1}: Let \( Ax + b \leq 0 \) (\( A \in \mathbb{R}^{m \times n}, b \in \mathbb{R}^m \)) be a system of linear inequalities over integer variables \( x = (x_1, \ldots, x_n) \), and \( c^T x + d \leq 0 \) (\( c \in \mathbb{Z}^n, d \in \mathbb{R} \)) be a linear inequality. If there is \( \lambda \in \mathbb{R}^m, i \in \mathbb{Z} \) and \( f \in \mathbb{R} \) such that \( \lambda \geq 0, c^T = \lambda^T A, \lambda^T b = i - f, 0 \leq f < 1 \) and \( i \geq d \), then \( Ax + b \leq 0 \) entails \( c^T x + d \leq 0 \).

Lemma 1 allows transforming an \( \exists y \) problem into an \( \exists \) problem. If all coefficients in the premise are known values, the resulting satisfiability problem is an SMT problem over LA. Otherwise, an SMT problem over NA is obtained. Furthermore, as some unknowns are integer (the coefficients) and some are real (the multipliers), the resulting problems have mixed types.

\texttt{Cpplnv} uses Barcelogic [23] for solving the generated constraints. The Max-SMT(NA) solver for mixed non-linear arithmetic in Barcelogic extends the techniques presented in [21] for solving SMT(NA) problems. This is achieved by allowing integer and real variables in the underlying linear arithmetic solver, and wrapping this solver with a branch-and-bound scheme for optimization [18].

V. EXPERIMENTAL EVALUATION

In this section we show experiments that evaluate the performance of \texttt{Cpplnv} on a wide set of examples, which have been taken from the online programming learning environment \texttt{Jutge.org} [7] (see \url{www.jutge.org}), and from benchmark suites in [8] and in [24]. We provide here a comparison with the new version of \texttt{T2}, which according to the results given in [8] is performing much better when proving termination than most of the existing tools, including Terminator [12], AProVE [25] or ARMC [24], among others. We have also tried CProver [13] and Loopfrog [14], but the results were not good on these sets of benchmarks. All experiments were performed on an Intel Core i7 with 3.40GHz clock speed and 16 GB of RAM.

The first two considered sets of benchmarks are those provided by the \texttt{T2} developers. Following the experiments in [8], we have set a 300 secs. timeout. To show the impact of the different techniques described in the paper, Table I presents the number of instances in each set (\#ins.) and the number of those we proved terminating with the following settings:

- \textit{(noMS)} implements the generation of invariants and ranking functions using a translation to SMT(NA), but without using Max-SMT, i.e. with all constraints hard. The fact that this plain version can already prove many instances hints on the goodness of our underlying algorithm and the impact of using our NA-solver in this application.
- \textit{(MS)} implements the generation of invariants and ranking functions using Max-SMT(NA), where the constraints imposed by the ranking function are added as soft.
- \textit{(MS+QR)} adds to the previous case the possibility to use quasi-ranking functions.
- \textit{(MS+QR+TI)} adds to the previous case the possibility to infer termination implications.

Note that every added improvement allows us to prove some more instances, while none is lost due to the additional complexity of the constraints generated.

Moreover, by looking into the results in more detail, we have observed that our tool and \texttt{T2} complement each other to some extent: in Set1 \texttt{Cpplnv} can prove 7 instances which cannot be proved by \texttt{T2}, while we cannot prove 14 which can be handled by \texttt{T2}; similarly, in Set2 \texttt{Cpplnv} can prove 8 programs which cannot be proved by \texttt{T2}, while we cannot prove 11 that can be handled by \texttt{T2}. The average time in YES answers of \texttt{T2} is 2.9 secs and of \texttt{Cpplnv} is 12.8 secs.

In Table II we show the comparison of \texttt{Cpplnv} (with all described techniques) and \texttt{T2} on our benchmarks from the programming learning environment \texttt{Jutge.org}, which is

\begin{table}[h]
\caption{RESULTS WITH BENCHMARKS FROM T2}
\begin{tabular}{|c|c|c|c|c|c|c|}
\hline
\#ins. & \texttt{Cpplnv} & \texttt{T2} \\
\hline
Set1 & 449 & 212 & 220 & 228 & 238 & 243 \\
Set2 & 72 & 245 & 252 & 202 & 206 & 227 \\
\hline
\end{tabular}
\end{table}

\begin{table}[h]
\caption{RESULTS WITH BENCHMARKS FROM Jutge.org.}
\begin{tabular}{|c|c|c|c|c|c|c|}
\hline
\#ins. & \texttt{Cpplnv} & \texttt{T2} \\
\hline
P11635 & 367 & 324 & 328 & P40685 & 362 & 324 & 329 \\
P186703 & 149 & 143 & 140 & P845965 & 854 & 780 & 793 \\
P13298 & 783 & 707 & 710 & P270754 & 280 & 243 & 235 \\
P16415 & 98 & 81 & 81 & P19366 & 642 & 2663 & 926 \\
P28474 & 177 & 171 & 168 & P82660 & 196 & 174 & 177 \\
P33412 & 603 & 478 & 471 & P84219 & 413 & 325 & 243 \\
\hline
\end{tabular}
\end{table}
currently being used in several programming courses in the Universitat Politècnica de Catalunya. The benchmark suite consists of thousands of solutions written by students to 12 different programming problems. These programs can be considered challenging since most often they are not the most elegant solution but one with many more conditional statements than necessary (e.g., the largest instance we can successfully handle has nearly 700 transitions). Here, due to the size of the benchmark suites (see column #ins.), for the execution of both tools we have set a 120 secs. timeout. The average time in YES answers of T2 is 1.7 secs. and of CppInv is 1.6 secs. Note that, in order to run these benchmarks in T2, we have translated them into T2 format using our intermediate transition graph. This may be a disadvantage for T2, as it happens in the reverse way when CppInv is run on T2 benchmark set. In particular, we think the bad performance of T2 in sets P33412, P81966 and P84219 may be related to the way we handle division, which is crucial in these examples.

VI. CONCLUSIONS AND FUTURE WORK

In short, the contributions of this paper are:

- a novel Max-SMT constraint-based approach to proving termination. Thanks to expressing the synthesis of a ranking function and a supporting invariant as a Max-SMT problem, we achieve a better guided and more fine-grained termination analysis than SMT-based methods. Max-SMT reveals to be a convenient framework for constraint-based termination analysis. In addition to our method, other techniques such as unaffection score maximization \[10\] can be naturally modeled in Max-SMT.
- a prototype of termination analyzer for (a subset of) C++.

One of the shortcomings of our approach is that invariant synthesis is restricted to a single SCC. If invariants from previous SCC’s have not been generated but are later required, our technique cannot prove termination. E.g., in the program shown in Fig. 4 the invariant \( x > 0 \) must be discovered at \( \ell_1 \) so as to prove that the rightmost transition is finitely executable, although it is not necessary for proving that the leftmost loop is terminating. For future work we plan to develop techniques to overcome this kind of situations. A promising idea is to consider initiation conditions as soft: then the generated quasi-invariants represent what is missing from previous SCC’s, and then can be propagated backwards. Alternatively, these quasi-invariants can be used to split the initial conditions of the current SCC. Finally, as a byproduct, this would allow us to solve the conditional termination problem as well.

ACKNOWLEDGMENT

This research was supported by Spanish MEC/MICINN under grant TIN 2010-21062-C02-01. We thank Jutge.org for providing benchmarks, and Byron Cook for giving us access to T2 and their benchmarks and for his helpful comments.

REFERENCES


\[ y > 0 \land y' = y - 1 \land x' = x - 1 \quad y \leq 0 \quad y < 0 \land y' = y + x \]

\[ \Theta(\ell_1) \equiv x > y \land y \geq 0 \quad \Theta(\ell_2) \equiv \text{false} \]

Fig. 4. Program that requires invariants from previous SCC’s.

\[ y > 0 \land y' = y - 1 \land x' = x - 1 \quad y \leq 0 \quad y < 0 \land y' = y + x \]

\[ \Theta(\ell_1) \equiv x > y \land y \geq 0 \quad \Theta(\ell_2) \equiv \text{false} \]