Introduction

- Safety properties, such as absence of assertion failures, over-shared-memory concurrent programs with unknown number of threads are decidable, yet of \textsc{ExpSpace} complexity.
- Systems that require extra threads to serve requests coming from their environment showcase such behavior, since the number of threads can't be determined a priori.
- We consider an incomplete method, that can effectively decide a large number of benchmarks.

Method Overview

- Encode the reachability problem as a set of over-approximating integer linear constraints. If the constraints are unsatisfiable, then the safety property is verified.
- Otherwise, incrementally strengthen the constraints.
- If the constraints are still unsatisfiable, check if the safety property is violated, using a guided explicit-state search.

Thread-Transition Systems (TTS)

Finite-state models extracted through predicate abstraction of procedures executed by threads. Defined over
- the set of thread states \( T = S \times L \) where \( S \) and \( L \) are the finite sets of shared (valuations of shared variables) and local states (valuations of local variables) respectively.
- the set of transitions \( R \subseteq T \times T \)

For \( n \) threads, a TTS gives rise to the state space \( V_n = S \times L^n \) of configurations of the form \( v = (s_l, \ldots, s_l) \in V_n \). Transitions can asynchronously fire given that their source shared state is the same as the shared state of the current configuration, and they affect the local state of exactly one thread.

Connectivity Constraints for TSE

- No guarantee that the transitions of the satisfying assignment of TSE give rise to a connected path from \( t_i \) to \( t_f \).
- Define as active the transitions with a non-zero assignment.
- Require that they form a path in the shared-state projection of \( (T, R) \).
- Augment TSE with \( C_{\text{TSE}} := \bigwedge_{s \in\{1, \ldots, |S|\}} \text{act}(s_l) \land \text{act}(s_r) \implies \mathcal{P}(s_l, s_r) \)

safety property is violated, using a set of over-approximating integer linear constraints. If the constraints are unsatisfiable, then the safety property is violated, using a set of over-approximating integer linear constraints.

Problem Statement

Given an initial thread state \( t_i = (s_l, l_i) \in T \), a final thread state \( t_f = (s_l, l_f) \in T \) is reachable if there exists a finite sequence of configurations \( \forall v_i = (s_l, l_i, \ldots, l_i) \) where for all \( i \in \{1, \ldots, n\} \), \( l_i = l_i \), and ending at \( v_f = (s_l, l_i', \ldots, l_i') \) where there exists \( i \in \{1, \ldots, n\} \) such that \( l_i' = l_f \).

A Constraint-Based Approach to Multi-Threaded Program Location Reachability

Konstantinos Athanasiou  
Northeastern University, Boston

Joint work with Peizun Liu and Thomas Wahl. Supported by NSF grant no. 1253331.