Decision Procedures and Verification

Martin Bлича

Charles University

21.5.2018
Interpolation in verification
Craig Interpolants

Definition (Craig interpolant)

For $A, B$ such that $A \land B \Rightarrow \bot$, $I$ is a (Craig) interpolant when:

- $A \Rightarrow I$
- $I \land B \Rightarrow \bot$
- $\mathcal{L}(I) \subseteq \mathcal{L}(A) \cap \mathcal{L}(B)$

Theorem (Craig ‘57)

In first-order logic, if $\varphi \Rightarrow \psi$ and they share at least one atomic variable, then there exists $\rho$ such that $\varphi \Rightarrow \rho$, $\rho \Rightarrow \psi$ and every nonlogical symbol in $\rho$ occurs both in $\varphi$ and $\psi$. 
Set representation of Craig interpolation
Unbounded Model Checking

- Transition system
  - Finite state machine
  - Kripke structure
- Problem defined by triple (Initial state, Transition relation, Error state)
  - Goal: Check whether an error state is reachable from initial state
- Bounded Model Checking
  - Transition relation unwound $k$ times.
- Unbounded Model Checking
  - Interpolants used to over-approximate the set of reachable states.
  - McMillan, *Interpolation and SAT-Based Model Checking*, 2003
Lazy Abstraction with Interpolants

- Basic idea:
  - Model-checking sequential programs
  - Looking for *safety invariant*
  - Unwinding control-flow graph
  - Labeling nodes of unwinding
  - Looking for *safe, complete, well-labeled* unwinding.
- Labels over-approximate set of reachable states at given point of the program.
- Can be computed using interpolants from proofs of unfeasibility of concrete paths.
Function Summaries

- Assumes functions define precise input-output relation.
  - Without side-effects.

- Function summary over-approximates function’s input-output relation.

- Can be computed using interpolation from successful verification run.

- Useful in incremental and upgrade-checking scenario.

- Sery and al. *Interpolation-Based Function Summaries in Bounded Model Checking*, 2011