Decidability of Inferring Inductive Invariants

Dingchao Gao

Institute of Software Chinese Academy of Sciences

March 7, 2023

outline

backgroud

- a system S
- property ϕ
- verification: Is there a behavior of S that violated the property?

transition system

- transition system $TS = (S, S_0, R)$
- a safe property $P \subseteq S$
- a inductive invariants I iff.
  - $S_0 \subseteq I$
  - $R(I) = I$
  - $I \subseteq P$

why EPR?

- Z3, CVC4, MathSAT,...
- Horn,EPR,...

effectively-propositional fragment of first-prder logic

- relation, but no function
- $\exists^\star\forall^\star$, but no $\forall^\star\exists^\star$
- satisfiablity:

$$\begin{aligned} & \exists x, y. \forall z. r(x, z) \leftrightarrow r(z, y) \\ =_{\mathrm{SAT}} & \forall z \cdot r\left(c_1, z\right) \leftrightarrow r\left(z, c_2\right) \\ =_{\mathrm{SAT}} & \left(r\left(c_1, c_1\right) \leftrightarrow r\left(c_1, c_2\right)\right) \wedge\left(r\left(c_1, c_2\right) \leftrightarrow r\left(c_2, c_2\right)\right) \end{aligned} \tag{1}$$

automatic checking invariants

- input:
  - program P: Init, TR
  - alternation-Free Inductive Invariant Inv
  - Safety Property φ
- verification conditions generator
- : EPR SMT Solver
- output:
  - Counterexample To inductiveness
  - Proof

deduction

- Gap: deductive power of automated provers and verification productivity
- Danfy,Ivy

target

- the decidability of the problem of inferring inductive invariants in a given language
- input:
    - program
    - safe property
    - a given language

results

- decidability: $INV[\mathcal{C}_{n^\star}, \mathcal{L}_{\forall^\star}]$
- undecidability: $INV[\mathcal{C}_{n^\star}, \mathcal{L}_{AF}]$,$INV[\mathcal{C}, \mathcal{L}]$

basis denfintion

for any language $L \subset 2^S$

- $\sqsubseteq_L$ on S:$s_1 \sqsubseteq s_2$ iff.$\forall A \in L$,$s_2 \in A \rightarrow s_1 \in A$
- $\mathrm{Avoid}_L(s) = A$:$\forall A' \in L, s \notin A' \rightarrow A' \subseteq A$
- L-relaxed transition:$(s, s') \in R$ iff.$(s, s') \in R$ or $s' \sqsubseteq_L s$

outline of $INV[\mathcal{C}_{n^\star}, \mathcal{L}_{n^\star}]$

- L-relaxed Trace reached bad property
- Establish WQO using Krusal's Tree theorem

well quasi order

- possible case:
  - no universal inductive Invariant
  - no relaxed trace reaches bad
- solution: well quasi order

Krusal's Tree theorem

- If $(X, \leq)$is a wqo, then so is $(\mathcal{T}(X), \leq)$.
- construct tree

extend decidability result

Corollary

Extending the vocabulary Σ by adding an arbitrary relation (i.e., with any arity) and extending L by adding to the bodies of L any number $\leqslant k$ of occurrences of the new relation symbol, for some fixed $k \geqslant 0$, maintains the wqo and computability of AvoidL.

outline of undecidability results

- Minsky machine: $M = (Q, c_1, c_2)$
- Safe problem: c_3
- basic idea:
  - reduction constructs $(TS, P, L) \in (\mathcal{C}, \mathcal{L})$
  - halts of M and decidability

reduction from counter Machines to $INV[\mathcal{C}, \mathcal{L}]$

- $inc_i, dec_i, id_i, zero_i, init$
- $\varphi_I = \bigvee_{(q_i,\ell_1,\ell_2,\ell_3)\in \text{Reach}} \; q_i \wedge \varphi_{\mathcal{E}}(\ell_1, \ell_2, \ell_3)$

$INV\left[\mathcal{C}_{n^*}, \mathcal{L}_{AF}\right]$

- encoding
- witness formula:
  - $\forall x . n^*\left(h_i, x\right) \wedge n^*\left(h_j, x\right) \rightarrow i = j$
  - $\exists x_1 \ldots x_{\ell_i} . . \text{ distinct } \left(h_i, x_1, \ldots, x_{\ell_i}\right) \wedge \bigwedge_{j=1}^{\ell_i} n^*\left(h_i, x_j\right)$
  - $\forall x_0 \ldots x_{\ell_i} \cdot \neg\left(\text{distinct}\left(h_i, x_0, \ldots, x_{\ell_i}\right) \wedge \bigwedge_{j=0}^{\ell_i} n^*\left(h_i, x_j\right)\right)$

Summary

- L-relaxed trace
- decidability and undecidability results

disscussion

- BSCC in QMC

END
Thank you