

Decidability of Inferring Inductive Invariants

Dingchao Gao

Institute of Software Chinese Academy of Sciences

March 7, 2023

outline

1 Induction

- background
- EPR logic

2 Results of This Paper

- basis of this paper
- some proof of results

3 Summary

background

- 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-order logic

- relation, but no function
- $\exists^*\forall^*$, but no $\forall^*\exists^*$
- satisfiability:

$$\begin{aligned} & \exists x, y. \forall z. r(x, z) \leftrightarrow r(z, y) \\ &=_{\text{SAT}} \forall z. r(c_1, z) \leftrightarrow r(z, c_2) \\ &=_{\text{SAT}} (r(c_1, c_1) \leftrightarrow r(c_1, c_2)) \wedge (r(c_1, c_2) \leftrightarrow r(c_2, c_2)) \end{aligned} \quad (1)$$

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,lvy

target

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

results

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

basis denfintion

for any language $L \subset 2^S$

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

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

- 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 $\leq k$ of occurrences of the new relation symbol, for some fixed $k \geq 0$, maintains the wqo and computability of $\text{Avoid}L$.

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 $INV[\mathcal{C}, \mathcal{L}]$

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

$INV[C_{n^*}, \mathcal{L}_{AF}]$

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

Summary

- L-relaxed trace
- decidability and undecidability results

discussion

- decidable problems about reachability of quantum systems

END
Thank you