Unsolvability Certificates for Classical Planning

Salomé Eriksson Gabriele Röger Malte Helmert

University of Basel, Switzerland

ICAPS 2017

Motivation

Validating correctness of planner output:

- Why?

  $\rightsquigarrow$ Software bugs, hardware faults, malicious reasons ...
- How?

  (a) Planner outputs a plan: VAL/INVAL

  (b) Planner claims unsolvability: ?

Proving Unsolvability

Goal

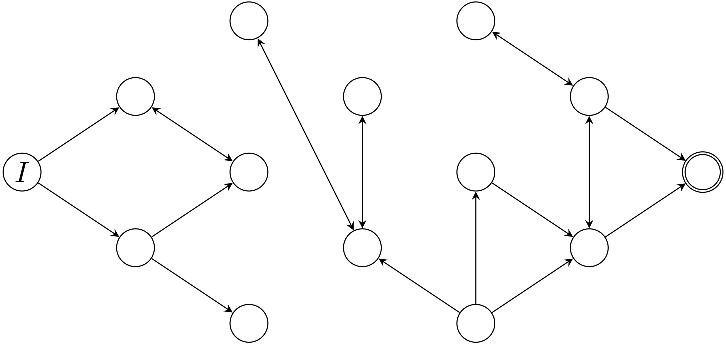
Generate unsolvability certificate which can be verified

Desired properties:

- Soundness & Completeness
- Efficient generation
- Efficient verification
- Generality

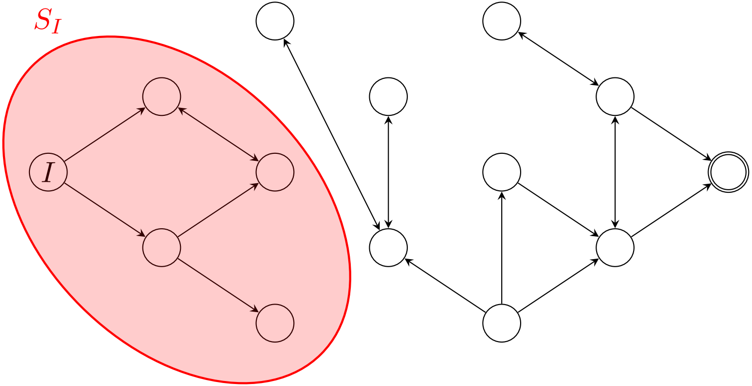
General Idea

Unsolvable planning problems ⇝ No path from I to goal



General Idea

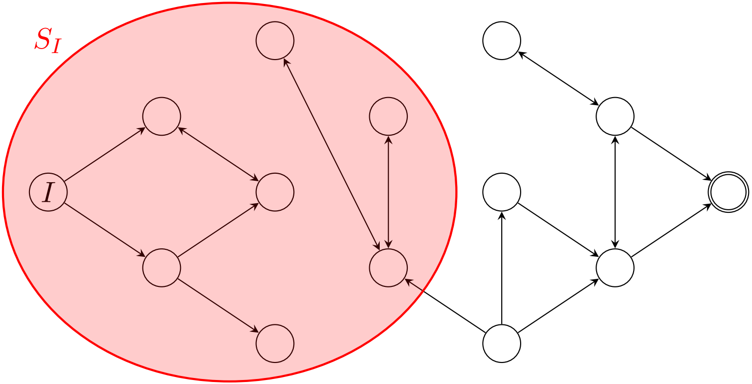
Unsolvable planning problems ⇝ No path from I to goal



Split graph into S_I and $S_G(= \overline{S_I})$ s.t. no outgoing edges from S_I

General Idea

Unsolvable planning problems $\rightsquigarrow$ No path from I to goal



Split graph into S_I and $S_G(=\overline{S_I})$ s.t. no outgoing edges from S_I

Inductivity

Inductive Set

A state set S is inductive if for all $s \in S$,
all operator applications lead to a $s' \in S$.

Inductive Certificate

If a state set

1. contains the initial state
2. contains no goal state
3. is inductive

the planning task is unsolvable.

Representation of State Sets

Representation of state sets as logical formulas

We focus on the following representations:

- (RO)BDD
- 2CNF
- Horn Formulas

Conjunctive/Disjunctive Certificates

Not all state sets compactly representable

Conjunctive/Disjunctive Certificate

$\mathcal{S} = \{S_1, \ldots, S_n\}$ is a

- conjunctive certificate: $\bigcap_{S_i \in \mathcal{S}} S_i$ is inductive certificate
- disjunctive certificate: $\bigcup_{S_i \in \mathcal{S}} S_i$ is inductive certificate

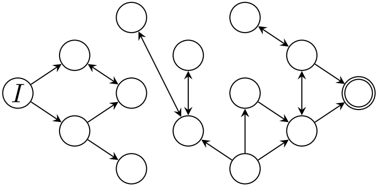
Efficient Verification? in general not feasible

$\leadsto$only consider up to r sets at once

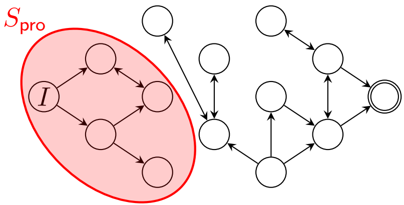
Suitable Representations

Certificate Type	BDD	2CNF	Horn Formulas
Inductive Certificate	Yes	Yes	Yes
Conjunctive Certificate	No	Yes	Yes
r-conjunctive Certificate	Yes	Yes	Yes
Disjunctive Certificate	No	No	No
r-disjunctive Certificate	Yes	No	No
1-disjunctive Certificate	Yes	Yes	Yes

Blind Search

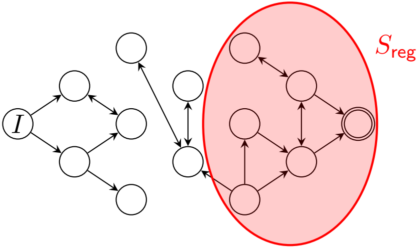


Blind Search



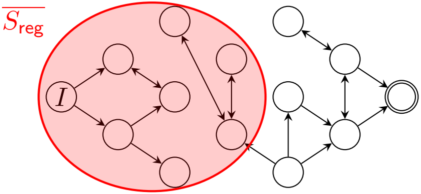
- Progression: expanded = reachable from I
  $\rightsquigarrow$ inductive certificate

Blind Search



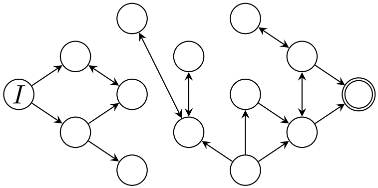
- Progression: expanded = reachable from I
  $\rightsquigarrow$ inductive certificate
- Regression: expanded = backwards-reachable from goal

Blind Search



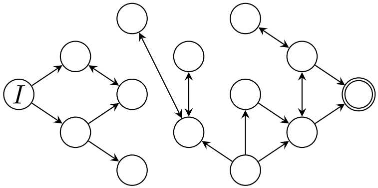
- Progression: expanded = reachable from I
  $\rightsquigarrow$ inductive certificate
- Regression: expanded = backwards-reachable from goal
  $\rightsquigarrow$ complement is inductive certificate

Blind Search



- Progression: expanded = reachable from I
  $\rightsquigarrow$ inductive certificate
- Regression: expanded = backwards-reachable from goal
  $\rightsquigarrow$ complement is inductive certificate
- Bidirection: whichever direction shows unsolvability

Blind Search



- Progression: expanded $=$ reachable from I
  $\rightsquigarrow$ inductive certificate
- Regression: expanded $=$ backwards-reachable from goal
  $\rightsquigarrow$ complement is inductive certificate
- Bidirection: whichever direction shows unsolvability

Suitable representation: BDDs (for symbolic search)

Merge & Shrink

Union of states s where $h^{\text{M\&S}}(s) = \infty$ is inductive & no goal states
$\rightsquigarrow$ If $h^{\text{M\&S}}(I) = \infty$, this union is inductive certificate

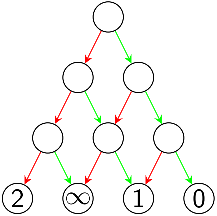
For linear merge strategies:

1. Represent cascading tables as ADD
2. Compress to BDD: finite h-values lead to $\bot$, infinite to $\top$

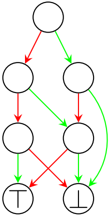
		$v_1 = 0$	$v_1 = 1$
v_2	0	0	1
	1	1	2

		$v_3 = 0$	$v_3 = 1$
$v_{1,2}$	0	2	∞
	1	∞	1
	2	2	0

Cascading tables



ADD



BDD

Delete Relaxation Heuristics

$h^+(s) = \infty$ if part of the goal is relaxed unreachable

- $U^+(s)$: relaxed unreachable variables
- $\varphi_{U^+(s)} = \bigwedge_{v \in U^+(s)} \neg v$ is inductive & no goal states

$\rightsquigarrow$ If $h^+(I) = \infty$, $\varphi_{U^+(s)}$ represents inductive certificate

Covers all delete-relaxation heuristics ($h^{\text{max}}, h^{\text{add}}, h^{\text{FF}}, h^{\text{LM-Cut}}, \dots$)

Suitable representation: BDDs, Horn Formulas, 2CNF

h^m-Family

Similar idea to h^+, but with unreachable conjunctions:

$$\bigwedge_{c \in U^m(I)} \bigvee_{v \in c} \neg v$$

Suitable representation: Horn Formulas, 2CNF (for $m \leq 2$),
BDDs (as 1-conjunctive Certificate)

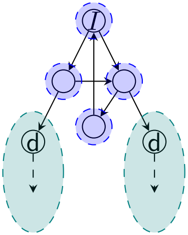
Heuristic Search

Heuristic certificates sufficient if $h(I) = \infty$

General heuristic search:

- $\mathcal{S}_{\text{exp}} = \{\{s\} \mid s \in \text{ expanded states}\}$
- $\mathcal{S}_{\infty}$: family of inductive sets covering all detected dead ends

$\rightsquigarrow$ $\mathcal{S}_{\text{exp}} \cup \mathcal{S}_{\infty}$ is 1-disjunctive certificate



Suitable representation: BDDs, Horn Formulas, 2CNF

Limitation:

- all sets must have same representation
- sets cannot be conjunctive/disjunctive

Trapper

Trapper [Lipovetzky et al. 2016]:

- only considers states not violating mutexes M (based on h^2)
- no escape from φ_{trap} $\rightsquigarrow$ inductive
- no goal states (in considered states)

Observations:

- φ_{trap} alone no certificate (goal states)
- states not violating mutexes ($= \varphi_{\neg M}$) inductive

$\rightsquigarrow$ $\varphi_{\text{trap}} \wedge \varphi_{\neg M}$ represents inductive certificate (even 1-disjunctive)

Suitable representation: 2CNF, Horn Formulas

Experiments

Proof of concept implementation of

- FD$^{\text{cert}}$: generates BDD certificates for $A^* + h^{\text{max}} / h^{\text{M\&S}}$
- Verifier: vanilla, r-conjunctive, r-disjunctive BDD certificates

limits: 30 min generation, 4 hours verification

	h^{max}			$h^{\text{M\&S}}$		
	FD	FD$^{\text{cert}}$	Ver.	FD	FD$^{\text{cert}}$	Ver.
Coverage (702)	212	136	123	223	191	155

all certificates valid

Conclusion

unsolvability certificates based on inductive sets

- completeness: yes
- efficient generation: yes/no
- efficient verification: mostly yes (if efficient generation)
- generality: yes/no

Future Work

- cover more techniques (heuristics, pruning, . . .)
- combined certificate with different formalisms