A Proof System for Unsolvable Planning Tasks

Salomé Eriksson Gabriele Röger Malte Helmert
University of Basel

Motivation

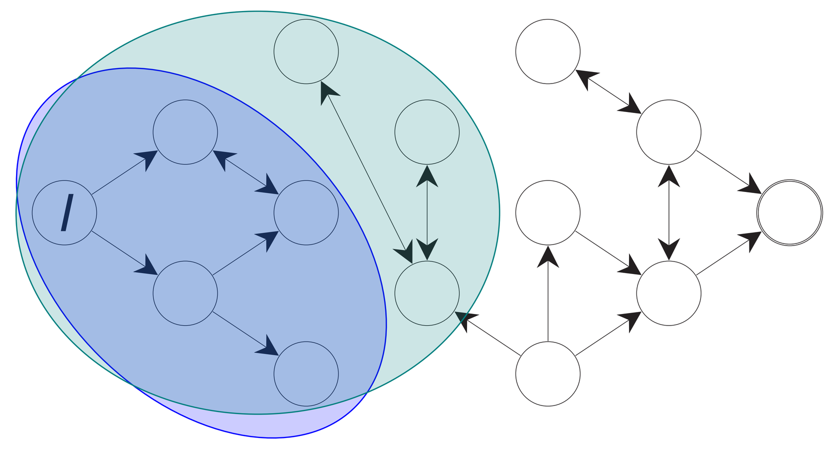
planner should emit proof for its output:

- solvable: plan
- unsolvable: inductive certificate [Eriksson et al. 2017]

weakness of inductive certificates: not compositional

⇝ new approach: proof system

Inductive Certificates



no path from I to goal
⇝ partition into S_I and S_G

S_I is inductive
⇝ no outgoing edges

A state set S is an inductive certificate iff

1. $I \in S$,
2. S contains no goal and
3. applying any $a \in A$ to any $s \in S$ leads to some $s' \in S$. (written $S[A] \subseteq S$)

Proof System

build up a knowledge base:

- basic statements
  - state facts about concrete objects
  - need to be verified
- derivation rules
  - derive new knowledge from existing knowledge
  - universally true (only correct application needs to be verified)

Example: Set Theory

objects: elements a,b,c,d,e and sets $A = \{a,b\}$, $B = \{b,c,e\}$, $C = \{b,c\}$

basic statements:

- $(A \cap B) \subseteq C$
- $b \in (A \cap B)$

derivation rules:

- $X \subseteq Y, Y \subseteq Z \rightarrow X \subseteq Z$
- $x \in X, X \subseteq Y \rightarrow x \in Y$

Unsolvability Proof System

objects: state sets S described by

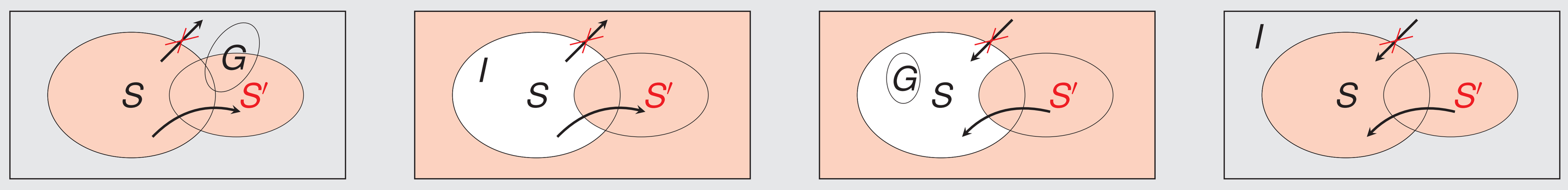
- BDDs
- Horn formulas
- 2CNF formulas
- explicit

types of statements:

- S is dead (no plan through any $s \in S$)
- $S \subseteq S'$
- task unsolvable

Derivation Rules

D1			$\emptyset$ is dead
D2	S dead, S' dead	$\rightarrow$	$S \cup S'$ dead
D3	$S' \subseteq S$, S dead	$\rightarrow$	S' dead
D4	$\{I\}$ dead	$\rightarrow$	task unsolvable
D5	G dead	$\rightarrow$	task unsolvable
D6	$S[A] \subseteq S \cup S'$, S' dead, $S \cap G$ dead	$\rightarrow$	S dead
D7	$S[A] \subseteq S \cup S'$, S' dead, $\{I\} \subseteq S$	$\rightarrow$	$\overline{S}$ dead
D8	$[A]S \subseteq S \cup S'$, S' dead, $\overline{S} \cap G$ dead	$\rightarrow$	$\overline{S}$ dead
D9	$[A]S \subseteq S \cup S'$, S' dead, $\{I\} \subseteq \overline{S}$	$\rightarrow$	S dead



D6 D7 D8 D9

Basic Statements

restrict basic statements to cases that are verifiable in polynomial time:

B1	$L \subseteq L'$	mixed representations for L,L' in some cases
B2	$X \subseteq X' \cup X''$	
B3	$L \cap G \subseteq L'$	
B4	$X[A] \subseteq X \cup L'$	
B5	$[A]X \subseteq X \cup L'$	

X: constant ($\{I\}$, G, $\emptyset$) or set variable (explicitly represented set)

L: constant, set variable or their complement

Proof Generation

examples of covered planning techniques:

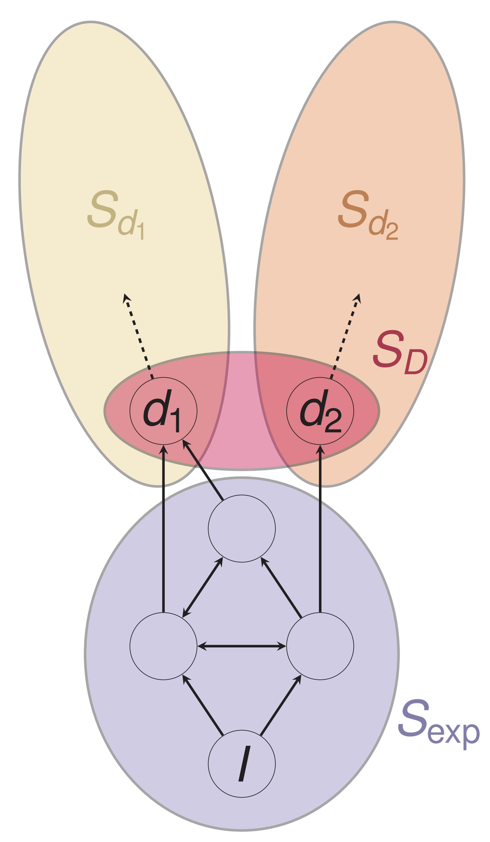
- explicit and symbolic blind search
- heuristic search with
  - delete-relaxation heuristic
  - $h^{\mathrm{M\&S}}$ with linear merge strategy
  - h^C
  - ⇝ combination of multiple heuristics now possible
- trapper [Lipovetzky et al. 2016]
- clause learning state space search [Steinmetz and Hoffmann 2016]
- h^2-based preprocessing [Alcázar and Torralba 2015]

Translating Inductive Certificates

inductive certificate S: no successor, no goal and contains I

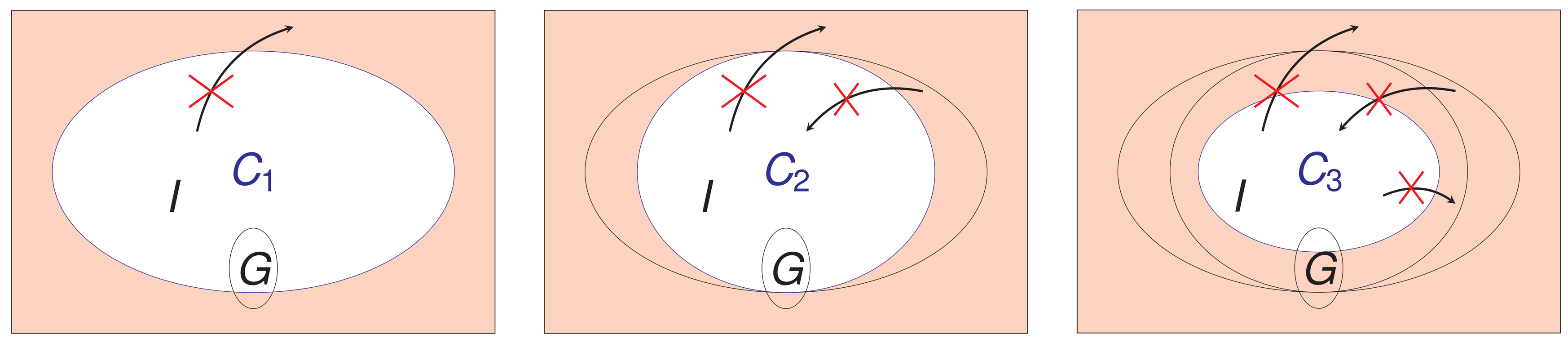
(1)	$\emptyset$ dead	D1	(5)	S dead	D6 (2),(1),(4)
(2)	$S[A] \subseteq S \cup \emptyset$	B4	(6)	$\{I\} \subseteq S$	B1
(3)	$S \cap G \subseteq \emptyset$	B3	(7)	$\{I\}$ dead	D3 (6),(5)
(4)	$S \cap G$ dead	D3 (3),(1)	(8)	task unsolvable	D4 (7)

Heuristic Search



(1)	$\emptyset$ dead	D1	
(2)	$S_{d_1}[A] \subseteq S_{d_1} \cup \emptyset$	B4	
(3)	$S_{d_1} \cap G \subseteq \emptyset$	B3	
(4)	$S_{d_1} \cap G$ dead	D3	(3),(1)
(5)	S_{d_1} dead	D6	(2),(1),(4)
(6)	$\{d_1\} \subseteq S_{d_1}$	B1	
(7)	$\{d_1\}$ dead	D3	(6),(5)
	...		
(8)	$\{d_2\}$ dead	D3	...
(9)	$\{d_1\} \cup \{d_2\}$ dead	D2	(7),(8)
(10)	$S_D \subseteq \{d_1\} \cup \{d_2\}$	B2	
(11)	S_D dead	D3	(10),(9)
(12)	$S_{\exp}[A] \subseteq S_{\exp} \cup S_D$	B4	
(13)	$S_{\exp} \cap G \subseteq \emptyset$	B3	
(14)	$S_{\exp} \cap G$ dead	D3	(13),(1)
(15)	$S_{\exp}$ dead	D6	(12),(11),(14)
(16)	$\{I\} \subseteq S_{\exp}$	B1	
(17)	$\{I\}$ dead	D3	(16),(15)
(18)	task unsolvable	D4	(17)

h^2-based Preprocessing



$C_1[A] \subseteq C_1 \cup \emptyset$	$[A]C_2 \subseteq C_2 \cup \overline{C_1}$	$C_3[A] \subseteq C_3 \cup \overline{C_2}$
$\emptyset$ dead, $I \in C_1$	$\overline{C_1}$ dead, $\overline{C_2} \cap G$ dead	$\overline{C_2}$ dead, $I \in C_3$
$\rightarrow \overline{C_1}$ dead	$\rightarrow \overline{C_2}$ dead	$\rightarrow \overline{C_3}$ dead

Experimental Evaluation

	base	certifying	verifier
FD-$h^{\max}$	211	168 (135)*	167 (125)*
FD-$h^{\mathrm{M\&S}}$	230	191 (200)*	184 (163)*
FD-h^2	183	177	177
FD-max($h^{\mathrm{M\&S}}$, h^2)	204	199	195
DFS-CL	385	386	383

*inductive certificate approach