

THIS DOCUMENT IS THE ONLINE-ONLY APPENDIX TO:

## A Counterexample Guided Abstraction-Refinement Framework for Markov Decision Processes

ROHIT CHADHA and MAHESH VISWANATHAN

Dept. of Computer Science, University of Illinois at Urbana-Champaign

ACM Transactions on Computational Logic, Vol. V, No. N, Month 20YY, Pages 1–45.

### A. SEMANTICS OF PCTL

We first give the semantics of PCTL for MDPs (since every DTMC can be thought of as a MDP, this suffices). Assume that we are given a MDP  $\mathcal{M} = (\mathbb{Q}, q_0, \delta, L)$ . As described in Section 2, given a scheduler  $\mathcal{S} : \mathbb{Q}^+ \rightarrow \text{Prob}_{\leq 1}(\mathbb{Q})$ , let  $((\mathbb{Q} \cup \{\perp\})^\omega, E, \mu_{\mathcal{S}})$  be the  $\sigma$ -algebra generated by  $\mathcal{M}$  and  $\mathcal{S}$ . Given  $q \in \mathbb{Q}$  and a PCTL formula  $\psi$ , the relation  $q \Vdash_{\mathcal{M}} \psi$  is defined by induction on  $\psi$  in Table I.

$q \Vdash_{\mathcal{M}} \text{tt}$	always
$q \Vdash_{\mathcal{M}} \text{ff}$	never
$q \Vdash_{\mathcal{M}} \neg\psi$	if $q \not\Vdash \psi$
$q \Vdash_{\mathcal{M}} \psi_1 \vee \psi_2$	if $q \Vdash_{\mathcal{M}} \psi_1$ or $q \Vdash_{\mathcal{M}} \psi_2$
$q \Vdash_{\mathcal{M}} \psi_1 \wedge \psi_2$	if $q \Vdash_{\mathcal{M}} \psi_1$ and $q \Vdash_{\mathcal{M}} \psi_2$
$q \Vdash_{\mathcal{M}} \mathcal{P}_{\triangleleft}(X\psi)$	if for each scheduler $\mathcal{S}$ , $\mu_{\mathcal{S}}(\{\pi \in (\mathbb{Q} \cup \{\perp\})^\omega \mid q \Vdash_{\pi, \mathcal{M}} X\psi\}) \triangleleft p$
$q \Vdash_{\mathcal{M}} \mathcal{P}_{\triangleleft}(\psi_1 \mathcal{U} \psi_2)$	if for each scheduler $\mathcal{S}$ , $\mu_{\mathcal{S}}(\{\pi \in (\mathbb{Q} \cup \{\perp\})^\omega \mid q \Vdash_{\pi, \mathcal{M}} \psi_1 \mathcal{U} \psi_2\}) \triangleleft p$

Where the relations  $q \Vdash_{\pi, \mathcal{M}} (X\psi)$  and  $q \Vdash_{\pi, \mathcal{M}} (\psi_1 \mathcal{U} \psi_2)$  for  $\pi = q_0 q_1 \dots$  are defined as follows—  
 $q \Vdash_{\pi, \mathcal{M}} (X\psi)$  if  $q_0 = q$ ,  $q_1 \neq \perp$  and  $q_1 \Vdash_{\mathcal{M}} \psi$   
 $q \Vdash_{\pi, \mathcal{M}} (\psi_1 \mathcal{U} \psi_2)$  if  $q_0 = q$  and there is a  $j \geq 0$  such that  $q_i \neq \perp$  for all  $i \leq j$ ,  
 $q_j \Vdash \psi_2$  and  $q_r \Vdash \psi_1$  for all  $r < j$ .

Table I. Semantics for PCTL for DTMCs

### B. EXISTENCE OF CANONICAL SIMULATIONS

**PROPOSITION 2.8.** *Given disjoint MDPs  $\mathcal{M} = (\mathbb{Q}, q_{\mathcal{I}}, \delta, L)$  and  $\mathcal{M}' = (\mathbb{Q}', q'_{\mathcal{I}}, \delta', L')$ , let  $\mathcal{R} \subseteq (\mathbb{Q} + \mathbb{Q}') \times (\mathbb{Q} + \mathbb{Q}')$  be a simulation relation on the direct sum of  $\mathbb{Q}$  and  $\mathbb{Q}'$ . Let  $\mathcal{R}_1 = \mathcal{R} \cap (\mathbb{Q} \times \mathbb{Q}')$ . Then the relation  $\mathcal{R}_0 = \text{rel}_{id_{\mathbb{Q}}} \cup \mathcal{R}_1 \cup \text{rel}_{id_{\mathbb{Q}'}}$  is a simulation relation.*

Permission to make digital/hard copy of all or part of this material without fee for personal or classroom use provided that the copies are not made or distributed for profit or commercial advantage, the ACM copyright/server notice, the title of the publication, and its date appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee.

© 20YY ACM 1529-3785/20YY/0700-0001 \$5.00

PROOF. Clearly  $\mathcal{R}_0$  is reflexive and transitive. Fix  $q \in Q$  and  $q' \in Q'$  such that  $q \mathcal{R}_0 q'$ . Please note that by definition  $q \mathcal{R} q'$ . Hence,  $L(q) = L(q')$ . It suffices to show that given  $\mu \in \delta(q)$  there is a  $\mu_1 \in \delta'(q')$  such that  $\mu \preceq_{\mathcal{R}_0} \mu_1$ . Since  $\mathcal{R}$  is a simulation relation there is a  $\mu' \in \delta'(q')$  such that  $\mu \preceq_{\mathcal{R}} \mu'$ . Fix one such  $\mu'$ .

Therefore, the result will follow if we can show that  $\mu \preceq_{\mathcal{R}_0} \mu'$  also. In order to establish this, we need to show that for any  $\mathcal{R}_0$ -closed set  $Q_0 \subseteq Q \cup Q'$ , we have that  $\mu(Q_0) \leq \mu'(Q_0)$ . Now let  $Q_1 = Q_0 \cap Q$  and  $Q_2 = Q_0 \cap Q'$ . We have that  $\mu(Q_0) = \mu(Q_1)$  and  $\mu'(Q_0) = \mu'(Q_2)$ . Thus, we need to show that  $\mu(Q_1) \leq \mu'(Q_2)$ .

Now, consider the set  $\mathcal{R}(Q_1) = \{q_b \in Q \cup Q' \mid \exists q_a \in Q_1 \text{ s.t. } q_a \mathcal{R} q_b\}$ . Now since  $\mathcal{R}$  is a preorder,  $\mathcal{R}(Q_1)$  is  $\mathcal{R}$ -closed and  $Q_1 \subseteq \mathcal{R}(Q_1)$ . From  $Q_1 \subseteq \mathcal{R}(Q_1)$ , we can conclude that  $\mu(Q_1) \leq \mu(\mathcal{R}(Q_1))$ . Also, since  $\mathcal{R}(Q_1)$  is  $\mathcal{R}$ -closed and  $\mu \preceq_{\mathcal{R}} \mu'$  we have that  $\mu(\mathcal{R}(Q_1)) \leq \mu'(\mathcal{R}(Q_1))$ . Hence, we get that  $\mu(Q_1) \leq \mu'(\mathcal{R}(Q_1))$ . Now, please note that  $\mu'(\mathcal{R}(Q_1)) = \mu'(\mathcal{R}(Q_1) \cap Q')$ . Hence, the result will follow if we can show that  $\mathcal{R}(Q_1) \cap Q' \subseteq Q_2$ .

Pick  $q_b \in \mathcal{R}(Q_1) \cap Q'$ . We have by definition that  $q_b \in Q'$  and there exists  $q_a \in Q_1$  such that  $q_a \mathcal{R} q_b$ . Now, please note that as  $Q_1 \subseteq Q$ , we get  $q_a \mathcal{R}_0 q_b$  (by definition of  $\mathcal{R}_0$ ). Also as  $Q_1 \subseteq Q_0$ , we get that  $q_a \in Q_0$ . Since  $Q_0$  is a  $\mathcal{R}_0$ -closed set,  $q_b \in Q_0$ . As  $q_b \in Q'$ , we get  $q_b \in Q_2$  also. Since  $q_b$  was an arbitrary element of  $\mathcal{R}(Q_1) \cap Q'$ , we can conclude that  $\mathcal{R}(Q_1) \cap Q' \subseteq Q_2$ .  $\square$

### C. SIMULATIONS AND PCTL

LEMMA 2.11. *Let  $\mathcal{M} = (Q, q_I, \delta, L)$  be a MDP. For any states  $q, q' \in Q$ ,  $q \preceq q'$  implies that for every liveness formula  $\psi_L$ , if  $q \Vdash_{\mathcal{M}} \psi_L$  then  $q' \Vdash_{\mathcal{M}} \psi_L$  and that for every safety formula  $\psi_S$ , if  $q' \Vdash_{\mathcal{M}} \psi_S$  then  $q \Vdash_{\mathcal{M}} \psi_S$ .*

PROOF. The proof is by induction on the length of the safety and liveness formulas. We discuss the case when  $\psi_S$  is of the form  $\text{Pr}_{\triangleleft p}(\psi_{L_1} \mathcal{U} \psi_{L_2})$ . Assume that  $q' \Vdash_{\mathcal{M}} \psi_S$ . We need to show that  $q \Vdash_{\mathcal{M}} \psi_S$ .

There are two cases to consider.

- The first case is when  $q \not\Vdash_{\mathcal{M}} \psi_{L_1}$ . There are two further possibilities.
  - (1)  $q \Vdash_{\mathcal{M}} \psi_{L_2}$ . Then (by induction hypothesis),  $q' \Vdash_{\mathcal{M}} \psi_{L_2}$  also. Since  $q' \Vdash \text{Pr}_{\triangleleft p}(\psi_{L_1} \mathcal{U} \psi_{L_2})$ , we must have that  $p$  is 1 and  $\triangleleft$  is  $\leq$ . Clearly  $q \Vdash_{\mathcal{M}} \text{Pr}_{\leq 1}(\psi_{L_1} \mathcal{U} \psi_{L_2})$  also.
  - (2)  $q \not\Vdash_{\mathcal{M}} \psi_{L_2}$ . Now, if  $p > 0$ , then  $q \Vdash_{\mathcal{M}} \text{Pr}_{\triangleleft p}(\psi_{L_1} \mathcal{U} \psi_{L_2})$  trivially. If  $p$  is 0 then since  $q' \Vdash_{\mathcal{M}} \psi_S$ , it follows that  $\triangleleft$  must be  $\leq$ . Now,  $q \Vdash_{\mathcal{M}} \text{Pr}_{\leq 0}(\psi_{L_1} \mathcal{U} \psi_{L_2})$  and the result follows in this case.

— The second case is when  $q \Vdash_{\mathcal{M}} \psi_{L_1}$ . By induction hypothesis,  $q' \Vdash_{\mathcal{M}} \psi_{L_1}$  also. Let  $\mathcal{R} \subseteq Q \times Q$  be a simulation relation such that  $q \mathcal{R} q'$ . Now, let  $Q_0 \subset Q$  be the set  $\{q_0 \in Q \mid q_0 \Vdash_{\mathcal{M}} \psi_{L_1} \vee \psi_{L_2}\}$ . Clearly  $q, q' \in Q_0$ . Let  $\delta_0$  be the restriction of  $\delta$  on  $Q_0$ . That is  $\delta_0(q_0) = \{\mu \mid q_0 \in \mu \mid \mu \in \delta(q_0)\}$  for each  $q_0 \in Q_0$ . Pick a new label  $P_{\psi_{L_2}}$  and for each  $q_0 \in Q_0$  let  $L_0(q_0) = \{P_{\psi_{L_2}}\}$  if  $q_0 \Vdash_{\mathcal{M}} \psi_{L_2}$  and  $\emptyset$  otherwise. Consider the MDP  $\mathcal{M}_0 = (Q_0, q, \delta_0, L_0)$ . It is easy to see that for any  $q_0 \in Q_0$ ,  $q_0 \Vdash_{\mathcal{M}} \psi_S$  iff  $q_0 \Vdash_{\mathcal{M}_0} \text{Pr}_{\triangleleft p}(\diamond P_{\psi_{L_2}})$ .

Let  $\mathcal{R}_0$  be the restriction of  $\mathcal{R}$  to  $Q_0$ , i.e.,  $\mathcal{R}_0 = \mathcal{R} \cap (Q_0 \times Q_0)$ . We make the following observations on  $\mathcal{R}_0$ .

- (1)  $q \mathcal{R}_0 q'$ .

- (2)  $\mathcal{R}_0$  is reflexive and transitive (which follows from reflexivity and transitivity of  $\mathcal{R}$ ).
- (3) We claim that if  $\mu \preceq_{\mathcal{R}} \mu'$  then  $\mu|_{\mathbb{Q}_0} \preceq_{\mathcal{R}_0} \mu'|_{\mathbb{Q}_0}$  also. For this claim, it suffices to show that if  $A \subseteq \mathbb{Q}_0$  is  $\mathcal{R}_0$ -closed then  $A$  must be  $\mathcal{R}$ -closed also. In order to demonstrate this, fix a  $\mathcal{R}_0$ -closed set  $A_0$ . Now, let  $q_1$  be any element of  $\mathbb{Q}$  such that  $q_1 \in \mathcal{R}(A_0)$ . Then there must be a  $q_0 \in \mathbb{Q}_0$  such that  $q_0 \mathcal{R} q_1$ . Now, since  $q_0 \in \mathbb{Q}_0$ , it must be the case that  $q_0 \Vdash \psi_{L_1}$  or  $q_0 \Vdash \psi_{L_2}$ . In either case, by induction hypothesis, we get that  $q_1 \Vdash \psi_{L_1}$  or  $q_1 \Vdash \psi_{L_2}$  (since  $\mathcal{R}$  is a simulation relation). Therefore  $q_1 \in \mathbb{Q}_0$ , and hence by definition  $q_0 \mathcal{R}_0 q_1$ . Since  $A_0$  is  $\mathcal{R}_0$ -closed set, we get that  $q_1 \in A_0$ . Thus,  $A_0$  is  $\mathcal{R}$ -closed set.
- (4) Now, let  $q_0 \mathcal{R}_0 q'_0$ . From the above claim and the fact that  $\mathcal{R}$  is a simulation, it can be easily shown that for each  $\mu_0 \in \delta_0(q_0)$  there is a  $\mu'_0 \in \delta_0(q'_0)$  such that  $\mu_0 \preceq_{\mathcal{R}_0} \mu'_0$ .
- (5) Similarly we can show that if  $q_0 \mathcal{R}_0 q'_0$  then if  $P_{\psi_{L_2}} \in L_0(q_0)$  then  $P_{\psi_{L_2}} \in L_0(q'_0)$  also. Thus the set  $Q_1 = \{q_0 \in \mathbb{Q}_0 \mid P_{\psi_{L_2}} \in L_0(q_0)\}$  is  $\mathcal{R}_0$ -closed set.
- (6) Since  $\mathcal{R}_0$  enjoys properties 2, 4 and 5, results of [D'Argenio et al. 2001] imply that for any  $q_0 \mathcal{R}_0 q'_0$ , if  $q'_0 \Vdash_{\mathcal{M}_0} \text{Pr}_{\triangleleft p}(\diamond P_{\psi_{L_2}})$  then  $q_0 \Vdash_{\mathcal{M}_0} \text{Pr}_{\triangleleft p}(\diamond P_{\psi_{L_2}})$  also.

The result now follows from observations 1 and 6 above.  $\square$

#### D. HARDNESS OF FINDING MINIMAL COUNTEREXAMPLES

**THEOREM 3.10.** *Given a MDP  $\mathcal{M}$ , a safety formula  $\psi_S$  such that  $\mathcal{M} \not\models \psi_S$ , and a number  $k \leq 2|\mathcal{M}|$ , deciding whether there is a counterexample  $(\mathcal{E}, \mathcal{R})$  of size  $\leq k$  is NP-complete.*

**PROOF.** The problem is in NP because one can guess a counterexample  $(\mathcal{E}, \mathcal{R})$  of size  $k$  and check if  $\mathcal{E}$  violates  $\psi_S$ . The hardness result is achieved by a reduction from the exact 3-cover problem [Garey and Johnson 1979] which is formally defined as follows.

Given a set  $X$  such that  $|X| = 3r$  and a collection  $\mathcal{C}$  of subsets of  $X$  such that for each  $C \in \mathcal{C}$ ,  $|C| = 3$ , is there an *exact 3-cover* for  $X$ . In other words, is there a collection of pairwise disjoint sets  $\mathcal{B} \subseteq \mathcal{C}$  such that  $X = \cup_{B \in \mathcal{B}} B$ .

Before, outlining the proof, it is useful to recall what a *3-cover* (not necessarily exact) for  $X$  is: the collection  $\mathcal{B}$  is said to be a *3-cover*, if  $\mathcal{B} \subseteq \mathcal{C}$  is a collection (not necessarily disjoint) such that  $X = \cup_{B \in \mathcal{B}} B$ .

Note that without loss of generality we can assume that for each  $x \in X$  there is a  $C \in \mathcal{C}$  such that  $x \in C$  (if this is not the case, we can simply answer no in polynomial time). Note that  $|\mathcal{B}| = r$  for an exact cover. Also note that  $X$  has an exact 3-cover  $\mathcal{B} \subseteq \mathcal{C}$  iff there is cover  $\mathcal{B}' \subseteq \mathcal{C}$  such that  $|\mathcal{B}'| \leq r$ . (Actually no collection  $\mathcal{B}'$  such that  $|\mathcal{B}'| < r$  can cover  $X$ , so  $\leq$  is mainly a matter of convenience.)

The reduction is as follows. We first construct a MDP  $\mathcal{M} = (\mathbb{Q}, q_{\mathcal{I}}, \delta, L)$  as follows. For the set of states, we take  $\mathbb{Q} = X \cup \mathcal{C} \cup \{s, t\}$  where  $s$  and  $t$  are two distinct elements not in  $X \cup \mathcal{C}$ . The initial state  $q_{\mathcal{I}}$  is taken to be  $s$ . There is one probabilistic transition out of  $s$ ,  $\mu_s$ , such that  $\mu_s(x) = \frac{1}{3r}$  for each  $x \in X$  and  $\mu_s(q) = 0$  for all  $q \in \mathbb{Q} \setminus X$ . From each  $x \in X$ ,  $\delta(x) = \{\mu_{x,C} \mid x \in C, C \in \mathcal{C}\}$

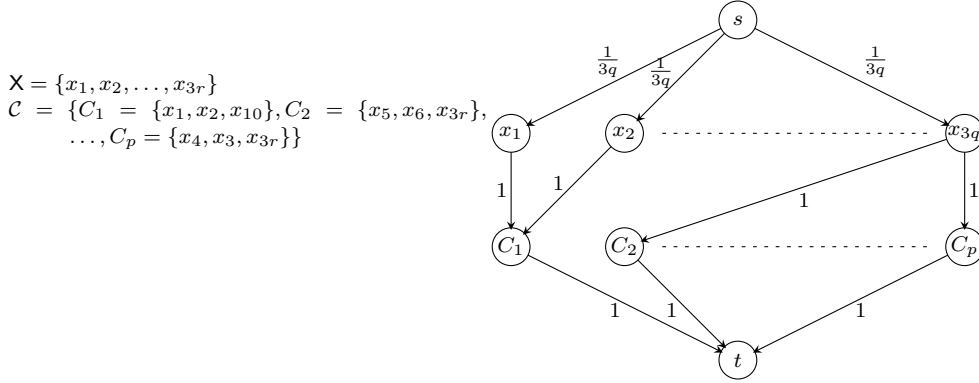


Fig. 22. A problem instance of exact 3-cover and the constructed MDP

where  $\mu_{x,C}$  assigns probability 1 to  $C$  and 0 otherwise. For each  $C$ , there is one probabilistic transition out of  $C$ ,  $\mu_C$ , which assigns probability 1 to  $t$  and is 0 otherwise. There is no transition out of  $t$ . Finally, for the set of propositions, we will pick a proposition  $P_q$  for each  $q \in Q$  and  $P_q$  will be true only in the state  $q$ . For the safety formula, we take  $\psi_S = \mathcal{P}_{<1}(\text{tt} \mathcal{U} P_t)$ . Clearly  $\mathcal{M}$  violates  $\psi_S$ . The reduction is shown in Figure 22. The result now follows from the following claim.

**Claim:**  $X$  has an exact 3-cover  $\mathcal{B} \subseteq \mathcal{C}$  iff there is a counterexample  $(\mathcal{E}, \mathcal{R})$  for  $\mathcal{M}$  and  $\psi_S$  of size  $\leq 2(2 + 4r) + 7r + 3r(1 + \lceil \log 3r \rceil) + 4r$ .

**Proof of the claim:**

$(\Rightarrow)$  Assume that  $\mathcal{B} \subseteq \mathcal{C}$  is an exact 3-cover of  $X$ . We have  $|\mathcal{B}| = r$ . Consider a MDP  $\mathcal{M}'$  which is the same as  $\mathcal{M}$  except that its states are  $\{\bar{q} \mid q \in Q\}$  instead of  $Q$ . Now delete all states  $\bar{C}$  of  $\mathcal{M}'$  such that  $C \notin \mathcal{B}$ . Let the resulting MDP be called  $\mathcal{E}$  and the set of its states be denoted by  $Q_{\mathcal{E}}$ . Note that the  $G(\mathcal{E})$  has  $2 + 4r$  nodes and  $7r$  edges. Furthermore, from the initial state there is a probabilistic transition which assigns probability  $\frac{1}{3r}$  to each  $\{\bar{x} \mid x \in X\}$ . It takes  $1 + \lceil \log 3r \rceil$  bits to represent  $\frac{1}{3r}$  (1 for the numerator and  $\lceil \log 3r \rceil$  for the denominator). For each  $\bar{x}$  such that  $x \in X$ , there is a probabilistic transition which assigns probability 1 to  $\bar{B}$  where  $B \in \mathcal{B}$  is such that  $x \in B$ . Finally, from each  $B \in \mathcal{B}$  there is a probabilistic transition that assigns probability 1 to  $\bar{t}$ . The size of the MDP  $\mathcal{E}$  is seen to be  $2 + 4r + 7r + 3r(1 + \lceil \log 3r \rceil) + 4r$ . Now, let  $\mathcal{R}$  be the relation  $\{(\bar{q}, q) \mid q \in Q_{\mathcal{E}}\}$ . Clearly  $(\mathcal{E}, \mathcal{R})$  is a counterexample and one can easily check that  $|\mathcal{E}, \mathcal{R}| = 2(2 + 4r) + 7r + 3r(1 + \lceil \log 3r \rceil) + 4r$ .

$(\Leftarrow)$  Assume that there is a counterexample  $(\mathcal{E}, \mathcal{R})$  of size  $\leq 2(2 + 4r) + 7r + 3r(1 + \lceil \log 3r \rceil) + 4r$ . Thus we have that  $\mathcal{E} \preceq \mathcal{M}$ ,  $\mathcal{R}$  is a canonical simulation and  $\mathcal{E}$  violates  $\psi_S$ . Now note that since every node of  $\mathcal{M}$  is labeled by a unique proposition,  $\mathcal{R}$  is functional. In other words each state  $q_1$  of  $\mathcal{E}$  is related to at most one state of  $Q$ . Observe that since the safety formula  $\psi_S$  is  $\mathcal{P}_{<1}(\text{tt} \mathcal{U} P_t)$ , there is a memoryless scheduler  $\mathcal{S}$  such that  $\mathcal{E}^{\mathcal{S}}$  violates  $\psi_S$ . Let  $\mathcal{E}^{\mathcal{S}} = (Q_{\mathcal{E}}, q_{\mathcal{E}}, \delta_{\mathcal{E}}, L_{\mathcal{E}})$ . For each  $q_1 \in Q_{\mathcal{E}}$ , let  $\mu_{q_1}$  denote the unique probabilistic transition out of  $\mathcal{E}^{\mathcal{S}}$ .

Note that we have  $q_{\mathcal{E}} \mathcal{R} s$ . Consider the set  $Q_X = \text{post}(q_{\mathcal{E}}, \mu_{q_{\mathcal{E}}})$ . Since  $\mathcal{E}$  is simulated by  $\mathcal{M}$ ; it follows that each element of  $Q_X$  must be labeled by some proposition  $P_x$

for some  $x \in X$ . Given  $x \in X$ , if  $Q_x \subseteq Q_X$  is the set of states labeled by  $P_x$  then we must have  $qR_x$  for each  $q \in Q_x$ . We also have that  $\mu_{q_\mathcal{E}}(Q_x) \leq \frac{1}{3r}$  and  $Q_{x_1} \cap Q_{x_2} = \emptyset$  for  $x_1 \neq x_2$ . Now note that the probability of reaching  $P_t$  from  $q_\mathcal{E}$  is 1 in  $\mathcal{E}^S$ . Hence it must be the case that  $\mu_{q_\mathcal{E}}(Q_X) = 1$  and thus  $Q_x \neq \emptyset$  for any  $x \in X$ . Therefore  $|Q_X| \geq 3r$  and the total size of the numbers  $\{\mu_{q_\mathcal{E}}(q) \mid \mu_{q_\mathcal{E}}(q) > 0, q \in Q_X\}$  is at least  $|Q_X|(1 + \lceil \log 3r \rceil)$ .

Now given  $q \in Q_x$  consider  $\text{post}(q, \mu_q)$ . Again as the total probability of reaching  $P_t$  is 1 in  $\mathcal{E}^S$ ,  $\text{post}(q, \mu_q)$  cannot be empty. Furthermore, as each  $q \in Q_x$  is simulated by  $x$ , it follows that each element  $q' \in \text{post}(q, \mu_q)$  must be labeled by a single  $P_B \in \mathcal{C}$  such that  $x \in B$ . Let  $Q_C = \cup_{q \in Q_X} \text{post}(q, \mu_q)$ . By the above observations it follows that if we consider the set  $\mathcal{B} = \{B \in \mathcal{C} \mid P_B \text{ labels a node in } Q_C\}$  then  $\mathcal{B}$  covers  $X$ . Also since every state of  $Q_C$  is labeled by a single proposition, we get  $|Q_C| \geq |\mathcal{B}|$ .

We can show by similar arguments that for each  $q \in Q_C$  the set  $\text{post}(q, \mu_q)$  is non-empty and each node of  $\text{post}(q, \mu_q)$  must be labeled by  $P_t$ . Let  $Q_t = \cup_{q \in Q_C} \text{post}(q, \mu_q)$ . We have that  $|Q_t| \geq 1$ .

Note that the sets  $Q_X$ ,  $Q_t$  and  $Q_C$  are pairwise disjoint and do not contain  $q_\mathcal{E}$ . Hence, the labeled underlying graph of  $\mathcal{E}$ ,  $G_\ell(\mathcal{E})$ , has at least  $1 + |Q_X| + |Q_C| + |Q_t|$  vertices. It is easy to see that  $\mathcal{R}$  also contains at least  $1 + |Q_X| + |Q_C| + |Q_t|$  elements. Furthermore, it is easy to see that the underlying graph has at least  $2|Q_X| + |Q_C|$  edges; and the total size of numbers used as probabilities in  $\mathcal{E}$  is at least  $|Q_X|(1 + \lceil \log(3r) \rceil) + |Q_X| + |Q_C|$ . Hence the total size of  $(\mathcal{E}, R)$  is at least  $2(1 + |Q_X| + |Q_C| + |Q_t|) + 2|Q_X| + |Q_C| + |Q_X|(1 + \lceil \log(3r) \rceil) + |Q_X| + |Q_C|$ . Since  $|Q_t| \geq 1$  and  $|Q_X| \geq 3r$ ; the total size is at least  $2(2 + 3r + |Q_C|) + 6r + |Q_C| + 3r(1 + \lceil \log(3r) \rceil) + 3r + |Q_C|$ . By hypothesis, the total size is  $\leq 2(2 + 4r) + 7r + 3r(1 + \lceil \log 3r \rceil) + 4r$  and we get that  $|Q_C| \leq r$ . But  $|Q_C| \geq |\mathcal{B}|$  and hence  $|\mathcal{B}| \leq r$ . Since  $\mathcal{B}$  is a cover; it follows that  $X$  must have an exact 3-cover.  $\square$

**THEOREM 3.11.** *Given a MDP  $\mathcal{M}$ , a safety formula  $\psi_S$  and  $n = |\mathcal{M}| + |\psi_S|$  such that  $\mathcal{M} \not\models \psi_S$ . The smallest counterexample for  $\mathcal{M}$  and  $\psi_S$  cannot be approximated in polynomial time to within  $O(2^{\log^{1-\epsilon} n})$  unless  $\text{NP} \subseteq \text{DTIME}(n^{\text{poly} \log(n)})$ .*

**PROOF.** The in-approximability follows from a reduction of the Directed Network Steiner Problem [Dodis and Khanna 1999]. Directed Network Steiner Problem is formally defined as follows.

Given a directed graph  $G$  and  $m$  pairs  $\{s_i, t_i\}_{i=1}^m$  of vertices of  $G$ , a sub-graph  $G' = (V', E')$  of  $G$  satisfies the Steiner condition if  $s_i$  has path in  $G'$  to  $t_i$  for all  $i$ . The Directed Network Steiner problem asks for a sub-graph  $G'$  such that  $G'$  satisfies the Steiner condition and has the smallest size amongst all subgraphs of  $G$  which satisfy the Steiner condition.

It is shown in [Dodis and Khanna 1999] that the smallest sub-graph cannot be approximated to within  $O(2^{\log^{1-\epsilon}(n_g)})$  where  $n_g$  is the sum  $m +$  size (vertices+edges) of  $G$  unless  $\text{NP} \subseteq \text{DTIME}(n_g^{\text{poly} \log(n_g)})$ . Also note that since  $\epsilon$  is arbitrary the smallest sub-graph cannot be found to within  $O(2^{\log^{1-\epsilon}(n_g \log(n_g))})$  (changing  $n_g$  to  $n_g \log(n_g)$  does not make a difference  $\text{DTIME}(n_g^{\text{poly} \log(n_g)})$ ).

We now give the reduction. Given a graph  $G = (V, E)$ , let  $|V| = n_v$ ,  $|E| = n_e$ ,  $n_g = n_e + n_v$ . Recall, that the Directed Network Steiner problem has  $m$  pairs  $(s_i, t_i)$ . Let  $n_s$  be the number of distinct  $s_i$ 's in  $(s_i, t_i)$ . In other words  $n_s$  is the cardinality of the set  $\{s_i \mid 1 \leq i \leq m\}$ . Clearly  $n_s \leq n_g$ . Please note that for the Directed Network Steiner problem we can assume that  $n_g$  is  $O(n_e)$ .

We construct a DTMC  $\mathcal{M}$  with set of states  $V \cup \{s\}$ , where  $s$  is a new vertex.  $s$  is the initial state of  $\mathcal{M}$  and has a probabilistic transition  $\mu_s$  such that  $\mu_s(s_i) = \frac{1}{n_g}$  for each  $1 \leq i \leq m$  and  $\mu_s(v) = 0$  if  $v \notin \{s_i \mid 1 \leq i \leq m\}$ . Every other state  $v$  has a transition  $\mu_v$  such that  $\mu_v(v') = \frac{1}{n_g}$  if  $(v, v') \in E$ ; otherwise  $\mu_v(v') = 0$ . Finally, we will have as propositions  $\{P_v \mid v \in V \cup \{s\}\}$ , where the proposition  $P_v$  holds at exactly the state  $v$ . Since it takes  $O(\log(n_g))$  bits to represent  $\frac{1}{n_g}$ , the size of DTMC  $\mathcal{M}$  is easily seen to be  $n_v + 1 + n_e + n_s + (n_e + n_s)(O(\log(n_g)))$ .

Consider the safety formula  $\psi_S = \psi_{S_1} \vee \psi_{S_2}$  where  $\psi_{S_1} = \bigvee_{i=1}^m \mathcal{P}_{\leq 0}(\diamond(s_i \wedge (\neg \mathcal{P}_{\leq 0}(\diamond t_i))))$  and  $\psi_{S_2} = \bigvee_{i=1}^{n_s} \mathcal{P}_{\leq 0}(X s_i)$ .

The sum  $n_m = |\mathcal{M}| + |\psi_S|$  is easily seen to be  $O(n_g \log(n_g))$ .

**Claim:**

- (1) If  $G$  has a sub-graph  $G' = (V', E')$  with  $|V'_1| = n_1$  and  $|E'| = n_2$  such that  $G'$  satisfies Steiner condition then there is a counterexample for  $\mathcal{M}$  and  $\psi_S$  of size  $= 2n_1 + 2 + n_2 + n_s + (n_2 + n_s)(\log(n_g))$ .
- (2) If there is a counterexample  $(\mathcal{E}, \mathcal{R})$  for  $\mathcal{M}$  and  $\psi_S$  such that  $G_\ell(\mathcal{E})$ , the underlying labeled graph of  $\mathcal{E}$ , has  $n_1 + 1$  vertices and  $n_2 + n_s$  edges then the graph  $G$  has a sub-graph  $G' = (V', E')$  with  $|V'_1| \leq n_1$  and  $|E'| \leq n_2$  such that  $G'$  satisfies the Steiner condition. Furthermore,  $|(\mathcal{E}, \mathcal{R})| \geq 2n_1 + 2 + n_2 + n_s + (n_2 + n_s)(\log(n_g))$ .

**Proof of the claim:**

- (1) First assume that  $G$  has a sub-graph  $G' = (V', E')$  with  $n_1$  vertices and  $n_2$  edges such that  $G'$  satisfies the Steiner condition. Consider the DTMC  $\mathcal{M}'$  obtained from  $\mathcal{M}$  by restricting the set of states to  $V' \cup \{s\}$ . Now take an isomorphic copy of  $\mathcal{M}'$  with  $\{\bar{v} \mid v \in V'\} \cup \bar{s}$  as the set of states and call it  $\mathcal{E}$ . Clearly,  $\mathcal{E}$  violates  $\psi_S$  and the relation  $\{(\bar{u}, u) \mid u \in V' \cup s\}$  is a canonical simulation of  $\mathcal{E}$  by  $\mathcal{M}$ . Hence  $(\mathcal{E}, \mathcal{R})$  is a counterexample and it is easy to see that  $|(\mathcal{E}, \mathcal{R})| = 2n_1 + 2 + n_2 + n_s + (n_2 + n_s)(\log(n_g))$ .
- (2) Let  $\mathcal{E} = (Q_\mathcal{E}, q_\mathcal{E}, \delta_\mathcal{E}, L_\mathcal{E})$  and  $G_\ell(\mathcal{E}) = (V', \{E'_j\}_{j=1}^k)$ . Note that since each state of  $\mathcal{M}$  is labeled by a unique proposition and  $\mathcal{R}$  is a canonical simulation,  $\mathcal{R}$  must be total and functional (totality is a consequence of the fact that we can remove any nodes of  $\mathcal{E}$  that are not reachable from  $q_\mathcal{E}$ ). In other words there is a function  $g : Q \rightarrow V \cup \{s\}$  such that  $\mathcal{R} = \text{rel}_g$ . Again the definition of simulation and the construction of DTMC  $\mathcal{M}$  gives us that if  $(q_1, q_2) \in \cup_{j=1}^k E'_j$ , we must have  $(g(q_1), g(q_2)) \in E \cup \{(s, s_i) \mid 1 \leq i \leq m\}$  and  $\mu'_{q_1}(q_2) \leq \frac{1}{n_g}$  for any probabilistic transition  $\mu'_{q_1} \in \delta_\mathcal{E}(q_1)$ . From the latter observation, we get that  $|(\mathcal{E}, \mathcal{R})| \geq 2n_1 + 2 + n_2 + n_s + (n_2 + n_s)(\log(n_g))$ .

Now, consider the equivalence relation  $q_1 \equiv q_2$  defined on  $Q$  as  $q_1 \equiv q_2$  iff  $g(q_1) = g(q_2)$ . Let  $[q]$  denote the equivalence class of  $q$  under  $\equiv$ . Let  $G_2 =$

$\{V'', E''\}$  be the graph such that  $V''$  is the set of equivalence classes under the relation  $\equiv$  and  $([q_1], [q_2]) \in E''$  if  $(q_1, q_2) \in \cup_{j=1}^k E'$ . Please observe first that  $G_2$  is isomorphic to a subgraph of  $(V \cup \{s\}, E \cup \{(s, s_i) \mid 1 \leq i \leq n_s\})$  with the function  $h([q]) = g(q)$  witnessing this graph isomorphism. Please note that by the fact that  $\mathcal{M}_1$  violates  $\psi_1$ , it can be easily shown that there is a path from  $[s_i]$  to  $[t_i]$  in  $G_2$ . Also since  $\mathcal{M}_1$  violates  $\psi_2$ ,  $G_2$  contains edges  $([s], [s_i])$  for each  $1 \leq i \leq n_s$ . We get by the above observations  $G$  must contain a subgraph  $G' = (V', E')$  with paths from  $s_i$  to  $t_i$  for all  $i$  such that  $|V'_1| \leq n_1$  and  $|E'| \leq n_2$ . **(End proof the claim.)**

From the above two observations it easily follows that if  $G$  has a Steiner sub-graph of minimum size  $n_{\min_1}$  and  $\mathcal{M}$  has a counterexample of minimum size  $n_{\min_2}$  then  $\frac{n_{\min_2}}{n_{\min_1}} = O(\log(n_g))$ . Now assume that there is a polynomial time algorithm to compute the minimal counterexample within a factor of  $O(2^{\log^{1-\epsilon}(n_m)})$  then this algorithm produces a counterexample of size  $k \leq O(2^{\log^{1-\epsilon}(n_m)})n_{\min_2}$ . Thus the counterexample size is  $\leq O(2^{\log^{1-\epsilon}(n_m)})O(\log(n_g))n_{\min_1}$ . From the proof of the part 2 of the above claim it follows that we can extract from the counterexample in polynomial time a Steiner sub-graph of  $G$  of size  $\leq O(2^{\log^{1-\epsilon}(n_m)})n_{\min_1}$ . Now  $n_m$  is  $O(n_g \log(n_g))$  and thus we have achieved an approximation within  $O(2^{\log^{1-\epsilon}(n_g \log(n_g))})$ . The result now follows.  $\square$

## E. CEGAR LOOP CAN BE FASTER THAN DIRECT MODEL CHECKING

*Example E.1.* Consider the MDP  $\mathcal{M} = (\mathbf{Q}, \delta, q_{\mathcal{I}}, \mathbf{L})$  where

—The set of states  $\mathbf{Q}$  has  $n + 2$  states. We let  $\mathbf{Q} = \{q_i \mid 1 \leq i \leq n\} \cup \{q_{\text{fail}}, q_{\text{delay}}\}$ .

— $q_{\mathcal{I}} = q_1$ .

— $\delta$  is defined as follows. For each  $1 \leq i \leq n$ ,  $\delta(q_i) = \{\mu_i^1, \mu_i^2\}$  where

(1)  $\mu_i^1(q_i) = 0$ ,  $\mu_i^1(q_j) = \frac{1}{4(n-1)}$  if  $j \neq i$ ,  $\mu_i^1(q_{\text{delay}}) = \frac{1}{4}$  and  $\mu_i^1(q_{\text{fail}}) = \frac{1}{4}$ .

(2)  $\mu_i^2(q_j) = \frac{1}{3n}$  for each  $j$ ,  $\mu_i^2(q_{\text{delay}}) = 0$  and  $\mu_i^2(q_{\text{fail}}) = \frac{1}{3}$ .

From state  $q_{\text{delay}}$ , there is only one probabilistic transition and this transition assigns probability 1 to  $q_{\text{fail}}$ . There is no transition out of state  $q_{\text{fail}}$ .

—The state  $q_{\text{fail}}$  is labeled by proposition  $P$ . No other state is labeled by proposition  $P$ .

The property we want to check is  $\phi = \mathcal{P}_{\leq \frac{2}{3}}(\diamond P)$ .

Our CEGAR algorithm proceeds as follows. The initial equivalence classes are  $\{q_{\text{fail}}\}$  and  $\mathbf{Q} \setminus \{q_{\text{fail}}\}$ . The initial abstraction  $\mathcal{M}_1$  has two states—  $\{q_{\text{fail}}\}$  and  $\mathbf{Q} \setminus \{q_{\text{fail}}\}$ . There are three transitions out of the initial state  $\mathbf{Q} \setminus \{q_{\text{fail}}\}$ . The first one assigns probability 1 to  $\{q_{\text{fail}}\}$ , the second one assigns probability  $\frac{1}{2}$  to  $\mathbf{Q} \setminus \{q_{\text{fail}}\}$  and  $\frac{1}{4}$  to  $\{q_{\text{fail}}\}$  and the third one assigns probability  $\frac{1}{3}$  to  $\mathbf{Q} \setminus \{q_{\text{fail}}\}$  and  $\frac{1}{3}$  to  $\{q_{\text{fail}}\}$ . There is no transition out of  $\{q_{\text{fail}}\}$ . While constructing this abstraction, we have to do  $O(n^2)$  additions (for each state  $q_i$  and each transition out of  $q_i$ , we have to add  $n$  numbers). Therefore the cost of constructing this abstraction is  $O(n^2)$ .

Now, we check  $\mathcal{M}_1$  against the property  $\phi$ , which turns out to be false and the counterexample generation algorithm gives exactly one counterexample  $\mathcal{E}$ . The counterexample  $\mathcal{E}$  is a DTMC with two states — one corresponding to  $\mathbf{Q} \setminus \{q_{\text{fail}}\}$  and the other corresponding to  $\{q_{\text{fail}}\}$ . The transition out of  $\mathbf{Q} \setminus \{q_{\text{fail}}\}$  assigns probability

1 to  $\{q_{\text{fail}}\}$  (there is no transition out of  $\{q_{\text{fail}}\}$ ). Please note that the constructed  $\mathcal{M}_1$  and the counterexample  $\mathcal{E}$  are independent of  $n$ . So the time-complexity of model checking  $\mathcal{M}_1$  and generating  $\mathcal{E}$  is  $O(1)$ .

Now, we check whether  $\mathcal{E}$  is a valid counterexample. In this case, it turns out that counterexample validity checking is also  $O(n^2)$ . This is because we have to check if the concrete state  $q_i$  simulates the abstract  $\mathbb{Q} \setminus \{q_{\text{fail}}\}$  and for this we have to check if any of the two transitions out of  $q_i$  in the concrete MDP  $\mathcal{M}$  simulates the transition out of  $\mathbb{Q} \setminus \{q_{\text{fail}}\}$  in the counterexample, and for checking each transition we have to add  $n$  numbers. The check immediately gives that each  $q_i$  is indeed not simulated by  $\mathbb{Q} \setminus \{q_{\text{fail}}\}$  and thus the counterexample is not valid. The refinement step now splits  $\mathbb{Q} \setminus \{q_{\text{fail}}\}$  into two equivalence classes—  $\mathbb{Q}_n = \{q_i \mid 1 \leq i \leq n\}$  and  $\{q_{\text{delay}}\}$ . So in total, the time-complexity of these two steps is  $O(n^2)$ .

The new abstraction  $\mathcal{M}_2$  which occurs as a result of this splitting consists of 3 states:  $\mathbb{Q}_n$ ,  $\{q_{\text{delay}}\}$  and  $\{q_{\text{fail}}\}$ . There are two transitions out of  $\mathbb{Q}_n$ . The first one assigns probability  $\frac{1}{4}$  each to  $\mathbb{Q}_n$ ,  $\{q_{\text{delay}}\}$  and  $\{q_{\text{fail}}\}$ . The second one assigns probability  $\frac{1}{3}$  each to  $\mathbb{Q}_n$  and  $\{q_{\text{fail}}\}$  and assigns probability 0 to  $\{q_{\text{delay}}\}$ . There is only one transition out of  $\{q_{\text{delay}}\}$  which assigns probability 1 to  $\{q_{\text{fail}}\}$ . There is no transition out of  $q_{\text{fail}}$ . The construction of this new abstraction also takes  $O(n^2)$  time.

Now  $\mathcal{M}_2$  satisfies  $\phi$  and the CEGAR algorithm ends by saying that the property  $\phi$  is satisfied. Please note again that model checking  $\mathcal{M}_2$  is independent of  $n$ .

Therefore, the whole CEGAR algorithm takes  $O(n^2)$  time.

On the other hand, were we to do the model checking by value iteration [Rutten et al. 2004], each step of value iteration involves  $O(n^2)$  multiplications and  $O(n^2)$  additions. Furthermore, strictly speaking, the value iteration will never terminate (since the convergence to  $\frac{2}{3}$  is in the limit). In practice, we stop the value iteration assuming some predefined machine error. In that case, the number of value iteration steps depend on this predefined machine error and indeed can be very large.

*Remark E.2.* Please note that we have used a MDP in the above example. One can also give examples in which model checking DTMCs for safety properties is also going to be faster using our approach. For example, consider the DTMC  $\mathcal{M}'$  which is the same as  $\mathcal{M}$  in Example E.1 except that  $\delta(q_i)$  consists of only one transition, namely  $\mu_i^1$ . Now, an analysis similar to the one given in Example E.1 will demonstrate that model checking  $\mathcal{M}'$  against the property  $\phi = \mathcal{P}_{\leq \frac{2}{3}}(\diamond P)$  is going to be faster than model checking by value iteration.