

## Series 6, Solution

1

~~11/12~~

EA Given: MDP  $M = (S, Act, P, l_{init}, AP, L)$

Subsystem: MDP  $M' = (S', s'_{init}, Act', P', L')$  is subsystem of  $M$  if  $S' \subseteq S$ ,  $s'_{init} = s_{init}$ ,  $L'(s) = L(s)$  for all  $s \in S'$ ,  $Act' \subseteq Act$ ,  $P'(s, \alpha, s') \neq 0 \Rightarrow P'(s, \alpha, s') = P(s, \alpha, s')$  for all  $s, s' \in S'$  and  $\alpha \in Act'$ .

minimization:

introduce:  $x_s \in [0, 1] \subseteq \mathbb{R}$  for all  $s \in S$   
 $p_s \in [0, 1] \subseteq \mathbb{R}$  "  
 $\sigma_{s, \alpha} \in [0, 1] \subseteq \mathbb{R}$  for all  $s \in S, \alpha \in Act$

minimize

$$\sum_{s \in S} x_s$$

2

s.t.  $p_{s_T} > \lambda$

prob of initial state shall at least exceed  $\lambda$

$\forall s \in T: p_s = x_s$

if target included, prob will be 1

$\forall s \in SIT: \sum_{\alpha \in Act} \sigma_{s,\alpha} = x_s$

if  $s$  included, exactly 1 action is chosen

$\forall s \in SIT \forall \alpha \in Act: p_s \leq (1 - \sigma_{s,\alpha}) + \sum_{s' \in succ_n(s,\alpha)} P(s,\alpha,s') \cdot p_{s'}$

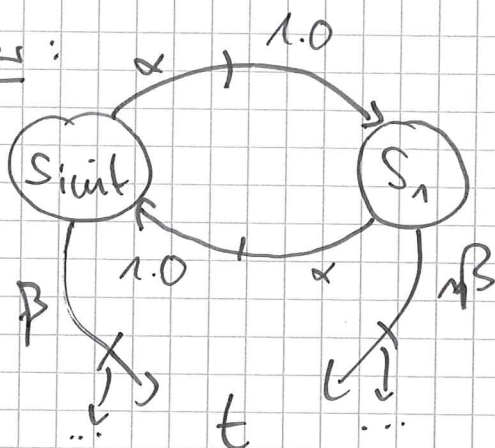
if  $\alpha$  at  $s$ ,  
 $= 0$ , otherwise  
 $= 1$ , trivially  
 fulfills  
 constraint

reachability prob  
 of  $s$

2. Question: Is this correct?

3

Consider:

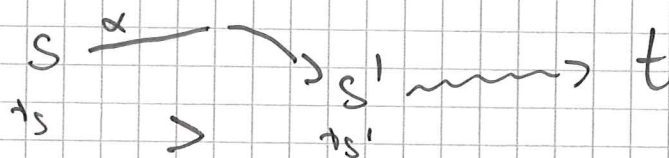


- selecting  $\alpha$  in both states prevents reaching the target states  $\rightarrow$  problematic states

$$P_{S_{init}} = 1 \cdot P_{S_1} \quad P_{S_1} = 1 \cdot P_{S_{init}}$$

for all  $\alpha \in [0, 1]$ :  $P_{S_{init}} = P_{S_1} = \alpha$  is a solution,  
although  $t$  is not reachable.

Solution: \*Variable  $\tau_s \in \mathbb{R}$  to problematic states.



not possible, strictly increasing!

$\rightarrow$  ensures existence of loop-free path from problematic state to  $t$ !

## Encoding:

4

$$\text{Let } \text{Act}_M^{\text{Probl}} = \{(s, \alpha) \in S \times \text{Act} \mid \text{succ}_M(s, \alpha) \subseteq S_M^{\text{Probl}}\}$$

$$s \xrightarrow{\alpha} \begin{matrix} s_1 \\ s_1 \end{matrix} \} \text{problematic!}$$

(only problematic states reachable via  $s$  and  $\alpha$ !)

$$\forall s \in S^{\text{Probl}}: \tau_s \in \mathbb{R} \text{ (partial order on problematic states)}$$

$$\forall s, s' \in S^{\text{Probl}}: t_{ss'} \in \mathbb{R}^B: \text{transition in the MCS between states } s, s'$$

$$\forall (s, \alpha) \in \text{Act}^{\text{Probl}} \forall s' \in \text{succ}(s, \alpha): t_{ss'} \leq x_{s'}$$

if  $s'$  in MCS, transition might exist

$$\forall (s, \alpha) \in \text{Act}^{\text{Probl}} \forall s' \in \text{succ}(s, \alpha): \tau_s < \tau_{s'} + (1 - t_{ss'})$$

partial order

if transition is chosen

$$\forall (s, \alpha) \in \text{Act}^{\text{Probl}}: (1 - \sigma_{s, \alpha}) + \sum_{s' \in \text{succ}(s, \alpha)} t_{ss'} \geq x_s$$

if scheduler assigns  $\alpha$  at  $s$

1) if  $s$  chosen, transition is needed

$$s \rightarrow s' \rightarrow s'' \rightarrow \dots \rightarrow t$$

$$\tau_s < \tau_{s'} < \tau_{s''} < \dots$$

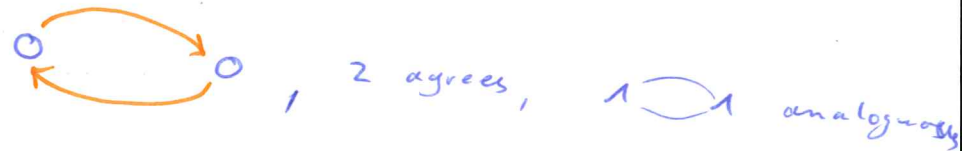
not  $\tau_t$ !

"escapes at target states!"

## Exercise 2

~~1/2/18~~ Prove that if nobody lies then for an even (odd) number of cryptographers, the actual number of agrees is even (odd).

I.B.: Even:



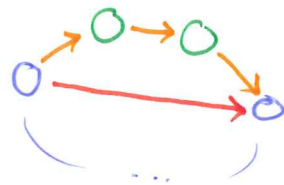
0 1, 0 agrees, 1 0 symmetric

Odd: [Go through all cases for 3 cryptographers]

I.H.: The number of agrees for an even (odd) number of  $n$  cryptographers is even (odd).

I.S.: [Insert 2 new cryptographers into the circle]

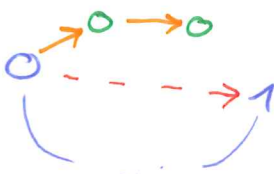
Case 1:



$k - 1 + 3 = k + 2$  agrees,

1 1 1 1 analogous

Case 2:

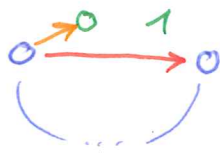


$k - 0 + 2 = k + 2$  agrees,

1 0 0 0 symmetric,

1 1 1 0, 0 1 1 0 analogous

Case 3:

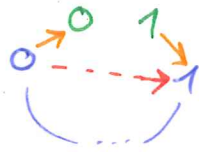


$$k - 1 + 1 = k \text{ agrees,}$$

0 1 0 0 symmetric,

1 1 0 1, 1 0 1 1 analogous.

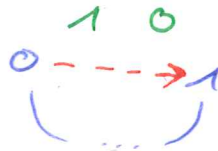
Case 4:



$$k - 0 + 2 = k + 2 \text{ agrees,}$$

1 1 0 0 symmetric and analogous.

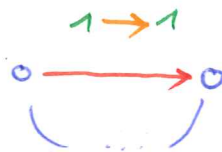
Case 5:



$$k - 0 = k \text{ agrees,}$$

1 0 1 0 symm. and analog.

Case 6:



$$k - 1 + 1 = k \text{ agrees,}$$

1 0 0 1 analogous

So if the number of agrees was an even (odd) number  $k$ , it is after the insertion of two new cryptographers also even (odd), namely  $k$ , or  $k+2$ .

If one guy lies, the number of stated agrees differs by one and is therefore odd (even).