RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

LEHRSTUHL FÜR INFORMATIK 2
RWTH Aachen · D-52056 Aachen
http://moves.rwth-aachen.de

Prof. Dr. Ir. J.-P. Katoen
N. Jansen & B. Kaminiski

Modeling and Verification of Probabilistic Systems
Summer term 2014

– Series 6 –

Hand in on June 17 before the lecture.

Exercise 1 (5 points)

For an MDP $\mathcal{M} = (S, Act, \mathbf{P}, \iota_{\text{init}}, AP, L)$, a *subsystem* is an MDP $\mathcal{M}' = (S', Act', \mathbf{P}', \iota'_{\text{init}}, AP', L')$ with $S' \subset S$. M' shall have the exact same behavior as M for those states, that are included in S'.

a) Give a formal definition for a subsystem of an MDP. What changes need to be made to the original Definition of MDPs?

b) A *mixed integer linear program* is a linear program where certain variables are allowed to be integer. The formal definition reads as follows: Let $A \in \mathbb{Q}^{m \times n}$, $B \in \mathbb{Q}^{m \times k}$, $b \in \mathbb{Q}^m$, $c \in \mathbb{Q}^n$, and $d \in \mathbb{Q}^k$. A *mixed integer linear program* (MILP) consists in computing $\min c^T x + d^T y$ such that $Ax + By \leq b$ and $x \in \mathbb{R}^n,\ y \in \mathbb{Z}^k$.

Consider an MDP $\mathcal{M} = (S, Act, \mathbf{P}, s_{\text{init}}, AP, L)$ with a single initial state (i.e. $\iota_{\text{init}}(s_{\text{init}}) = 1$) and a reachability property $\varphi = \mathbb{P}_{\leq \lambda}(\Diamond \texttt{target})$ that is violated for s_{init}.

Give an MILP formulation that computes a subsystem $\mathcal{M}'$ of an MDP $\mathcal{M}$ which is minimal in terms of the number of states such that s_{init} is included in S' and φ is also violated for s_{init} inside M'. (*Hint:* Use integer variables to count the states of the subsystem.)

Exercise 2 (5 points)

Prove the correctness of Chaum's algorithm for solving the dining cryptographers problem by induction on the number of cryptographers!