Quantitative Verification 9

Remark

We use the following notation short-hands:

- $F_{\sim p}\,\phi := \mathcal{P}_{\sim p}\,[F\,\phi]$, and

- $G_{\sim p}\,\phi := \mathcal{P}_{\sim p}\,[G\,\phi]$

for $\sim\,\in\,\{=,<,\leq,>,\geq\}$, $p\,\in\,[0,1]$, and $\phi\,\in\,\mathsf{PCTL}$. We define analogous abbreviations for the step-bounded versions of F and G.

Ex 1: Logic Modelling

Translate the following formulae to English

1. $\texttt{send}\implies F_{\geq 0.95}^{\leq 10}\,\texttt{deliver}$

2. $\mathcal{P}_{\leq 0.05}\left[F\,F_{\geq 0.9}\,\texttt{error}\right]$

3. $\mathcal{P}\left[G\,(\texttt{send}\implies(\texttt{empty}\,U\,\texttt{receive}))\right] \geq 0.5$

4. $\mathcal{P}_{\geq 0.8}\left[\texttt{empty}\,U\,(\texttt{send}\wedge G_{\leq 0.5}\,\neg\texttt{receive})\right]$

Translate the following specifications into PCTL / PLTL formulae

1. The system with two processes satisfy mutual exclusion almost surely ($\texttt{crit}_i$ holds if process i is in the critical section)

2. The probability that every $\texttt{request}$ will eventually be $\texttt{grant}$ed with a probability greater than 0.95 is 0.99.

3. The probability that component B fails ($\texttt{B\_fail}$) before component A ($\texttt{A\_fail}$) is less than 0.4.

4. If the system is not operational ($\neg\texttt{up}$), it almost surely reaches a state from which it has a greater than 0.99 chance of staying operational ($\texttt{up}$) for 100 time units.

Ex 2: PCTL Satisfiability

For each of the following properties, draw a labelled Markov Chain which satisfies it or argue why the property is unsatisfiable.

1. $G_{\leq 0.5}\,(a\wedge\neg b)$

2. $G_{=1}\,(\neg a\wedge F_{=1}\,a)$

3. $\neg a\wedge\mathcal{P}_{\geq 1}\,[b\,U\,a]$

4. $F_{=1}\,(\texttt{a}\implies(G_{=1}\,((b\implies c)\,U\,\neg a\wedge(F_{\geq 0.5}\,c\vee\neg b))))$

5. $G_{>0}\,(\neg a\wedge F_{>0}\,a)$ (*Note*: Tricky)

Ex 3: Automata

Draw a Rabin automaton for the following formulae:

1. $G\,\neg a\wedge G\,F\,b$

2. $G\,(a\implies F\,b)$