Analysis and Control of Cyber-Physical Systems

Homework 2 — 25 March 2025

Problem 1. Consider the nondeterministic finite automaton $G_n = (X, E, \Delta, x_0, X_m)$ with

$$X = \{x_0, x_1, x_2, x_3, x_4\}; \qquad E = \{a, b\}; \qquad X_m = \{x_0, x_3\};$$

$$\Delta = \{(x_0, a, x_1), (x_0, a, x_2), (x_1, a, x_4), (x_2, \varepsilon, x_3), (x_2, b, x_1), (x_3, \varepsilon, x_1), (x_3, b, x_0), (x_4, b, x_3)\}.$$

(a) Show the graphical representation of this NFA. Which are the nondeterministic structures in this model?

(b) Determine if the following words belong to the language $L(G_n)$ and to the language $L_m(G_n)$. You must also write all runs that generate these words if applicable.

$$w_1 = abab; \qquad w_2 = aab; \qquad w_3 = aa.$$

(c) Determine a DFA G_d equivalent to G_n, i.e., the observer $Obs(G_n)$.

(d) In general, if an NFA G_n is blocking, is $Obs(G_n)$ blocking? Motivate your answer by means of a proof or by a counterexample.

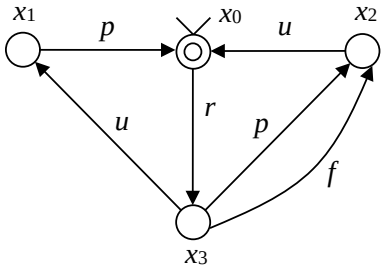
(e) Determine an NFA on alphabet $\{a, b\}$ with $n = 3$ states whose equivalente DFA has $2^3 - 1$ states.

(f) An NFA is said to be *current-state opaque* with respect to a set of secret states $S \subseteq X$ if for any observation $w \in E^*$ one cannot conclude that the current state belongs to set S, i.e., $\mathcal{X}(w) \not\subseteq S$. Discuss if G_n is current state opaque w.r.t. the following two secrets:

$$S_1 = \{x_2\}, \qquad S_2 = \{x_1, x_3\}.$$

Problem 2. A website adopts the following user/password recovery procedure: when a request arrives (event r) the username (event u) and password (event p) are sent in random order by means of two different email messages. Event u and p are logged in a file while event r is not. When a password is sent before the username, the transmission could fail and in this case no event is logged (event f).

This recovery procedure can be modeled by the DFA G shown in the figure below, where the set of observable events is $E_o = \{u, p\}$, the set of unobservable events is $E_{uo} = \{r, f\}$, and the fault event set is $E_f = \{f\}$.



(a) Determine the words in E_o^* that are logged when the following sequences of events are generated:

$$i) \quad s_1 = rup; \qquad ii) \quad s_2 = rfurp.$$

(b) Determine for each logged word $w \in E_o^*$ listed below the set $\mathcal{S}(w)$ of strings consistent with w and the set $\mathcal{X}(w)$ of states consistent with w:

$$i) \quad w_1 = \varepsilon; \qquad ii) \quad w_2 = u.$$

(c) Determine the diagnoser $Diag(G)$. What is the diagnosis state $\varphi(w)$ for the words listed below?

$$i) \quad w_1 = up; \qquad ii) \quad w_2 = pup; \qquad iii) \quad w_3 = uu.$$

(d) Discuss if the diagnoser contains uncertain or indeterminate cycles. Is the fault diagnosable?