Realistic Cases for the Verification of Current-state Opacity

Yifan Dong, Zhiwu Li, and Naiqi Wu

In this note, we provide the descriptions of two realistic cases, namely a robot manipulation system and a manufacturing system.

1 A robot manipulation system

The system of robot manipulation is modeled with an LPN that is shown in Fig. 1. It is a model to simulate the initialization and movement of a machine. Each marking represents a step of the robot, and the system runs when transitions fire. However, due to the limitation of the number of sensors, only a part of transitions is observable. Assume that transitions t_1 and t_8 are labeled with a, i.e., the two events (processes) can be observed by the sensor "a", while transitions t_6, t_7 and t_{11} are labeled with b. The intruder can estimate the behavior of the system by the five observed events with two sensors (a and b). The initial states are parameterized by k, where $M_0 = (2k+1)p_1 + 2kp_7 + 2kp_{13}$.

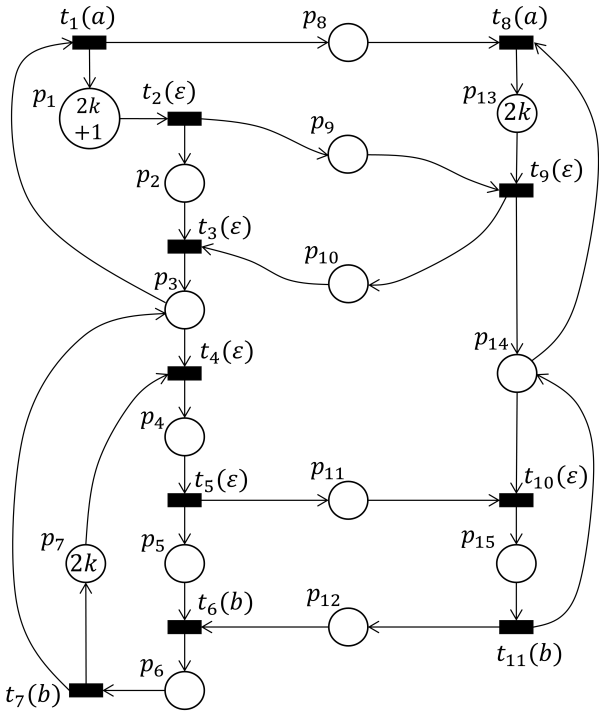

Figure 1: A robot manipulation system modeled by a parameterized Petri net.

2 A manufacturing system

This is a more complex system, namely a parameterized manufacturing system modeled by Petri nets shown in Fig. 2. In our experiments, a series of tests with the increase of two parameters α and β are conducted. There are 2β production lines in this system, where each transition represents an operation of a product. The number of tokens in a place denotes the sources in each station. Given a parameterized manufacturing system modeled by LPNs, we assume that there are two sensors, where the first and last operations of each production line are observed separately. Namely, transitions $t'_{11}, t'_{12}, \ldots, t'_{1\beta}$ and $t''_{11}, t''_{12}, \ldots, t''_{1\beta}$ are labeled with a, while transitions $t'_{(\eta+1)1}, t'_{(\eta+1)2}, \ldots, t'_{(\eta+1)\beta}$ and $t''_{(\eta+1)1}, t''_{(\eta+1)2}, \ldots, t''_{(\eta+1)\beta}$ are labeled with b (the remaining transitions are unobservable labeled with ε). The initial states are parameterized by β, where $M_0 = 2\beta p_1$.

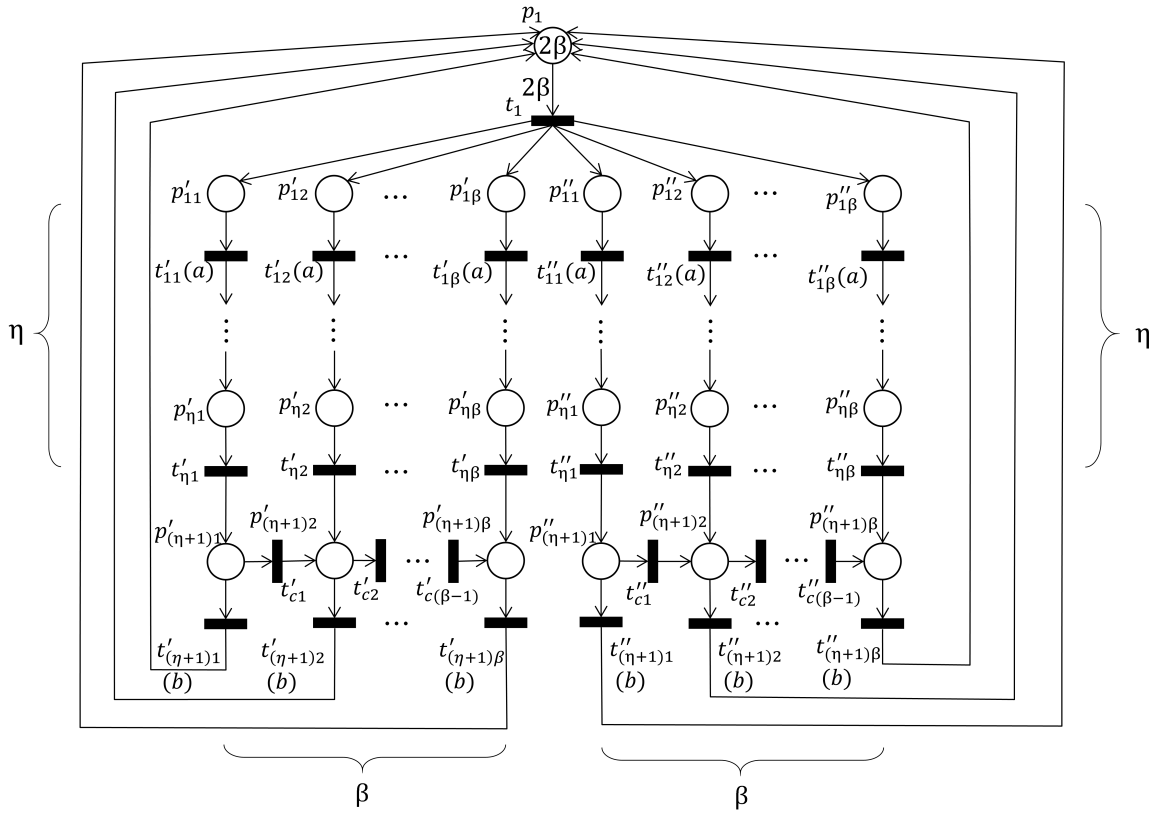

Figure 2: A manufacturing system modeled by a parameterized Petri net.