Prof. Gabriele Taentzer
Alexander Lauer

Formal Methods
Homework 3

1 Formalisation of system properties (6 points)

Given the set $AP \coloneqq \{x = 0, x > 1, y = 0\}$ of atomic statements and a (non-terminating, sequential) program that changes the value of the variable x. Formalise the following informal statements as LT properties, i.e. as sets $P \subseteq (2^{AP})^\omega$. Specify the type of property in each case (invariant; safety property, but not invariant; liveliness property; none) and give reasons.

a) The variable x never has the value 0 and a value > 1 assigned at the same time.

b) The variable x is only finitely often assigned the value 0 and only finitely often a value > 1.

c) The variable x alternates between 0 and values that are >1.

d) The variables x and y have the same value before x has a value > 1 for the first time.

2 Verification of system properties (8 points)

In this exercise, we consider a modified version of the ATM from homework sheet 1 (Figure 1). Instead of the logger, this system contains a mechanism that checks whether the desired payout amount is available in the customer's account. For this transition system with $AP = \{\mathit{start}, \mathit{cardIn}, \mathit{pinEntered}, \mathit{pinCorrect}, \mathit{pinNotCorrect}, \mathit{moneyRequested}, \mathit{amountCovered}\}$, the following properties P_1, P_2 and P_3 are to be analysed:

$$
\begin{aligned}
P_1 &\coloneqq \{A_0A_1A_2... \in (2^{AP})^\omega \mid \forall j \geq 0 : A_j \models \neg\, \mathit{moneyRequested} \vee \mathit{pinCorrect}\} \\
P_2 &\coloneqq \{A_0A_1A_2... \in (2^{AP})^\omega \mid (\exists j \geq 0 : A_j \models \mathit{moneyRequested}) \Rightarrow (\exists k > j : A_k \models \mathit{start})\} \\
P_3 &\coloneqq \{A_0A_1A_2... \in (2^{AP})^\omega \mid \exists j \leq 10 : A_j \models \mathit{pinCorrect}\}
\end{aligned}
$$

Here, *start* symbolises that the machine is in the start state, *cardIn* a card in the machine, *pinEntered* a PIN entry, *pinCorrect* a user 'logged in' by entering the correct PIN, *pinNotCorrect* an incorrect PIN entry, *moneyRequested* the entry of a desired payout amount and *amountCovered* that the desired amount is available.

a) Formulate the meaning of the property in your own words. What types of property are involved in each case? [3 point]

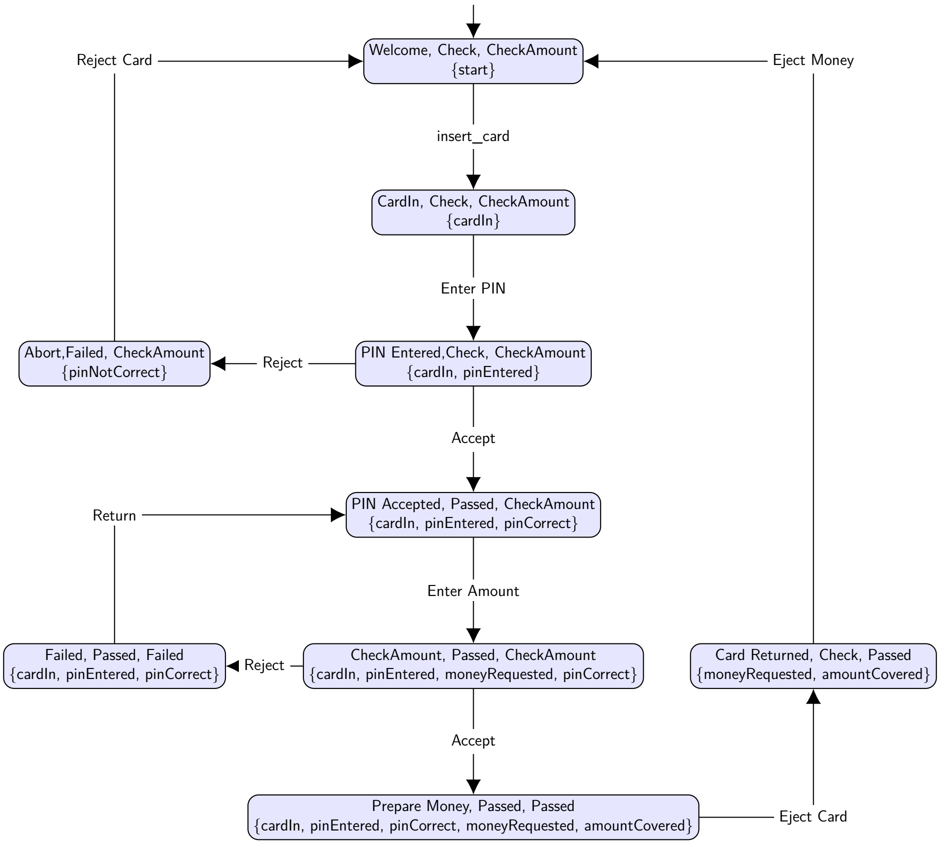

Figure 1: Transition system of the ATM from the first exercise sheet

b) Check the validity of the invariant using the algorithm presented in the lecture. To do this, work through the algorithm step by step and note the current values of the variables R, U, s' and s'' in each step. To increase clarity, mark the start of each new loop iteration. [3 points]

c) Justify the validity or invalidity of the other properties. [2 points]

3 Decomposition of LT properties (*)

Let $AP = \{a, b, c\}$ and the LT property P be given as: There exists an $n \geq 0$ such that for all $0 \leq i < n : A_i \models (a \wedge c)$ and $A_n \models (b \wedge c)$ and there are infinitely many $k > n$ such that $A_k \models (b \vee c)$. Find a safety property P_{safe} and a liveliness property P_{live} such that $P = P_{safe} \cap P_{live}$.