Model Checking
SoSe 2022
20. April 2022

Peter Reithofer, 394407
László Dirks, 398777
Khulan Bayarkhuu, 394604

Exercise Sheet 1

62,5/100

Exercise 1 (Open a Bank Account) 10/10

Our friend performs tests for a few initial inputs. The input values seem to be chosen to cover edge cases regarding the amount of the initial deposit. However this does not deal with what happens with the deposit once it has been accepted to have a valid initial amount.

In Line 2 of Algorithm 1 the user is free to "do something" with the deposit. This could mean that the user withdraws more than they deposited, leading to a negative balance. This case would not necessarily be detected by simply testing various initial inputs as it further depends on the possible actions of the user.

Model checking might allow us to detect such a flaw by reasoning about the entire possible state space and not only a few selected scenarios.

Exercise 2 (Transition Systems) 28/30

5/6

a) $TS_1 = (\{s_0, s_1, s_2, s_3, s_4\}, \{\alpha, \beta, \gamma\},$
$\{(s_0, \alpha, s_2), (s_0, \gamma, s_1), (s_1, \gamma, s_1), (s_1, \alpha, s_3), (s_1, \beta, s_4), (s_2, \alpha, s_0), (s_2, \beta, s_4), (s_4, \alpha, s_2), (s_4, \gamma, s_3)\},$
$\{s_0\}, \{\{a\}, \{b\}, \{a, b\}\}, L_1)$ -1
with $L_1 : \{\{s_0 \mapsto \{a\}, s_1 \mapsto \{a\}, s_2 \mapsto \{a, b\}, s_3 \mapsto \{b\}, s_4 \mapsto \{a, b\}\}$.

AP={a,b}
$2^{AP} = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$

b) Here is an example for a finite execution: $\rho_{finite} = s_0\gamma s_1\alpha s_3$ and an example for an infinite execution: $\rho_{infinite} = s_0\gamma s_1\gamma s_1\gamma s_1 \ldots$

3/3

c) (i) TS_1 is AP-deterministic, because $| I |=| \{s_0\} |= 1 \leq 1$ and there are only at most 2 states s and s' for which $L(s) = L(s')$ holds: For these pairs (s_0, s_1) with $L(s_0) = L(s_1) = \{a\}$ and (s_2, s_4) which $L(s_2) = L(s_4) = \{a, b\}$ are never both in $Post(s'')$ for all $s'' \in S$.

6/6

(ii) TS_1 is also $action - deterministic$, because both conditions hold:

* $| I |=| \{s_0\} \leq 1$
* $|Post(s_0, \alpha)| = |Post(s_0, \gamma)| = |Post(s_1, \alpha)| = |Post(s_1, \beta)| = |Post(s_1, \gamma)| = |Post(s_2, \alpha)| = |Post(s_2, \beta)| = |Post(s_4, \alpha)| = |Post(s_4, \gamma)| = 1$ and for every other pair (s_i, σ) with $s_i \in \{s_0, s_1, s_2, s_3, s_4\}$ and $\sigma \in \{\alpha, \beta, \gamma\}$ holds $|Post(s_i, \sigma)| = 0$.

d) $TS_2 = (\{s_0, s_1, s_2, s_3\}, \{\alpha, \beta, \gamma\},$
$\{(s_0, \alpha, s_2), (s_0, \gamma, s_1), (s_1, \gamma, s_1), (s_1, \alpha, s_3), (s_1, \beta, s_2), (s_2, \alpha, s_0), (s_2, \beta, s_1), (s_3, \beta, s_2), (s_3, \beta, s_3)\},$
$\{s_0\}, \{\{a\}, \{b\}, \{a, b\}\}, L_2)$ -1
with $L_2 : \{\{s_0 \mapsto \{a\}, s_1 \mapsto \{a\}, s_2 \mapsto \{a, b\}, s_3 \mapsto \{b\}\}$.

5/6

e) An example for a path in TS_2 is $\pi := (s_0, s_1, s_1, s_1, \ldots)$ and therefore $trace(\pi) = \{a\}\{a\}\{a\}\ldots$.

3/3

f) (i) TS_2 is not $AP-deterministic$, because the second condition does not hold: $|Post(s_2) \cap \{s' \in S \mid L(s') = A\}| = |\{s_0, s_1\} \cap \{s' \in S \mid L(s') = \alpha\}| = |\{s_0, s_1\}| = 2 \not\leq 1$.

6/6

(ii) TS_2 is not $action - deterministic$, because the second condition does not hold for state s_3 and action β: $|Post(s_3, \beta)| = |\{s_2, s_3\}| = 2 \not\leq 1$.

Aufgabe 3 (Program Graphs) 22/25

a)

b)

c)

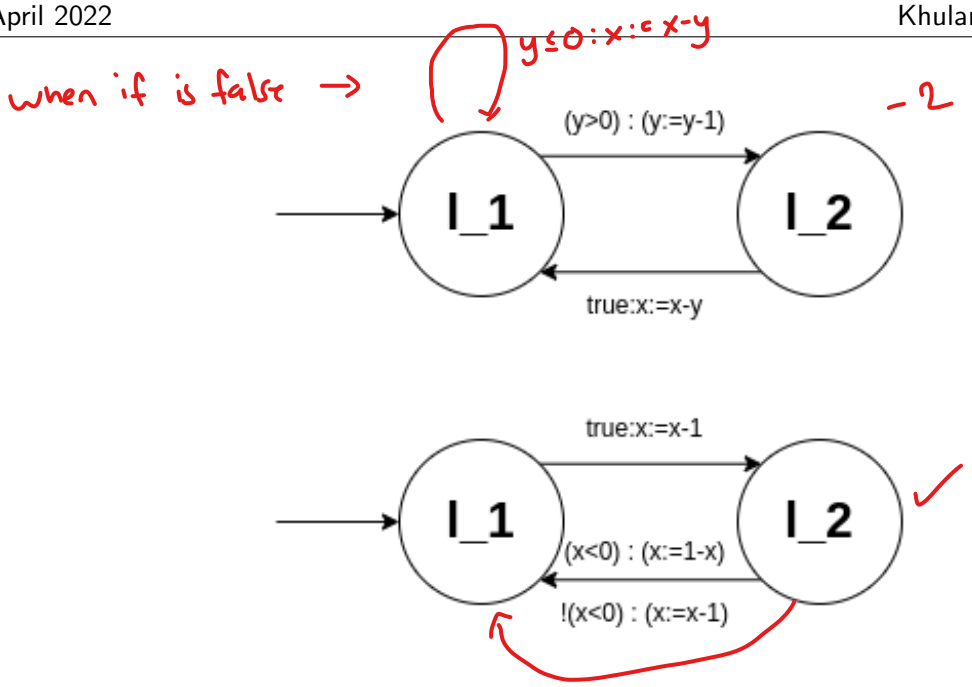


Abbildung 1:

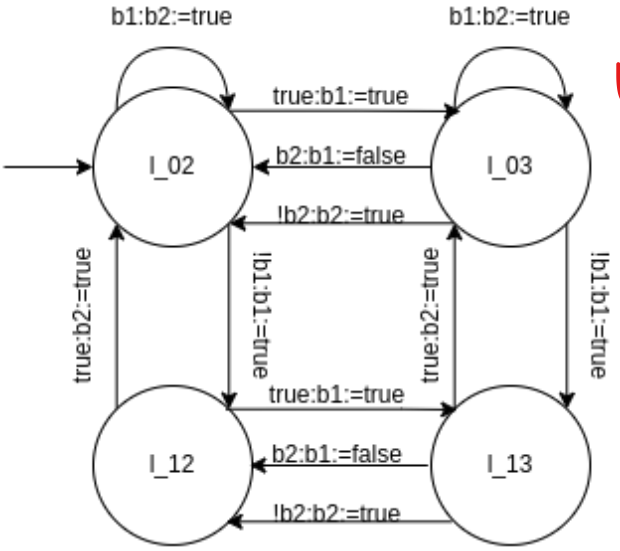


Abbildung 2:

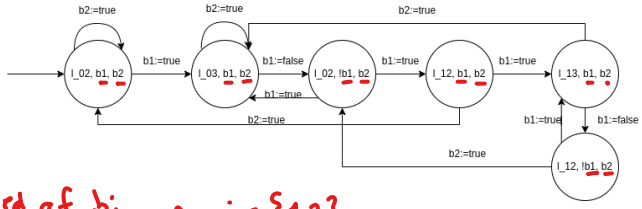
Aufgabe 4 (Handshaking)

a)

b)

c)

6/7



(true) t instead of bi for i ∈ {1,2}

(false) f instead of !bi

Abbildung 3:

− 1

Peter Reithofer, 394407
László Dirks, 398777
Khulan Bayarkhuu, 394604

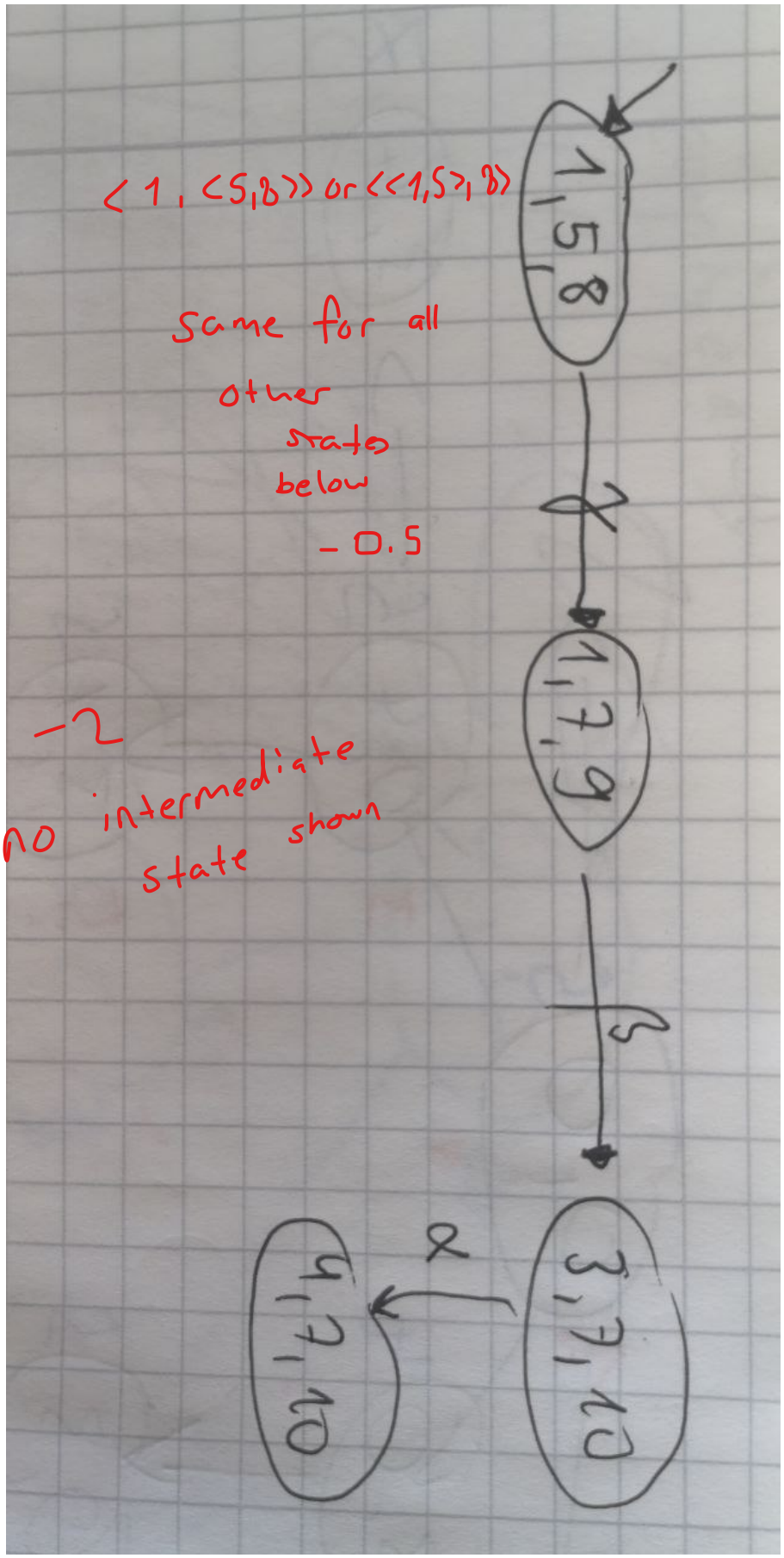


Abbildung 4: 4b) - $(TS_1||TS_2)||TS_3$