Cyber Physical Systems - Discrete Models
Exercise Sheet 11 Solution

Alper Ari
aa508@uni-freiburg.edu

Onur Sahin
os141@uni-freiburg.de

January 16, 2023

1	2	3	Σ
11.5/12	5/6	6/3+3	22.5

Exercise 1: Satisfaction under Fairness Assumptions

a) 8/8

1. Unconditional fairness for $A = \{\gamma\}$
   - Fair: $s_0 \xrightarrow{\alpha} s_4 \xrightarrow{\beta} \left(s_5 \xrightarrow{\gamma}\right)^\omega$
   - Unfair: $\left(s_0 \xrightarrow{\alpha} s_4 \xrightarrow{\delta}\right)^\omega$
2. Unconditional fairness for $A_1 = \{\alpha\}$ and $A_2 = \{\gamma\}$
   - Fair: No such execution exist.
   - Unfair: $\left(s_0 \xrightarrow{\alpha} s_4 \xrightarrow{\delta}\right)^\omega$
3. Unconditional fairness for $A = \{\alpha, \gamma\}$
   - Fair: $s_0 \xrightarrow{\alpha} s_4 \xrightarrow{\beta} \left(s_5 \xrightarrow{\gamma}\right)^\omega$
   - Unfair: $\left(s_0 \xrightarrow{\eta} s_1 \xrightarrow{\eta} s_3 \xrightarrow{\eta}\right)^\omega$
4. Strong fairness for $A = \{\beta\}$
   - Fair: $\left(s_0 \xrightarrow{\eta} s_1 \xrightarrow{\eta} s_3 \xrightarrow{\eta}\right)^\omega$
   - Unfair: $\left(s_0 \xrightarrow{\alpha} s_4 \xrightarrow{\delta}\right)^\omega$
5. Strong fairness for $A_1 = \{\alpha\}$ and for $A_2 = \{\beta\}$
   - Fair: $s_0 \xrightarrow{\eta} \left(s_1 \xrightarrow{\delta} s_2 \xrightarrow{\delta}\right)^\omega$
   - Unfair: $\left(s_0 \xrightarrow{\alpha} s_4 \xrightarrow{\delta}\right)^\omega$
6. Strong fairness for $A_1 = \{\alpha\}$ and for $A_2 = \{\beta\}$ and for $A_3 = \{\eta\}$
   - Fair: $s_0 \xrightarrow{\alpha} s_4 \xrightarrow{\beta} \left(s_5 \xrightarrow{\gamma}\right)^\omega$
   - Unfair: $\left(s_0 \xrightarrow{\alpha} s_4 \xrightarrow{\delta}\right)^\omega$
7. Weak fairness for $A = \{\eta\}$
   - Fair: $\left(s_0 \xrightarrow{\eta} s_1 \xrightarrow{\eta} s_3 \xrightarrow{\eta}\right)^\omega$
   - Unfair: $\left(s_0 \xrightarrow{\eta} s_1 \xrightarrow{\delta} s_2 \xrightarrow{\delta}\right)^\omega$ (✓)
8. Weak fairness for $A_1 = \{\eta\}$ and for $A_2 = \{\beta\}$ and for $A_3 = \{\eta\}$
   - Fair: $s_0 \xrightarrow{\alpha} s_4 \xrightarrow{\beta} \left(s_5 \xrightarrow{\gamma}\right)^\omega$

- Unfair: $s_0 \xrightarrow{\eta} \left(s_1 \xrightarrow{\delta} s_2 \xrightarrow{\delta}\right)^\omega$

b) 3.5/4

this is not a trace, but a path. (sequence of states) traces are sequences of sets of APs.

1. The only fair trace is $s_0 s_4 s_5^\omega$. Which executes the edge $s_0 \xrightarrow{\alpha} s_4$ therefore it satisfies the property P
2. There is no trace that is fair for this assumption. Since there are no traces, the system satisfies the property trivially. Because all traces satisfy the property P if there are no traces.
3. Similar to 1., only valid trace is $s_0 s_4 s_5^\omega$. Therefore similary it satisfies the property P. What about $(s_0 s_4)^\omega$ (fair path where {a} never holds)? −0.5
4. No, counterexample trace: $(s_0 s_1 s_3)^\omega$
5. No, counterexample trace: $s_0 (s_1 s_2)^\omega$
6. The only fair trace is $s_0 s_4 s_5^\omega$. Therefore, similar to 1. it satisfies the proprety P.
7. No, counterexample trace: $(s_0 s_1 s_3)^\omega$
8. No, because the same counterexample from 7. can be used.

Exercise 2: Fairness Assumptions 5/6

TODO: Starvation is "once a resource is requested, it should be eventually accessed"

Read carefully: In exercise two, you should give the weakest F.A. on action "enter".

a)

Weakly fair for $A = \{$~~request~~ enter$\}$. (✓)

sequence of sets of APs ≠ sequence of actions

It is sufficient because we aim to force the trace $(\text{nc } w\ c)^\omega$. Only two traces possible are: $(\text{nc } w\ c)^\omega$ and nc w^ω. But nc w^ω continuously enables enter because ot loop in state w which has an edge labeled with enter. Therefore it's an unfair trace. But $(\text{nc } w\ c)^\omega$ does not enable enter continuously so it's fair.

It is the weakest because weakly fair is the weakest condition and it only uses a single set so it can't get any weaker. (✓)

b)

Strongly fair for $A = \{\text{enter}\}$. ✓

It is sufficient because we have two possible traces: nc $(w_1 w_2)^\omega$ and $(\text{nc } w_1 w_2 c)^\omega$. Trace nc $(w_1 w_2)^\omega$ is not fair because w_2 makes enter infinitely available but never enters to the critical section. Therefore, only fair trace is $(\text{nc } w_1 w_2 c)^\omega$ which eventually enters to the critical section.

Represent behavior of TS with:
- executions $s_0 \xrightarrow{\alpha} s_1 \xrightarrow{\alpha} \dots$
- paths: $s_0 s_1 \dots$
- traces: $L(s_0) L(s_1) \dots = \{a\}\{b\}\dots$

remember to use one of these & correct terminology −1

It is the weakest, because for any weakly fair requirement, nc $(w_1 w_2)^\omega$ is fair since there is no label between w_1 and w_2. (✓)

c)

Unconditionally fair for $A = \{\text{enter}\}$. ✓

It is sufficient because we have three possible traces which only $(\text{nc } w_1 w_2 c)^\omega$ eventually enters to the critical section. The unconditional fairness only makes this trace fair. By definition of the unconditional fairness, only traces that visit enter are accepted.

It is the weakest, because without unconditional fairness the trace nc $(w_1)^\omega$ is also fair. Because nothing is available in state w_1, both strong and weak fairnes doesn't constraint it. (✓)

Exercise 3: Closure Properties of LT Properties

An LT property P is a Liveness property when $\text{pref}(P) = (2^{\text{AP}})^*$

1.5/ 1.5

a) P union P' is a liveness property

$$
\begin{aligned}
\text{pref}(P \cup P') &= \bigcup_{\sigma \in (P \cup P')} \text{pref}(\sigma) \\
&= \bigcup_{\sigma \in P} \text{pref}(\sigma) \cup \bigcup_{\sigma \in P'} \text{pref}(\sigma) \\
&= \text{pref}(P) \cup \text{pref}(P') \\
&= (2^{\text{AP}})^+ \cup (2^{\text{AP}})^+ \\
&= (2^{\text{AP}})^+
\end{aligned}
$$

✓

Since $\text{pref}(P \cup P') = (2^{\text{AP}})^+$, $P \cup P'$ is a liveness property ■.

1.5/ 1.5

b) P sect P' is a liveness property

No, one counter example: Let

$$
P = \left\{ A_0 A_1 \ldots \in (2^{\text{AP}})^\omega \mid \overset{\infty}{\forall} i \in \mathbb{N} \cdot \{a\} = A_i \right\}
$$

$$
P' = \left\{ A_0 A_1 \ldots \in (2^{\text{AP}})^\omega \mid \overset{\infty}{\forall} i \in \mathbb{N} \cdot \{b\} = A_i \right\}
$$

P and P' are liveness properties since both of them have prefix set $(2^{\text{AP}})^+$. Because any prefix can be extended by infinite $\{a\}$ or infinite $\{b\}$. But start with $P \cap P' = \{A_0A_1 \ldots \in (2^{AP})^\omega \mid \exists j \in \mathbb{N}. \forall i \in \mathbb{N}. i > j \to \{a\} = A_i \land \exists k \in \mathbb{N}. \forall l \in \mathbb{N}\ l > k \to \{b\} = A_l\}$,

then do a case distinction ① $j = k$ ② $j > k$ ③ $j < k$ and lead all to contradiction

$$P \cap P' \cancel{=} \left\{A_0A_1 \ldots \in \left(2^{\mathrm{AP}}\right)^\omega \mid \overset{\infty}{\forall} i \in \mathbb{N} \cdot \{a\} = A_i \land \{b\} = A_i\right\}\}$$

this chain of equations is not correct, since you need two different indices to represent $P \cap P'$!

No points deducted, since writing $P \cap P' = \emptyset$ would have been sufficient, given your counter examples.

$$\cancel{=} \left\{A_0A_1 \ldots \in \left(2^{\mathrm{AP}}\right)^\omega \mid \overset{\infty}{\forall} i \in \mathbb{N} \cdot \{a\} = \{b\} = A_i\right\}$$

$$\cancel{=} \left\{A_0A_1 \ldots \in \left(2^{\mathrm{AP}}\right)^\omega \mid \overset{\infty}{\forall} i \in \mathbb{N} \cdot \mathrm{false}\right\}$$

$$= \emptyset$$

Since $\{a\} \neq \{b\}$, $P \cap P' = \emptyset$. Therefore $\mathrm{pref}(P \cap P') = \mathrm{pref}(\emptyset) = \emptyset$ ■ (✓)

c) 3/3

1) P union P'

An LT property P is a safety property if $\mathrm{cl}(P) = P$

$$\mathrm{cl}(P \cup P') = \mathrm{cl}(P) \cup \mathrm{cl}(P')$$
$$= P \cup P'$$

Since $\mathrm{cl}(P \cup P') = \mathrm{cl}(P \cup P')$, $P \cup P'$ is a safety property. ✓

2) P sect P'

Using the other definition of safety properties, if $P \cap P'$ is a safety property, then for all $\sigma \in \left(2^{\mathrm{AP}}\right)^\omega \setminus P \cap P'$: there exists a finite prefix $\hat{\sigma}$ of σ s.th.

$$P \cap P' \cap \left\{\sigma' \in \left(2^{\mathrm{AP}}\right)^\omega \mid \underbrace{\exists \hat{\sigma} \in \left(2^{\mathrm{AP}}\right)^* \cdot \hat{\sigma} \in \mathrm{pref}(\sigma) \land \hat{\sigma} \in \mathrm{pref}(\sigma')}_{\hat{\sigma} \text{ is a finite prefix of } \sigma'}\right\} = \emptyset$$

must hold.

We define

$$S(\sigma) = P \cap P' \cap \left\{\sigma' \in \left(2^{\mathrm{AP}}\right)^\omega \mid \exists \hat{\sigma} \in \left(2^{\mathrm{AP}}\right)^* \cdot \hat{\sigma} \in \mathrm{pref}(\sigma) \land \hat{\sigma} \in \mathrm{pref}(\sigma')\right\}$$

$P \cap P'$ is a safety property if the following condition holds:
$\forall \sigma \in \left(2^{\mathrm{AP}}\right)^\omega \setminus (P \cap P') \cdot S(\sigma) = \emptyset$.

Assume any $\sigma \in \left(2^{\mathrm{AP}}\right)^\omega \setminus P \cap P'$. There are 3 cases:

1. $\sigma \in P \land \sigma \notin P'$: Then $\sigma \in \left(2^{\mathrm{AP}}\right)^\omega \setminus P'$. Therefore, by using that P' is a safety property, we can say:
   $P' \cap \left\{\sigma' \in \left(2^{\mathrm{AP}}\right)^\omega \mid \exists \hat{\sigma} \in \left(2^{\mathrm{AP}}\right)^* \cdot \hat{\sigma} \in \mathrm{pref}(\sigma) \land \hat{\sigma} \in \mathrm{pref}(\sigma')\right\} = \emptyset$. Then substituting it, $S(\sigma) = P \cap \emptyset = \emptyset$.
2. $\sigma \in P' \land \sigma \notin P$: Then $\sigma \in \left(2^{\mathrm{AP}}\right)^\omega \setminus P$. Therefore, by using that P is a safety property, we can say:

$P \cap \left\{\sigma' \in \left(2^{\text{AP}}\right)^{\omega} \mid \exists \hat{\sigma} \in \left(2^{\text{AP}}\right)^{*} \cdot \hat{\sigma} \in \text{pref}(\sigma) \wedge \hat{\sigma} \in \text{pref}(\sigma')\right\} = \emptyset$. Then, substituting it, $S(\sigma) = P' \cap \emptyset = \emptyset$.

3. $\sigma \notin P' \wedge \sigma \notin P$: Then $\sigma \in \left(2^{\text{AP}}\right)^{\omega} \setminus P'$ and $\sigma \in \left(2^{\text{AP}}\right)^{\omega} \setminus P$. So we can either use the result from 1. or 2. to show that $S(\sigma) = \emptyset$.

Since $\forall \sigma \in \left(2^{\text{AP}}\right)^{\omega} \setminus (P \cap P') \cdot S(\sigma) = \emptyset$, $P \cap P'$ is a safety property ■