Exercise 1

Assume an arbitrary CCS defining equation $K \overset{\text{def}}{=} P$ where K is a process constant and P is a CCS expression. Prove that $K \sim P$. (Hint: by using SOS rules for CCS, examine the possible transitions from K and P.)

Solution of Exercise 1

Let $K \overset{\text{def}}{=} P$. We define

$$R = \{(K, P)\} \cup \{(P', P') \mid P' \text{ is a CCS process}\}.$$

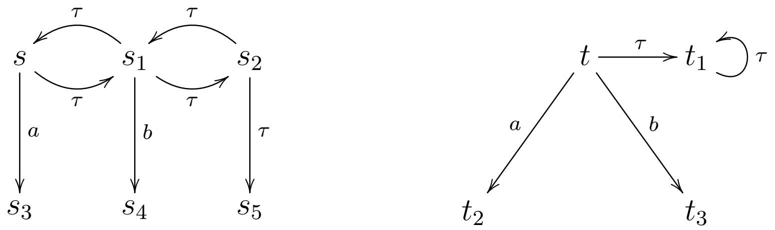
We will argue that R is a strong bisimulation. We analyze only the pair (K, P) from R as any pair of the form (P', P') can be safely added to R (why?).

Let $K \xrightarrow{a} P'$. We must find $\tilde{P}$ such that $P \xrightarrow{a} \tilde{P}$ and $(P', \tilde{P}) \in R$. The transition $K \xrightarrow{a} P'$ must have been derived using the CON-rule with the premise $P \xrightarrow{a} P'$. Then we can just let $\tilde{P} = P'$ as we know that $P \xrightarrow{a} P'$, and $(P', P') \in R$.

Let $P \xrightarrow{a} P'$. Then using the SOS rule CON we know that also $K \xrightarrow{a} P'$ and again $(P', P') \in R$.

Exercise 2*

Consider the following labelled transition system.



Show that $s \approx t$ by finding a weak bisimulation R containing the pair (s, t).

Solution of Exercise 2

Let $R = \{(s, t), (s_1, t), (s_2, t), (s_3, t_2), (s_4, t_3), (s_5, t_1)\}$. Now one can argue that R is a weak bisimulation as follows.

- Transitions from the pair (s, t): if $s \xrightarrow{a} s_3$ then $t \overset{a}{\Longrightarrow} t_2$ and $(s_3, t_2) \in R$. If $s \xrightarrow{\tau} s_1$ then $t \overset{\tau}{\Longrightarrow} t$ and $(s_1, t) \in R$. If $t \xrightarrow{a} t_2$ then $s \overset{a}{\Longrightarrow} s_3$ and $(s_3, t_2) \in R$. If $t \xrightarrow{b} t_3$ then $s \overset{b}{\Longrightarrow} s_4$ and $(s_4, t_3) \in R$. If $t \xrightarrow{\tau} t_1$ then $s \overset{\tau}{\Longrightarrow} s_5$ and $(s_5, t_1) \in R$.
- The transitions from the remaining pairs can be checked in a similar way.

Exercise 3*

Decide whether the following claims are true or false. Support your claims either by using bisimulation games or directly the definition of strong/weak bisimilarity.

- $a.\tau.\mathit{Nil} \overset{?}{\sim} \tau.a.\mathit{Nil}$
- $\tau.a.A + b.B \overset{?}{\sim} \tau.(a.A + b.B)$
- $\tau.\mathit{Nil} + (a.\mathit{Nil} \,|\, \overline{a}.\mathit{Nil}) \smallsetminus \{a, b\} \overset{?}{\sim} \tau.\mathit{Nil}$
- $a.(\tau.\mathit{Nil} + b.B) \overset{?}{\sim} a.\mathit{Nil} + a.b.B$

The same processes but weak bisimilarity instead of the strong one.

- $a.\tau.\mathit{Nil} \overset{?}{\approx} \tau.a.\mathit{Nil}$
- $\tau.a.A + b.B \overset{?}{\approx} \tau.(a.A + b.B)$
- $\tau.\mathit{Nil} + (a.\mathit{Nil} \,|\, \overline{a}.\mathit{Nil}) \smallsetminus \{a, b\} \overset{?}{\approx} \tau.\mathit{Nil}$
- $a.(\tau.\mathit{Nil} + b.B) \overset{?}{\approx} a.\mathit{Nil} + a.b.B$

Hint: draw first the LTS generated by the CCS processes.
Home exercise: try to verify your claims by using the tool CAAL.

Solution of Exercise 3

- $a.\tau.\mathit{Nil} \not\sim \tau.a.\mathit{Nil}$
  - The attacker plays the action a in the left process and the defender does not have any a-move available in the right process and looses.
- $\tau.a.A + b.B \not\sim \tau.(a.A + b.B)$
  - The attacker plays the action b from the left process, there is no action b available in the right process in the first round. The attacker clearly wins.
- $\tau.\mathit{Nil} + (a.\mathit{Nil} \,|\, \overline{a}.\mathit{Nil}) \smallsetminus \{a, b\} \sim \tau.\mathit{Nil}$
  - $R = \{(\tau.\mathit{Nil} + (a.\mathit{Nil} \,|\, \overline{a}.\mathit{Nil}) \smallsetminus \{a, b\}, \tau.\mathit{Nil}), (\mathit{Nil}, \mathit{Nil}), ((\mathit{Nil} \,|\, \mathit{Nil}) \smallsetminus \{a, b\}, \mathit{Nil})\}$ is a strong bisimulation.
- $a.(\tau.\mathit{Nil} + b.B) \not\sim a.\mathit{Nil} + a.b.B$
  - In the first round the attacker plays from the left the action a and in the second round he plays again from left the action τ. The defender looses as he can never play the same sequence of a followed by τ from the right process.

The same processes but weak bisimilarity instead of the strong one.

- $a.\tau.\mathit{Nil} \approx \tau.a.\mathit{Nil}$
  - $R = \{(a.\tau.\mathit{Nil}, \tau.a.\mathit{Nil}), (\tau.\mathit{Nil}, \mathit{Nil}), (\mathit{Nil}, \mathit{Nil}), (a.\tau.\mathit{Nil}, a.\mathit{Nil})\}$ is a weak bisimulation.
- $\tau.a.A + b.B \not\approx \tau.(a.A + b.B)$
  - The attacker plays the action τ from the left and reaches the process $a.A$. The defender can either answer by (i) doing nothing on the right and staying in the process $\tau.(a.A + b.B)$ or (ii) by playing the action τ and reaching $a.A + b.B$. In case (i) the attacker will play in second round on the right the action τ, the defender can only stay in $a.A$ and in the next round the attacker wins by making the b-move on the right. In case (ii) the attacker wins already in the second round by playing b from the right process.
- $\tau.\mathit{Nil} + (a.\mathit{Nil} \,|\, \overline{a}.\mathit{Nil}) \smallsetminus \{a, b\} \approx \tau.\mathit{Nil}$
  - These two processes are even strongly bisimilar so they must be also weakly bisimilar.
- $a.(\tau.\mathit{Nil} + b.B) \not\approx a.\mathit{Nil} + a.b.B$
  - The attacker plays $a.\mathit{Nil}+a.b.B \xrightarrow{a} b.B$ on the right, the defender can answer either by $a.(\tau.\mathit{Nil} + b.B) \overset{a}{\Longrightarrow} \tau.\mathit{Nil} + b.B$ or by $a.(\tau.\mathit{Nil} + b.B) \overset{a}{\Longrightarrow} \mathit{Nil}$. In the first case the attacker plays $\tau.\mathit{Nil}+b.B \xrightarrow{\tau} \mathit{Nil}$ and the defender can only do nothing and will loose in the next round. In the second case, the attacker plays the action b from the left and the defender looses.

Exercise 4

Prove that for any CCS process P the following law (called idempotency) holds.

- $P + P \sim P$

By using the fact that $\sim \subseteq \approx$ conclude that also $P + P \approx P$.

Solution of Exercise 4

We now argue that $P + P \sim P$ using the game characterization. We start from the configuration $(P + P, P)$. Suppose the attacker chooses $P + P \xrightarrow{a} P'$. Then we know (from the SOS transition rules) that this transition can only have been derived if $P \xrightarrow{a} P'$. So, of course, the defender replies by doing $P \xrightarrow{a} P'$. The current configuration becomes (P', P') from which the defender always has a winning strategy by simply doing exactly the same as the attacker. Conversely, if the attacker from $(P + P, P)$ chooses $P \xrightarrow{a} P'$ then the defender responds by playing $P + P \xrightarrow{a} P'$ and the current configuration becomes again (P', P').

Exercise 5

In the weak bisimulation game the attacker is allowed to use $\xrightarrow{a}$ moves for the attacks and the defender can use $\overset{a}{\Longrightarrow}$ in response. Argue that if we modify the game rules so that the attacker can also use the long moves $\overset{a}{\Longrightarrow}$ then this does not provide any additional power for the attacker. Conclude that both versions of the game provide the same answer about bisimilarity/nonbisimilarity of two processes.

Solution of Exercise 5

Observe that each long attack can be simulated (in more rounds) by doing in series all single steps that are contained in the long move, so the defender in fact has an answer even to the long move by combining the answers to the series of single steps.

Exercise 6 (optional)

Define two CCS process constants A and B such that

- A has infinitely many reachable states,
- B has only finitely many reachable states, and
- $A \sim B$.

Challenging continuation of the exercise:
Can you think of a CCS process C with infinitely many reachable states such that there is no CCS process with only finitely many reachable states strongly bisimilar to it? How would you support your claim?

Exercise 7 (optional)

Consider the simple communication protocol from Lecture 4.

- Draw the labelled transition system generated by the processes Spec and Impl.
- Devise a strategy for the defender showing $\mathit{Spec} \approx \mathit{Impl}$. (Hint: CAAL is your friend).