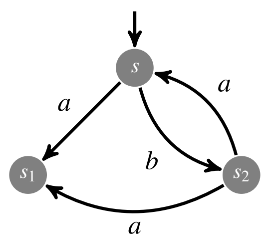
Software Specification
Supplementary Exercise HML with Recursion

Note that its is assumed that the operators $[\_]\_$ and $\langle\_\rangle\_$ bind stronger than the logical connectives $\wedge$ and $\vee$.

Exercise 1 (based on Exercise 6.4 of Aceto) Consider the following labeled transition system.



Compute $O_{[b]false \wedge [a]X}(S)$ for each $S \subseteq \{s, s_1, s_2\}$.

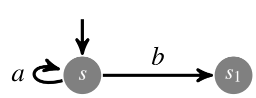
Exercise 2 If possible, give a labeled transition system for which the formula X with X defined by $X \overset{\text{max}}{=} \langle a\rangle X$ is valid but for which X defined by $X \overset{\text{min}}{=} \langle a\rangle X$ is not valid.

If possible, give a labeled transition system for which the formula X with X defined by $X \overset{\text{min}}{=} \langle a\rangle X$ is valid but for which X defined by $X \overset{\text{max}}{=} \langle a\rangle X$ is not valid.

If possible, give a labeled transition system for which the formula X with X defined by $X \overset{\text{max}}{=} [a]X$ is valid but for which X defined by $X \overset{\text{min}}{=} [a]X$ is not valid.

If possible, give a labeled transition system for which the formula X with X defined by $X \overset{\text{min}}{=} [a]X$ is valid but for which X defined by $X \overset{\text{max}}{=} [a]X$ is not valid.

Exercise 3 Consider the following labeled transition system.



Compute $[\![X]\!]$ for the following recursive equations defining X:

1. $X \overset{\text{min}}{=} [Act \setminus \{a\}]X$
2. $X \overset{\text{max}}{=} [Act \setminus \{a\}]X$

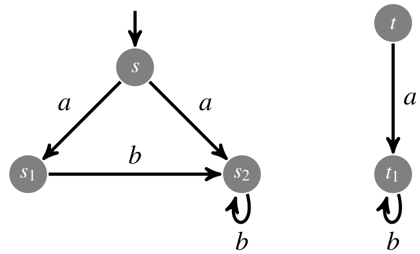
3. $X \overset{\text{min}}{=} \langle a\rangle true \vee [Act \setminus \{a\}]X$

4. $X \overset{\text{max}}{=} \langle a\rangle true \vee [Act \setminus \{a\}]X$

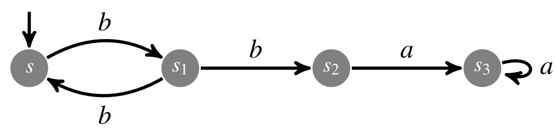
Exercise 4 (Exercise 6.6 from Aceto) Compute the set of states that satisfy the formula X where

$$X \overset{\text{min}}{=} \langle b\rangle true \vee \langle \{a,b\}\rangle X$$

for the following labeled transition system



Exercise 5 Consider the following labeled transition system.



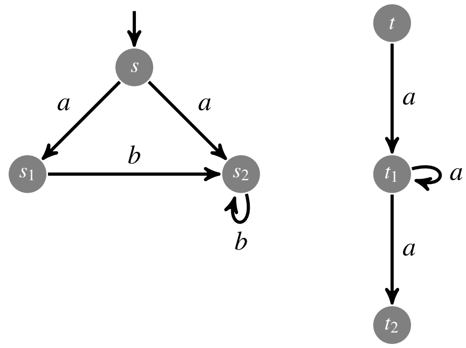
Determine for each of the following formulas for which states it holds.

1. X with $X \overset{\text{min}}{=} \langle a\rangle true \vee \langle b\rangle X$
2. X with $X \overset{\text{max}}{=} \langle b\rangle true \wedge [b]X$
3. X with $X \overset{\text{max}}{=} \langle a\rangle true \wedge [a]X$
4. X with $X \overset{\text{min}}{=} \langle a\rangle true \vee ([b]X \wedge \langle b\rangle true)$

Also explain what these properties mean informally.

Exercise 6 Give a labeled transition system for which the formula X where X is defined by $X \overset{\text{min}}{=} [Act \setminus \{a\}]X$ is not valid, but the formula X where X is defined by $X \overset{\text{min}}{=} \langle a\rangle true \vee [Act \setminus \{a\}]X$ is valid. Explain the difference between the two formulae in words.

Exercise 7 (based on Exercise 6.7 from Aceto) Consider the following labeled transition system.



1. Determine $[\![X]\!]$ with $X \overset{\mathsf{max}}{=} \langle b \rangle true \wedge [b]X$.

2. Determine $[\![X]\!]$ with $X \overset{\mathsf{min}}{=} \langle b \rangle true \wedge \langle \{a, b\} \rangle X$.

Exercise 8 Give a formula that expresses the following property: "It is not possible to do action *b* without having done *a* first".

Exercise 9 Give formulas in the modal μ-calculus that capture the following properties:

1. Along every *a*-path it is possible to perform *b*
2. On every *a*-path *c* can be executed while *b* fails
3. On all infinite length *a*-paths, eventually *b* followed by *c* are possible
4. there is an *a*-path such that *c* can be executed and until then *b* cannot be executed

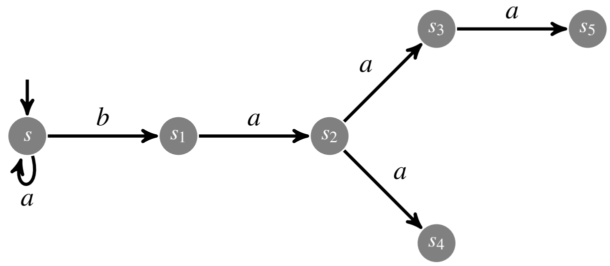
For each of these properties give a labeled transition system for which it is valid. Can you also give a single labeled transition system in which all of these properties are valid?

Exercise 10 Finish the proof of monotonicity of O_F, i.e., provide proofs for the cases $F \vee G$ and $[a]F$.

Exercise 11 Consider the formula X where X is defined by the recursive equation

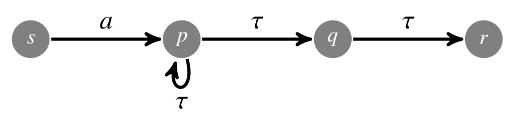
$$X \overset{\mathsf{min}}{=} [a]false \vee \langle a \rangle \langle a \rangle X$$

Establish for which states this formula holds in the following labeled transition system

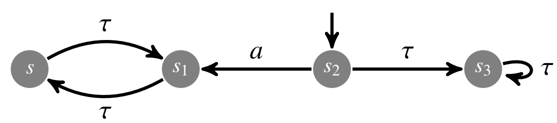


State the requirement that is expressed by this formula in words.

Exercise 12 (Based on Exercise 6.16 and Exercise 6.17 from Aceto) Consider the following labeled transition system



Compute the states for which the formula X with X defined by $X \stackrel{\max}{=} \langle\tau\rangle X$ is satisfied. Repeat the same question for the following labeled transition system



Exercise 13 Prove that *Inv*(F) and $F \ \mathcal{U}^w$ *false* are logically equivalent. Prove that *Even*(F) and *true* $\mathcal{U}^s \ F$ are logically equivalent.

Exercise 14 Give F and G such that $F \ \mathcal{U}^w \ G$ and $F \ \mathcal{U}^s \ G$ are not logically equivalent. Motivate your answer by giving a labeled transition system for which one of the formulas is valid and the other one is not.

Exercise 15 Express the property that as long as no *error* happens, a deadlock will not occur.

Exercise 16 Express the property that after a *send* action a *receive* action is possible as long as it has not happened yet.

Exercise 17 Express the property that whenever an a happens, a b can happen, except if it is canceled by a c.

Exercise 18 Consider the following simplified railroad system. For the system the following events are modeled:

- *enter*: a train enters the crossing
- *leave*: a train leaves the crossing
- *down*: the gate is closed
- *up*: the gate is opened

Express the following properties by means of temporal logic formulas:

1. When the gate is up it can be closed. When the gate is down it can be opened.
2. The gate must remain closed until the train has left the crossing.
3. The closing and opening of the gate only occur alternatingly.
4. After entering the crossing, the train will eventually leave the crossing.
5. It must never be the case that the train is in the crossing when the gate is opened.