Systems Verification Lab
Exercises on Linear Time Properties with (Some) Solutions

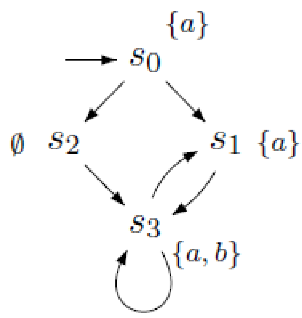
Teacher: Luca Tesei

Master of Science in Computer Science - University of Camerino

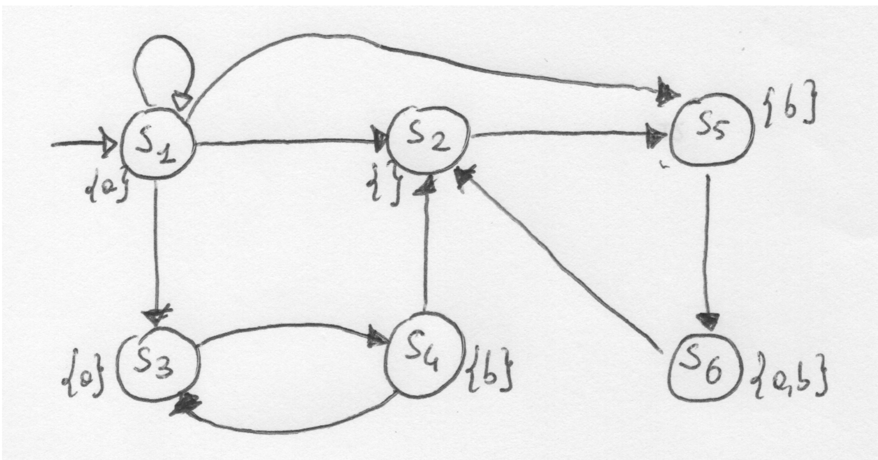
Contents

1 Linear Time Properties

Exercise 1.1. *Give the traces on the set of AP=a,b of the following transition system:*



Exercise 1.2. *Consider the following transition system:*



1. *Define formally the traces on the alphabet* 2^{AP}, *where* $\mathrm{AP} = \{a, b\}$

Exercise 1.3. *Consider the set AP of atomic propositions defined by* $AP = \{x = 0, x > 1\}$ *and consider a non -terminating sequential computer program P that manipulates the variable* x*. Formulate the following informally stated properties as LT properties:*

a) *false.*
b) *initially* x *is equal to zero.*
c) *initially* x *differs from zero .*
d) *initially* x *is equal to zero, but at some point* x *exceeds one.*
e) x *exceeds one only finitely many times.*
f) x *exceeds one infinitely often.*
g) *the value of* x *alternates between zero and two.*
h) *true*

Exercise 1.4. *Consider the set of atomic propositions* AP $= \{a, b, c\}$. *Consider the following linear time properties informally stated:*

1. *initially a holds and b does not hold*
2. *c holds only finitely many times*
3. *from some point on the truth value of a alternates between true and false*
4. *whenever c holds, then a holds afterwards*
5. *b holds infinitely many times and whenever b holds then c holds afterwards*
6. *whenever c holds then a or b holds*
7. *a holds only finitely many times and c holds infinitely many times*
8. *whenever a holds then b and c holds after one step*
9. *never a and b hold at the same time and eventually c holds*
10. *at any point the number of times a held in the past is always greater than or equal to the number of times b held in the past.*

For each property above, (a) formally write it as a set of infinite traces on 2^{AP} and (b) determine whether it is a safety, liveness or mixed (safety and liveness) linear time property. Justify your answers!
Hint: you may use the special quantifiers $\overset{\infty}{\forall}$ i ("for nearly all i") and $\overset{\infty}{\exists}$ i ("there exists infinitely many is") as they are defined in the book.

Exercise 1.5. *Give an algorithm (in pseudo–code) for invariant checking such that in case the invariant is refuted, a minimal counterexample, i.e. a counterexample of minimal length, is provided as error indication.*

Exercise 1.6. *Let P denote the set of traces of the form $A_0A_1A_2... \in (2^{AP})^\omega$ such that:*

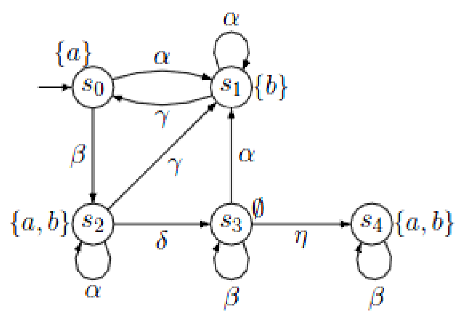
$$\overset{\infty}{\exists} k.\ A_k = \{a, b\} \quad \wedge \quad \exists n \geq 0.\ \forall k > n.\ \big(a \in A_k \Rightarrow b \in A_{k+1}\big).$$

Consider the following fairness assumptions with respect to the transition system TS outlined on the right:

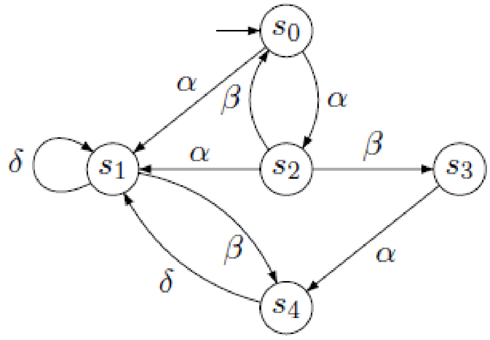
a) $\mathcal{F}_1 = (\{\{\alpha\}\}, \{\{\beta\}, \{\delta, \gamma\}, \{\eta\}\}, \emptyset)$.
Decide whether $TS \models_{\mathcal{F}_1} P$.

b) $\mathcal{F}_2 = \big(\{\{\alpha\}\}, \{\{\beta\}, \{\gamma\}\}, \{\{\eta\}\}\big)$.
Decide whether $TS \models_{\mathcal{F}_2} P$.

Justify your answers!

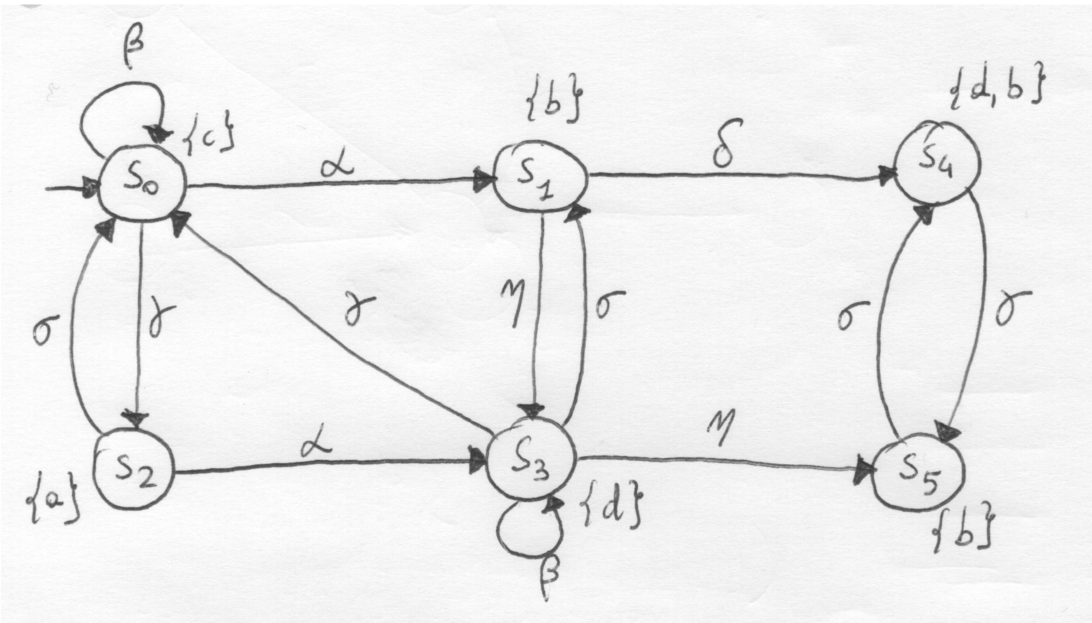


Exercise 1.7. *Consider the transition system TS on the right (where atomic propositions are omitted). Decide which of the following fairness assumption $\mathcal{F}_i$ are realizable for TS.*
justify your answers!



a) $\mathcal{F}_1 = (\{\{\alpha\}\}, \{\{\delta\}\}, \{\{\alpha, \beta\}\})$
b) $\mathcal{F}_2 = (\{\{\delta, \alpha\}\}, \{\{\alpha, \beta\}\}, \{\{\gamma\}\})$
c) $\mathcal{F}_3 = (\{\{\alpha, \delta\}, \{\beta, \}\}, \{\{\alpha, \beta\}\}\{\{\gamma\}\})$

Exercise 1.8. *Consider the following transition system* TS*:*



Consider the following linear time properties, where $\mathrm{AP} = \{a, b, c, d\}$*:*

$$E_1 = \{A_0A_1A_2 \dots \in (2^{\mathrm{AP}})^\omega \mid \overset{\infty}{\exists}\, i\colon b \in A_i\}$$

$$E_2 = \{A_0A_1A_2 \dots \in (2^{\mathrm{AP}})^\omega \mid \overset{\infty}{\exists}\, i\colon d \in A_i\}$$

Finally, consider the following fairness assumptions:

$$\begin{aligned} \mathcal{F}_1 &= (\{\{\beta\}\}, \{\{\gamma\}, \{\delta\}\}, \{\{\alpha\}\}) \\ \mathcal{F}_2 &= (\{\{\beta\}\}, \{\{\gamma\}\}, \{\{\alpha\}\}) \\ \mathcal{F}_3 &= (\{\{\beta\}\}, \{\{\gamma\}\}, \{\}) \end{aligned}$$

Decide whether the following model checking statements hold or not:

1. TS $\models_{\mathcal{F}_1} E_1$
2. TS $\models_{\mathcal{F}_1} E_2$
3. TS $\models_{\mathcal{F}_2} E_1$
4. TS $\models_{\mathcal{F}_2} E_2$
5. TS $\models_{\mathcal{F}_3} E_1$
6. TS $\models_{\mathcal{F}_3} E_2$

Justify your answers!

Exercise 1.9. *Let $n \geq 1$. Consider the language $L_n \subseteq \sum^*$ over the alphabet $\sum = \{A, B\}$ that consists of all finite words where the symbol B is on position n from the right, i.e., L_n contains exactly the words $A_1A_2...A_k \in \{A, B\}^*$ where $k \geq n$ and $A_{k-n+1} = B$. For instance, the word $ABBAABAB$ is in L_3.*
a) Construct an NFA An with at most $n+1$ states such that $L(A_n) = Ln$.
b) Determinize this NFA An using the powerset construction algorithm.

Exercise 1.10. *Let $AP = \{A, B, C, D\}$ be a set of atomic propositions. Consider the following informally stated linear time properties:*

(a) *Whenever A holds then, at the same time, B holds and C does not hold*

(b) *A and D hold together at least once*

(c) *A and D hold together at least twice*

(d) *A and D hold together infinitely many times*

(e) *Whenever B holds then C holds after some steps*

(f) *Always B or C hold*

(g) *Eventually C holds*

(h) *If A and C hold together once then eventually B holds continuously for infinitely many times*

(i) *C holds at least once and only finitely many times*

(j) *If A holds infinitely many times then C must hold only finitely many times*

(k) *Whenever B holds then after two steps C holds*

(l) *Whenever C holds then it continues to hold until D holds*

For each property above:

1. *formalise it as a set of infinite traces on the alphabet 2^{AP} (use set expressions and first order logic)*
2. *determine whether it is a safety, liveness or mixed (safety and liveness) linear time property. Justify your answers!*

Exercise 1.11. *Consider the alphabet $AP = \{A, B, C, D\}$ and the following linear time properties:*

(a) *Whenever A holds then B does not hold for two steps*

(b) *B and C hold together only finitely many times*

(c) *If C holds infinitely many times then D holds only finitely many times*

(d) *C holds at least once and whenever D holds also A must hold*

For each property:

1. *formalise it using set expressions and first order logic;*
2. *formalise it in LTL (you can use the operators next, until, box and diamond, together with all boolean connectives);*
3. *tell if it is a safety, liveness or mixed property; in case it is a safety property provide an NFA for the language of the* ***minimal*** *bad prefixes.*

Exercise 1.12. *Consider the alphabet $AP = \{A, B, C\}$ and the following linear time properties:*

(a) *Whenever A holds then B holds immediately and in the next step*

(b) *B holds infinitely many times and C holds only finitely many times*

(c) *A holds at least twice and whenever B holds also C must hold*

For each property:

1. *formalise it using set expressions and first order logic;*
2. *formalise it in LTL (you can use the operators next, until, box and diamond, together with all boolean connectives);*
3. *tell if it is a safety, liveness or mixed property. In case it is a pure safety property provide an NFA for the language of the* ***minimal bad prefixes****. In case it is a pure liveness property provide an NBA for the language of* ***bad behaviours****.*

Solutions

Solution of Exercise 1.1

$$Traces(TS) = (\{a\}\{a\} + \{a\}\emptyset)(\{a,b\} + \{a,b\}\{a\})^{\omega}$$

How many traces? 2, both infinite.

Solution of Exercise 1.2

All possible paths are of five kinds:

1. s_1^{ω}
2. $s_1^{+}(s_5 s_6 s_2)^{\omega}$
3. $s_1^{+}(s_3 s_4)^{+} s_2 (s_5 s_6 s_2)^{\omega}$
4. $s_1^{+}(s_3 s_4)^{\omega}$
5. $s_1^{+}(s_2 s_5 s_6)^{\omega}$

The corresponding traces are:

$\{\{a\}^{\omega}\} \cup \{\{a\}^{+}(\{b\}\{a,b\}\{\})^{\omega}\} \cup \{\{a\}^{+}(\{a\}\{b\})^{+}(\{\}\{b\}\{a,b\})^{\omega}\} \cup$

$\{\{a\}^{+}(\{a\}\{b\})^{\omega}\} \cup \{\{a\}^{+}(\{\}\{b\}\{a,b\})^{\omega}\}$

Solution of Exercise 1.3

$(a)\ P = \varnothing$
$(b)\ P = \{A_0, A_1, A_2 ... \in (2^{AP})^{\omega} | x_0 \in A_0\}$
$(c)\ P = \{A_0, A_1, A_2 ... \in (2^{AP})^{\omega} | x_0 \notin A_0\}$
$(d)\ P = \{A_0, A_1, A_2 ... \in (2^{AP})^{\omega} | x_0 \in A_0 \wedge \exists i : (x > i) \in A_i \wedge i > 0\}$
$(e)\ P = \{A_0, A_1, A_2 ... \in (2^{AP})^{\omega} | \exists i \geq 0 : \forall j \geq i,\ (x > i) \notin A_j\}$
$(f)\ P = \{A_0, A_1, A_2 ... \in (2^{AP})^{\omega} | \forall i \geq 0 : \exists j \geq i,\ (x > i) \in A_j\}$
$(g)\ P = \{A_0, A_1, A_2 ... \in (2^{AP})^{\omega} | (\forall\ (x = 0) \in A_i\ \wedge\ (x > 1) \in A_{i+1}\ \wedge\ i\ mod_2 = 0)\ \vee$
$(\forall\ (x = 0) \in A_i\ \wedge\ (x > 1) \in A_{i+1}\ \wedge\ i\ mod_2 = 1)\}$
$(h)\ P = (2^{AP})^{\omega}$

Solution of Exercise 1.4

1. The property can be formally stated as
   $P = \{A_0, A_1, ... \in (2^{AP})^{\omega}\ |\ a \in A_0 \wedge b \notin A_0\}$
   This property is a SAFETY PROPERTY as a bad prefix can be any prefix of a word in $(2^{AP})^{\omega}$ starting with { } or $\{b\}$ or $\{c\}$ or $\{a,b\}$or $\{b,c\}$or $\{a,b,c\}$.

2. $P = \{A_0, A_1, ... \in (2^{AP})^{\omega}\ |\overset{\infty}{\forall}\ i \in N,\ c \notin A_i\}$
   This is a LIVENESS PROPERTY because no prefix can be classified as bad because the information on the occurrences of "c" in the tail of the word is missing.

3. $P = \{A_0, A_1, ... \in (2^{AP})^\omega \mid \exists i \in N : \forall j \geq i \; a \in A_j \Leftrightarrow a \notin A_j + i\}$
LIVENESS: no prefix can be classified as bad without the information on the tail of the word.

4. $P = \{A_0, A_1, ... \in (2^{AP})^\omega \mid \forall i \in N : (c \in A_i \implies \exists j \geq i \; : \; a \in A_j)\}$
LIVENESS: as above.

5. $P = \{A_0, A_1, ... \in (2^{AP})^\omega \mid (\overset{\infty}{\exists} \; i \in N : b \in A_i) \wedge (\forall i \in N : (b \in A_i \implies \exists j \geq i : c \in Aj))\}$
LIVENESS.

6. $P = \{A_0, A_1, ... \in (2^{AP})^\omega \mid \forall i \in N(c \in A_i \implies (a \in A_i \vee b \in A_i))\}$
SAFETY: a bad prefix is, for instance, $\{c\}\{\}\{\}\{\}...$

7. $P = \{A_0, A_1, ... \in (2^{AP})^\omega \mid (\overset{\infty}{\forall} \; i \in N : a \notin A_i) \wedge (\overset{\infty}{\exists} \; i \in N : c \in A_i)\}$
LIVENESS

8. $P = \{A_0, A_1, ... \in (2^{AP})^\omega \mid \forall i \in N : a \in A_i \implies (b \in A_{i+1} \wedge c \in A_{i+1})\}$
SAFETY: a bad prefix is for instance $\{a\}\{a\}\{a\}...$

9. $P = \{A_0, A_1, ... \in (2^{AP})^\omega \mid (\forall i \in N : a \in A_i \Leftrightarrow b \notin A_i) \wedge \exists i \in N : c \in A_i\}$ MIXED: a bad prefix for the first part is $\{a, b\}\{\}\{\}...$
The part on " eventually " c cannot have a bad prefix, so it is liveness property.

10. $P = \{A_0, A_1, ... \in (2^{AP})^\omega \mid \forall i \in N : \mid \{0 \leq j \leq i : a \in A_j\} \mid \geq \mid \{0 \leq j \leq i : b \in A_j\} \mid\}$
Where $\mid \{...\} \mid$ is set cardinality.
SAFETY: a bad prefix for example $\{b\}\{\}\{\}...$

Solution of Exercise 1.5

The algorithm works as follows:

Algorithm 1 Invariant Checking using Breadth–First Search

Require: finite transition system TS and propositional formula Φ
Ensure: **true** or the shortest counterexample

---

queue of states $Q = \varepsilon$;
finite trace $\hat{\sigma} = \varepsilon$;
set of states R;
set of tuples $P \subseteq S \times S$;

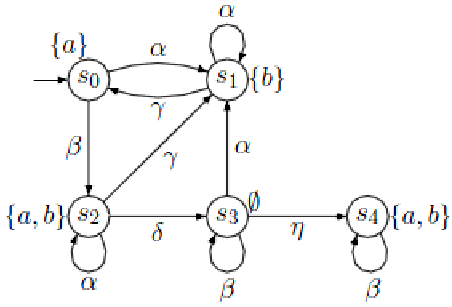
---

procedure bfs(state s)
enqueue(Q, s);
$P := \{(s, \perp)\}$;
$R := \{s\}$;
while $(Q \neq \varepsilon) \wedge (\text{first}(Q) \models \Phi)$ **do**
  let $p :=$ dequeue(Q);
  for all $p' \in \text{Post}(p) \setminus R$ **do**
    enqueue(Q, p');
    $R := R \cup \{p'\}$;
    $P := P \cup \{(p', p)\}$;
  end for
end while
if $Q \neq \varepsilon$ **then**
  let $p := \text{first}(Q)$;
  while $p \neq \perp$ **do**
    $\hat{\sigma} := p.\hat{\sigma}$;
    let $(p, p') \in P$;
    $p := p'$;
  end while
  return false; shortest counterexample $\hat{\sigma}$;
else
  return true;
end if

Solution of Exercise 1.6

We consider each of the fairness assumptions $\mathcal{F}_i$ for $i \in \{1, 2\}$:

We have $TS \models_{\mathcal{F}_i} P$ iff $FairTraces_{\mathcal{F}_i}(TS) \subseteq P$. Because of $\overset{\infty}{\exists}\, k.\ A_k = \{a, b\}$, each trace has to visit at least one of s_2 or s_4 infinitely many times. Additionally, from some point onwards, each a-state must be followed by a state that is annotated with (at least) b.



a) $TS \models_{\mathcal{F}_1} P_2$:

- Any trace that reaches s_4 is not $\mathcal{F}_1$-fair as α is executed only finitely many times. This is in contradiction to our $\mathcal{F}_{1,ucond} = \{\{\alpha\}\}$.
- Therefore $s_3 \xrightarrow{\eta} s_4$ is never taken.
- Because of $\{\eta\} \in \mathcal{F}_{1,strong}$ and because η actions cannot be executed infinitely often (in fact, only once from s_3 to s_4), the state s_3 must not be visited infinitely often.
- We cannot stay in states s_1 or s_2 by only taking transitions $s_1 \xrightarrow{\alpha} s_1$ and $s_2 \xrightarrow{\alpha} s_2$ because of the enabled γ transitions to s_0 or s_1, respectively.
- As β is enabled in s_0, all $\mathcal{F}_1$–fair paths visit exactly s_0, s_1 and s_2 infinitely often.

Therefore $FairTraces_{\mathcal{F}_1}(TS) \subseteq P$ and $TS \models_{\mathcal{F}_1} P$.

b) $TS \not\models_{\mathcal{F}_2} P$:
Consider the path $\pi = (s_0 s_2 s_3 s_1)^\omega$ with its corresponding trace $\sigma = (\{a\}\{a, b\}\emptyset\{b\})^\omega$.
We have $\pi \in FairPaths_{\mathcal{F}_2}(TS)$, but $\sigma \notin P$.
$\implies FairTraces_{\mathcal{F}_2}(TS) \not\subseteq P$.

Solution of Exercise 1.7

Realizable fairness assumptions:

a) $\mathcal{F}_1 = (\{\{\alpha\}\}, \{\{\delta\}\}, \{\{\alpha, \beta\}\})$ is not realizable fair. Consider the states s_1 and s_4. There are no $\mathcal{F}_1$ fair path fragments starting from s_1 or s_4, as on each such path fragment, α transitions never occur. This violates the unconditional fairness constraint $\{\{\alpha\}\}$.

b) $\mathcal{F}_2 = (\{\{\delta, \alpha\}\}, \{\{\alpha, \beta\}\}, \{\{\gamma\}\})$ is realizable fair, as the SCC $\{s_1, s_4\}$ is reachable from every state and $(s_1, s_4)^\omega$ is a $\mathcal{F}_2$ fair path fragment.

c) $\mathcal{F}_3 = (\{\{\alpha, \delta\}, \{\beta, \}\}, \{\{\alpha, \beta\}\}\{\{\gamma\}\})$ is realizable fair. Consider the same SCC $\{s_1, s_4\}$ and again the path fragment $(s_1, s_4)^\omega$.

Solution of Exercise 1.8

let's consider F_1.
The unconditional fairness on $\{\beta\}$ excludes the paths in which states S_4 and S_5 are reached.
The strong fairness on $\{\gamma\}$ excludes the paths ending with S_0^ω or S_3^ω.
The strong fairness on $\{\delta\}$ excludes the paths in which s_1 is visited infinitely many times because otherwise the state s_4 is reached.

The weak fairness on $\{\alpha\}$ excludes the paths cycling between states s_0 and s_2.
Thus the only fair paths are those the visit infinitely often the states s_0,s_2 and s_3, but not s_1.
in the light of the observations above we can conclude that $TS \not\models_{F_1} E_1$ and $TS \models_{F_1} E_2$.

let's consider F_2.
The missing strong fairness on $\{\delta\}$ allows also the paths in which state s_1 is visited infinitely often.
However, the paths in which only the states s_0,s_2 and s_3 are still fair, so we have to conclude, as far F_1: $TS \not\models_{F_2} E_1$ and $TS \models_{F_2} E_2$.
let's consider F_3.
The missing weak fairness on $\{\alpha\}$ allows, in addition to the ones fair for F_2, the paths that visit infinitely often only the statess_0 and s_1.
Thus the only fair paths are those the visit infinitely often the states s_0,s_2 and s_3, but not s_1.
Thus, we conclude that $TS \not\models_{F_3} E_1$ and $TS \not\models_{F_3} E_2$.

Solution of Exercise 1.9

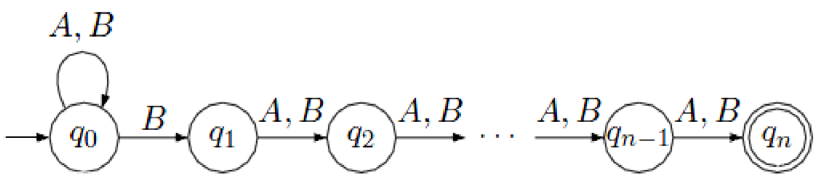
a) Formally, we define the NFA $A_n = (Q_n, \sum, \delta_n, Q_0, F)$ where

- $Q_n = \{q_0, q_1, ..., q_n\}$
- transition relation defined by δ_n:

$$\delta_n(q_0, A) = \{q_0\} \qquad \delta_n(q_0, B) = \{q_0, q_1\}$$
$$\delta_n(q_0, A) = \{q_{q_i+1}\} for 0 < i < n \qquad \delta_n(q_i, B) = \{q_{i+1}\} for 0 < i < n$$

- the set of initial states: $Q_0 = \{q_0\}$
- $F = \{q_n\}$

This can also be outlined as follows:



b) Applying the powerset construction to the NFA A_n yields the DFA $A'_n = (2^{Q_n}, \sum, \delta'_n, \{q_0\}, F'_n)$ where

- the transition function δ'_n is defined (for $k \in \{0, ..., n\}$) as follows:

$$\delta'_n(\{q_0, q_{i1}, ..., q_{ik}\}, A) = \{q_{ij+1} | i_j < n, j \in \{1, ..., k\}\} \cup \{q_0\}$$

$$\delta'_n(\{q_0, q_{i1}, ..., q_{ik}\}, A) = \{q_{ij+1} | i_j < n, j \in \{0, ..., k\}\} \cup \{q_0\}$$

- The acceptance set is given by $F'_n = \{Q' \in 2^{Q_n} | q_n \in Q'\}$

Solution of Exercise 1.10

(a) Whenever A holds then, at the same time, B holds and C does not hold

1. $E_{\mathrm{a}} = \{X_0 X_1 \cdots \in (2^{\mathrm{AP}})^\omega \mid \forall i \in \mathbb{N}\,(A \in X_i \Rightarrow (B \in X_i \wedge C \notin X_i))\}$
2. The property is an invariant, thus it is a SAFETY property. A bad prefix is, for instance, $\{A\}$.

(b) A and D hold together at least once

1. $E_{\mathrm{b}} = \{X_0 X_1 \cdots \in (2^{\mathrm{AP}})^\omega \mid \exists i \in \mathbb{N}\,(A \in X_i \wedge D \in X_i)\}$
2. The property is a LIVENESS because it is not possible to find a bad prefix: any prefix in which A and D have not occurred simultaneously yet can always be completed into a trace in which the required event happened.

(c) A and D hold together at least twice

1. $E_{\mathrm{c}} = \{X_0 X_1 \cdots \in (2^{\mathrm{AP}})^\omega \mid \exists i, j \in \mathbb{N}\,(i \neq j \wedge A \in X_i \wedge D \in X_i \wedge A \in X_j \wedge D \in X_j)\}$
2. As in the previous case the property is a LIVENESS, with similar motivation.

(d) A and D hold together infinitely many times

1. $E_{\mathrm{d}} = \{X_0 X_1 \cdots \in (2^{\mathrm{AP}})^\omega \mid \overset{\infty}{\exists}\, i \in \mathbb{N}\,(A \in X_i \wedge D \in X_i)\}$
2. This is a typical LIVENESS property, no bad prefix exists for traces that do not belong to E_{d}.

(e) Whenever B holds then C holds after some steps

1. $E_{\mathrm{e}} = \{X_0 X_1 \cdots \in (2^{\mathrm{AP}})^\omega \mid \forall i \in \mathbb{N}\,(B \in X_i \Rightarrow (\exists j \in \mathbb{N}\,(j > i \wedge C \in X_j)))\}$
2. This is a typical request-response property, which is a LIVENESS property. No bad prefix exists for traces that do not belong to E_{e}.

(f) Always B or C hold

1. $E_{\mathrm{f}} = \{X_0 X_1 \cdots \in (2^{\mathrm{AP}})^\omega \mid \forall i \in \mathbb{N}\,(B \in X_i \vee C \in X_i)\}$
2. The property is an invariant, thus it is a SAFETY property. A bad prefix is, for instance, $\{\}$.

(g) Eventually C holds

1. $E_{\mathrm{g}} = \{X_0 X_1 \cdots \in (2^{\mathrm{AP}})^\omega \mid \exists i \in \mathbb{N}\,(C \in X_i)\}$
2. The property is a LIVENESS because it is not possible to find a bad prefix: any prefix in which C has not occurred yet can always be completed into a trace in which the required event happened.

(h) If A and C hold together once then eventually B holds continuously for infinitely many times

1. $E_{\mathrm{h}} = \{X_0 X_1 \cdots \in (2^{\mathrm{AP}})^\omega \mid (\exists i \in \mathbb{N}\,(A \in X_i \wedge C \in X_i)) \Rightarrow (\overset{\infty}{\forall}\, j \in \mathbb{N}\,(B \in X_j))\}$
2. The property is a LIVENESS because it is not possible to find a bad prefix: any prefix in which A and C held together can always be completed into a trace in which the tail contains B continuously.

(i) C holds at least once and only finitely many times

1. $E_{\text{i}} = \{X_0X_1 \cdots \in (2^{\text{AP}})^\omega \mid \exists i \in \mathbb{N}\,(C \in X_i) \wedge (\overset{\infty}{\forall}\, j \in \mathbb{N}\,(C \notin X_j))\}$
2. The property is a LIVENESS because it is not possible to find a bad prefix: any prefix in which C held can always be completed into a trace in which the tail contains no C continuously.

(j) If A holds infinitely many times then C must hold only finitely many times

1. $E_{\text{j}} = \{X_0X_1 \cdots \in (2^{\text{AP}})^\omega \mid (\overset{\infty}{\exists}\, i \in \mathbb{N}\,(A \in X_i)) \Rightarrow (\overset{\infty}{\forall}\, j \in \mathbb{N}\,(C \notin X_j))\}$
2. The property is a LIVENESS, combination of two typical liveness properties

(k) Whenever B holds then after two steps C holds

1. $E_{\text{k}} = \{X_0X_1 \cdots \in (2^{\text{AP}})^\omega \mid \forall i \in \mathbb{N}\,(B \in X_i) \Rightarrow (C \in X_{i+2})\}$
2. The property is an invariant, thus it is a SAFETY property. A bad prefix is, for instance, $\{B\}\{B\}\{B\}$.

(l) Whenever C holds then it continues to hold until D holds

1. $E_{\text{l}} = \{X_0X_1 \cdots \in (2^{\text{AP}})^\omega \mid \begin{array}{l} \forall i \in \mathbb{N}\,(C \in X_i) \Rightarrow \exists j \in \mathbb{N}\,(j > i \wedge D \in X_j \wedge \\ \forall k \in \mathbb{N}\,(i \leq k < j \Rightarrow C \in X_k))\} \end{array}$
2. This a typical "until" property within an invariance, which is a MIXED property. Indeed $\{C\}\{A\}$ is a bad prefix but any prefix $\{C\}\{C\}\{C\}\cdots$ can be extended to a trace that satisfies the required constraint.

Solution of Exercise 1.11

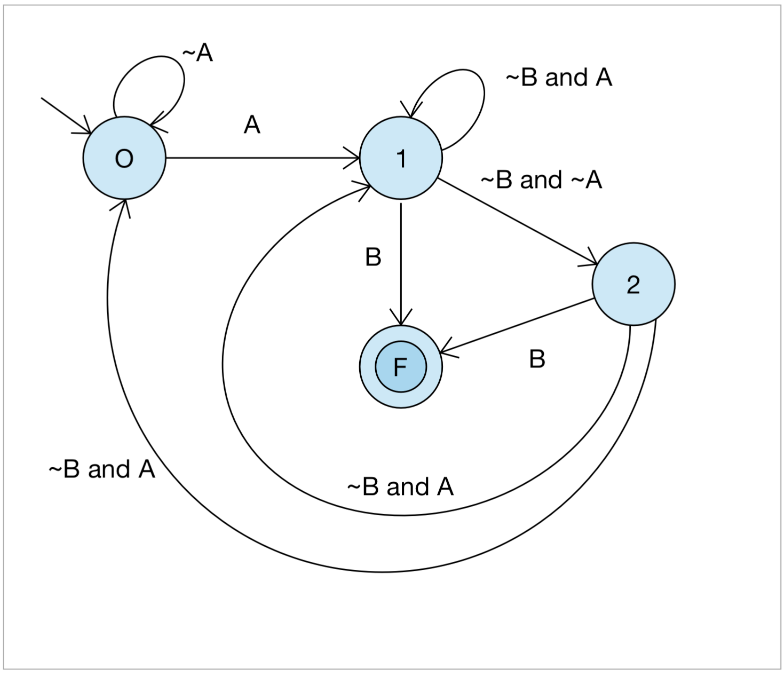
(a) This is a safety property. The set of all words belonging to the property is

$$\left\{X_0X_1 \ldots \in \left(2^{AP}\right)^\omega \mid \forall i \in \mathbb{N}. A \in X_i \Rightarrow (B \notin X_{i+1} \wedge B \notin X_{i+2})\right\}$$

An LTL formula expressing the property is

$$\Box\,(A \Rightarrow (\bigcirc\neg B \wedge \bigcirc\bigcirc\neg B))$$

An NFA accepting all the minimal bad prefixes is the following one ($\sim$ stands for $\neg$)



(b) This is a liveness property. The set of all words belonging to the property is

$$\left\{X_0X_1\ldots \in \left(2^{AP}\right)^{\omega} \mid \overset{\infty}{\forall}\, i \in \mathbb{N}. D \notin X_i \vee C \notin X_i\right\}$$

An LTL formula expressing the property is

$$\Diamond\Box\left(\neg B \vee \neg C\right)$$

(c) This is a liveness property. The set of all words belonging to the property is

$$\left\{X_0X_1\ldots \in \left(2^{AP}\right)^{\omega} \mid \left(\overset{\infty}{\exists}\, i \in \mathbb{N}\colon C \in X_i\right) \Rightarrow \left(\overset{\infty}{\forall}\, i \in \mathbb{N}. D \notin X_i\right)\right\}$$

An LTL formula expressing the property is

$$(\Box\Diamond C) \Rightarrow (\Diamond\Box\neg D)$$

(d) This is a mixed property. The set of all words belonging to the property is

$$\left\{X_0X_1\ldots \in \left(2^{AP}\right)^{\omega} \mid (\exists i \in \mathbb{N}\colon C \in X_i) \wedge (\forall i \in \mathbb{N}. D \in X_i \Rightarrow A \in X_i)\right\}$$

An LTL formula expressing the property is

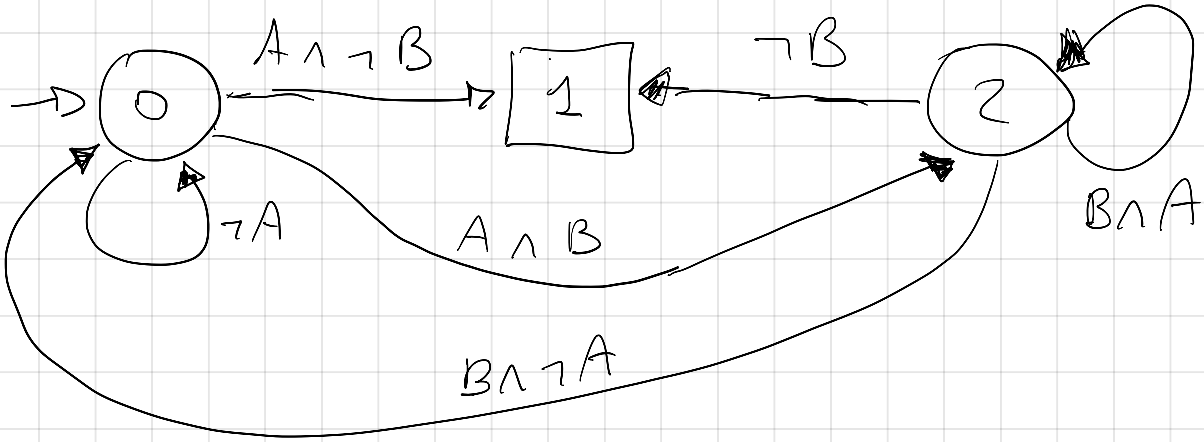
$$\Diamond C \Rightarrow \Box(D \Rightarrow A)$$

Solution of Exercise 1.12

Ex 2) a) $E_a = \{ A_0 A_1 \dots \in (2^{AP})^\omega \mid \forall i \in \mathbb{N}$
$A \in A_i \Rightarrow (B \in A_i \land B \in A_{i+1}) \}$

In LTL: $\Box(A \rightarrow (B \land \bigcirc B))$

This is a pure safety property. The NFA accepting the language of minimal bad prefixes is:



where 1 is the accepting state.

---

b) $E_b = \{ A_0 A_1 \dots \in (2^{AP})^\omega \mid \overset{\infty}{\exists} i \in \mathbb{N} : B \in A_i \land$
$\overset{\infty}{\forall} j \in \mathbb{N}.\ C \notin A_i \}$

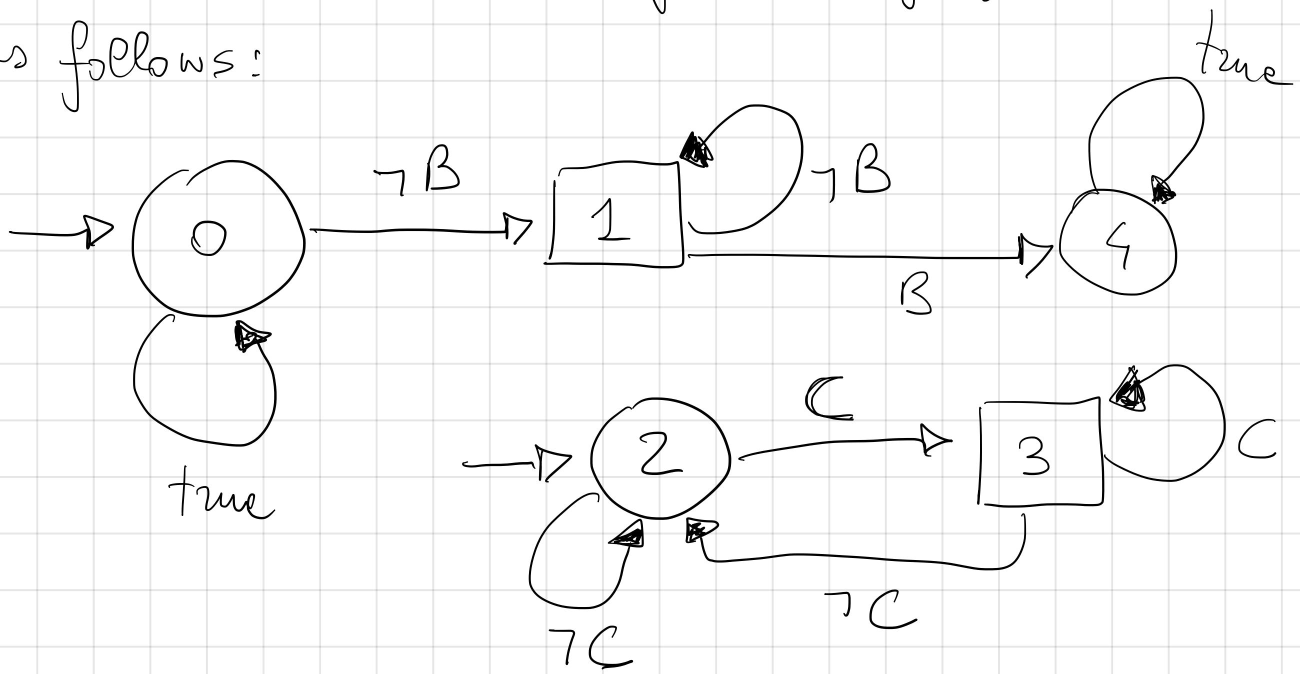
In LTL: $\Box \Diamond B \land \Diamond \Box \neg C$

This is a pure liveness property. To derive an NBA accepting the bad behaviours

We first negate the formula:

$$\neg(\Box\Diamond B \wedge \Diamond\Box\neg C) \equiv \Diamond\Box\neg B \vee \Box\Diamond C$$

A simple NFA accepting this language is as follows:



where the set of initial states is $\{0,2\}$ and the set of accepting states is $\{1,3\}$.

c) $E_c = \{ A_0 A_1 \cdots \in (2^{AP})^\omega \mid (\exists i, j \in \mathbb{N} : i \neq j \wedge A \in A_i \wedge A \in A_j) \wedge (\forall k \in \mathbb{N} : B \in A_k \Rightarrow C \in A_k) \}$

In LTL: $\Diamond(A \wedge \bigcirc(\Diamond A)) \wedge \Box(B \rightarrow C)$

This is a mixed property.