Cyber Physical Systems - Discrete Models
Exercise Sheet 12 Solution

Alper Ari
aa508@uni-freiburg.edu

Onur Sahin
os141@uni-freiburg.de

January 21, 2023

Exercise 1: Lecture Evaluation

We did the lecture evaluation.

Exercise 2: LTL Properties

(a)

$$\varphi_1 = a \land \bigcirc\, b : \tau = \{a\}\{b\}^\omega \vDash \varphi_1$$
$$\varphi_2 : \tau = \{a\}\{a\}\{a\}\{b\}^\omega$$
$$\varphi_3 : \tau = \{a\}\{a\}\{b\}\{a\}^\omega$$
$$\varphi_4 : \tau = \{b\}\{b\}\{c\}\{a\}^\omega$$
$$\varphi_5 : \tau = \{c\}\{c\}\{a\}^\omega$$
$$\varphi_6 : \tau = \{b\}\{b\}(\{a\}\{c\})^\omega$$

(b)

$$\neg\varphi_1 : \tau = \{a\}^\omega$$
$$\neg\varphi_2 : \tau = \{c\}^\omega$$
$$\neg\varphi_3 : \tau = \{a\}\{b\}^\omega$$
$$\neg\varphi_4 : \tau = \{c\}^\omega$$
$$\neg\varphi_5 : \tau = (\{b\}\{a\})^\omega$$
$$\neg\varphi_6 : \tau = \{c\}\{a\}^\omega$$

(c)

Let T be the Transition System

- $T \nvDash \varphi_1$. Counterexample: $\text{trace}(s_0 s_2 \ldots) = \{b\}\{a\}\ldots$
- $T \vDash \varphi_2$. Because first trace is $\{b\}\{a\}\ldots$ which immediately starts with b therefore satisfies and the second trace is $\{a, c\}\{a\}\{a, b\}\ldots$ which also contains a until b.

- $T \not\models \varphi_3$. Counterexample: $\text{trace}(s_1 s_2 s_3^\omega) = \{a, c\}\{a\}\{a, b\}^\omega$. Which satisfies $a \cup \Box b$ therefore violates φ_3.
- $T \not\models \varphi_4$. Counterexample: $\text{trace}(s_0 s_2 s_3) = \{b\}\{a\}\{a, b\}^\omega$ doesn't contain a in the initial state and also there is no eventually c for the first state. Therefore it is not in $\text{Words}(\varphi_4)$.
- $T \models \varphi_5$. The infinite parts of each trace satisfies "always a". Therefore, all traces are in $\text{Words}(\varphi_5)$.
- $T \not\models \varphi_6$. Counterexample: $\text{trace}(s_0 s_2 s_3^\omega) = \{b\}\{a\}\{a, b\}^\omega$ doesn't have c at all. Therefore, "eventually c" can't be satisfied.

(d)

$\text{Words}(\varphi_1) =$

$\left\{A_0 A_1 \ldots \in \left(2^{\text{AP}}\right)^\omega \mid a \in A_0 \land b \in A_1\right\}$

$\text{Words}(\varphi_2) =$

$\left\{A_0 A_1 \ldots \in \left(2^{\text{AP}}\right)^\omega \mid \exists i \in \mathbb{N}.\ \left(\forall j < i.\ a \in A_j\right) \land b \in A_i\right\}$

$\text{Words}(\varphi_3) =$

$\left\{A_0 A_1 \ldots \in \left(2^{\text{AP}}\right)^\omega \mid \forall i \in \mathbb{N}.\ \left(\exists j < i.\ a \notin A_j\right) \lor \left(\exists j \geq i.\ b \notin A_j\right)\right\}$

$\text{Words}(\varphi_4) =$

$\left\{A_0 A_1 \ldots \in \left(2^{\text{AP}}\right)^\omega \mid \exists i \in \mathbb{N}.\ (\forall j < i.\ (\exists k \geq j.\ c \in A_k)) \land \left(\forall j \geq i.\ a \in A_j\right)\right\}$

$\text{Words}(\varphi_5) =$

$\left\{A_0 A_1 \ldots \in \left(2^{\text{AP}}\right)^\omega \mid \exists i \in \mathbb{N}.\ \left(\forall j \geq i.\ a \in A_j\right)\right\}$

$\text{Words}(\varphi_6) =$

$\left\{A_0 A_1 \ldots \in \left(2^{\text{AP}}\right)^\omega \mid \forall i \in \mathbb{N}.\ \exists j \geq i.\ c \in A_j\right\}$

Exercise 3: Stating properties in LTL

$$\varphi_a = \Box(\neg \text{ Peter.use} \vee \neg \text{ Betsy.use})$$

The wording is ambiguous. "a user can print only for a finite amount of time" can be either interpreted as:

1. For each time the user starts printing, user stops printing in a finite amount of time.
2. Each user only prints finitely many times in total.

We choose the interepratation 1.

$$\begin{aligned}\varphi_b = {} & \Box(\text{Peter.use} \to \Diamond\neg \text{ Peter.use}) \wedge \\ & \Box(\text{Betsy.use} \to \Diamond\neg \text{ Betsy.use})\end{aligned}$$

$$\begin{aligned}\varphi_c = {} & \Box(\text{Peter.request} \to \Diamond \text{ Peter.use}) \wedge \\ & \Box(\text{Betsy.request} \to \Diamond \text{ Betsy.use})\end{aligned}$$

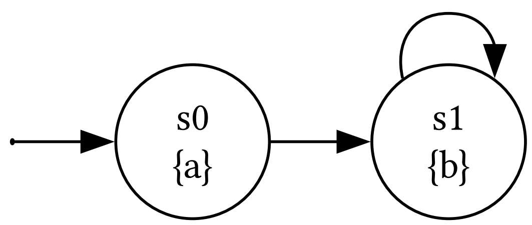
$$\begin{aligned}\varphi_d = {} & (\Box(\text{Peter.request} \to \Diamond\neg \text{ Peter.request})) \wedge \\ & (\Box(\text{Betsy.request} \to \Diamond\neg \text{ Betsy.request}))\end{aligned}$$

$$\begin{aligned}\varphi_e = {} & \Box(\text{Peter.use} \to (\neg \text{ Peter.use}) \cup \text{Betsy.use}) \wedge \\ & \Box(\text{Betsy.use} \to (\neg \text{ Betsy.use}) \cup \text{Peter.use})\end{aligned}$$

Exercise 4: Equivalence of LTL formulas

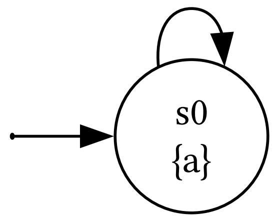
Note: Atomic propositions of the Transition System are notated under the state name.

- $\Box a \wedge \bigcirc \Diamond a \stackrel{?}{\equiv} \Box a = \text{true}$
- $\Diamond a \wedge \bigcirc \Box a \stackrel{?}{\equiv} \Diamond a = \text{false}$. Counter example TS:



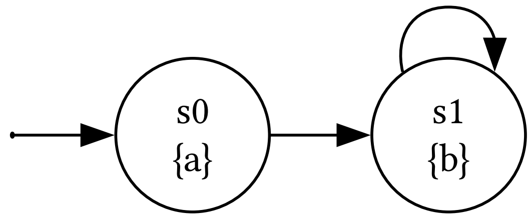
satisfies $\Diamond a$ but not for $\bigcirc \Box a$

- $\Box a \to \Diamond b \stackrel{?}{\equiv} a \cup (b \vee \neg a) = \text{true}.$
- $a \cup \text{false} \stackrel{?}{\equiv} \Box a = \text{false}$. Counter example TS:



satisfies $\square a$ but not for $a \cup \text{false}$.

- $\square \bigcirc b \stackrel{?}{\equiv} \square b = \text{false}$. Counter example:



satisfies $\square \bigcirc b$ but not for $\square b$.

Proofs

Proof 1: $\square a \land \bigcirc \Diamond a \equiv \square a$
Assuming $\text{Words}(\square a) \subseteq \text{Words}(\bigcirc \square a)$, $\square a \land \bigcirc \Diamond a \equiv \square a$ because intersection with a subset results with the subset.

Proving $\text{Words}(\square a) \subseteq \text{Words}(\bigcirc \Diamond a)$:

$$\text{Words}(\square a) = \left\{ A_0 A_1 \ldots \in \left(2^{\text{AP}}\right)^{\omega} \mid \forall i \in \mathbb{N}.\ a \in A_i \right\}$$
$$\text{Words}(\bigcirc \Diamond a) = \left\{ A_0 A_1 \ldots \in \left(2^{\text{AP}}\right)^{\omega} \mid \forall i > 0.\ \exists j \geq i.\ a \in A_i \right\}$$

Let $\sigma \in \text{Words}(\square a)$. $\sigma \in \text{Words}(\bigcirc \Diamond a)$ because for any σ, we can take $i = 1$ and $j = 1$ which contains a and therefore $\sigma \vDash \bigcirc \Diamond a$.

■

Proof 2: $\square a \to \Diamond b \equiv a \cup (b \lor \neg a)$
$a \cup (b \lor \neg a) \equiv (\text{true} \cup (b \lor \neg a))$, because a must necessarily hold until $b \lor \neg a$ occurs otherwise $b \lor \neg a$ would hold earlier. Also $\text{true} \cup (b \lor \neg a) \equiv \Diamond(b \lor \neg a)$ from the definition of $\Diamond$ operator.

For $\square a \to \Diamond b$:

$$\begin{aligned} \square a \to \Diamond b &\equiv \neg \square a \lor \Diamond b \\ &\equiv \Diamond \neg a \lor \Diamond b \\ &\equiv \Diamond(\neg a \lor b) \end{aligned}$$

Since both equations are equivalent for another LTL formula they are equivalent to each other as well.

■