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 2: LTL Properties

(a)

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

(b)

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

(c)

Let T be the Transition System

- $T \nvDash \varphi_1$. Counterexample: 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.
- $T \nvDash \varphi_3$. Counterexample: 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)

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

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

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

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

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

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

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

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

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

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

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

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

Exercise 3: Stating properties in LTL

$$\varphi_a = \neg\ \text{Peter.use} \lor \neg\ \text{Betsy.use}$$

$$\varphi_b = (\Diamond\Box\neg\ \text{Peter.use}) \land (\Diamond\Box\neg\ \text{Betsy.use})$$

$$\varphi_c = (\text{Peter.request} \rightarrow \Diamond\ \text{Peter.use}) \land (\text{Betsy.request} \rightarrow \Diamond\ \text{Betsy.use})$$

$$\varphi_d = (\Box\Diamond\ \text{Peter.request} \rightarrow \Box\Diamond\ \text{Peter.use}) \land (\Box\Diamond\ \text{Betsy.request} \rightarrow \Box\Diamond\ \text{Betsy.use})$$

$$\varphi_e = (\text{Peter.use} \rightarrow (\neg\ \text{Peter.use}) \cup \text{Betsy.use}) \land (\text{Betsy.use} \rightarrow (\neg\ \text{Betsy.use}) \cup \text{Peter.use})$$

Exercise 4: Equivalence of LTL formulas

- $\Box a \wedge \bigcirc \Diamond a \stackrel{?}{\equiv} \Box a = \text{true}$
- $\Diamond a \wedge \bigcirc \Box a \stackrel{?}{\equiv} \Diamond a = \text{false}$. Counter example: $\{a\}\{b\}^\omega$ satisfies $\Diamond a$ but not $\bigcirc \Box a$.
- $\Box a \rightarrow \Diamond b \stackrel{?}{\equiv} a \cup (b \vee \neg a) = \text{true}$.
- $a \cup \text{false} \stackrel{?}{\equiv} \Box a = \text{false}$. Counter example: $\{a\}^\omega$ holds for $\Box a$ but not for $a \cup \text{false}$ because there isn't a step satisfying false.
- $\Box \bigcirc b \stackrel{?}{\equiv} \Box b = \text{false}$. Counter example: $\{a\}\{b\}^\omega$ holds for $\Box \bigcirc b$ but not for $\Box b$.

Proofs

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

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

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

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

■

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

For $\Box a \rightarrow \Diamond b$:

$$\begin{aligned}
\Box a \rightarrow \Diamond b &\equiv \neg \Box a \vee \Diamond b \\
&\equiv \Diamond \neg a \vee \Diamond b \\
&\equiv \Diamond(\neg a \vee b)
\end{aligned}$$

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

■