Cyber Physical Systems - Discrete Models
Exercise Sheet 8 Solution

Alper Ari
aa508@uni-freiburg.edu

Onur Sahin
os141@uni-freiburg.de

December 10, 2023

2.5 / 4

15.75 / 22

Exercise 1: Prefixes and Closure I

1 / 1

Part A

$$P \subseteq \text{cl}(P)$$

Solution

Let $\omega \in P$, then $\text{pref}(\omega) \subseteq \text{pref}(P)$ trivially. Since $\text{pref}(\omega) \subseteq \text{pref}(P)$ is the predicate for closure, then we can conclude $\forall \omega \in P \to \omega \in \text{cl}(P)$, thefore $P \subseteq \text{cl}(P)$.

1.5 / 2

Part B

$$\text{pref}(\text{cl}(P)) = \text{pref}(P)$$

Solution

If we prove both $\text{pref}(\text{cl}(P)) \subseteq \text{pref}(P)$ and $\text{pref}(P) \subseteq \text{pref}(\text{cl}(P))$, then we can conclude $\text{pref}(\text{cl}(P)) = \text{pref}(P)$.

Direction 1: $\text{pref}(\text{cl}(P)) \subseteq \text{pref}(P)$

Let $\omega \in \text{pref}(\text{cl}(P))$, then $\exists \sigma \in \text{cl}(P) \to \omega \in \text{pref}(\sigma)$. By the definition of closure, $\forall \sigma \in \text{cl}(P) \to \text{pref}(\sigma) \subseteq \text{pref}(P)$. Hence, $w \in \text{pref}(P)$. Which concludes that $\forall \omega \in \text{pref}(\text{cl}(P)) \to \omega \in \text{pref}(P)$.

Direction 2: $\text{pref}(P) \subseteq \text{pref}(\text{cl}(P))$

Let $\omega \in \text{pref}(P)$, then $\exists \sigma \in P \to \omega \in \text{pref}(\sigma)$. By proof in part a, we can claim $\forall \sigma \in P \to \sigma \in \text{cl}(P)$. Therefore, $\omega \in \text{pref}(P) \to \omega \in \text{pref}(\text{cl}(P))$.

Your line of thinking is correct, but the way you wrote it down is not syntactically correct. -0.5

For example: $\forall \sigma \in cl(P) \to pref(\sigma) \subseteq pref(P)$ is an implication with no precondition (only a quantifier), thus makes no syntactical sense.

To be safe in the exam, express as much in words as possible.

Exercise 2: Prefixes and Closure II

3.75 / 6

Part A

1.25 / 2

$$P_1 = \{A_0 A_1^{\in(2^{AP})^\omega} \ldots \mid \exists S \subseteq \overset{\mathbb{N}}{\cancel{N}} \cdot (|S| = 1 \land \forall i \in S a \in A_i)\}$$ $\land\ \forall i \notin S,\ a \notin A_i$ -0.5

$$P_2 = \{A_0 A_1^{\in(2^{AP})^\omega} \ldots \mid \forall i^{\in\mathbb{N}} \cdot (a \in A_i \to b \in A_{i+1})\}$$ -0.25 (✓)

$$P_3 = \{A_0 A_1^{\in(2^{AP})^\omega} \ldots \mid \exists i^{\in\mathbb{N}} \cdot (\forall j^{\in\mathbb{N}} \cdot (j \geq i \to a \notin A_j))\}$$ (✓)

$$P_4 = \left\{A_0 A_1^{\in(2^{AP})^\omega} \ldots \mid a \in A_0 \land \overset{\infty}{\exists} i^{\in\mathbb{N}} \cdot a \in A_i\right\}$$ (✓)

Part B

1.25 / 2

$$\text{pref}(P_1) = \{A_0 A_1 \ldots A_k^{\in(2^{AP})^+} \mid \exists S \subseteq \overset{\{0,\ldots,k\} = \mathbb{N}_{\leq k}}{\cancel{N}} \cdot (|S| \leq 1 \land \forall i \in S a \in A_i)\}$$ $\land\ \forall i \notin S,\ a \notin A_i$ -0.5

$$\text{pref}(P_2) = \{A_0 A_1 \ldots A_k^{\in(2^{AP})^+} \mid \forall i^{\in\mathbb{N}} \cdot (i < k \land a \in A_i \to b \in A_{i+1})\}$$ (✓) -0.25

$$\text{pref}(P_3) = \{A_0 A_1 \ldots A_k^{\in(2^{AP})^+} \mid \text{true}\}$$ (✓)

$$\text{pref}(P_4) = \{A_0 A_1 \ldots A_k^{\in(2^{AP})^+} \mid a \in A_0\}$$ (✓)

Part C

1.25 / 2

$$\text{cl}(P_1) = \{A_0 A_1^{\in(2^{AP})^\omega} \ldots \mid \exists S \subseteq \overset{\mathbb{N}}{\cancel{N}} \cdot (|S| \leq 1 \land \forall i \in S a \in A_i)\}$$ $\land\ \forall i \notin S,\ a \notin A_i$ -0.5

$$\text{cl}(P_2) = \{A_0 A_1^{\in(2^{AP})^\omega} \ldots \mid \forall i \cdot (a \in A_i \to b \in A_{i+1})\}$$ (✓) -0.25

$$\text{cl}(P_3) = \{A_0 A_1^{\in(2^{AP})^\omega} \ldots \mid \text{true}\}$$ (✓)

$$\text{cl}(P_4) = \{A_0 A_1^{\in(2^{AP})^\omega} \ldots \mid a \in A_0\}$$ (✓)

9.5/12

Exercise 3: Safety & Liveness Properties

Part A

P_1

- Is an invariant.
- Invariation condition: $a \notin S$.

The invariant condition is a propositional logic formula ϕ over the set of atomic propositions, here $\{a,b\}$.
$\phi = \neg a$ -0.5

P_2

- Not an invariant.
- Example trace: $(w = \{a\}^\omega) \notin P_2$. However, $(\forall \sigma \in w \cdot \sigma = \{a\})$, and we can give trace $\{a\}\{b\}^\omega \in P_2$ as a counter example, since the set $\{a\}$ also occurs in $\{a\}\{b\}^\omega$. -0.5

w is a single trace, not a set. Just write that w contains only $\{a\}$.

P_3

- Is an invariant.
- Invariant condition: $a \in S \to b \in S$. $\phi = b \to a$ -0.5

P_4

- Not an invariant.
- Example trace: $(w = \{b\}^\omega) \notin P_4$. However, $(\forall \sigma \in w \cdot \sigma = \{b\})$, and we can give trace $\{b\}\{a\}^\omega \in P_2$ as a counterexample, since the set $\{b\}$ also occurs in $\{b\}\{a\}^\omega$. -0.5

w contains only $\{b\}$

Part B

P_1

- Is a safety property.
- Set of bad prefixes: $\text{BadPref} = \{A_0 A_1 \ldots A_n \mid \exists i \in \{0, \ldots, n\} \cdot a \in A_i\}$.

$\in (2^{AP})^+$ -0.25

P_2

- Not a safety property.
- Example trace: $(\sigma = \{a\}^\omega) \in \left(2^{\text{AP}}\right)^\omega \setminus P_2$. But $\forall w \in \text{pref}(\sigma)$, we can always extend it with $\sigma\{b\}^w \in P_2$ so no σ can be a bad prefix.

P_3

- Is a safety property.
- Set of bad prefixes:
  $\text{BadPref} = \{A_0 A_1 \ldots A_n \mid \exists i \in \{0, \ldots, n\} \cdot b \in A_i \land a \notin A_i\}$.

$\in (2^{AP})^+$

P_4

- Is a safety property.
- Set of bad prefixes:
  $\text{BadPref} = \{A_0 A_1 \ldots A_n \mid \exists S \subseteq \{0, \ldots, n\} \cdot |S| > 1 \land (\forall i \in S \cdot b \in S_i)\}$

$\in (2^{AP})^+$

Part C

P_1

- Is not a liveness property.
- Example bad prefix: $\{a\}$. $\forall w \in \left(2^{\mathrm{AP}}\right)^{\omega} \cdot (\{a\}w) \notin P_1$.

P_2

- Is a liveness property.
- We can extend any finite trace with $\{b\}^{\omega}$. $\forall w \in \left(2^{\mathrm{AP}}\right)^{*} \cdot w\{b\}^{\omega} \in P_2$.

P_3

- Is not a liveness property.
- Example bad prefix: $\{b\}$. $\forall w \in \left(2^{\mathrm{AP}}\right)^{\omega} \cdot (\{b\}w) \notin P_3$.

P_4

- Is not a liveness property.
- Example bad prefix: $\{b\}\{b\}$. $\forall w \in \left(2^{\mathrm{AP}}\right)^{\omega} \cdot (\{b\}\{b\}w) \notin P_4$.