CSC410

# LINEAR TEMPORAL LOGIC

(with solutions)

---

## Writing LTL Specifications

Use atomic propositions with the obvious meaning (e.g. $cs_1$ = "process 1 is in its critical section"). Events (a request, a button press, ...) are modelled as propositions that hold at the step where the event occurs. You may use the weak until $\varphi \,\mathsf{W}\, \psi \equiv (\varphi \,\mathsf{U}\, \psi) \vee \Box\varphi$.

1. **Mutual Exclusion**: processes 1 and 2 are never simultaneously in their critical sections.

   **Solution.** $\Box\neg(cs_1 \wedge cs_2)$

2. **Client-Server Systems**: the system responds to all requests, but provides no guarantee on the timeline for responses.

   **Solution.** $\Box(req \rightarrow \Diamond resp)$.

3. **Process Scheduler**: (i) a process that, from some point on, is continuously ready to run is scheduled infinitely often; (ii) a process that is ready infinitely often (but perhaps not continuously) is scheduled infinitely often. Which of the two is the stronger requirement?

   **Solution.** (i) $\Diamond\Box ready \rightarrow \Box\Diamond run$ (weak fairness); (ii) $\Box\Diamond ready \rightarrow \Box\Diamond run$ (strong fairness).

4. **Leader Election**: among nodes 1, 2, 3, there are never two leaders at the same time; moreover, provided the network eventually becomes stable for good, some node is eventually elected leader and remains leader forever.

   **Solution.** $\Box\big(\neg(l_1 \wedge l_2) \wedge \neg(l_1 \wedge l_3) \wedge \neg(l_2 \wedge l_3)\big) \;\wedge\; \big(\Diamond\Box stable \rightarrow \Diamond(\Box l_1 \vee \Box l_2 \vee \Box l_3)\big)$.

   Pitfall: $\Diamond\Box(l_1 \vee l_2 \vee l_3)$: from some point on *some* node is leader; leadership could rotate forever. $\Diamond(\Box l_1 \vee \Box l_2 \vee \Box l_3) \equiv \Diamond\Box l_1 \vee \Diamond\Box l_2 \vee \Diamond\Box l_3$.

5. **Elevator**: the doors are never open while the cabin is moving, and every call from floor $k$ is eventually served, i.e. the cabin eventually stops at floor $k$ with its doors open.

   **Solution.** $\Box(moving \rightarrow \neg open) \;\wedge\; \Box\big(call_k \rightarrow \Diamond(at_k \wedge open)\big)$.

6. **Railway Crossing**: whenever a train is approaching, it does not enter the crossing until the gate is down, and the gate then stays down until the train has exited the crossing.

   **Solution.** $\Box\Big(approach \rightarrow \big(\neg in \,\mathsf{U}\, (down \wedge (down \,\mathsf{U}\, exit))\big)\Big)$. If safety-only (e.g. the train may stop before the crossing forever), replace both U by W.

7. **ATM**: within a session, cash is dispensed only after the PIN has been verified, and at most once; a session starts when a card is inserted and ends when it is ejected.

   **Solution.** $\square\big(\mathit{cardIn} \rightarrow (\neg \mathit{dispense}\ \mathsf{W}\ \mathit{pinOK})\big)\ \wedge\ \square\big(\mathit{dispense} \rightarrow \bigcirc(\neg \mathit{dispense}\ \mathsf{W}\ \mathit{eject})\big)$.

## Proving/Disproving LTL Equalities

---

**Proof notation and legends:** A trace is $\sigma = A_0A_1A_2\ldots$ with $A_i \subseteq AP$; $\sigma[i\ldots] = A_iA_{i+1}\ldots$; $\varphi \equiv \psi$ iff $\forall\sigma.\ (\sigma \models \varphi \iff \sigma \models \psi)$. In counterexamples, $p, q \in AP$.

(At) $\sigma \models a \iff a \in A_0$
(∧) $\sigma \models \varphi_1 \wedge \varphi_2 \iff \sigma \models \varphi_1$ and $\sigma \models \varphi_2$
(¬) $\sigma \models \neg\varphi \iff \sigma \not\models \varphi$
(∨) $\sigma \models \varphi_1 \vee \varphi_2 \iff \sigma \models \varphi_1$ or $\sigma \models \varphi_2$ (derived: $\varphi_1 \vee \varphi_2 := \neg(\neg\varphi_1 \wedge \neg\varphi_2)$)
(◯) $\sigma \models \bigcirc\varphi \iff \sigma[1\ldots] \models \varphi$
(U) $\sigma \models \varphi_1\ \mathsf{U}\ \varphi_2 \iff \exists j \geq 0.\ \sigma[j\ldots] \models \varphi_2$ and $\sigma[i\ldots] \models \varphi_1$ for all $0 \leq i < j$
(□) $\sigma \models \square\varphi \iff \forall i.\ \sigma[i\ldots] \models \varphi$
(◇) $\sigma \models \Diamond\varphi \iff \exists i \geq 0.\ \sigma[i\ldots] \models \varphi$
(Suf) $\sigma[0\ldots] = \sigma$, $\sigma[i\ldots][j\ldots] = \sigma[i{+}j\ldots]$, $\sigma[i\ldots] = A_iA_{i+1}\ldots$

**Note:** in all the cases below where the equivalence does not hold, giving the counterexample and the reasoning for why it is a counterexample is *sufficient* to prove that it does not hold. The reason you see the proof of the direction that does hold is to squeeze more out of the example for you. For instance, you can assume the reasoning for the first direction of (a) given below as the *proof of validity* of the following LTL formula:

$$\Diamond(\varphi \wedge \psi) \implies \Diamond\varphi \wedge \Diamond\psi$$

and the counterexample given for the opposite direction as the *proof of satisfiability* of the following LTL formula:

$$\neg\big(\Diamond(\varphi \wedge \psi) \impliedby \Diamond\varphi \wedge \Diamond\psi\big)$$

---

(a) $\Diamond(\varphi \wedge \psi) \equiv \Diamond\varphi \wedge \Diamond\psi$

**Solution.** Not equivalent.

($\Rightarrow$) holds:

| | | |
|---|---|---|
| | $\sigma \models \Diamond(\varphi \wedge \psi)$ | |
| $\iff$ | $\exists i \geq 0.\ \sigma[i\ldots] \models \varphi \wedge \psi$ | [◇] |
| $\iff$ | $\exists i \geq 0.\ (\sigma[i\ldots] \models \varphi\ \wedge\ \sigma[i\ldots] \models \psi)$ | [∧] |
| $\implies$ | $(\exists i \geq 0.\ \sigma[i\ldots] \models \varphi) \wedge (\exists i \geq 0.\ \sigma[i\ldots] \models \psi)$ | [∃ forward-distributes over ∧] |
| $\iff$ | $\sigma \models \Diamond\varphi\ \wedge\ \sigma \models \Diamond\psi$ | [◇] |
| $\iff$ | $\sigma \models \Diamond\varphi \wedge \Diamond\psi$ | [∧] |

($\Leftarrow$) fails. Let $\sigma = \{p\}\{q\}\emptyset^\omega$, i.e. $A_0 = \{p\}$, $A_1 = \{q\}$, $A_i = \emptyset$ for $i \geq 2$.

$$
\begin{array}{lll}
& \sigma \models \Diamond p \wedge \Diamond q & \\
\Longleftarrow & \sigma[0\ldots] \models p \ \wedge\ \sigma[1\ldots] \models q & [\wedge, \Diamond] \\
\Longleftarrow & p \in A_0 \ \wedge\ q \in A_1 & [\text{At, Suf; def. } \sigma]
\end{array}
$$

$$
\begin{array}{lll}
& \sigma \not\models \Diamond(p \wedge q) & \\
\Longleftarrow & \forall i \geq 0.\ \sigma[i\ldots] \not\models p \wedge q & [\Diamond] \\
\Longleftarrow & \forall i \geq 0.\ \neg(p \in A_i \wedge q \in A_i) & [\wedge, \text{At, Suf; def. } \sigma]
\end{array}
$$

(b) $\Diamond(\varphi \vee \psi) \equiv \Diamond\varphi \vee \Diamond\psi$

**Solution.** Equivalent.

$$
\begin{array}{lll}
& \sigma \models \Diamond(\varphi \vee \psi) & \\
\Longleftrightarrow & \exists i \geq 0.\ \sigma[i\ldots] \models \varphi \vee \psi & [\Diamond] \\
\Longleftrightarrow & \exists i \geq 0.\ (\sigma[i\ldots] \models \varphi \ \vee\ \sigma[i\ldots] \models \psi) & [\vee] \\
\Longleftrightarrow & (\exists i \geq 0.\ \sigma[i\ldots] \models \varphi) \vee (\exists i \geq 0.\ \sigma[i\ldots] \models \psi) & [\exists \text{ distributes over } \vee] \\
\Longleftrightarrow & \sigma \models \Diamond\varphi \ \vee\ \sigma \models \Diamond\psi & [\Diamond] \\
\Longleftrightarrow & \sigma \models \Diamond\varphi \vee \Diamond\psi & [\vee]
\end{array}
$$

(c) $\Box(\varphi \vee \psi) \equiv \Box\varphi \vee \Box\psi$

**Solution.** Not equivalent.

($\Leftarrow$) holds:

$$
\begin{array}{lll}
& \sigma \models \Box\varphi \vee \Box\psi & \\
\Longleftrightarrow & \sigma \models \Box\varphi \ \vee\ \sigma \models \Box\psi & [\vee] \\
\Longleftrightarrow & (\forall i.\ \sigma[i\ldots] \models \varphi) \vee (\forall i.\ \sigma[i\ldots] \models \psi) & [\Box] \\
\Longrightarrow & \forall i.\ (\sigma[i\ldots] \models \varphi \ \vee\ \sigma[i\ldots] \models \psi) & [\forall \text{ forward-contracts over } \vee] \\
\Longleftrightarrow & \forall i.\ \sigma[i\ldots] \models \varphi \vee \psi & [\vee] \\
\Longleftrightarrow & \sigma \models \Box(\varphi \vee \psi) & [\Box]
\end{array}
$$

($\Rightarrow$) fails. Let $\sigma = (\{p\}\{q\})^\omega$, i.e. $A_{2k} = \{p\}$, $A_{2k+1} = \{q\}$ for all $k \geq 0$.

$$
\begin{array}{lll}
& \sigma \models \Box(p \vee q) & \\
\Longleftarrow & \forall i.\ \sigma[i\ldots] \models p \vee q & [\Box] \\
\Longleftarrow & \forall i.\ (p \in A_i \vee q \in A_i) & [\vee, \text{At, Suf; def. } \sigma]
\end{array}
$$

$$
\begin{array}{lll}
& \sigma \not\models \Box p \vee \Box q & \\
\Longleftarrow & \sigma \not\models \Box p \ \wedge\ \sigma \not\models \Box q & [\vee] \\
\Longleftarrow & \sigma[1\ldots] \not\models p \ \wedge\ \sigma[0\ldots] \not\models q & [\Box; \text{ witnesses } i := 1,\ i := 0] \\
\Longleftarrow & p \notin A_1 \ \wedge\ q \notin A_0 & [\text{At, Suf; def. } \sigma]
\end{array}
$$

(d) $\varphi \,\mathsf{U}\, \psi \equiv \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$

**Solution.** Equivalent (the expansion law for U). Let $\sigma' := \sigma[1\ldots]$, so $\sigma'[j\ldots] = \sigma[j{+}1\ldots]$ (Suf), and $P(j) :\equiv \sigma[j\ldots] \models \psi \wedge \forall i.\ 0 \le i < j \to \sigma[i\ldots] \models \varphi$.

$$
\begin{aligned}
& \sigma \models \varphi \,\mathsf{U}\, \psi \\
\iff & \exists j \ge 0.\ P(j) \\
& \quad \text{[U]} \\
\iff & P(0) \vee \exists j \ge 0.\ P(j{+}1) \\
& \quad \text{[case } j = 0 \text{ or } j \ge 1\text{; shift } j\text{]} \\
\iff & \sigma \models \psi \vee \exists j \ge 0.\ \big(\sigma'[j\ldots] \models \psi \wedge \sigma \models \varphi \wedge \forall i.\ 0 \le i < j \to \sigma'[i\ldots] \models \varphi\big) \\
& \quad \text{[def. } P, \sigma'\text{; } \forall \text{ over empty range; case } i = 0 \text{ or } i \ge 1\text{]} \\
\iff & \sigma \models \psi \vee \Big(\sigma \models \varphi \wedge \exists j \ge 0.\ \big(\sigma'[j\ldots] \models \psi \wedge \forall i.\ 0 \le i < j \to \sigma'[i\ldots] \models \varphi\big)\Big) \\
& \quad \text{[}\wedge \text{ pulled out of } \exists \text{ (}j \text{ not free in } \sigma \models \varphi\text{)]} \\
\iff & \sigma \models \psi \vee \big(\sigma \models \varphi \wedge \sigma' \models \varphi \,\mathsf{U}\, \psi\big) \\
& \quad \text{[U]} \\
\iff & \sigma \models \psi \vee \big(\sigma \models \varphi \wedge \sigma \models \bigcirc(\varphi \,\mathsf{U}\, \psi)\big) \\
& \quad \text{[}\bigcirc\text{]} \\
\iff & \sigma \models \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi)) \\
& \quad \text{[}\wedge\text{, }\vee\text{]}
\end{aligned}
$$

**Alternative proof (by cases), if you are not comfortable enough with logic to do the proof above.** *Idea:* $\varphi \,\mathsf{U}\, \psi$ holds if $\psi$ holds now, or if $\varphi$ holds now and $\varphi \,\mathsf{U}\, \psi$ holds from the next step on. We prove each direction by splitting on where $\psi$ becomes true.

($\Rightarrow$) Assume $\sigma \models \varphi \,\mathsf{U}\, \psi$. By U there is a $j \ge 0$ with $\sigma[j\ldots] \models \psi$ and $\sigma[i\ldots] \models \varphi$ for all $0 \le i < j$.

- *Case* $j = 0$. Then $\sigma = \sigma[0\ldots] \models \psi$. For all such $\sigma$, we have $\sigma \models \psi \vee (\varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi))$ because it satisfies the first disjunct.
- *Case* $j \ge 1$. This assumption gives us the following two facts:
  - $\sigma \models \varphi$, because $\sigma = \sigma[0\ldots]$ and $0 < j$.
  - $\sigma[1\ldots] \models \varphi \,\mathsf{U}\, \psi$, with witness $j{-}1$: we have $\sigma[1\ldots][j{-}1\ldots] = \sigma[j\ldots] \models \psi$, and for $0 \le i < j{-}1$ we have $\sigma[1\ldots][i\ldots] = \sigma[i+1\ldots] \models \varphi$, because $0 \le i{+}1 < j$.

  By $\bigcirc$, $\sigma \models \bigcirc(\varphi \mathsf{U} \psi)$. So $\sigma \models \varphi \wedge \bigcirc(\varphi \mathsf{U} \psi)$, and therefore, we have $\sigma \models \psi \vee (\varphi \wedge \bigcirc(\varphi \mathsf{U} \psi))$ because it satisfies the second disjunct.

($\Leftarrow$) Assume $\sigma \models \psi$ or $\sigma \models \varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi)$.

- *Case* $\sigma \models \psi$. Take $j = 0$: $\sigma[0\ldots] \models \psi$, and the condition "for all $0 \le i < 0$" is empty. So $\sigma \models \varphi \,\mathsf{U}\, \psi$.
- *Case* $\sigma \models \varphi \wedge \bigcirc(\varphi \,\mathsf{U}\, \psi)$. Then $\sigma \models \varphi$ and $\sigma[1\ldots] \models \varphi \,\mathsf{U}\, \psi$. By U there is a $k \ge 0$ with $\sigma[1\ldots][k\ldots] = \sigma[k+1\ldots] \models \psi$ and $\sigma[1\ldots][i\ldots] = \sigma[i+1\ldots] \models \varphi$ for all $0 \le i < k$. Take $j = k{+}1$. Then $\sigma[j\ldots] \models \psi$, and for $0 \le i < j$:

* if $i = 0$: $\sigma[0\ldots] = \sigma \models \varphi$;
* if $1 \leq i \leq k$: $\sigma[i\ldots] = \sigma[1\ldots][i{-}1\ldots] \models \varphi$, because $0 \leq i{-}1 < k$.

So $j$ is a witness, and $\sigma \models \varphi \,\mathsf{U}\, \psi$.

Fundamentally, the original proof is easier and cleaner for me. This second proof is more messy, but perhaps more intuitive.

(e) $\Diamond\Box(\varphi \vee \psi) \equiv \Diamond\Box\varphi \vee \Diamond\Box\psi$

**Solution.** Not equivalent.

($\Leftarrow$) holds:

$$
\begin{array}{lll}
 & \sigma \models \Diamond\Box\varphi \vee \Diamond\Box\psi & \\
\iff & \sigma \models \Diamond\Box\varphi \;\vee\; \sigma \models \Diamond\Box\psi & [\vee] \\
\iff & (\exists i \geq 0.\ \forall j.\ \sigma[i+j\ldots] \models \varphi) \vee (\exists i \geq 0.\ \forall j.\ \sigma[i+j\ldots] \models \psi) & [\Diamond, \Box, \text{Suf}] \\
\iff & \exists i \geq 0.\ \big((\forall j.\ \sigma[i+j\ldots] \models \varphi) \vee (\forall j.\ \sigma[i+j\ldots] \models \psi)\big) & [\exists \text{ distributes over } \vee] \\
\implies & \exists i \geq 0.\ \forall j.\ (\sigma[i+j\ldots] \models \varphi \;\vee\; \sigma[i+j\ldots] \models \psi) & [\forall \text{ forward-contracts over } \vee] \\
\iff & \exists i \geq 0.\ \forall j.\ \sigma[i+j\ldots] \models \varphi \vee \psi & [\vee] \\
\iff & \sigma \models \Diamond\Box(\varphi \vee \psi) & [\Diamond, \Box, \text{Suf}]
\end{array}
$$

($\Rightarrow$) fails. Let $\sigma = (\{p\}\{q\})^\omega$ as in (c).

$$
\begin{array}{lll}
 & \sigma \models \Diamond\Box(p \vee q) & \\
\impliedby & \sigma[0\ldots] \models \Box(p \vee q) & [\Diamond; \text{witness } i := 0] \\
\impliedby & \sigma \models \Box(p \vee q) & [\text{Suf; shown in (c)}]
\end{array}
$$

$$
\begin{array}{lll}
 & \sigma \not\models \Diamond\Box p \vee \Diamond\Box q & \\
\impliedby & \forall i \geq 0.\ (\sigma[i\ldots] \not\models \Box p \;\wedge\; \sigma[i\ldots] \not\models \Box q) & [\vee, \Diamond] \\
\impliedby & \forall i \geq 0.\ (\sigma[i\ldots][i{+}1\ldots] \not\models p \;\wedge\; \sigma[i\ldots][i\ldots] \not\models q) & [\Box; \text{witnesses } j := i{+}1,\ j := i] \\
\impliedby & \forall i \geq 0.\ (p \notin A_{2i+1} \;\wedge\; q \notin A_{2i}) & [\text{At, Suf; def. } \sigma]
\end{array}
$$