CSE 541 - Logic in Computer Science

Solutions for Selected Exercises on Temporal Logic

Exercise 3.4.9

A CTL formula EFp is true for a state if p is true for that state already, wheras $EX\,EFp$ need not be true if p is true for the present state.

A formula AGp is true for a state s if, and only if, p is true for the present state s and all states reachable from s, wheras $AX\,AGp$ is true for s and if, and only if, it is true for all states reachable from s.

A formula $E[pUq]$ is true for a state if q is true for that state already. The formula $p \wedge EX\,E[pUq]$, on the other hand, requires that (i) q be true in a future state, not including the present state, and (ii) p be true in all preceding states, including the present state.

Exercise 3.4.10

a. $EF\,\phi$ and $EG\,\phi$ are not equivalent.

Let ϕ be p and $\mathcal{M}$ be a transition system with

States: $S = \{s_0, s_1\}$
Transitions: $s_0 \to s_1$, $s_1 \to s_1$
Labels: $L(s_0) = \{p\}$, $L(s_1) = \emptyset$

We have $\mathcal{M}, s_0 \models EF\,p$ but $\mathcal{M}, s_0 \not\models EG\,p$.

b. $EF\,\phi \vee EF\,\psi$ and $EF(\phi \vee \psi)$ are equivalent.

c. $AF\,\phi \vee AF\,\psi$ and $AF(\phi \vee \psi)$ are not equivalent.

Take $\phi = p$ and $\psi = q$ and let $\mathcal{M}$ be a transition system with

States: $S = \{s_0, s_1, s_2\}$
Transitions: $s_0 \to s_1$, $s_0 \to s_2$, $s_1 \to s_1$, $s_2 \to s_2$
Labels: $L(s_0) = \emptyset$, $L(s_1) = \{p\}$ $L(s_2) = \{q\}$

Then $\mathcal{M}, s_0 \models AF(p \vee q)$ but $\mathcal{M}, s_0 \not\models AF\,p \vee AF\,q$.

d. $AF\,\neg\phi$ is equivalent to $\neg EG\,\phi$.

e. $EF\,\neg\phi$ and $\neg AF\ \phi$ are not equivalent.

Take the same formula $\phi = p$ and transition system $\mathcal{M}$ as in 1(a). Then $\mathcal{M}, s_0 \models EF\,\neg p$ and $\mathcal{M}, s_0 \models AF\,p$ and hence $\mathcal{M}, s_0 \not\models \neg AF\,p$

f. $\psi = A[\phi_1\,U\,A[\phi_2\,U\,\phi_3]]$ and $\psi' = A[A[\phi_1\,U\,\phi_2]U\,\phi_3]$ are not equivalent.

Take $\phi_1 = p$, $\phi_2 = q$, and $\phi_3 = r$; and let $\mathcal{M}$ be a transition system with

States: $S = \{s_0, s_1\}$
Transitions: $s_0 \to s_1$, $s_1 \to s_1$
Labels: $L(s_0) = \{p\}$, $L(s_1) = \{r\}$

Then $\mathcal{M}, s_0 \models A[p\,U\,A[q\,U\,r]]$ but $\mathcal{M}, s_0 \not\models A[A[p\,U\,q]\,U\,r]$.

Also, let $\mathcal{M}'$ be a transition system with

States: $S = \{s_0, s_1, s_2, s_3, s_4\}$
Transitions: $s_0 \to s_1$, $s_1 \to s_2$, $s_2 \to s_3$, $s_3 \to s_4$, $s_4 \to s_4$
Labels: $L(s_0) = L(s_2) = \{p\}$, $L(s_1) = L(s_3) = \{q\}$, $L(s_4) = \{r\}$

Then $\mathcal{M}', s_0 \not\models A[p\,U\,A[q\,U\,r]]$ but $\mathcal{M}', s_0 \models A[A[p\,U\,q]\,U\,r]$.

g. $AG\,\phi \to EG\,\phi$ is equivalent to $\top$.

h. $EG\,\phi \to AG\,\phi$ is not equivalent to $\top$.

Let $\mathcal{M}$ be a transition system with

States: $S = \{s_0, s_1\}$
Transitions: $s_0 \to s_0$, $s_0 \to s_1$, $s_1 \to s_1$
Labels: $L(s_0) = \{p\}$, $L(s_1) = \emptyset$

Then $\mathcal{M}, s_0 \not\models EG\,p \to AG\,p$.

Exercise 3.4.11.

a. $AG(\phi \wedge \psi) \equiv AG\,\phi \wedge AG\,\psi$

b. $EF\,\neg\phi \equiv \neg AG\,\phi$

Exercise 3.4.13. Let $\mathcal{M}$ be a CTL model and s be a state of $\mathcal{M}$. Then

$s \models \neg AX\,\phi$
iff $s \not\models AX\,\phi$
iff *not* for all s' such that $s \to s'$ we have $s' \models \phi$
iff for some s' such that $s \to s'$ we have $s' \not\models \phi$
iff for some s' such that $s \to s'$ we have $s' \models \neg\phi$
iff $s \models EX\,\neg\phi$

This proves that $\neg AX\,\phi \equiv EX\,\neg\phi$.

Exercise 3.5.1. We express informal statements as formulas.

a. *Whenever p is followed by q (after finitely many steps), then the system enters an "interval" in which no r occurs until t.*

If "finitely many steps" means "zero or more steps," we may use

$$AG(p \to AG\,(q \to A[\neg r\,U\,t])).$$

If zero steps are not admissible, we get

$$AG(p \to AX\,AG\,(q \to A[\neg r\,U\,t])).$$

b. *Event p precedes s and t on all computation paths.*

We express this via negation, that it is not the case that on some computation path p does not precede s and t:

$$\neg E[\neg p\,U\,((s \vee t) \wedge \neg p)].$$

c. *After p, q is never true (on all computation paths).*

$$AG(p \to AX\,AG\,\neg q)$$

or

$$AG(p \to \neg EX\,EF\,q)$$

d. *Between the events q and r, p is never true (on all computation paths).*

$$[AG(q \to \neg EF\,(p \wedge EF\,r))] \wedge [AG(r \to \neg EF\,(p \wedge EF\,q))]$$

e. *Transitions to states satisfying p occur at most twice (on all computation paths).*

$$\neg(EX\,EF(p \wedge EX\,EF(p \wedge EX\,EF\,p)))$$

Exercise 3.5.3. Let ϕ_1 be the formula $Fp \to Fq$, ϕ_2 be $AFp \to AFq$, and ϕ_3 be $AG(p \to AFq)$.

(a) Let $\mathcal{M}$ be a transition system with

States: $S = \{s\}$
Transitions: $s \to s$
Labels: $L(s) = \emptyset$ (or $L(s) = \{q\}$)

Then $\mathcal{M}, s \not\models p$ and $\mathcal{M}, s \not\models AFp$, and consequently $\mathcal{M}, s \models A[\phi_1] \wedge \phi_2 \wedge \phi_3$.

(b) Let $\mathcal{M}$ be a transition system and s be a state in $\mathcal{M}$. First observe that if $Fp \to Fq$ is satisfied by all paths π starting at s and $\mathcal{M}, s \models AFp$, then $\mathcal{M}, s \models AFq$. In short, if ϕ_1 is satisfied by s, so is ϕ_2. Thus, ϕ_1 can not be the only formula satisfied $\mathcal{M}$.

Secondly, if $\mathcal{M}, s \models AG(p \to AFq)$, then $\mathcal{M}, s \models AFp \to AFq$, and hence ϕ_3 can not be the only formula satisfied either.

Finally, if $\mathcal{M}$ is a transition system with

States: $S = \{s_0, s_1, s_2\}$
Transitions: $s_0 \to s_1$, $s_0 \to s_2$, $s_1 \to s_1$, $s_2 \to s_2$
Labels: $L(s_0) = L(s_1) = \emptyset$ and $L(s_2) = \{p\}$

then $\mathcal{M}, s \not\models AFp$ and, hence, $\mathcal{M}, s_0 \models AFp \to AFq$. On the other hand, s_0 satisfies neither $Fp \to Fq$ (because the path $s_0 \to s_2 \to s_2 \cdots$ satisfies Fp but not Fq) nor $AG(p \to AFq)$ (because $s_0 \to s_2$ and s_2 satisifes p but not AFq). Thus, s_0 satisfies only ϕ_2 (but note that s_2 does not satisfy ϕ_2).

(c) Let $\mathcal{M}$ be a transition system with

States: $S = \{s\}$
Transitions: $s \to s$
Labels: $L(s) = \{p\}$

Then $\mathcal{M}, s \models p$ and $\mathcal{M}, s \models AFp$, but $\mathcal{M}, s \not\models AFq$. Since there is only one computation path in this system, we may conclude that s_0 satisfies none of the formulas $A[\phi_1]$, ϕ_2, and ϕ_3.

Exercise 3.5.4. In terms of the order of occurrences of events p, s, and t, the formula $AG(p \to AF(s \wedge AX(AF\,t)))$ expresses that event p is accompanied or followed by s, which in turn is followed by t.

Exercise 3.5.6.

a. See remark 3.18 on pp. 219-220.

b. $AG\,F\,p$ and $AG\,EF\,p$ are not equivalent.

Let $\mathcal{M}$ be a transition system with

States: $S = \{s_0, s_1\}$
Transitions: $s_0 \to s_0$, $s_0 \to s_1$, $s_1 \to s_1$
Labels: $L(s_0) = \emptyset$, $L(s_1) = \{p\}$

Then $\mathcal{M}, s_0 \models AG\,EF\,p$ but $\mathcal{M}, s_0 \not\models AG\,F\,p$.

c. $A[(pUr) \vee (qUr)]$ and $A[(p \vee q)Ur]$ are not equivalent.

Let $\mathcal{M}$ be a transition system with

States: $S = \{s_0, s_1, s_2\}$
Transitions: $s_0 \to s_1$, $s_1 \to s_2$, $s_2 \to s_2$
Labels: $L(s_0) = \{p\}$, $L(s_1) = \{q\}$, $L(s_2) = \{r\}$

Then $\mathcal{M}, s_0 \models A[(p \vee q)Ur]$ but $\mathcal{M}, s_0 \not\models A[(pUr) \vee (qUr)]$.

d. $A[Xp \vee XXp]$ and $AXp \vee AX\,AXp$ are not equivalent.

Let $\mathcal{M}$ be a transition system with

States: $S = \{s_0, s_1, s_2, s_3\}$
Transitions: $s_0 \to s_1$, $s_0 \to s_2$, $s_1 \to s_2$, $s_2 \to s_3$, $s_3 \to s_3$
Labels: $L(s_0) = L(s_2) = \emptyset$, $L(s_1) = L(s_3) = \{p\}$

Then $\mathcal{M}, s_0 \models A[Xp \vee XXp]$ but $\mathcal{M}, s_0 \not\models AXp \vee AX\,AXp$.

e. $E(G\,F\,p)$ and $EG\,EF\,p$ are not equivalent.

Let $\mathcal{M}$ be a transition system with

States: $S = \{s_0, s_1, s_2\}$
Transitions: $s_0 \to s_0$, $s_0 \to s_1$, $s_1 \to s_2$, $s_2 \to s_2$
Labels: $L(s_0) = L(s_2) = \emptyset$, $L(s_1) = \{p\}$

Then $\mathcal{M}, s_0 \models EG\,EF\,p$ but $\mathcal{M}, s_0 \not\models E(GF\,p)$.

Exercise 3.5.8

- We first show that $\neg q\,U\,(\neg p \wedge \neg q) \to \neg Gp$ is valid.

  Suppose $\pi \models \neg q\,U\,(\neg p \wedge \neg q)$. Then $\pi^i \models \neg p \wedge \neg q$, for some i. But if $\pi^i \models \neg p \wedge \neg q$, then $\pi^i \models \neg p$, and hence $\pi^i \not\models p$. Consequently, $\pi \not\models Gp$ and hence $\pi \models \neg Gp$. In sum, we may conclude that $\pi \models \neg q\,U\,(\neg p \wedge \neg q) \to \neg Gp$, for all paths π.

- We next show that $(G\neg q \wedge F\neg p) \rightarrow \neg q\, U\, (\neg p \wedge \neg q)$ is valid.

  Suppose $\pi \models G\neg q \wedge F\neg p$. Then $\pi \models G\neg q$ and $\pi \models F\neg p$. The latter assertion implies that $\pi^i \models \neg p$, for some i. Since $\pi \models G\neg q$ we obtain, in particular, that $\pi^j \models \neg q$ for all j with $j \leq i$. Thus, $\pi^i \models (\neg p \wedge \neg q)$ and $\pi \models \neg q\, U\, (\neg p \wedge \neg q)$. We conclude that $\pi \models (G\neg q \wedge F\neg p) \rightarrow \neg q\, U\, (\neg p \wedge \neg q)$, for all paths π.

- Using the above facts and basic propositional and LTL equivalences we obtain:

$$\begin{aligned}
&\neg((p\, U\, q) \vee Gp) \\
&\quad\equiv \neg(p\, U\, q) \wedge \neg Gp \\
&\quad\equiv [(\neg q\, U\, (\neg p \wedge \neg q)) \vee \neg Fq] \wedge \neg Gp \\
&\quad\equiv [(\neg q\, U\, (\neg p \wedge \neg q)) \wedge \neg Gp] \vee [\neg Fq \wedge \neg Gp] \\
&\quad\equiv [(\neg q\, U\, (\neg p \wedge \neg q)) \wedge \neg Gp] \vee [G\neg q \wedge F\neg p] \\
&\quad\equiv [\neg q\, U\, (\neg p \wedge \neg q)] \vee [G\neg q \wedge F\neg p] \\
&\quad\equiv \neg q\, U\, (\neg p \wedge \neg q) \\
&\quad\equiv \neg q\, U\, \neg(p \vee q)
\end{aligned}$$

Exercise 3.6.10. The assertion $s \models AG\, AF\, \phi$ means that ϕ is true infinitely often along every path starting at s.

Let π be an arbitrary path

$$s = s_1 \rightarrow s_2 \rightarrow \cdots \rightarrow s_n \rightarrow \cdots$$

starting at s.

First note that by the semantics of AG, from $s \models AG\, AF\, \phi$ we may infer that $s_i \models AF\, \phi$, for all $i \geq 1$. Thus, by the definition of AF, for each $i \geq 1$ there exists an index j with $i \leq j$, such that $s_j \models \phi$. Furthermore, whenever $s_j \models \phi$ there exists an index k with $j < k$, such that $s_k \models \phi$. (The latter observation follows from the fact that $s_{j+1} \models AF\, \phi$.)

Based on these assertions, we can inductively define an infinite sequence $k_1, k_2, \ldots$ such that $k_i < k_{i+1}$ and $s_{k_i} \models \phi$, for all $i \geq 1$. In other words, ϕ is true infinitely often along π.