Formal Methods in SE: Homework #2

Due on 2/14 at 11:59 a.m.

Professor Ciardo

Charles Dudley

Problem 1

a) $\mathcal{EF}(\overline{r_1} \wedge \overline{r_2})$
English: There exists a path where eventually neither `light_1` or `light_2` is red.
Safety or Liveness: Safety
$s_0 \not\models \mathcal{EF}(\overline{r_1} \wedge \overline{r_2})$

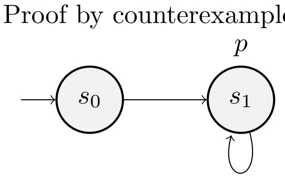
b) $\mathcal{AG}(\mathcal{AF}(g_1) \wedge \mathcal{AF}(g_2))$
English: On all paths it is always the case that `light_1` and `light_2` will be green infinitely often.
Safety or Liveness: Liveness
$s_0 \not\models \mathcal{EF}(\overline{r_1} \wedge \overline{r_2})$
Counterexample: $[s_0, s_1, s_1, \dots]$

c) $\mathcal{AG}((g_1 \Rightarrow \mathcal{A}(g_1 \mathcal{U} y_1)) \wedge (y_1 \Rightarrow \mathcal{A}(y_1 \mathcal{U} r_1)))$
English: On all paths it is always the case that if `light_1` is green then it will be green until it becomes yellow, and if `light_1` is yellow then it will be yellow until it becomes red.
Safety or Liveness: Safety
$s_0 \models \mathcal{AG}((g_1 \Rightarrow \mathcal{A}(g_1 \mathcal{U} y_1)) \wedge (y_1 \Rightarrow \mathcal{A}(y_1 \mathcal{U} r_1)))$

Problem 2

a) $\mathcal{AF}p \not\equiv \neg\mathcal{EF}p$

Proof by counterexample:



For this Kripke structure we clearly have $s_0 \models \mathcal{AF}p$, yet $s_0 \not\models \neg\mathcal{EF}p$. This demonstrates that these are not equivalent formulas.

b) $\mathcal{AX}(\mathcal{AG}(\phi)) \equiv \mathcal{AG}(\mathcal{AX}(\phi))$

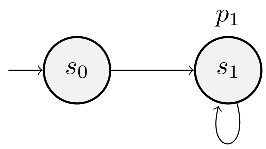
$$\begin{aligned} M, s \models \mathcal{AX}\phi &\Leftrightarrow \forall(p_0, p_1, \dots) \in Paths(s), p_1 \models \phi \\ \models \mathcal{AX}(\mathcal{AG}\phi) &\Leftrightarrow \forall(p_0, p_1, \dots) \in Paths(s), p_1 \models \mathcal{AG}\phi \\ \models \mathcal{AX}(\mathcal{AG}\phi) &\Leftrightarrow \forall(p_0, p_1, \dots) \in Paths(s), \forall i \geq 1, p_i \models \phi \end{aligned}$$

$$\begin{aligned} M, s \models \mathcal{AG}\phi &\Leftrightarrow \forall(p_0, p_1, \dots) \in Paths(s), \forall i \geq 0, p_i \models \phi \\ \models \mathcal{AG}(\mathcal{AX}\phi) &\Leftrightarrow \forall(p_0, p_1, \dots) \in Paths(s), \forall i \geq 0, p_i \models \mathcal{AX}\phi \\ \models \mathcal{AG}(\mathcal{AX}\phi) &\Leftrightarrow \forall(p_0, p_1, \dots) \in Paths(s), \forall i \geq 1, p_i \models \phi \end{aligned}$$

c) $\mathcal{A}(p_0 \mathcal{U} \mathcal{AX}(p_1)) \not\equiv p_0 \wedge \mathcal{AX}(\mathcal{A}(p_0 \mathcal{U} p_1))$

Problem 2 continued on next page...

Proof by counterexample:



For this Kripke structure we clearly have $s_0 \vDash \mathcal{AX}p_1$, therefore we have $s_0 \vDash \mathcal{A}(p_0 \mathcal{U} \mathcal{AX}(p_1))$, regardless of p_0. We also have $s_0 \nvDash p_0$, therefore $s_0 \nvDash (p_0 \wedge \mathcal{AX}(\mathcal{A}(p_0 \mathcal{U} p_1)))$. This demonstrates that these are not equivalent formulas.

Problem 3

a) If $\mathcal{AF}(\mathcal{AG}\neg p)$ holds in $s \in S$, then p appears finitely many times in the computation tree of s.

The statement "p appears finitely many times in the computation tree of s" can be rewritten as

$$\neg \mathcal{EG}(\mathcal{EF}p)$$

Then the problem statement may be translated into the implication

$$\mathcal{AF}(\mathcal{AG}\neg p) \Rightarrow \neg \mathcal{EG}(\mathcal{EF}p)$$

Let us assume, for contradiction, that we have the negation of this implication

$$\mathcal{AF}(\mathcal{AG}\neg p) \wedge \neg(\neg \mathcal{EG}(\mathcal{EF}p))$$

This formula can be rewritten as

$$\begin{aligned} \mathcal{AF}(\mathcal{AG}\neg p) &\equiv \mathcal{AF}(\neg \mathcal{EF}p) && (1) \\ &\equiv \neg \mathcal{EG}(\mathcal{EF}p) && (2) \end{aligned}$$

$$\begin{aligned} \neg(\neg \mathcal{EG}(\mathcal{EF}p)) &\equiv \mathcal{EG}(\mathcal{EF}p) && (3) \\ &\equiv \mathcal{EG}(\mathcal{EF}p) && (4) \end{aligned}$$

$$\mathcal{AF}(\mathcal{AG}\neg p) \wedge \neg(\neg \mathcal{EG}(\mathcal{EF}p)) \equiv \neg \mathcal{EG}(\mathcal{EF}p) \wedge \mathcal{EG}(\mathcal{EF}p) \quad (5)$$

The resulting formula $\neg \mathcal{EG}(\mathcal{EF}p) \wedge \mathcal{EG}(\mathcal{EF}p)$ is clearly unsatisfiable. Therefore we have reached a contradiction. Thus, the assumption that $\mathcal{AF}(\mathcal{AG}\neg p) \wedge \neg(\neg \mathcal{EG}(\mathcal{EF}p))$ was incorrect, implying that $\mathcal{AF}(\mathcal{AG}\neg p) \Rightarrow \neg \mathcal{EG}(\mathcal{EF}p)$ holds.

b) $\forall (p_0, p_1 \ldots) \in Paths(s), p_i \vDash p$ if i is even

This statement is false. CTL gives us the $\mathcal{X}$ operator, which allows us to count any number of steps ahead, but it is impossible for a state to determine whether or not it is even itself.

Problem 4

a) The English translation of this formula is the problem definition of a $win - state$.