The Exam

Problem 1: Model Checking

(20 points) Consider the labeled transition system below where each state is labeled with the set of atomic propositions that hold true in it.

Answer the two questions below, but keep in mind that a wrong answer carries a negative weight. For example, “correct answer 1, correct answer 2” will get more marks than “correct answer 1, correct answer 2, incorrect answer 1”. Otherwise, you can just list all states for every item, and you are guaranteed to include all correct answers! No justification is necessary. We will only mark the list of states.

(a) List the states that satisfy the LTL formula $\neg \square (a \lor b)$.

$q_0$

(b) List the states that satisfy the CTL formula $\exists (b \lor \forall (a \lor c))$.

$q_2, q_3, q_4$
Problem 2: LTL

(25 points) For arbitrary LTL formulas $\phi$ and $\psi$:

(a) Prove or disprove $\phi U (\phi \rightarrow \psi) \equiv (\phi U \psi)$, with the appropriate formal justification.

Let $\phi = a$ and $\psi = b$ for atomic propositions $a$ and $b$. The following path is a counterexample to $\phi U (\phi \rightarrow \psi) \implies (\phi U \psi)$

$$\pi : \neg a \land \neg b \longrightarrow \neg a \land \neg b \longrightarrow \ldots \longrightarrow \neg a \land \neg b \longrightarrow \ldots$$

Since $\pi \models a U (a \rightarrow b)$ and $\pi \not\models (a U b)$.

(b) Prove or disprove $\Diamond \Box \phi \land \Box \Diamond \psi \equiv \Diamond \Box (\phi \land \psi)$, with the appropriate formal justification.

$$\pi \models \Diamond \Box \phi \land \Box \Diamond \psi \iff \left(\exists i : \forall j \geq i : \pi[j] \models \phi \wedge \Box \pi[j] \models \psi\right) \iff \text{(Let } i, k = m \text{ for the backward direction.)}$$

$$\exists m : \forall j \geq m : \pi[j] \models \phi \land \psi \iff \left(\exists m : \max(i, k) \text{ for the forward direction.}\right)$$

Note: the above proof is ever so slightly sloppy, since we are short-circuiting both directions and use each justification given in a different direction. If we write the two directions separately, then we get the cleanest way. But, this level of sloppiness is fine, because anyone with mathematical maturity would immediately understand the precise proof in both directions. There exists no leap in reasoning.

(c) (15 points) Formalize the following English specification as an LTL formula. You may use the following atomic propositions $\{req_1, res_1, req_2, res_2\}$. “The system has two clients and wants to be fair to them. Every time it receives a request from a client, it will eventually issue a response to that client. Moreover, it will treat the clients in a first-in-first-served manner; that is, it will first respond to the client that made their request first. The clients also act fairly by not issuing a subsequent request to the system if the system has not yet responded to their previous request yet.”. For simplicity, assume that no two request or response events can simultaneously happen at the same time. Therefore, the system will see at most one of the aforementioned atomic propositions as true at any given state.

$$\Diamond (\begin{align*}
(req_1 & \implies \Box (\neg req_1 U res_1)) \land \\
(req_2 & \implies \Box (\neg req_2 U res_2)) \land \\
(req_1 \land \Box (\neg res_1 U req_2)) & \implies \Box (\neg res_2 U res_1) \land \\
(req_2 \land \Box (\neg res_2 U req_1)) & \implies \Box (\neg res_2 U res_1)
\end{align*})$$

Problem 3: CTL

(a) (10 points) Prove or disprove $\neg \forall (\phi U \psi) \equiv \exists (\neg \psi U \neg \phi)$, with the appropriate formal justification.

Let $\phi = a$ and $\psi = b$ for atomic propositions $a$ and $b$. The following transition system or the corresponding tree are both counterexamples to $\exists (\neg \psi U \neg \phi) \implies \neg \forall (\phi U \psi)$:
since it satisfies $\exists (\neg \psi \ U \neg \phi) = \exists (\neg b \ U \neg a)$ but not $\neg \forall (\phi \ U \psi) = \neg \forall (a \ U \ b)$

(b) (10 points) Formalize the following English specification as a CTL formula using the atomic propositions $\{\text{req, acc, den}\}$: “Every time the system receives a request, the following three choices are available to it: it can immediately deny it in the next step, immediately accept it in the next step, or ignore it. But, if ignored, no future acceptances or denials should be issued.”. Note that ignoring a request means that neither an acceptance or a denial is issued in the next step. Hence, you may not assume that $\neg \text{acc} \rightarrow \text{den}$ and vice versa.

$$\forall \square (\text{req} \implies (\exists \bigcirc \text{acc} \land \exists \bigcirc \text{den} \land \exists \bigcirc \forall \square (\neg \text{acc} \land \neg \text{den})))$$

Problem 4: Fixed Points and Invariants

(20 points) This problem is the only nonstandard one in this exam. It is not difficult or complicated, but you have not seen something exactly like it in homework or class. It is there to let the students who gained a deep understanding the course material shine.

Consider a (potentially infinite) grid, and two players $P_1$ and $P_2$ playing a game of tag on it. At each clock tick, each player (simultaneously) makes a move to a neighbouring cell; that is, the cell above, below, to the left or to the right of the current cell (and not the diagonal neighbours). $P_1$ is chasing $P_2$ and the game will end, if $P_1$ and $P_2$ will eventually occupy the same cell. The goal of to show that starting from the configuration below, no matter how cleverly $P_1$ plays or how stupidly $P_2$ plays, $P_1$ will never catch $P_2$ and the game never ends.

You will show this through the following steps.

(a) Consider the coloured grid below. The colouring in the grid is the clue to solving this problem.
Let $p_1$ (respectively $p_2$) be the atomic propositions that indicate that the player $P_1$ (respectively $P_2$) is in a white cell. Naturally $\neg p_1$ then indicates that the player is in a black cell. Explain in short clean English why any play of the above game satisfies the LTL formula below. This is the only place in this example that English will be graded, because we are not looking for a formal argument but a clean informal one.

$$p_1 \land \neg p_2 \land \Box((p_1 \implies \Box \neg p_1) \land (\neg p_1 \implies \Box p_1) \land (p_2 \implies \Box \neg p_2) \land (\neg p_2 \implies \Box p_2))$$

Originally, player $P_1$ is in a white cell and player $P_2$ is in a black cell, an hence any play will satisfy $p_1 \land \neg p_2$. The structure of the grid dictates that all neighbours of a white cell are black and all neighbours of a black cell are white. Therefore, each player, will have to change the colour of its cell with every move. Hence each play satisfies:

$$\Box((p_1 \implies \Box \neg p_1) \land (\neg p_1 \implies \Box p_1))$$

and

$$\Box((p_2 \implies \Box \neg p_2) \land (\neg p_2 \implies \Box p_2))$$

Putting all three together and using the LTL equality $\Box(\phi \land \psi) \equiv \Box \phi \land \Box \psi$, we will get the desired result.

(b) Formally argue why assuming the above formula holds for all possible plays, we can then prove that the formula below holds for all possible plays:

$$\Box(p_1 \iff \neg p_2)$$

Below, you will see one of the many ways to structure this as a formal argument. There are other ones. Their key thing is the induction argument. You get the proof of the base case as a direct implication of the formula from part (a). You get the induction step proved, by referring to the same formula and the formal semantics of the the next ($\Box$) operator.

Let $\pi$ be an arbitrary play of the game. The goal is to prove:

$$\forall \pi : \pi \models \Box(p_1 \iff \neg p_2)$$

$$\iff \forall i \geq 0 : \pi[i] \models (p_1 \iff \neg p_2)$$

We prove the latter by induction on $i$. We start with our assumption:

$$\forall \pi : \pi \models p_1 \land \neg p_2 \land \Box((p_1 \implies \Box \neg p_1) \land (\neg p_1 \implies \Box p_1) \land (p_2 \implies \Box \neg p_2) \land (\neg p_2 \implies \Box p_2))$$

$$\implies \forall \pi : \pi[0] \models p_1 \land \neg p_2 \land \pi \models \Box((p_1 \implies \Box \neg p_1) \land (\neg p_1 \implies \Box p_1) \land (p_2 \implies \Box \neg p_2) \land (\neg p_2 \implies \Box p_2))$$

So far, we have $\pi[0] \models p_1 \land \neg p_2$ which implies $\pi[0] \models p_1 \iff \neg p_2$. Therefore, the base case holds.

Assume by induction hypothesis:

$$\forall i < n : \pi[i] \models (p_1 \iff \neg p_2)$$
and we will prove $\pi[n] \models (p_1 \iff \neg p_2)$. Continuing with our assumption:

$$
\forall i \geq 0 : \pi[i] \models ((p_1 \implies \circ \neg p_1) \land (\neg p_1 \implies \circ p_1) \land (p_2 \implies \circ \neg p_2) \land (\neg p_2 \implies \circ p_2))
$$

$\Rightarrow \pi[n - 1] \models ((p_1 \implies \circ \neg p_1) \land (\neg p_1 \implies \circ p_1) \land (p_2 \implies \circ \neg p_2) \land (\neg p_2 \implies \circ p_2))$

$\Rightarrow \pi[n - 1] \models (p_1 \iff \neg p_2) \land (\text{by induction hypothesis})$

$\Rightarrow \pi[n - 1] \models ((p_1 \implies \circ \neg p_1) \land (\neg p_1 \implies \circ p_1) \land (p_2 \implies \circ \neg p_2) \land (\neg p_2 \implies \circ p_2)) \land$

$\Rightarrow \pi[n - 1] \models (p_1 \iff \neg p_2) \land (\text{by induction hypothesis})$

$\Rightarrow \pi[n - 1] \models (p_1 \iff \neg p_2) \land (\text{true is always satisfied})$

$\Rightarrow \pi[n - 1] \models (p_1 \iff \circ (\circ p_2 \lor \circ \neg p_1)) \lor (\neg p_1 \iff (\circ \neg p_2 \lor \circ p_1))$

$\Rightarrow \pi[n - 1] \models (\circ p_2 \lor \circ \neg p_1) \lor (\circ \neg p_2 \lor \circ p_1) \lor (\text{by binary resolution})$

$\Rightarrow \pi[n] \models (\neg p_2 \lor \neg p_1) \lor (p_2 \lor p_1)$

(c) With a very short English explanation, conclude why player $P_1$ can never catch player $P_2$.

If $P_1$ catches $P_2$, then at that step the two have to be both in a white cell or both in a black cell. Since the property proved in (b) says the colours never agree, this cannot happen.