CSC410

Exam 3

Date: November 13, 2026
weight: 17% of course mark, length: 60 minutes

First Name: _____

Last Name: _____

Student Number: _____

Read Before You Start

- Write your name and student number, and please do it so that it matches your record on Quercus.
- This exam contains **5 problems** (with multiple subproblems). The idea with this exam was to make the weight of any one part very small, so that mistakes do not cost you much, but then you have many short answers to write instead. Pace yourself accordingly. **If an answer does not come to you quickly, move on to the next question.**
- There is an extra (un-numbered) problem for graduate students only. Undergraduate students need not answer this problem.
- The exam totals 41 points for undergraduate students and 47 points for graduate students.
- Unless explicitly asked for "justifications", you do not need to justify your answers.
- The exam is designed so that the answers require **no English** words. You are welcome to write English sentences, but be warned that they will not be graded. Only the formal components required for each answer are graded.
- The exam may look long, but all questions (with the exception of proofs) have very very short answers. The estimate is that you should not need more than 40 minutes, but you get 60 minutes to do the work carefully!

Problem 1: LTL and CTL Specifications (10 points)

(a) (3 points) The system under consideration is about the movements of a *drone*. We use the atomic proposition *lo* to indicate that the drone's battery is low, and *ch* to indicate that it is connected to its charger. Consider this specification in English:

> *Whenever the battery is low, it stays low until the drone is connected to the charger, which is guaranteed to eventually happen.*

For each candidate F_i in the table below, circle $\Longrightarrow$ if F_i is strictly stronger than the specification above, and $\Longleftarrow$ if it is strictly weaker than it, and $\equiv$ if it is equivalent to it.

F_1	$\square(lo \implies \Diamond ch)$	$\equiv$	$\Longrightarrow$	$\Longleftarrow$
F_2	$\square(lo \,\mathsf{U}\, ch)$	$\equiv$	$\Longrightarrow$	$\Longleftarrow$
F_3	$\square(lo \implies (lo \,\mathsf{U}\, ch))$	$\equiv$	$\Longrightarrow$	$\Longleftarrow$

Answer.

F_1	$\square(lo \implies \Diamond ch)$	$\equiv$	$\Longrightarrow$	$\boxed{\Longleftarrow}$
F_2	$\square(lo \,\mathsf{U}\, ch)$	$\equiv$	$\boxed{\Longrightarrow}$	$\Longleftarrow$
F_3	$\square(lo \implies (lo \,\mathsf{U}\, ch))$	$\boxed{\equiv}$	$\Longrightarrow$	$\Longleftarrow$

(b) Now switch gears to an online shop, where we use atomic propositions *paid* and *cancel* to stand for the corresponding English meanings wrt a unique order for this question. Write the CTL formula that precisely corresponds to the following English specifications:

(i) (3 points) In every reachable state, the client has at least one of the following options: pay for the order in the future or cancel it in the future.

Answer. $\forall\square(\exists\Diamond paid \vee \exists\Diamond cancel)$, or equivalently $\forall\square\exists\Diamond(paid \vee cancel)$

(ii) (4 points) On every execution, until an order is *paid* (which is guaranteed to happen in the future), a cancellation is always possible in the next step.

Answer. $\forall(\exists\bigcirc cancel \,\mathsf{U}\, paid)$.

Problem 2: Model Checking (8 points)

Consider the two transition systems below, where s_0/t_0 are the respective initial states.



For each temporal logic (i.e. LTL and CTL), give a formula F that holds for one transition system but not the other, and vice versa. So, you are expected to provide 4 formulas in total (write "none" if there is no such formula):

- an LTL formula that holds for the left but not for the right:

  Answer. $\Box(a \implies \bigcirc\neg a)$

- an LTL formula that holds for the right but not for the left:

  Answer. None! The right transition system has strictly more paths than the left one.

- a CTL formula that holds for the left but not for the right:

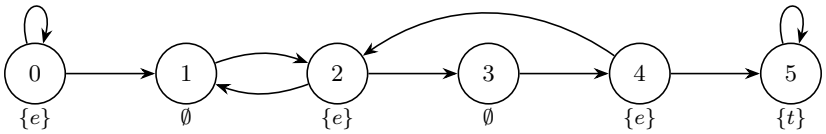
  Answer. $\forall\Box(a \implies \forall\bigcirc\neg a)$

- a CTL formula that holds for the right but not the left:

  Answer. $\exists\Box a$

Problem 3: CTL Model Checking (9 points)

Consider the transition system below on states $S = \{0, 1, 2, 3, 4, 5\}$.



List the set of states satisfying each formula in front of it.

(a) $\exists\bigcirc\forall\bigcirc e$:

Answer. 0,2

$\forall\bigcirc e$ is satisfied by 1 and 3, $\exists\bigcirc\{1, 3\}$ is {0,2} because those are the states with a successor in $\{1, 3\}$.

(b) $\forall\Diamond\exists(e \,\mathsf{U}\, t)$:

Answer. 3,4,5

$\exists(e \,\mathsf{U}\, t)$ is satisfied by $\{4, 5\}$, and $\forall\Diamond\{4, 5\}$ yields $\{3, 4, 5\}$. Naturally, 0,1, and 2 are excluded because they all have a path that can get trapped in the cycle between 1 and 2.

(c) $\exists\Box(e \implies \forall\bigcirc(\neg e \vee t))$:

Answer. 1, 2, 5

$(e \implies \forall\bigcirc(\neg e \vee t))$ is satisfied by $\{1, 3, 5\}$ trivially because e does not hold. It is also satisfied by 2, because it satisfies e and all the successors do not. It is not satisfied by 0 or 4, because at least one successor does satisfy e but not t. Hence, $\exists\Box(e \implies \forall\bigcirc(\neg e \vee t))$ is satisfied by any state from which there is a path that stays within the set $\{1, 2, 3, 5\}$. This means 1, 2, and 5.

Note: The justifications above are given for your benefit and are not required for a full mark. For grading, we cannot simply reward "correct" states. If so, a clever student may write all 6 states as answer to all questions and they are bound to hit all the right answers. So, while grading, we will have to penalize wrong states.

Problem 4: Model Checking Algorithms and Fixpoints (4 points)

(a) (2 points) Consider the following algorithm A for computing $\mathrm{Sat}(X)$ in variable T:

1. Start with $T := \mathrm{Sat}(p)$
2. While for some $s \in T$ we have $\mathrm{Post}(s) \not\subseteq T$, remove s from T.

Which CTL property is X?

Answer. $\forall\Box p$

(b) (2 points) Now consider the following algorithm B for computing $\mathrm{Sat}(Y)$ in variable T, where S is the set of all states in the transition system:

1. Start with $T := \mathrm{Sat}(X)$ (as computed above by algorithm A).
2. While for some $s \in S - T$ we have
   (i) $\mathrm{Post}(s) \subseteq T$, **and**
   (ii) $s \in \mathrm{Sat}(q)$,
   then add s to T.

Which CTL property is Y?

Answer. $\forall(q \,\mathsf{U}\, \forall\Box p)$

Problem 5: LTL Equivalences (10 points)

Prove or disprove the following claimed equalities. For disproving, it suffices to give a counterexample. To prove, we expect to see a formal proof (no English) for a full mark. If you are not comfortable with that, then you may write a **brief** high-level (yet precise) argument in English *for partial credit.*

(a) $p \mathsf{U} (q \vee r) \equiv (p \mathsf{U} q) \vee (p \mathsf{U} r)$.

(b) $(p \vee q) \mathsf{U} r \equiv (p \mathsf{U} r) \vee (q \mathsf{U} r)$.

Answer. (a) (7 points) Equivalent. Let $P(j) :\equiv \forall i.\ 0 \le i < j \to \sigma[i \ldots] \models p$.

$$
\begin{array}{lll}
 & \sigma \models p \mathsf{U} (q \vee r) & \\
\iff & \exists j \ge 0.\ (\sigma[j \ldots] \models (q \vee r) \wedge P(j)) & [\mathsf{U};\ \text{def. } P] \\
\iff & \exists j \ge 0.\ \big((\sigma[j \ldots] \models q \vee \sigma[j \ldots] \models r) \wedge P(j)\big) & [\vee] \\
\iff & \exists j \ge 0.\ \big((\sigma[j \ldots] \models q \wedge P(j)) \vee (\sigma[j \ldots] \models r \wedge P(j))\big) & [\wedge \text{ distributes over } \vee] \\
\iff & \big(\exists j \ge 0.\ \sigma[j \ldots] \models q \wedge P(j)\big) \vee \big(\exists j \ge 0.\ \sigma[j \ldots] \models r \wedge P(j)\big) & [\exists \text{ distributes over } \vee] \\
\iff & \sigma \models p \mathsf{U} q \vee \sigma \models p \mathsf{U} r & [\mathsf{U};\ \text{def. } P] \\
\iff & \sigma \models (p \mathsf{U} q) \vee (p \mathsf{U} r) & [\vee]
\end{array}
$$

Example of proper English explanation that would get 5/7 marks:

Assume $\sigma \models p \mathsf{U} (q \vee r)$, then $(q \vee r)$ will become true in the future of σ and meanwhile p remains true. There are two possibilities for $(q \vee r)$ becoming true:

1. *q becomes true: this case implies that p remains true until q becomes true, hence $\sigma \models p \mathsf{U} q$.*
2. *r becomes true: this case implies that p remains true until r becomes true, hence $\sigma \models p \mathsf{U} r$.*

Combining the two case splits, we will have: $\sigma \models (p \mathsf{U} q) \vee (p \mathsf{U} r)$.

Assume $\sigma \models (p \mathsf{U} q) \vee (p \mathsf{U} r)$, then by the semantics of $\vee$ we have $\sigma \models (p \mathsf{U} q)$ or $\sigma \models (p \mathsf{U} r)$.

1. *Case 1: $\sigma \models (p \mathsf{U} q)$: then q becomes true in futre of σ and p remains true meanwhile. If q becomes true, then $q \vee r$ becomes true. Hence $\sigma \models p \mathsf{U} (q \vee r)$.*
2. *Case 2: similar to case 1.*

Since both cases guarantee the same outcome, we can conclude: $\sigma \models p \mathsf{U} (q \vee r)$.

(b) (3 points) Not equivalent. ($\Rightarrow$) fails. Let $\sigma = \{p\}\{q\}\{r\}\emptyset^\omega$, that is, $\emptyset$ holds for the rest of the infinite traces.

We have $\sigma \models (p \vee q) \mathsf{U} r$, since $p \vee q$ remains true until r becomes true, but $\sigma \not\models (p \mathsf{U} r) \vee (q \mathsf{U} r)$ because neither disjunct holds true.

(Empty page to continue with the solution of Problem 5 if you need more space)

Graduate Students Only (6 points)

The *temporal depth* of a formula is the largest number of temporal operators nested inside one another. For example, $\Box\Diamond p$ has depth 2 and $\forall\Box a \wedge \exists\Diamond b$ has depth 1.

For each formula, write an equivalent formula, in the same temporal logic, of strictly smaller temporal depth.

	Formula	Equivalent of smaller depth
(a)	$(\Box p)\ \mathsf{U}\ q$	**Answer.** $q \vee (\Box p \wedge \Diamond q)$
(b)	$\Box(p \implies \bigcirc\Diamond p)$	**Answer.** $\Diamond p \implies \Box\Diamond p$
(c)	$\exists(b\ \mathsf{U}\ \exists\Diamond a)$	**Answer.** $\exists\Diamond a$

CTL Semantics

$s \models a$ iff $a \in L(s)$

$s \models \neg \Phi$ iff not $s \models \Phi$

$s \models \Phi \wedge \Psi$ iff $(s \models \Phi)$ and $(s \models \Psi)$

$s \models \exists \varphi$ iff $\pi \models \varphi$ for some $\pi \in Paths(s)$

$s \models \forall \varphi$ iff $\pi \models \varphi$ for all $\pi \in Paths(s)$

$\pi \models \bigcirc \Phi$ iff $\pi[1] \models \Phi$

$\pi \models \Phi \mathsf{U} \Psi$ iff $\exists j.\ \pi[j] \models \Psi \wedge \forall 0 \leq k < j.\ \pi[k] \models \Phi$

LTL Semantics

$\sigma \models \text{true}$

$\sigma \models a$ iff $a \in A_0$ (i.e., $A_0 \models a$)

$\sigma \models \varphi_1 \wedge \varphi_2$ iff $\sigma \models \varphi_1$ and $\sigma \models \varphi_2$

$\sigma \models \neg \varphi$ iff $\sigma \not\models \varphi$

$\sigma \models \bigcirc \varphi$ iff $\sigma[1 \ldots] = A_1 A_2 A_3 \ldots \models \varphi$

$\sigma \models \varphi_1 \mathsf{U} \varphi_2$ iff $\exists j \geqslant 0.\ \sigma[j \ldots] \models \varphi_2$ and $\sigma[i \ldots] \models \varphi_1$, for all $0 \leqslant i < j$

$\sigma \models \Box \varphi$ iff $\forall i.\ \sigma[i...] \models \varphi$

$\sigma \models \Diamond \varphi$ iff $\exists i \geq 0.\ \sigma[i...] \models \varphi$