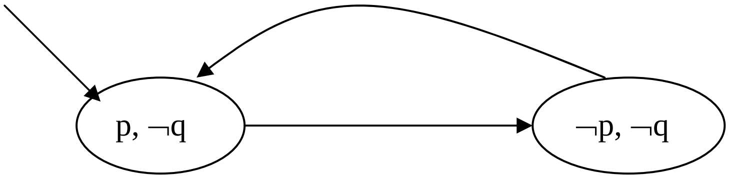
Formal Methods & Verification
Final Exam

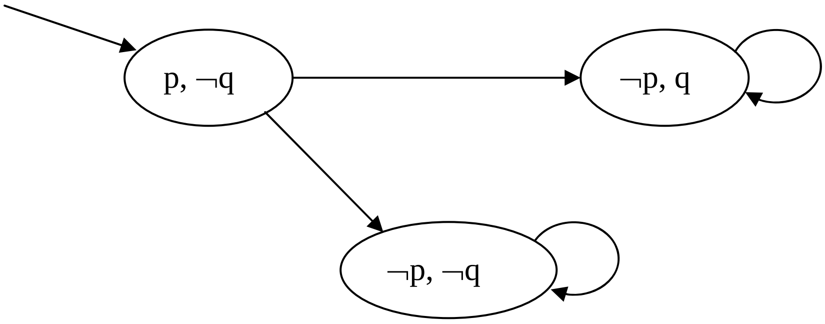
Instructor: Farn Wang
Class hours: 9:10-12:00 Tuesday Course Nr. 921 U7600
Room: BL 103 Spring 2008

Student name: Student ID:

1. Please construct a tree that can tell an LTL formula □(p⇒◇q) from another (□p) ⇒◇q. If you think there is no such a tree (or a Kripke structure that rolls out to a tree), please prove that there is no such a tree. (10/10)



2. Please construct a tree that can tell a CTL formula ∀□(p⇒∃◇q) from another ∀□(p⇒∀◇q). If you think there is no such a tree (or a Kripke structure that rolls out to a tree), please prove that there is no such a tree. (10/20)



3. Please construct a tree (or a Kripke structure that rolls out to a tree) that can tell $\forall\Box(p\Rightarrow\forall\Diamond q)$ from $\forall\Box(p\Rightarrow\Diamond q)$. If you think there is no such a tree, please prove that there is no such a tree. (10/30)

Proof:

We want to prove that no such a tree exists.

We first assume that there is a tree that does not satisfy $\forall\Box(p\Rightarrow\Diamond q)$. This implies that in the tree, there is a path ρ in the tree such that the head of ρ satisfies p while no states in ρ satisfy q. It is easy to see that that the head of ρ does not satisfy $\forall\Diamond q$. This implies that the tree does not satisfy $\forall\Box(p\Rightarrow\forall\Diamond q)$.

We then assume that there is a tree that does not satisfy $\forall\Box(p\Rightarrow\forall\Diamond q)$. This implies that there is a state υ in the tree such that υ satisfies p but does not satisfy $\forall\Diamond q$. This again implies that there is a path ρ from υ such that all states in ρ do not satisfy q. Then we also know that ρ does not satisfy $p\Rightarrow\Diamond q$ either. This again implies the path of the concatenation of the following two segments

- the finite path from the root of the tree to υ and
- ρ

does not satisfy $\Box(p\Rightarrow\Diamond q)$. This implies that the tree does not satisfy $\forall\Box(p\Rightarrow\Diamond q)$.

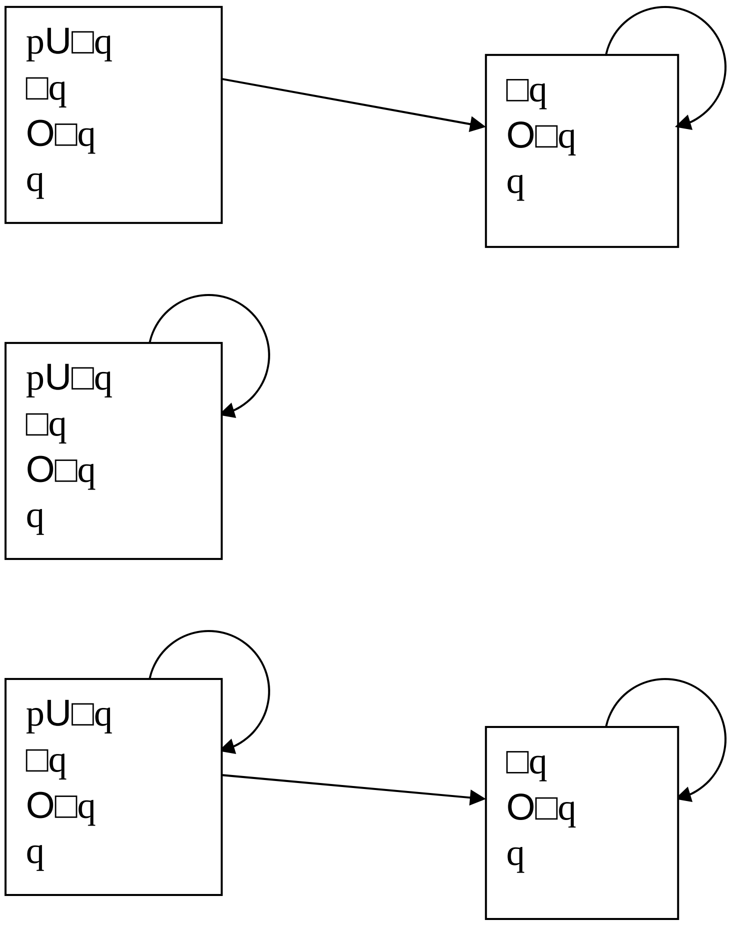
Thus there is no such a tree that can tell $\forall\Box(p\Rightarrow\forall\Diamond q)$ from $\forall\Box(p\Rightarrow\Diamond q)$.

Q.E.D.

4. Consider the tableau for an LTL formula pU□q. Please identify a structure in the tableau that proves the satisfiability of the formula. (10/40)

closure(pU□q)={ pU□q, p, □q, OpU□q, O□q, q}

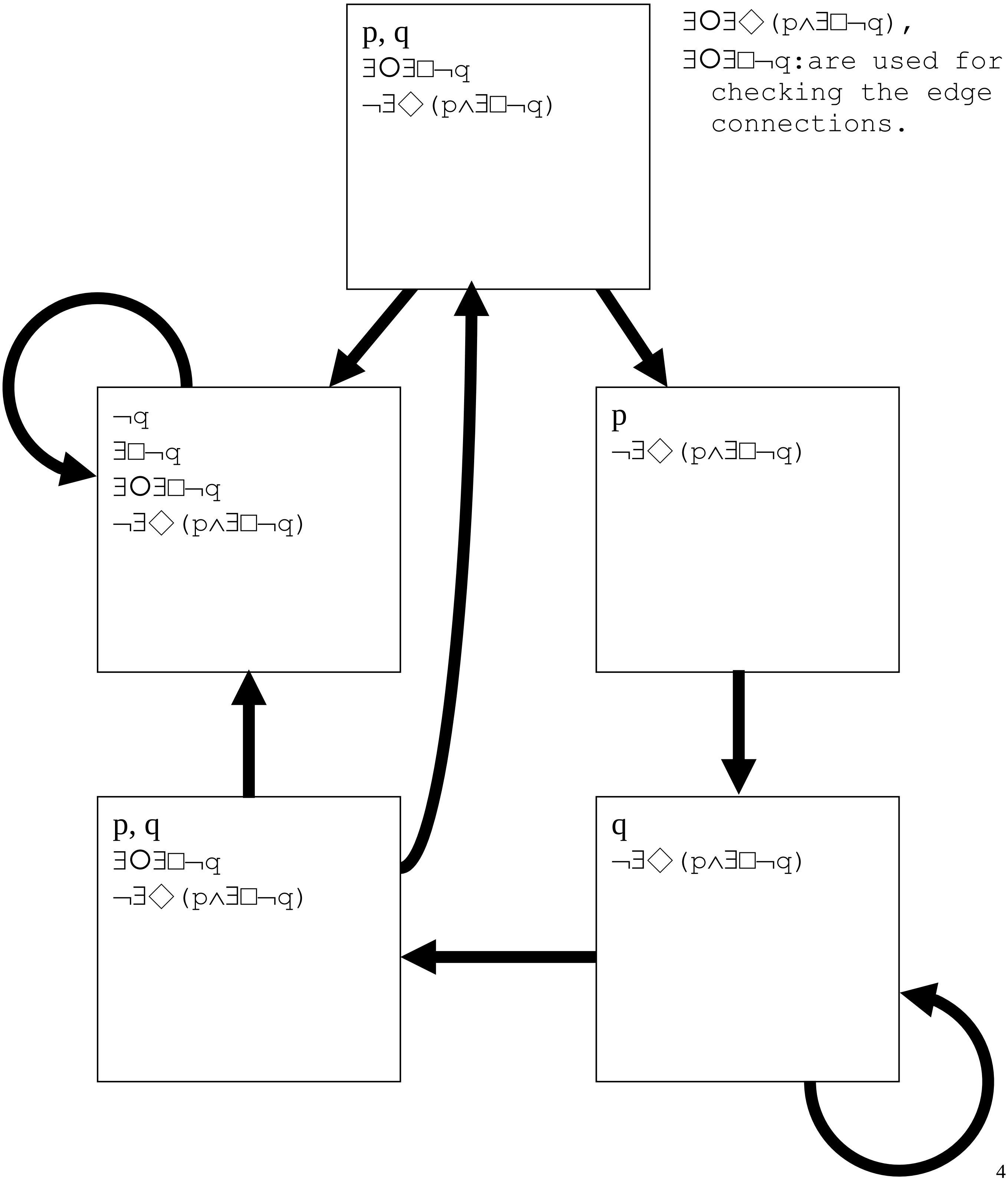
Some structures that can be used as the answer.



5. Please do labeling algorithm of CTL formula $\forall\Box(p\Rightarrow\forall\Diamond q)$ on the following automata. (The formula is already the negation of the specification.) (10/50)

Conversion to normal form: $\neg\exists\Diamond(p\wedge\exists\Box\neg q)$

Closure($\neg\exists\Diamond(p\wedge\exists\Box\neg q)$)={ $\neg\exists\Diamond(p\wedge\exists\Box\neg q)$, $\exists\Diamond(p\wedge\exists\Box\neg q)$, $\exists\bigcirc\exists\Diamond(p\wedge\exists\Box\neg q)$, $p\wedge\exists\Box\neg q$, p, $\exists\Box\neg q$, $\exists\bigcirc\exists\Box\neg q$, $\neg q$, $\neg p$, q }



$\exists\bigcirc\exists\Diamond(p\wedge\exists\Box\neg q)$, $\exists\bigcirc\exists\Box\neg q$: are used for checking the edge connections.

6. Please draw a communicating timed automata (CTA) with the following properties. (10/60)

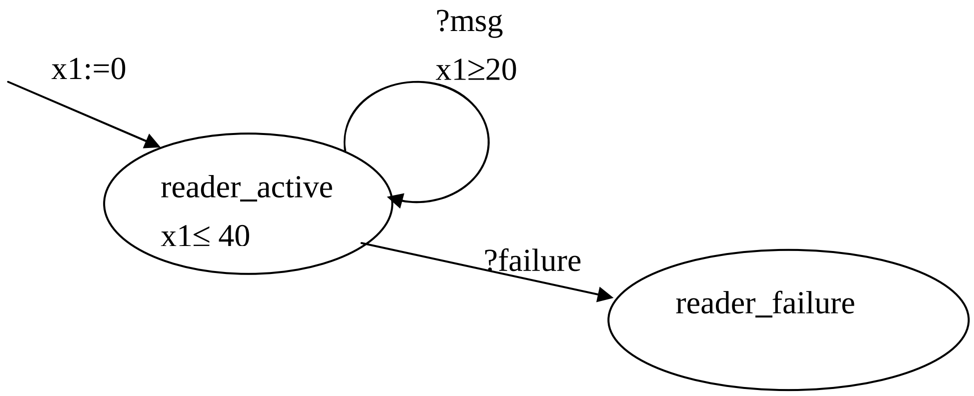
(a) There are two timed automatas, a reader and a writer, in this CTA that communicate with an event **msg.**

(b) The writer sends out an event **msg** in every 30 to 50 time units.

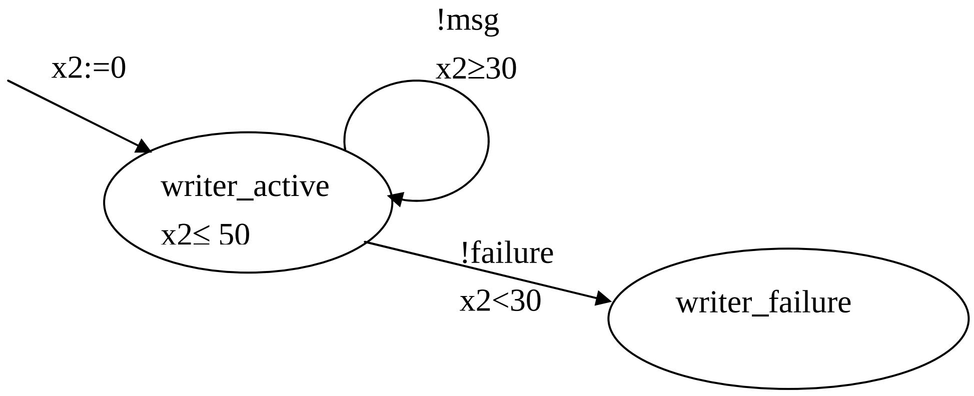
(c) The reader receives an event **msg** in every 20 to 40 time units.

(d) If at a moment, the reader wants to receive an event **msg** but the writer is not ready to correspond, then the reader must enter a failure mode and stop the whole CTA.

The reader:



The writer:



7. Please write down TCTL formulas for the following specifications.
(You cannot use atomic propositions that can only be checked with computation path exploration.) (10/70)

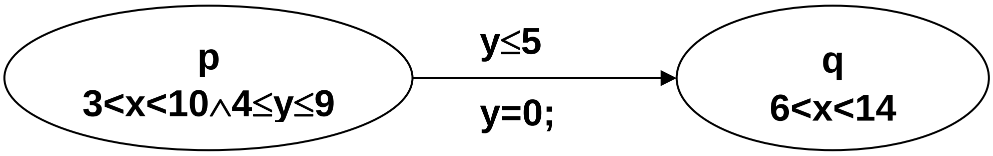
(a) If you are swimming and see two piranhas (食人魚), then either you or one of the piranhas will be in heaven in 30 seconds.

$$\begin{aligned}
&\forall\Box((\texttt{Swimming} \wedge \texttt{Piranha1} \wedge \texttt{Piranha1})\\
&\quad\Rightarrow\forall\Diamond_{\leq 30}\ (\texttt{in\_heaven}\\
&\qquad\qquad \vee\ \texttt{Piranha1\_in\_heaven}\\
&\qquad\qquad \vee\ \texttt{Piranha2\_in\_heaven}))
\end{aligned}$$

(b) When you are in heaven, if you are bored inevitably, you cannot move to the hell sometimes.

$$\forall\Box((\texttt{in\_heaven} \wedge \forall\Diamond\texttt{bored}) \Rightarrow \neg\exists\Diamond\ \texttt{to\_hell})$$

8. We have the following timed automata with one transition (p,q).



Now we have a state space in location q characterized with the following condition.

$$\eta \equiv \mathbf{q} \wedge 6<x<14 \wedge x-y\le 8$$

Please write down the precondition of η through (p,q). Note that the precondition that you construct can only use variable names **x**, **y**, **p**, **q**, inequalities, integer constants, and Boolean operators (∧, ∨, ¬). (15/85)

$p \wedge 3<x<10 \wedge 4\le y\le 9 \wedge y\le 5 \wedge \exists y\, \exists q\, (y=0 \wedge q \wedge 6<x<14 \wedge x-y\le 8)$

$\equiv p \wedge 3<x<10 \wedge 4\le y\le 9 \wedge y\le 5 \wedge \exists y\, (y=0 \wedge 6<x<14 \wedge x-y\le 8)$

$\equiv p \wedge 3<x<10 \wedge 4\le y\le 5 \wedge \exists y\, (y=0 \wedge 6<x<14 \wedge x-y\le 8 \wedge x \le 8)$

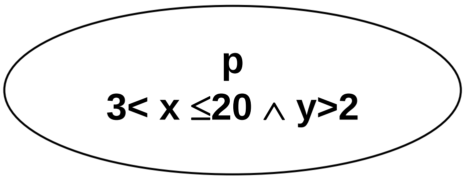
$\equiv p \wedge 3<x<10 \wedge 4\le y\le 5 \wedge \exists y\, (y=0 \wedge 6<x<14 \wedge x-y\le 8 \wedge x \le 8)$

$\equiv p \wedge 3<x<10 \wedge 4\le y\le 5 \wedge \exists y\, (y=0 \wedge 6< x \le 8 \wedge x-y\le 8)$

$\equiv p \wedge 3<x<10 \wedge 4\le y\le 5 \wedge 6< x \le 8$

$\equiv p \wedge 6< x \le 8 \wedge 4\le y\le 5$

9. We have the following timed automata with only one control location (or mode):



Now we have a state space in this mode p characterized with the following condition.

$$\eta \equiv \mathbf{3 < x \leq 20} \wedge 4 \leq y \leq 19$$

Please construct of the precondition of time progress of η in this mode p. Note that the precondition that you construct can only use variable names **x**, **y**, **p**, **q**, inequalities, integer constants, and Boolean operators ($\wedge$, $\vee$, $\neg$). (14/99)

$p \wedge 3 < x \leq 20 \wedge y > 2 \wedge \exists t\, ((t \geq 0 \wedge p \wedge 3 < x+t \leq 20 \wedge 4 \leq y+t \leq 19)$

$\equiv p \wedge 3 < x \leq 20 \wedge y > 2$

$\quad \wedge \exists t\, (\quad t \geq 0 \wedge p \wedge 3 < x+t \leq 20 \wedge 4 \leq y+t \leq 19$

$\qquad\qquad \wedge x \leq 20 \wedge y \leq 19 \wedge x-y \leq 16 \wedge y-x < 16)$

$\equiv p \wedge 3 < x \leq 20 \wedge y > 2 \wedge x \leq 20 \wedge y \leq 19 \wedge x-y \leq 16 \wedge y-x < 16$

$\equiv p \wedge 3 < x \leq 20 \wedge 2 < y \leq 19 \wedge x-y \leq 16 \wedge y-x < 16$

10. Please tell me what you think of the course. What is your opinion of the course ? What is your suggestions to the teacher ? (1/100)