<u>Formal Methods</u>

<u>Final Exam</u>

Instructor: Farn Wang

Class hours: 9:10-12:00 Tuesday Course Nr.921 U7600

Room: BL 103 Spring 2007

Student name: Student ID:

1. Suppose we have the following theorem. (10/10)

$$\forall x(P(x) \Rightarrow \exists y(Q(y))),\ \forall x(Q(x) \Rightarrow \exists y(R(y))),\ \forall x(R(x) \Rightarrow \exists y(S(y)))$$

$$\vDash \quad (\exists z(P(z))) \Rightarrow (\exists z(S(z)))$$

Please do the following steps.

(a) Covnert the theorem for proof by refutation.

$\forall x(P(x) \Rightarrow \exists y(Q(y))) \wedge \forall x(Q(x) \Rightarrow \exists y(R(y)))$

$\wedge\ \forall x(R(x) \Rightarrow \exists y(S(y)))$

$\wedge\ \neg((\exists z(P(z))) \Rightarrow (\exists z(S(z))))$

(b) Eliminate implication operators

$\forall x(\neg P(x) \vee \exists y(Q(y))) \wedge \forall x(\neg Q(x) \vee \exists y(R(y)))$

$\wedge \forall x(\neg R(x) \vee \exists y(S(y))) \wedge \neg(\neg(\exists z(P(z))) \vee (\exists z(S(z))))$

(c) Push all negation signs to the atom level

$\forall x(\neg P(x) \vee \exists y(Q(y))) \wedge \forall x(\neg Q(x) \vee \exists y(R(y)))$

$\wedge\ \forall x(\neg R(x) \vee \exists y(S(y))) \wedge (\exists z(P(z))) \wedge (\forall z(\neg S(z))))$

(d) Standardize variables

$\forall x1(\neg P(x1) \vee \exists y(Q(y1)))$

$\wedge\ \forall x2(\neg Q(x2) \vee \exists y2(R(y2)))$

$\wedge\ \forall x3(\neg R(x3) \vee \exists y3(S(y3)))$

$\wedge\ (\exists z4(P(z4))) \wedge (\forall z5(\neg S(z5))))$

(e) Eliminate existential quantifiers using <u>*Skolemization*</u>

$\forall x1(\neg P(x1) \vee Q(h1(x1)))$

$\wedge\ \forall x2(\neg Q(x2) \vee R(h2(x2)))$

$\wedge\ \forall x3(\neg R(x3) \vee S(h3(x3)))$

$\wedge\ P(a) \wedge \forall z5(\neg S(z5))$

(f) Convert it to the conjunctive normal form

$$\forall x1 \forall x2 \forall x3 \forall z5 \;\; (\neg P(x1) \vee Q(h1(x1)))$$
$$\wedge \;\; (\neg Q(x2) \vee R(h2(x2)))$$
$$\wedge \;\; (\neg R(x3) \vee S(h3(x3)))$$
$$\wedge \;\; P(a) \;\; \wedge \;\; (\neg S(z5))$$

(g) Eliminate the universal quantifiers

$$(\neg P(x1) \vee Q(h1(x1))) \;\; \wedge \;\; (\neg Q(x2) \vee R(h2(x2)))$$
$$\wedge \;\; (\neg R(x3) \vee S(h3(x3))) \;\; \wedge \;\; P(a) \;\; \wedge \;\; (\neg S(z5))$$

(h) Eliminate the conjunction operators

$(\neg P(x1) \vee Q(h1(x1)))$

$(\neg Q(x2) \vee R(h2(x2)))$

$(\neg R(x3) \vee S(h3(x3)))$

$P(a)$

$\neg S(z5)$

(i) Rename variables so that no variable occurs in more than one clause.

$\neg P(x1) \vee Q(h1(x1))$

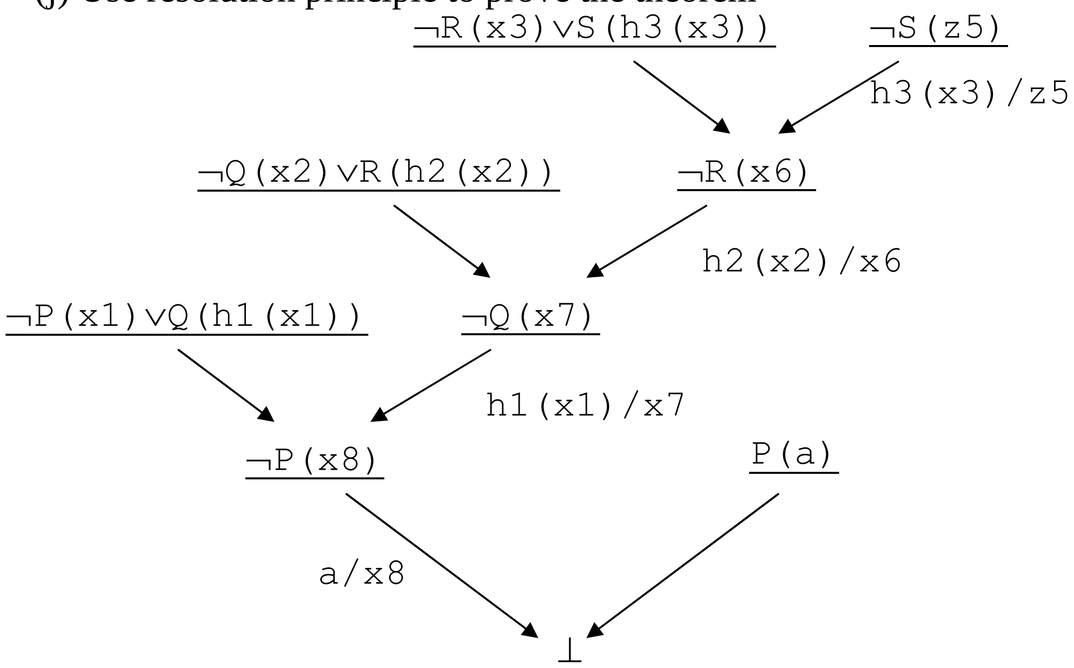
$\neg Q(x2) \vee R(h2(x2))$

$\neg R(x3) \vee S(h3(x3))$

$P(a)$

$\neg S(z5)$

(j) Use resolution principle to prove the theorem



2. Assume that we have a state s:(a=30,b=2,c=3) in a Kripke structure with three integer variables a, b, and c. Please write down the values of the following evaluations. (5/15)

(a) ⟨a+30*b, s⟩ = ?   `30+30*2 = 90`

(b) ⟨a+30*b < c, s⟩ = ?   `90<3 = false`

(c) ⟨¬a+b<30*c, s⟩ = ?   `¬30+2<30 = ¬true = false`

3. Given a statement E and a statement s, we let s[E] be the result state after executing E in s. Please write down the states of the following execution with respect to the Kripke structure in problem 2. (10/25)

(a) (a=30,b=2,c=3)[while (a < b) a = (a+b+c)/b; ]

`(a=30,b=2,c=3)`

(b) (a=30,b=2,c=3)[while (a > b) a = (a+b+c)/b; ]

`No such state exists since this is an infinite loop.`

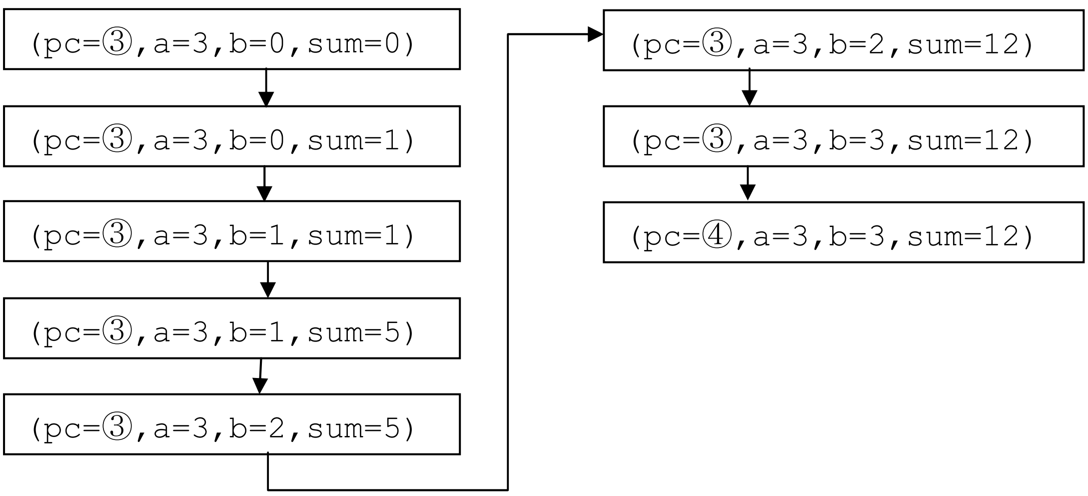
(c) (a=30,b=2,c=3)[while (a>b) a = (a+b+c) % (2*c); ]

`(a=2,b=2,c=3)`

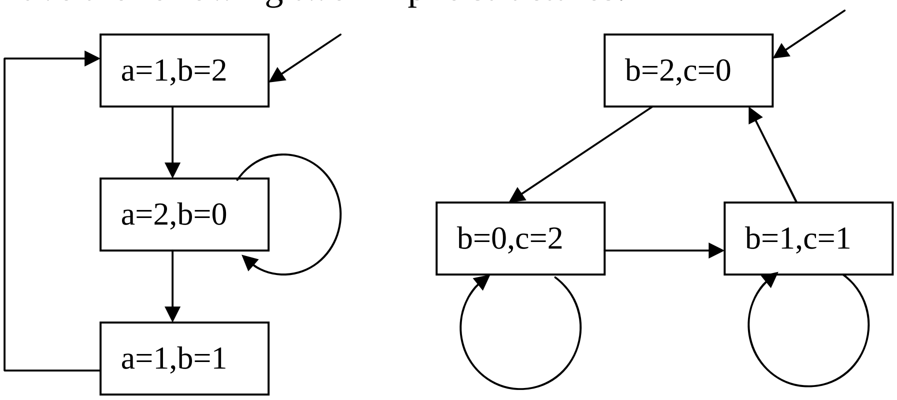
4. Suppose we have a simple C program in the following. (10/35)

main () {
  int a = 3, b = 0, sum = 0;
  for (b = 0; b < 3; b++) sum = sum + a*b + 1; ………③
} ……………………………………………………….④

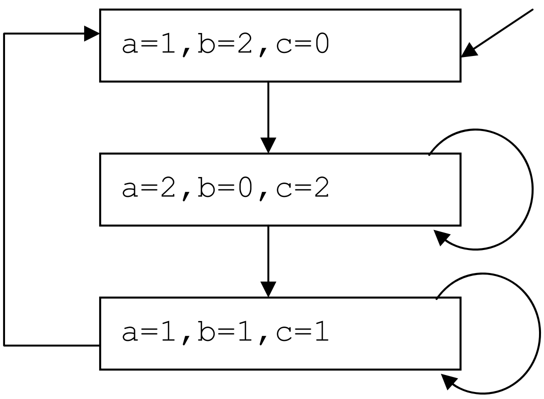
Please draw the Kripke structure of the program.



5. We have the following two Kripke structures:




Please draw the composition of the two structures. Note that in the composition, two states can be composed only if they agree in the values of the common variables. (10/45)



6. Please write LTL formulas for the following specifications. (5/50)
(The underlined phrases are atomic propositions.)

(a) Every day, I long for the true love.

$\Box\ \text{long for the true love}$

(b) One day, you will be food for monads (單細胞生物).

$\Diamond\ \text{food for monad}$

7. Please write CTL formulas for the following specifications. (5/55)
(The underlined phrases are atomic propositions.)

(a) When I find my true love, I will marry him/her by all means.

$\forall\Box\ (\text{find my true love} \rightarrow \forall\Diamond\ \text{marry him/her})$

(b) If you drink that wine, you will have 1 million fewer brain cells by tomorrow.

$\forall\Box\ (\text{drink that wine} \rightarrow \forall\circ\ \text{have 1 million fewer brain cells})$

8. Please write CTL* formulas for the following specifications. (5/60)
(The underlined phrases are atomic propositions.)

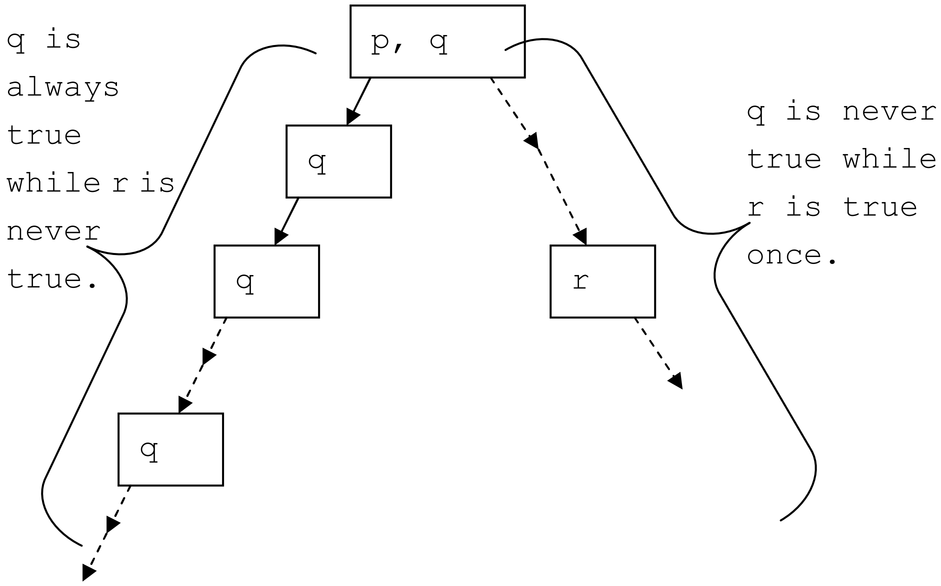
(a) If you try suicide too often, you go to hell eventually.

$\forall\ ((\Box\Diamond \text{try suicide}) \rightarrow \Diamond\ \text{go to hell})$

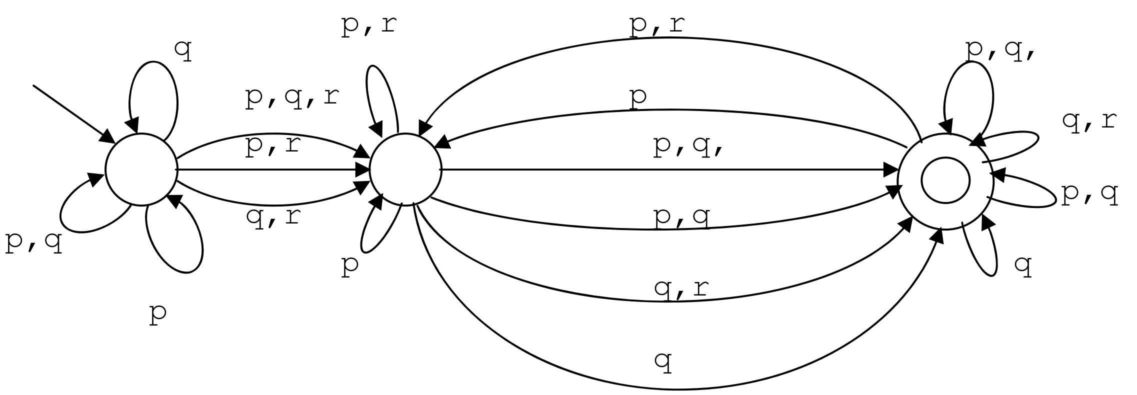
(b) If you marry me, I will buy you a ring and be happy forever.

$\forall\ \Box(\text{marry me} \rightarrow ((\Box\ \text{happy}) \wedge \Diamond\ \text{buy you a ring})$

9. Please construct a tree that can tell $\forall\Box(p\Rightarrow((\exists\Box q)\wedge\exists\Diamond r))$ from $\forall\Box(p\Rightarrow\exists((\Box q)\wedge\Diamond r))$. (10/70)

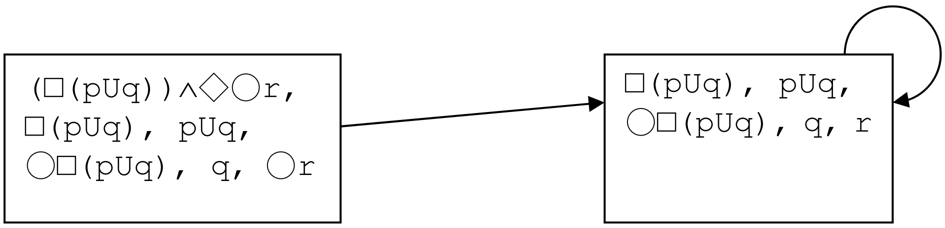



10. Please construct a Büchi automata for LTL formula $(\Box(pUq))\wedge\Diamond\bigcirc r$. (10/80)



11. Please construct the closure for LTL formula (□(pUq))∧◇○r. Then please construct a structure in the tableau of the formula that shows the formula is satisfiable. (10/90)

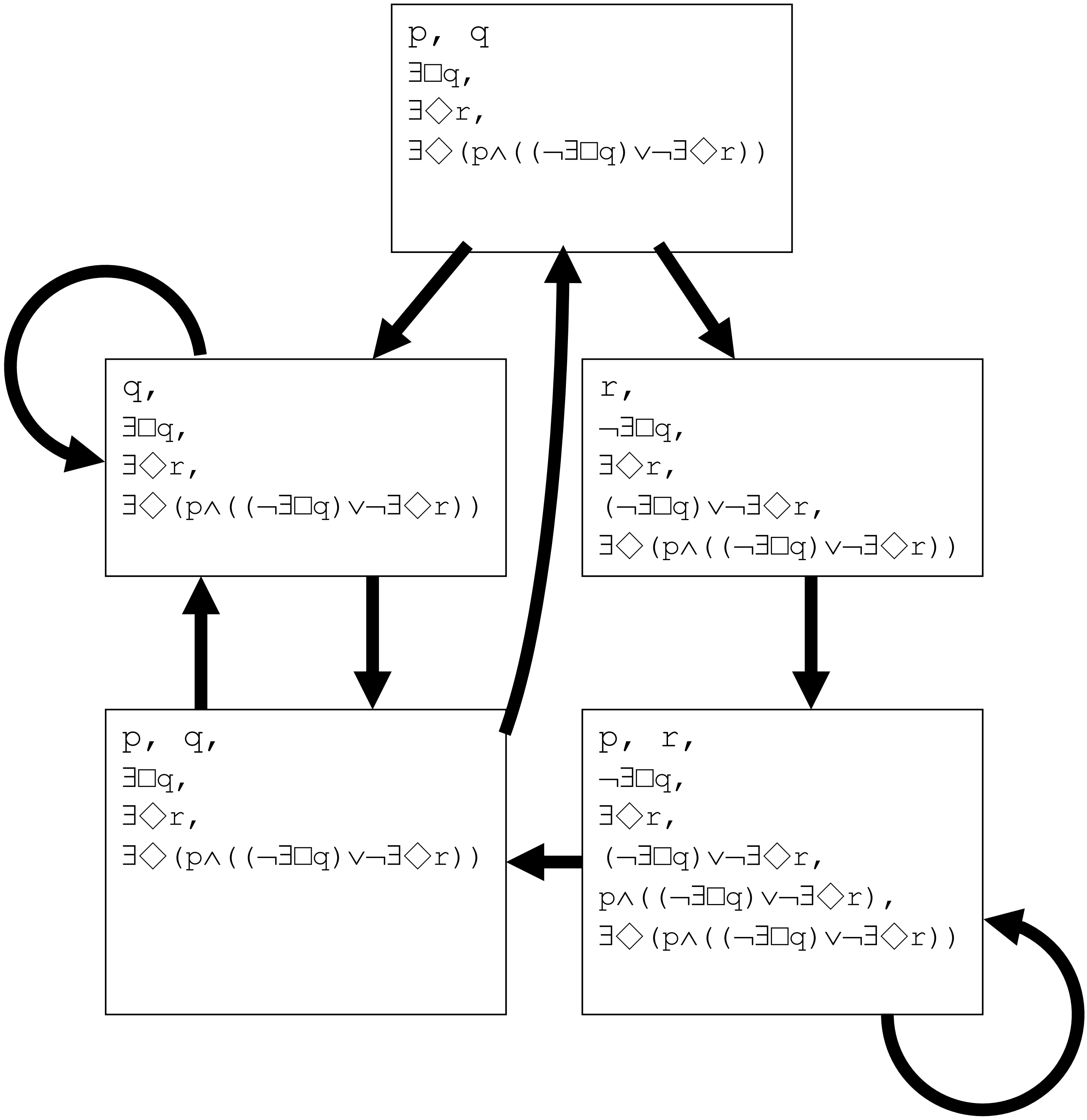
closure ={(□(pUq))∧◇○r, □(pUq), ○□(pUq), pUq, ○pUq, p, q, ◇○r, ○◇○r, ○r, r }.



12. Please do labeling algorithm of CTL formula ∀□(p⇒((∃□q)∧∃◇r)) on the following automata. (The formula is already the negation of the specification.) (10/100)

∀□(p⇒((∃□q)∧∃◇r))≡¬∃◇(p∧((¬∃□q)∨¬∃◇r))

set of subformulas ={¬∃◇(p∧((¬∃□q)∨¬∃◇r)), ∃◇(p∧((¬∃□q)∨¬∃◇r)), p∧((¬∃□q)∨¬∃◇r), p, (¬∃□q)∨¬∃◇r, ¬∃□q, ∃□q , q, ¬∃◇r, ∃◇r, r}



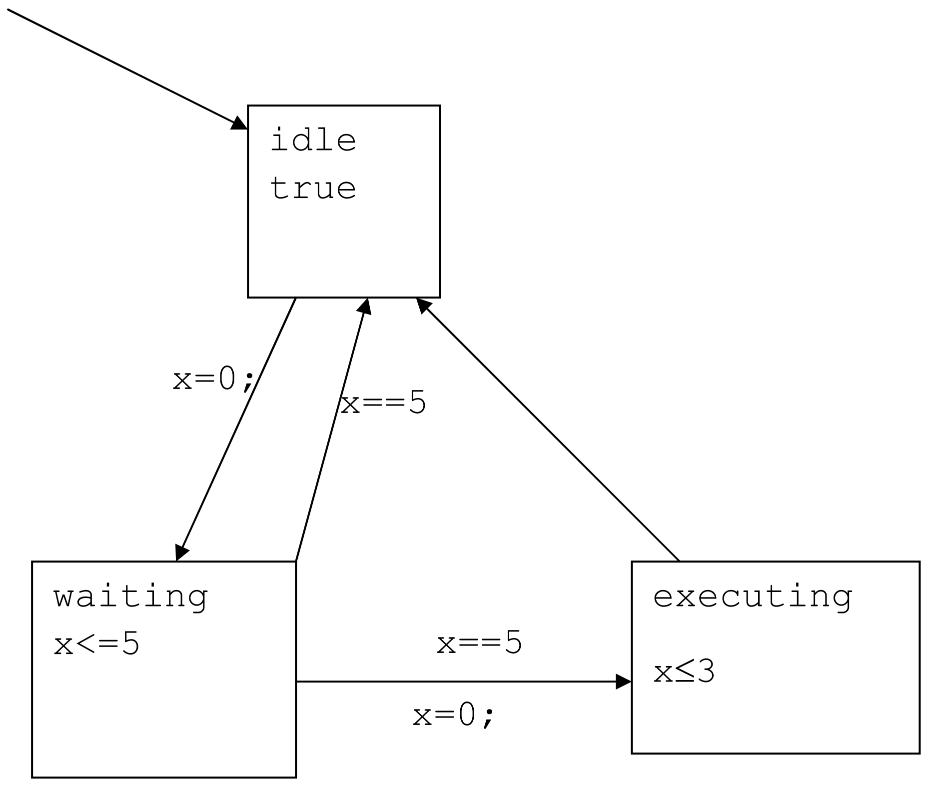
13. Please draw a timed automaton with the following properties. (5/105)

(a) There are three control locations, **idle**, **waiting**, **executing**.

(b) If the system is in the **idle** mode, sometimes it may want to execute and thus enter the **waiting** mode to wait for execution.

(c) If it is in the **waiting** mode, it must execute in 5 sec. Otherwise, it goes back to the **idle** mode.

(d) In the **executing** mode, it must finish in 3 sec. and move back to the **idle** mode.



14. Please write down TCTL formulas for the following specifications. (The underlined phrases are atomic propositions) (4/109)

(a) If you are swimming and see a piranha (食人魚), it is possible that you will be in heaven in 30 seconds.

∀□((swimming ∧ see a piranha)→∀◇$_{\leq 30}$ in heaven)

(b) When you are in heaven, if you are not happy forever, you cannot move to the hell.

∀□((in heaven ∧ ¬∀□ happy)→¬∃◇ move to the hell)

15. Please tell me what you think of the course. What is your opinion of the course ? What is your suggestions to the teacher ? (1/110)

I wish the teacher can treat me ice cream in every class.

16. Please draw the composition of the following two Büchi automata. (Black boxes are accepting states.) (10/120)