Solution of Homework#5

17th Dec, 2007

If you have any question, please send me e-mail(hongshin@gmail.com).

2-1

```
MODULE main
    VAR
        waitingWriters : 0..1 ;
        activeWriters : 0..1 ;
        waitingReaders : 0..2 ;
        activeReaders : 0..2 ;

        r1 : process reader(waitingWriters, activeWriters, waitingReaders, activeReaders) ;
        r2 : process reader(waitingWriters, activeWriters, waitingReaders, activeReaders) ;
        w1 : process writer(waitingWriters, activeWriters, waitingReaders, activeReaders) ;

    ASSIGN
        init(waitingReaders) := 0 ;
        init(waitingWriters) := 0 ;
        init(activeReaders) := 0 ;
        init(activeWriters) := 0 ;

    FAIRNESS running
    FAIRNESS (activeReaders = 2)
```

```
-- Concurrency
LTLSPEC G F (activeReaders = 2)

-- Exclusive Writing
LTLSPEC G(!(activeWriters = 1 & activeReaders > 0))
```

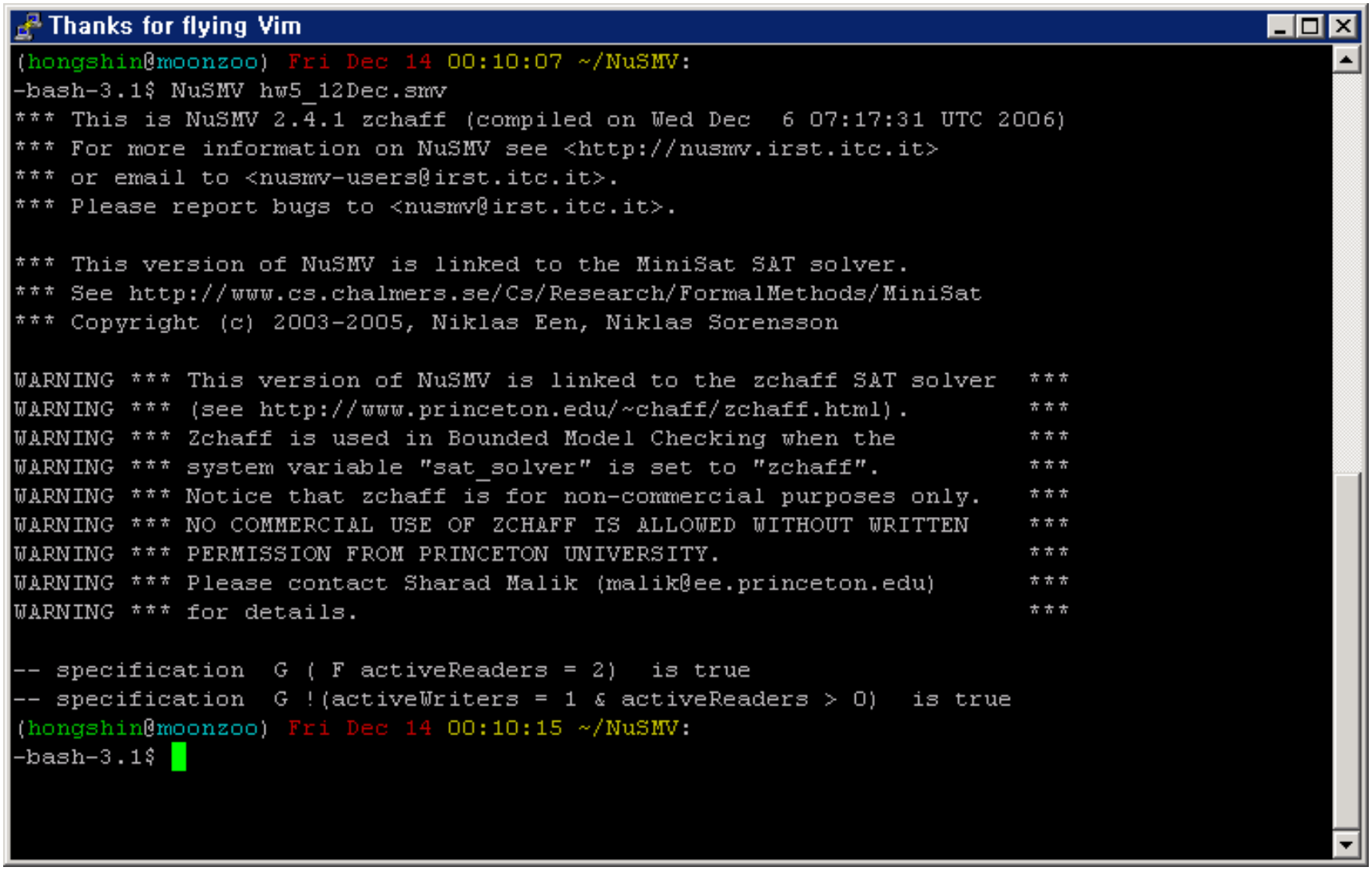
System properties (2.2)

```
MODULE reader(waitingWriters, activeWriters, waitingReaders, activeReaders)
    VAR
        state : {normal, ready, reading} ;
    ASSIGN
        init(state) := normal ;

        next(state) :=
            case
                (state = normal) : {normal, ready} ;
                (state = ready & activeWriters = 0 & waitingWriters = 0) : reading ;
                (state = reading) : {reading, normal} ;
                1 : state ;
            esac ;

        next(waitingReaders) :=
            case
                (state != ready & next(state) = ready) : waitingReaders = waitingReaders + 1 ;
                (state = ready & next(state) != ready) : waitingReaders = waitingReaders - 1 ;
                1 : waitingReaders ;
            esac ;

        next(activeReaders) :=
            case
                (state != reading & next(state) = reading) : activeReaders = activeReaders + 1 ;
                (state = reading & next(state) != reading) : activeReaders = activeReaders - 1 ;
                1 : activeReaders ;
            esac ;

    FAIRNESS running
    FAIRNESS (state = normal)
    FAIRNESS (state = ready)
    FAIRNESS (state = reading)
```

```
MODULE reader(waitingWriters, activeWriters, waitingReaders, activeReaders)
    VAR
        state : {normal, ready, reading} ;
    ASSIGN
        init(state) := normal ;

        next(state) :=
            case
                (state = normal) : {normal, ready} ;
                (state = ready & activeWriters = 0 & waitingWriters = 0) : reading ;
                (state = reading) : {reading, normal} ;
                1 : state ;
            esac ;

        next(waitingReaders) :=
            case
                (state != ready & next(state) = ready) : waitingReaders = waitingReaders + 1 ;
                (state = ready & next(state) != ready) : waitingReaders = waitingReaders - 1 ;
                1 : waitingReaders ;
            esac ;

        next(activeReaders) :=
            case
                (state != reading & next(state) = reading) : activeReaders = activeReaders + 1 ;
                (state = reading & next(state) != reading) : activeReaders = activeReaders - 1 ;
                1 : activeReaders ;
            esac ;

    FAIRNESS running
    FAIRNESS (state = normal)
    FAIRNESS (state = ready)
    FAIRNESS (state = reading)
```

```
MODULE writer(waitingWriters, activeWriters, waitingReaders, activeReaders)
    VAR
        state : {normal, ready, writing} ;
    ASSIGN
        init(state) := normal ;

        next(state) :=
            case
                (state = normal) : {normal, ready} ;
                (state = ready & activeWriters = 0 & activeReaders = 0) : writing ;
                (state = writing) : {writing, normal} ;
                1 : state ;
            esac ;

        next(waitingWriters) :=
            case
                (state != ready & next(state) = ready) : waitingWriters= waitingWriters + 1 ;
                (state = ready & next(state) != ready) : waitingWriters = waitingWriters - 1 ;
                1 : waitingWriters ;
            esac ;

        next(activeWriters) :=
            case
                (state != reading & next(state) = reading) : activeWriters= activeWriters + 1 ;
                (state = reading & next(state) != reading) : activeWriters = activeWriters - 1 ;
                1 : activeWriters ;
            esac ;

    FAIRNESS running
    FAIRNESS (state = normal)
    FAIRNESS (state = ready)
    FAIRNESS (state = reading)
```

2-2 The verification result from NuSMV



3.

1) $\pi = q_3\, q_4\, q_3\, q_4 \ldots.$, $\pi \models G\, a$

$\pi = q_3\, q_4\, q_3\, q_4 \ldots.$, $\pi \models a\, U\, b$

$\pi = q_3\, q_4\, q_3\, q_4 \ldots.$, $\pi \models a\, U\, X(a \wedge \neg b)$

$\pi = q_3\, q_1\, q_2 \ldots$, $\pi \models X\neg b \wedge G(\neg a \vee \neg b)$

$\pi = q_3\, q_4\, q_3\, q_1 \ldots$, $\pi \models X(a \wedge b) \wedge F(\neg a \wedge \neg b)$

2) $\mathcal{M}, q_3 \not\models G\, a$ $\quad \because \pi = q_3\, q_1$

$\mathcal{M}, q_3 \not\models a\, U\, b$ $\quad \because \pi = q_3\, q_1\, q_2 \ldots$

$\mathcal{M}, q_3 \not\models a\, U\, X(a \wedge \neg\, b)$ $\quad \because \pi = q_3\, q_1\, q_2 \ldots$

$\mathcal{M}, q_3 \not\models X\neg b \wedge G(\neg\, a \vee \neg\, b)$ $\quad \because \pi = q_3\, q_4 \ldots$

$\mathcal{M}, q_3 \not\models X(a \wedge b) \wedge F(\neg\, a \wedge \neg\, b)$ $\quad \because \pi = q_3\, q_1\, q_2 \ldots$

4.

$\pi \models \phi \, \mathrm{U} \, \psi$ means

$\exists \, i.(1 \leq i \wedge \pi^i \models \psi \wedge \forall \, j \, .(\, 1 \leq j < i \rightarrow \pi^j \models \phi)) = \phi_1$

$\pi \models \psi \, \mathrm{R} \, (\phi \vee \psi)$ means

$\exists \, i.(1 \leq i \wedge \pi^i \models \psi \wedge \forall \, j.(1 \leq j \leq i \rightarrow \pi^j \models \phi \vee \psi) \vee$

$\forall \, i.(1 \leq i \wedge \pi^i \not\models \psi \wedge \pi^i \models \phi \vee \psi \,)$

$\pi \models \mathrm{F} \, \psi$ means

$\exists \, i.(1 \leq i \wedge \pi^i \models \psi)$

So $\pi \models \psi \, \mathrm{R} \, (\phi \vee \psi) \wedge \mathrm{F} \, \psi$ means

$\{\exists \, i.(1 \leq i \wedge \pi^i \models \psi \wedge \forall \, j.(1 \leq j \leq i \rightarrow \pi^j \models \phi \vee \psi) \vee \forall \, i.(1 \leq i \wedge \pi^i \not\models \psi \wedge \pi^i \models \phi \vee \psi \,) \, \} \wedge \exists \, i.(1 \leq i \wedge \pi^i \models \psi)$

$\equiv \quad \exists \, i.(1 \leq i \wedge \pi^i \models \psi \wedge \forall \, j.(1 \leq j \leq i \rightarrow \pi^j \models \phi \vee \psi) = \phi_2$

$\equiv \quad \exists \, i.(1 \leq i \wedge \pi^i \models \psi \wedge \forall \, j \, .(\, 1 \leq j < i \rightarrow \pi^j \models \phi)) \because \phi_1 \wedge \phi_2 = \phi_1 \vee \phi_2 = \phi_2$

5.

$\pi \models \phi \, \mathrm{W} \, \psi \wedge \mathrm{F} \, \psi$ means that
$(\exists \, \mathrm{i}.(\pi^{\mathrm{i}} \models \psi \wedge \forall \, \mathrm{j}.(\mathrm{j} < \mathrm{i} \rightarrow \pi^{\mathrm{i}} \models \phi)) \vee \forall \, \mathrm{i}.(\pi^{\mathrm{i}} \not\models \psi \wedge (\pi^{\mathrm{i}} \models \phi)) \wedge \exists \, \mathrm{i}.((\pi^{\mathrm{i}} \models \psi).$

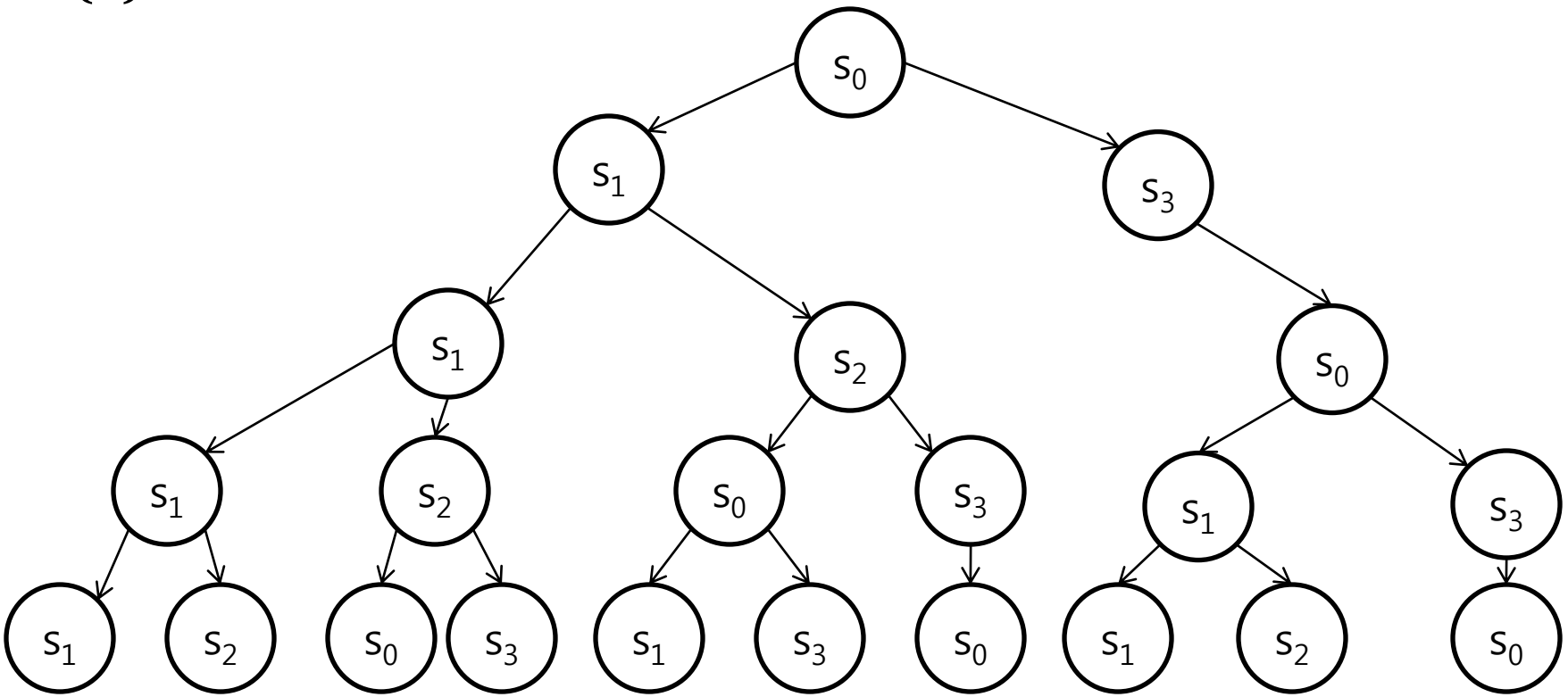
Using distributive law,

$(\exists \, \mathrm{i}.(\pi^{\mathrm{i}} \models \psi \wedge \forall \, \mathrm{j}.(\mathrm{j} < \mathrm{i} \rightarrow \pi^{\mathrm{i}} \models \phi)) \wedge \exists \, \mathrm{i}.((\pi^{\mathrm{i}} \models \psi)) \vee$
$(\forall \, \mathrm{i}.(\pi^{\mathrm{i}} \not\models \psi \wedge (\pi^{\mathrm{i}} \models \phi) \wedge \exists \, \mathrm{i}.((\pi^{\mathrm{i}} \models \psi))$

$\equiv \exists \, \mathrm{i}.(\pi^{\mathrm{i}} \models \psi \wedge \forall \, \mathrm{j}.(\mathrm{j} < \mathrm{i} \rightarrow \pi^{\mathrm{i}} \models \phi))$

And $\pi \models \phi \, \mathrm{U} \, \psi$ means $\exists \, \mathrm{i}.(\pi^{\mathrm{i}} \models \psi \wedge \forall \, \mathrm{j}.(\mathrm{j} < \mathrm{i} \rightarrow \pi^{\mathrm{i}} \models \phi))$.

6-(a)



6-(b)

(i) $\mathcal{M}, s_0 \models \neg p \rightarrow r$

(ii) $\mathcal{M}, s_0 \not\models AF\ t$ $\quad \because \pi = s_0\ s_1\ s_1\ s_1\ s_1 \ldots$

(iii) $\mathcal{M}, s_0 \models \neg EG\ r$ $\quad \because \mathcal{M}, s_0 \models AF \neg r$

(iv) $\mathcal{M}, s_0 \models E(t\ U\ q)$

(v) $\mathcal{M}, s_0 \models AF\ q$ $\quad \because s_0 \models q$

(vi) $\mathcal{M}, s_0 \models EF\ q$ $\quad \because s_0 \models q$

(vii) $\mathcal{M}, s_0 \not\models EG\ r$ $\quad \because s_0 \not\models r$

(viii) $\mathcal{M}, s_0 \not\models AG(r \vee q)$ $\quad \because s_2$ is reachable from s_0 but $s_2 \not\models r \vee q$.

6-(c)

(i) $\mathcal{M}, s_2 \models \neg p \rightarrow r$

(ii) $\mathcal{M}, s_2 \models AF\ t$ $\quad \because s_2 \models t$

(iii) $\mathcal{M}, s_2 \models \neg EG\ r$ $\quad \because \mathcal{M}, s_2 \models AF \neg r$

(iv) $\mathcal{M}, s_2 \models E(t\ U\ q)$ $\quad \because s_2 \models t$, $s_0 \models q$ and $s_3 \models q$ where s_0 and s_3 are only successors of s_2

(v) $\mathcal{M}, s_2 \models AF\ q$

(vi) $\mathcal{M}, s_2 \models EF\ q$

(vii) $\mathcal{M}, s_2 \not\models EG\ r$ $\quad \because s_0 \not\models r$

(viii) $\mathcal{M}, s_2 \not\models AG(r \vee q)$ $\quad \because s_2 \not\models r \vee q$.

7-(a)

(in LTL) $G((\ p \rightarrow F\ q) \rightarrow (\neg r\ U\ t))$

7-(b)

(in LTL) $G(s \rightarrow XG\neg p) \wedge G(t \rightarrow XG\neg p)$

(in LTL) $AG(s \rightarrow AXAG\neg p) \wedge AG(t \rightarrow AXAG\neg p)$

7-(c)

(in LTL) $G(p \rightarrow XG\neg q)$

(in CTL) $AG(p \rightarrow AXAG\neg q)$

7-(d)

(in LTL) $GF(q \rightarrow \neg p\ U\ r) \wedge GF(r \rightarrow \neg p\ U\ q)$

7-(e)

(in LTL)

$\neg p\ U\ p \rightarrow X(\neg p\ U\ p \rightarrow XG\neg p) \vee \neg p\ U\ p \rightarrow XG\neg p \vee G\ \neg p$

(in CTL)

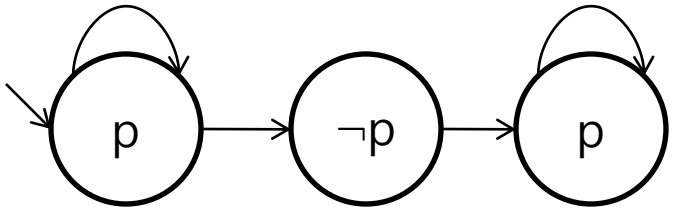
$A[\neg\ p\ U\ p \rightarrow AXA[(\neg\ p\ U\ p \rightarrow AXAG\neg\ p)] \vee A[\neg\ p\ U\ p \rightarrow AXAG\neg\ p] \vee AG\neg p$

7-(f)

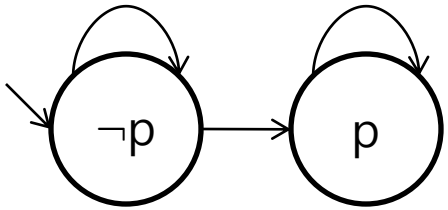
(in LTL) $Xp \wedge G(p \rightarrow XXp)$

(in CTL) $AXp \wedge AG(p \rightarrow AXAXp)$

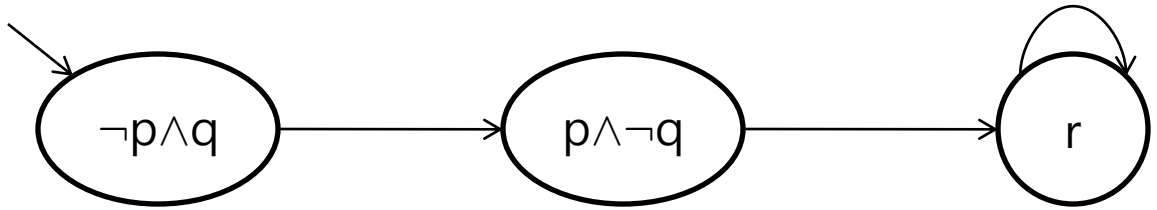
8-(a) $\mathcal{M}, s_0 \models$ AFG p , $\mathcal{M}, s_0 \not\models$ AFAG p



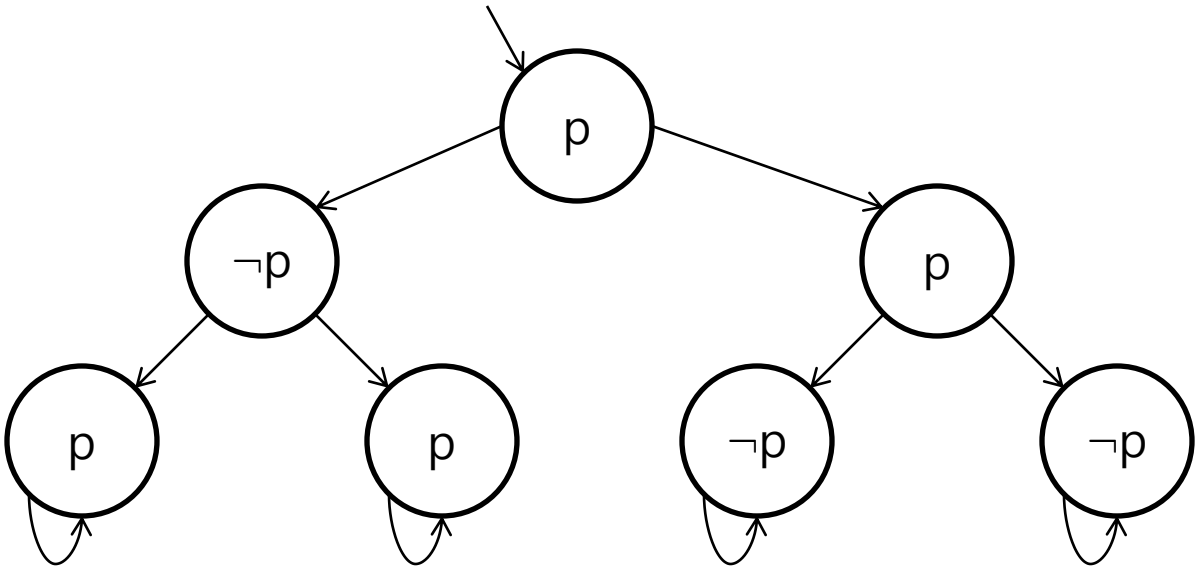
8-(b) $\mathcal{M}, s_0 \not\models$ AGFp $\mathcal{M}, s_0 \models$ AGEFp



8-(c) $\mathcal{M}, s_0 \models$ A[(p U r) ∨ (q U r)] $\mathcal{M}, s_0 \not\models$ A[(p ∨ q) U r]



8-(d) $\mathcal{M}, s_0 \models A[Xp \vee XXp]$ $\mathcal{M}, s_0 \not\models AX\,p \vee AXAX\,p$



8-(e) $\mathcal{M}, s_0 \not\models E[GFp]$ $\mathcal{M}, s_0 \models EGEFp$