CS3234 - Tutorial 9, Solutions

3.

function NNF-LTL(ϕ)

/* precondition: ϕ is implication free */
/* postcondition: NNF-LTL(ϕ) computes a negation normal form for ϕ */

begin function

case

ϕ is $\top$: **return** ϕ
ϕ is a propositional atom: **return** ϕ
ϕ is $(\neg\neg\phi_1)$: **return** NNF-LTL(ϕ_1)
ϕ is $(\phi_1 \wedge \phi_2)$: **return** NNF-LTL(ϕ_1) $\wedge$ NNF-LTL(ϕ_2)
ϕ is $(\phi_1 \vee \phi_2)$: **return** NNF-LTL(ϕ_1) $\vee$ NNF-LTL(ϕ_2)
ϕ is $\neg(\phi_1 \wedge \phi_2)$: **return** NNF-LTL($\neg\phi_1 \vee \neg\phi_2$)
ϕ is $\neg(\phi_1 \vee \phi_2)$: **return** NNF-LTL($\neg\phi_1 \wedge \neg\phi_2$)
ϕ is $(\phi_1 \mathrm{U}\ \phi_2)$: **return** NNF-LTL($\phi_1$) U NNF-LTL($\phi_2$)
ϕ is $\neg(\phi_1 \mathrm{U}\ \phi_2)$: **return** NNF-LTL($\neg\phi_2 \mathrm{U}\ (\neg\phi_1 \wedge \neg\phi_2) \ \vee\ \mathrm{G}\neg\phi_2$)
ϕ is $(\mathrm{G}\ \phi_1)$: **return** G NNF-LTL(ϕ_1)
ϕ is $\neg(\mathrm{G}\ \phi_1)$: **return** NNF-LTL($\mathrm{F}\neg\phi_1$)
ϕ is $(\mathrm{F}\ \phi_1)$: **return** F NNF-LTL(ϕ_1)
ϕ is $\neg(\mathrm{F}\ \phi_1)$: **return** NNF-LTL($\mathrm{G}\neg\phi_1$)
ϕ is $(\mathrm{X}\ \phi_1)$: **return** X NNF-LTL(ϕ_1)
ϕ is $\neg(\mathrm{X}\ \phi_1)$: **return** NNF-LTL($\mathrm{X}\neg\phi_1$)

end case

end function

function NNF-CTL*(ϕ)

/* precondition: ϕ is implication free */
/* postcondition: NNF-CTL*(ϕ) computes a negation normal form for ϕ */

begin function

case

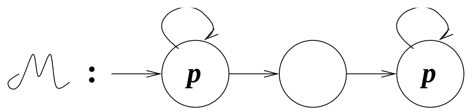
ϕ is $\top$: **return** ϕ
ϕ is a propositional atom: **return** ϕ
ϕ is $(\neg\neg\phi_1)$: **return** NNF-CTL*(ϕ_1)
ϕ is $(\phi_1 \wedge \phi_2)$: **return** NNF-CTL*(ϕ_1) $\wedge$ NNF-CTL*(ϕ_2)
ϕ is $(\phi_1 \vee \phi_2)$: **return** NNF-CTL*(ϕ_1) $\vee$ NNF-CTL*(ϕ_2)
ϕ is $\neg(\phi_1 \wedge \phi_2)$: **return** NNF-CTL*($\neg\phi_1 \vee \neg\phi_2$)
ϕ is $\neg(\phi_1 \vee \phi_2)$: **return** NNF-CTL*($\neg\phi_1 \wedge \neg\phi_2$)
ϕ is $(\phi_1 U\, \phi_2)$: **return** NNF-CTL*(ϕ_1) U NNF-CTL*(ϕ_2)
ϕ is $\neg(\phi_1 U\, \phi_2)$: **return** NNF-CTL*($\neg\phi_2 U\, (\neg\phi_1 \wedge \neg\phi_2) \ \vee\ G\neg\phi_2$)
ϕ is $(G\, \phi_1)$: **return** G NNF-CTL*(ϕ_1)
ϕ is $\neg(G\, \phi_1)$: **return** NNF-CTL*($F\neg\phi_1$)
ϕ is $(F\, \phi_1)$: **return** F NNF-CTL*(ϕ_1)
ϕ is $\neg(F\, \phi_1)$: **return** NNF-CTL*($G\neg\phi_1$)
ϕ is $(X\, \phi_1)$: **return** X NNF-CTL*(ϕ_1)
ϕ is $\neg(X\, \phi_1)$: **return** NNF-CTL*($X\neg\phi_1$)
ϕ is $(A[\phi_1])$: **return** A [NNF-CTL*(ϕ_1)]
ϕ is $\neg(A[\phi_1])$: **return** NNF-CTL*($E[\neg\phi_1]$)
ϕ is $(E[\phi_1])$: **return** E [NNF-CTL*(ϕ_1)]
ϕ is $\neg(E[\phi_1])$: **return** NNF-CTL*($A[\neg\phi_1]$)

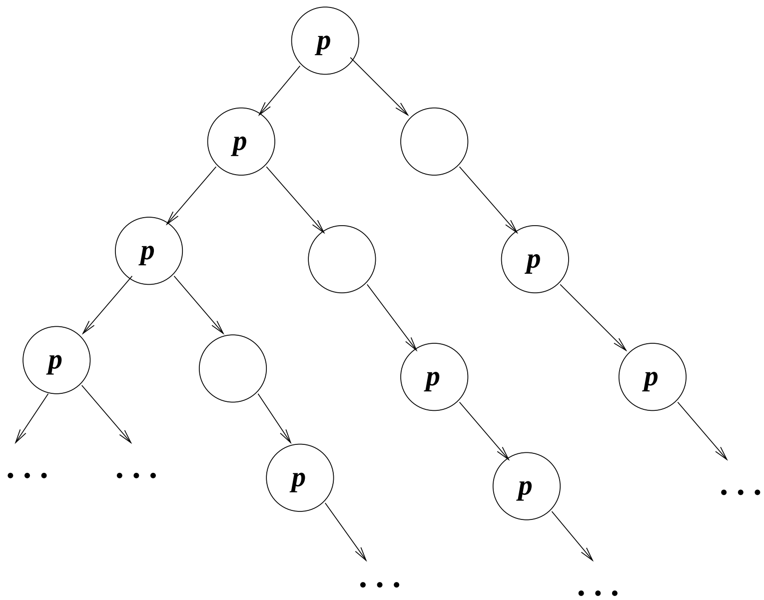
end case

end function

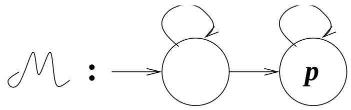
4.

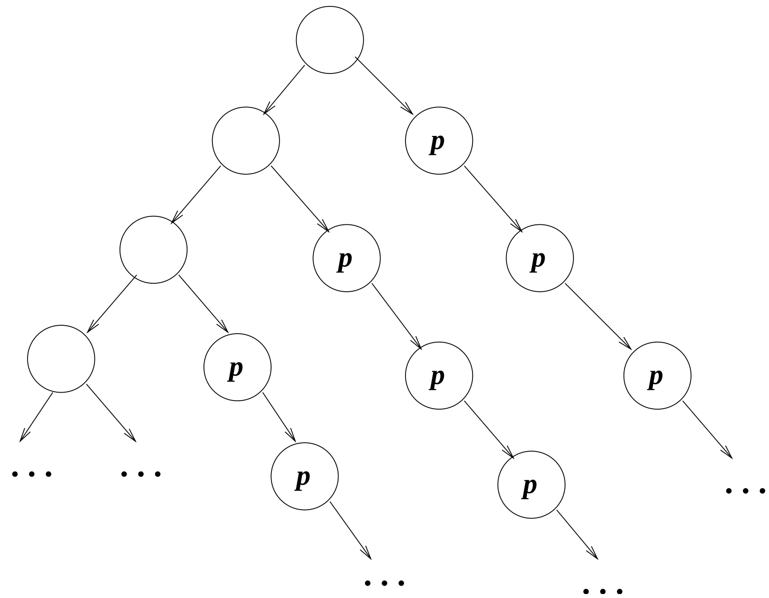
1. $\mathcal{M}, s_0 \models \mathrm{A}[\mathrm{FG}\ p]$ and $\mathcal{M}, s_0 \not\models \mathrm{AFAG}\ p$ (the path $p \to p \to p \to \ldots$)
.



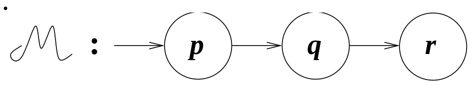


2. $\mathcal{M}, s_0 \models \mathrm{AGEF}\ p$ and $\mathcal{M}, s_0 \not\models \mathrm{A[GF}\ p]$ (the path $\neg p \rightarrow \neg p \rightarrow \ldots$)

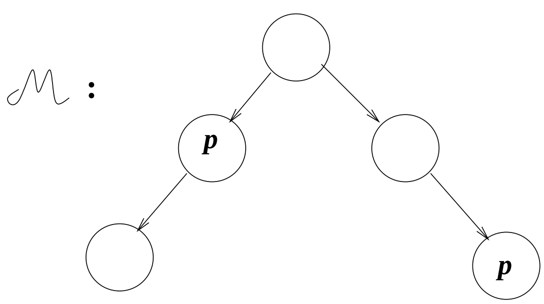




3. $\mathcal{M}, s_0 \models \mathrm{A}[(p \vee q)\mathrm{U}\ r]$ and $\mathcal{M}, s_0 \not\models \mathrm{A}[(p\ \mathrm{U}\ r) \vee (q\ \mathrm{U}\ r)$

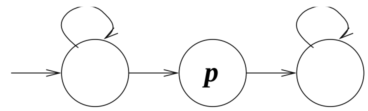


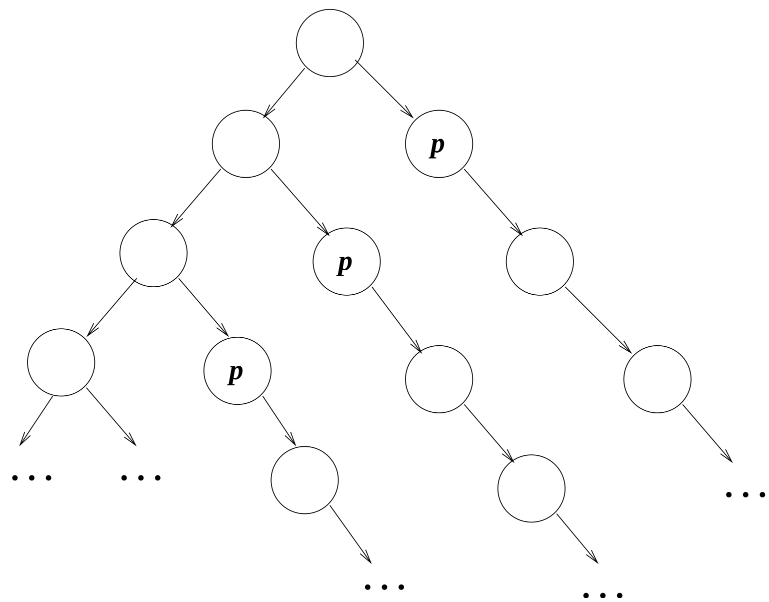
4. $\mathcal{M}, s_0 \models \mathrm{A}[\mathrm{X}\ p \vee \mathrm{XX}\ p]$ and $\mathcal{M}, s_0 \not\models \mathrm{AX}\ p\ \vee\ \mathrm{AXAX}\ p$



5. $\mathcal{M}, s_0 \models \text{EGEF } p$ and $\mathcal{M}, s_0 \not\models \text{E[GF } p]$ (the path $\neg p \to \neg p \to \ldots$)
.

$\mathcal{M}$:





5.

1. $\text{E[F } p \wedge (q \text{ U } r)] \;\equiv\; \text{E}[q \text{ U } (p \wedge \text{ E}[q \text{ U } r])] \;\vee\; \text{E}[q \text{ U } (r \wedge \text{EF } p)]$

2. $\text{E[F } p \wedge \text{G } q] \;\equiv\; \text{E}[q \text{ U } (p \wedge \text{EG } q)]$

3. $\text{E}[(p \text{ U } q) \wedge \text{F } p] \;\equiv\; \text{E}[p \text{ U } (p \wedge \text{E}[p \text{ U } q])] \;\vee\; \text{E}[p \text{ U } (q \wedge \text{EF } p)]$

4. $\text{A}[(p \text{ U } q) \wedge \text{G } p] \;\equiv\; \text{A}[p \text{ U } q] \wedge \text{AG } p$

5. $\text{A[F } p \to \text{F } q] \;\equiv\; \text{AF } p \to \text{AF } q$

6.

1. Let $Z_1 \subseteq Z_2$ be two elements from $\mathcal{P}(\{1,2,\ldots,10\})$
H_1 is monotone :
$H_1(Z_1) = Z_1 - \{1,4,7\} \subseteq Z_2 - \{1,4,7\} = H_1(Z_2)$
H_3 is monotone :
$H_3(Z_1) = \{1,2,3,4,5\} \cap (\{2,4,8\} \cup Z_1) \subseteq \{1,2,3,4,5\} \cap (\{2,4,8\} \cup Z_1) = H_1(Z_2)$

H_2 is not monotone :
$Z_1 = \{2\} \subseteq \{2,5\} = Z_2$ but $H_2(Z_1) = \{5,9\}$ and $H_2(Z_1) = \{9\}$
In fact H_2 is antimonotone (if $Z_1 \subseteq Z_2$ then $H_2(Z_1) \supseteq H_2(Z_2)$)

2. $\mu Z.\, H_3(Z) = \emptyset \cup H_3(\emptyset) \cup H_3^2(\emptyset) \cup \ldots = \emptyset \cup \{2,4\} \cup \{2,4\} \cup \ldots = \{2,4\}$
$\nu Z.\, H_3(Z) = \{1,2,\ldots,10\} \cap H_3(\{1,2,\ldots,10\}) \cap H_3^2(\{1,2,\ldots,10\}) \cap \ldots = \{1,2,\ldots,10\} \cap \{1,2,3,4,5\} \cap \{1,2,3,4,5\} \cap \ldots = \{1,2,3,4,5\}$

3. If H_2 has a fixed point Y, then $\{2,5,9\} - Y = Y$, which is not possible (because if $x \in Y$ then $x \in \{2,5,9\} - Y$ then $x \notin Y$, contradiction).
So H_2 doesn't have any fixed point.

7.

(a) AG and EG have greatest fixed point;
AF, EF, AU, and EU have least fixed point

(b) $??(X,Y) \ = \ \nu Z.\ X \cap (Y \cup \mathrm{AX}\ Z)$

$\mathrm{E}[\phi \mathrm{U}\ \psi] \ = \ \mu Z.\ \psi \vee (\phi \wedge \mathrm{EX}\ Z)$
$\neg\ \mathrm{E}[\phi \mathrm{U}\ \psi] \ = \neg\ (\mu Z.\ \psi \vee (\phi \wedge \mathrm{EX}\ Z)) \ = \ \nu Z.\ \neg\ (\psi \vee (\phi \wedge \mathrm{EX}\ Z)) \ =$
$= \ \nu Z.\ \neg\psi \wedge (\neg\phi \vee \neg(\mathrm{EX}\ Z)) \ = \ \nu Z.\ \neg\psi \wedge (\neg\phi \vee \mathrm{AX}\neg Z))$
If we replace ϕ with $\neg X$, and ψ with $\neg Y$, we observe that

$$??(X,Y) \ = \ \neg \mathrm{E}\ [\neg X\ \mathrm{U}\ \neg Y]$$

The semantic definition of $??(\cdot,\cdot)$ (derived from the semantics of EU):

$\mathcal{M}, s_0 \models ??(X,Y)$

iff *is not true that* (exists a path $s_0 \to s_1 \to s_2 \to \ldots$ such that exists $i \in \mathbb{N}$, with $\mathcal{M}, s_i \models \neg Y$, and for all $j < i$, $\mathcal{M}, s_j \models \neg X$)

iff for all paths $s_0 \to s_1 \to s_2 \to \ldots$ *is not true that* (exists $i \in \mathbb{N}$, with $\mathcal{M}, s_i \models \neg Y$, and for all $j < i$, $\mathcal{M}, s_j \models \neg X$)

iff for all paths $s_0 \to s_1 \to s_2 \to \ldots$ for all $i \in \mathbb{N}$, *is not true that* ($\mathcal{M}, s_i \models \neg Y$), **or** *is not true that* (for all $j < i$, $\mathcal{M}, s_j \models \neg X$)

iff for all paths $s_0 \to s_1 \to s_2 \to \ldots$ for all $i \in \mathbb{N}$, $\mathcal{M}, s_i \models \neg\neg Y$, **or** exists $j < i$, such that *is not true that* ($\mathcal{M}, s_j \models \neg X$)

iff for all paths $s_0 \to s_1 \to s_2 \to \ldots$ for all $i \in \mathbb{N}$, $\mathcal{M}, s_i \models Y$, **or** exists $j < i$, such that $\mathcal{M}, s_j \models \neg\neg X$

iff for all paths $s_0 \to s_1 \to s_2 \to \ldots$ for all $i \in \mathbb{N}$, $\mathcal{M}, s_i \models Y$, or exists $j < i$, such that $\mathcal{M}, s_j \models X$

CS3234 - Tutorial 10, Solutions

4.9.6.

Prove $\vdash_{\text{tot}} (\!|\ x \geq 0\ |\!)$ `Downfac` $(\!|\ y = x!\ |\!)$.

$(\!|\ x \geq 0\ |\!)$	
$(\!|\ (\ 1 = \frac{x!}{x!}\ \wedge\ x \geq 0\ )\ \wedge\ 0 \leq x\ |\!)$	Implied
`a = x;`	
	Assignment
$(\!|\ (\ 1 = \frac{x!}{a!}\ \wedge\ a \geq 0\ )\ \wedge\ 0 \leq a\ |\!)$	
`y = 1;`	
	Assignment
$(\!|\ (\ y = \frac{x!}{a!}\ \wedge\ a \geq 0\ )\ \wedge\ 0 \leq a = E\ |\!)$	$(\!|\ \eta \wedge 0 \leq E\ |\!)$
`while (a > 0) {`	
	Invariant Hyp. and guard
$(\!|\ (\ y = \frac{x!}{a!}\ \wedge\ a \geq 0\ )\ \wedge\ (\ a > 0\ )\ \wedge\ 0 \leq a\ = E_0\ |\!)$	$(\!|\ \eta\ \wedge\ B\ \wedge\ 0 \leq E = E_0\ |\!)$
$(\!|\ (\ y * a = \frac{x!}{(a-1)!}\ \wedge\ a-1 \geq 0\ )\ \wedge\ 0 \leq a-1 < E_0\ |\!)$	Implied
`y = y * a;`	
	Assignment
$(\!|\ (\ y = \frac{x!}{(a-1)!}\ \wedge\ a-1 \geq 0\ )\ \wedge\ 0 \leq a-1 < E_0\ |\!)$	
`a = a - 1;`	
	Assignment
$(\!|\ (\ y = \frac{x!}{a!}\ \wedge\ a \geq 0\ )\ \wedge\ 0 \leq a < E_0\ |\!)$	$(\!|\ \eta\ \wedge\ 0 \leq E < E_0\ |\!)$
`}`	
	Total-while
$(\!|\ (\ y = \frac{x!}{a!}\ \wedge\ a \geq 0\ )\ \wedge\ a \leq 0\ |\!)$	$(\!|\ \eta \wedge \neg B\ |\!)$
$(\!|\ y = x!\ |\!)$	Implied

4.8.1.

The invariant η for the `while` in `Min-sum` when we prove **S2** is:

$$\forall i, j(i \leq j < k \rightarrow s \leq S_{i,j}) \wedge \forall i(i < k \rightarrow t < S_{i,k-1}) \wedge \exists i_0, j_0(1 \leq i_0 \leq j_0 \leq n \wedge s = S_{i_0,j_0})$$

To prove total correctness for **S2** and `Min-sum` (exercise **4.9.5.**) we have to add to the partial correctness proof the expressions $E = n+1-k$, and $E_0 = n+1-2 = n-1$ (for the termination argumentation).