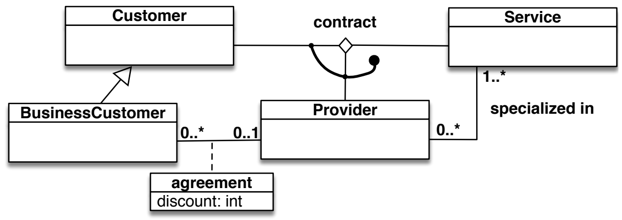
Formal Methods – July 12, 2019

(Time to complete the test: 2 hours)

Exercise 1. Express the following UML class diagram in FOL:



Exercise 2. Consider the above UML class diagram and the following (partial) instantiation:

Customer
c1
c2

BusiCustumer
b1
b2

Provider
p1
p2

agreement/disc		
b1	p1	30

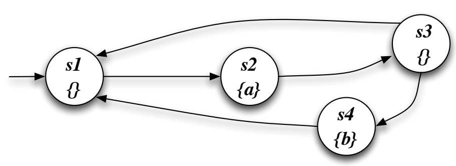
Service
s1
s2
s3
s4
s5

specializedin	
p1	s1
p1	s2
p1	s3
p2	s4
p2	s5

contacts		
c1	p1	s1
c1	p2	s2
c2	p1	s1
b1	p1	s4
b2	p2	s5

1. Check whether the above instantiation, once completed, is correct, and explain why it is or it is not.
2. Express in FOL the following queries and evaluate them over the completed instantiation:
   (a) Return those providers that are specialized in at least two services.
   (b) Return those business customers that have contracts only with providers with whom they have an agreement.
   (c) Return those business customers that have contracts with all providers with whom have an agreement .
   (d) Check whether there exists a customer with contracts for all services.

Exercise 3. Model check the Mu-Calculus formula $\nu X.\mu Y.((a \land \langle next\rangle X) \lor ([next]\neg b \land \langle next\rangle Y)$ and the CTL formula $EG(AFa \land (EFb \lor AG\neg b))$ (showing its translation in Mu-Calculus) against the following transition system:



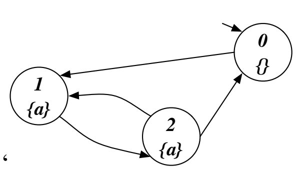
Exercise 4. Check whether the Hoare triple below is correct, by using $(x \geq 0 \land y \geq 0 \land x + y = 23)$ as invariant:

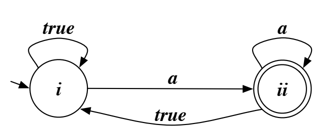
$$\{x = 23 \land y = 0\}\ \texttt{while(x>0) do (x=x-1; y:= y+1)}\ \{y = 23\}$$

Exercise 5. Check whether the following FOL formula is valid, by using tableaux:

$$(\forall x.(A(x) \equiv B(x)))\ \supset\ ((\forall y.A(y)) \equiv (\forall z.B(z)))$$

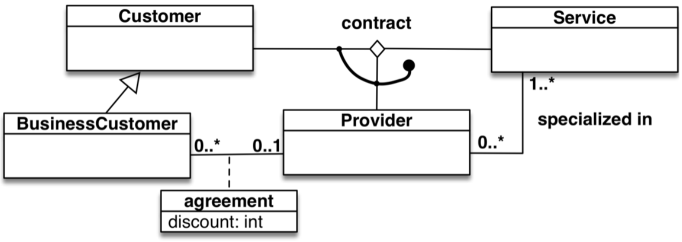
Exercise 6 (optional). [1] Model check the LTL formula $\Diamond\Box\neg a$ against the following transition system, by considering that the Büchi automaton for $\neg(\Diamond\Box\neg a)$ is the one below:





[1] *The student can get the maximum grade even without doing Exercise 6.*

Exercise 1. Express the following UML class diagram in FOL:



ALFABETO:

$C(x),\ BC(x),\ S(x),\ P(x)$

$A(x,y)$

$DISCOUNT(x,y,z)$

$CONTRACT(x,y,z)$

$SPECIN(x,y)$

RELAZIONI:

$\forall x,y.\ A(x,y) \supset BC(x) \wedge P(y)$

$\forall x.\ BC(x) \supset 0 \leq \#\{y \mid A(x,y)\} \leq 1$

$\forall y.\ P(y) \supset 0 \leq \#\{x \mid A(x,y)\}$

$\forall x,y,z.\ DISCOUNT(x,y,z) \supset A(x,y) \wedge INT(z)$

$\forall x,y.\ SPECIN(x,y) \supset S(x) \wedge P(y)$

$\forall x.\ S(x) \supset 0 \leq \#\{y \mid SPECIN(x,y)\}$

$\forall y.\ P(y) \supset 1 \leq \#\{x \mid SPECIN(x,y)\}$

$\forall x,y,z.\ CONTRACT(x,y,z) \supset C(x) \wedge P(y) \wedge S(z)$

$\forall x,y,z,z'.\ CONTRACT(x,y,z) \wedge CONTRACT(x,y,z') \supset z = z'$

ISA:

$\forall x.\ BC(x) \supset C(x)$

Exercise 2. Consider the above UML class diagram and the following (partial) instantiation:

Customer

c1
c2

BusiCustumer

b1
b2

Provider

p1
p2

agreement/disc

b1	p1	30

Service

s1
s2
s3
s4
s5

specializedin

p1	s1
p1	s2
p1	s3
p2	s4
p2	s5

contacts

c1	p1	s1
c1	p2	s2
c2	p1	s1
b1	p1	s4
b2	p2	s5

1. Check whether the above instantiation, once completed, is correct, and explain why it is or it is not.
2. Express in FOL the following queries and evaluate them over the completed instantiation:
   (a) Return those providers that are specialized in at least two services.
   (b) Return those business customers that have contracts only with providers with whom they have an agreement.
   (c) Return those business customers that have contracts with all providers with whom have an agreement .
   (d) Check whether there exists a customer with contracts for all services.

$C = \{c_1, c_2, b_1, b_2\}$

1) $\forall x,y.\ A(x,y) \supset BC(x) \land P(y)$

b_1 IS A BC
p_1 IS A P → CARDINALS OK!

$\forall x,y.\ SPECIN(x,y) \supset P(x) \land S(y)$

p_1, p_2 ARE PROVIDERS
→ CARDINALS OK!
s_1, s_2, s_3, s_4, s_5 ARE SERVICES

$\forall x,y,z.\ CONTRACT(x,y,z) \supset C(x) \land P(y) \land S(z)$

c_1, c_2, b_1, b_2 ARE CUSTOMERS

p_1, p_2 ARE PROVIDERS
→ CARDINALS OK!
s_1, s_2, s_3, s_4, s_5 ARE SERVICES

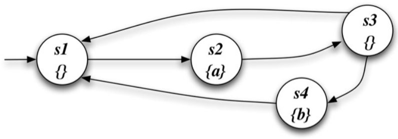
2) a) $\exists y,y'.\ P(x) \land SPECIN(x,y) \land SPECIN(x,y') \land y \neq y'$
$\{p_1, p_2\}$ ✓

b) $\forall p,s.\ (BC(x) \land CONCRACT(x,p,s)) \supset A(x,p)$
$\{b_1\}$ ✓

c) $\forall p.\ (BC(x) \land A(x,p)) \supset \exists s.\ CONCRACT(x,p,s)$
$\{b_1\}$ ✓

d) $\forall s.\ \exists x.\ C(x) \land (S(s) \supset \exists p.\ CONTRACT(x,p,s))$ ✗

Exercise 3. Model check the Mu-Calculus formula $\nu X.\mu Y.((a \wedge \langle next \rangle X) \vee ([next]\neg b \wedge \langle next \rangle Y))$ and the CTL formula $EG(AFa \wedge (EFb \vee AG\neg b))$ (showing its translation in Mu-Calculus) against the following transition system:



a) $\nu X.\mu Y.((a \wedge \langle NEXT \rangle X) \vee ([NEXT]\neg b \wedge \langle NEXT \rangle Y))$

$[X_0] = \{s_1, s_2, s_3, s_4\}$

$[X_1] = [\mu Y.((a \wedge \langle NEXT \rangle X_0) \vee ([NEXT]\neg b \wedge \langle NEXT \rangle Y))]$

$[Y_0] = \emptyset$

$[Y_1] = ([a] \cap PREE(NEXT, X_0)) \cup (PREA(NEXT, \neg b) \cap PREE(NEXT, Y_0)) =$

$= (\{s_2\} \cap \{s_1, s_2, s_3, s_4\}) \cup (\{s_1, s_2, s_4\} \cap \emptyset) = \{s_2\}$

$[Y_2] = ([a] \cap PREE(NEXT, X_0)) \cup (PREA(NEXT, \neg b) \cap PREE(NEXT, Y_1)) =$

$= (\{s_2\} \cap \{s_1, s_2, s_3, s_4\}) \cup (\{s_1, s_2, s_4\} \cap \{s_1\}) = \{s_1, s_2\}$

$[Y_3] = ([a] \cap PREE(NEXT, X_0)) \cup (PREA(NEXT, \neg b) \cap PREE(NEXT, Y_2)) =$

$= (\{s_2\} \cap \{s_1, s_2, s_3, s_4\}) \cup (\{s_1, s_2, s_4\} \cap \{s_1, s_3, s_4\}) = \{s_1, s_2, s_4\}$

$[Y_4] = ([a] \cap PREE(NEXT, X_0)) \cup (PREA(NEXT, \neg b) \cap PREE(NEXT, Y_3)) =$

$= (\{s_2\} \cap \{s_1, s_2, s_3, s_4\}) \cup (\{s_1, s_2, s_4\} \cap \{s_1, s_3, s_4\} = \{s_1, s_2, s_4\}$

$[Y_3] = [Y_4] = [X_1] = \{s_1, s_2, s_4\}$

$[X_2] = [\mu Y.((a \wedge \langle NEXT \rangle X_1) \vee ([NEXT]\neg b \wedge \langle NEXT \rangle Y))]$

$[Y_0] = \emptyset$

$[Y_1] = ([a] \cap PREE(NEXT, X_1)) \cup (PREA(NEXT, \neg b) \cap PREE(NEXT, Y_0)) =$

$= (\{s_2\} \cap \{s_1, s_3, s_4\}) \cup (\{s_1, s_2, s_4\} \cap \emptyset) = \emptyset \qquad [Y_0] = [Y_1] = [X_2] = \emptyset$

$[X_3] = [\mu Y.((a \wedge \langle NEXT \rangle X_2) \vee ([NEXT]\neg b \wedge \langle NEXT \rangle Y))]$

$[Y_0] = \emptyset$

$[Y_1] = ([a] \cap PREE(NEXT, X_2)) \cup (PREA(NEXT, \neg b) \cap PREE(NEXT, Y_0)) =$

$= (\{s_2\} \cap \emptyset) \cup (\{s_1, s_2, s_4\} \cap \emptyset) = \emptyset$

$[Y_0] = [Y_1] = [X_3] = \emptyset \qquad [X_2] = [X_3] = \emptyset$

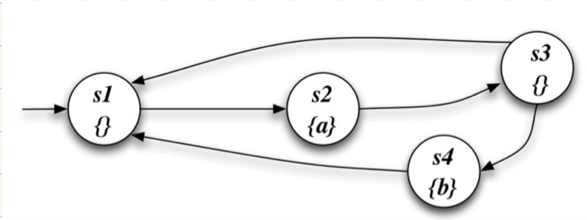
$s_1 \in [\nu X.\mu Y.((a \wedge \langle NEXT \rangle X) \vee ([NEXT]\neg b \wedge \langle NEXT \rangle Y))] = \emptyset$? NO!

b) $EG(\underbrace{AF\,a}_{\delta} \wedge (\underbrace{EF\,b}_{\beta} \vee \underbrace{AG\,\neg b}_{\alpha}))$

$\gamma = EF\,b \vee AG\,\neg b$

$\varepsilon = AF\,a \wedge (EF\,b \vee AG\,\neg b)$

$\eta = EG(AF\,a \wedge (EF\,b \vee AG\,\neg b))$



$[\alpha] = [AG\,\neg b] = [\nu Z.\ \neg b \wedge [NEXT]Z]$

$[Z_0] = \{1,2,3,4\}$

$[Z_1] = [\neg b] \cap PREA(NEXT, Z_0) =$

$= \{1,2,3\} \cap \{1,2,3,4\} = \{1,2,3\}$

$[Z_2] = [\neg b] \cap PREA(NEXT, Z_1) =$

$= \{1,2,3\} \cap \{1,2,4\} = \{1,2\}$

$[Z_3] = [\neg b] \cap PREA(NEXT, Z_2) =$

$= \{1,2,3\} \cap \{1,4\} = \{1\}$

$[Z_4] = [\neg b] \cap PREA(NEXT, Z_3) =$

$= \{1,2,3\} \cap \{4\} = \emptyset$

$[Z_5] = \emptyset$ $\qquad [Z_4] = [Z_5] = \emptyset = [\alpha]$

$[\beta] = [EF\,b] = [\mu Z.\ b \vee \langle NEXT \rangle Z]$

$[Z_0] = \emptyset$

$[Z_1] = [b] \cup PREE(NEXT, Z_0) =$

$= \{4\} \cup \emptyset = \{4\}$

$[Z_2] = [b] \cup PREE(NEXT, Z_1) =$

$= \{4\} \cup \{3\} = \{3,4\}$

$[Z_3] = [b] \cup PREE(NEXT, Z_2) =$

$= \{4\} \cup \{2,3\} = \{2,3,4\}$

$[Z_4] = [b] \cup PREE(NEXT, Z_3) =$

$= \{4\} \cup \{1,2,3\} = \{1,2,3,4\}$

$[Z_5] = [b] \cup PREE(NEXT, Z_4) =$

$= \{4\} \cup \{1,2,3,4\} = \{1,2,3,4\}$ $\qquad [Z_4] = [Z_5] = [\beta] = \{1,2,3,4\}$

$[\delta] = [AF\ \alpha] = [\mu Z.\ \alpha \vee [NEXT]Z]$

$[Z_0] = \phi$

$[Z_1] = [\alpha] \cup PREA(NEXT, Z_0) =$

$= \{2\} \cup \phi = \{2\}$

$[Z_2] = [\alpha] \cup PREA(NEXT, Z_1) =$

$= \{2\} \cup \{1\} = \{1,2\}$

$[Z_3] = [\alpha] \cup PREA(NEXT, Z_2) =$

$= \{2\} \cup \{1,4\} = \{1,2,4\}$

$[Z_4] = [\alpha] \cup PREA(NEXT, Z_3) =$

$= \{2\} \cup \{1,3,4\} = \{1,2,3,4\}$

$[Z_5] = [\alpha] \cup PREA(NEXT, Z_4) =$

$= \{2\} \cup \{1,2,3,4\} = \{1,2,3,4\}$ $[Z_4] = [Z_5] = \{1,2,3,4\} = [\delta]$

$[\gamma] = [\beta \vee \alpha] = [\beta] \cup [\alpha] = \{4\} \cup \phi = \{1,2,3,4\} \cup \phi = \{1,2,3,4\} = [\gamma]$

$[\varepsilon] = [\delta \wedge \gamma] = [\delta] \cap [\gamma] = \{1,2,3,4\} \cap \{1,2,3,4\} = \{1,2,3,4\} = [\varepsilon]$

$[\eta] = [EG\ \varepsilon] = [\nu Z.\ \varepsilon \wedge \langle NEXT \rangle Z]$

$[Z_0] = \{1,2,3,4\}$

$[Z_1] = [\varepsilon] \cap PREE(NEXT, Z_0) =$

$= \{1,2,3,4\} \cap \{1,2,3,4\} = \{1,2,3,4\}$

$[Z_0] = [Z_1] = \{1,2,3,4\} = [\eta]$

$\Upsilon_{s_1} \models \eta\ ? \rightarrow \quad s_1 \in [\eta] = \{1,2,3,4\}\ ?$ YES!

Exercise 4. Check whether the Hoare triple below is correct, by using $\overset{I}{(x \geq 0 \wedge y \geq 0 \wedge x + y = 23)}$ as invariant:

$$\overset{P}{\{x = 23 \wedge y = 0\}} \texttt{ while(}\overset{g}{\texttt{x>0}}\texttt{) do } \overset{\delta}{\texttt{(x=x-1; y:= y+1)}} \overset{Q}{\{y = 23\}}$$

1. $P \supset I$
2. $\neg g \wedge I \supset Q$
3. $\{g \wedge I\}\ \delta\ \{I\}$

1. $\{x=23 \wedge y=0\} \supset (x\geq 0 \wedge y \geq 0 \wedge x+y=23)$ ✓
2. $x \leq 0 \wedge (x\geq 0 \wedge y \geq 0 \wedge x+y=23) \supset y=23$ ✓

3. $\{x>0 \wedge (x\geq 0 \wedge y \geq 0 \wedge x+y=23)\}\ (x=x-1;\ y=y+1)\ \{x\geq 0 \wedge y \geq 0 \wedge x+y=23\}$

$\{x>0 \wedge (x\geq 0 \wedge y \geq 0 \wedge x+y=23)\} \supset wp(x=x-1;\ y=y+1)\{x\geq 0 \wedge y \geq 0 \wedge x+y=23\}$!

$\{x\geq 0 \wedge y \geq 1 \wedge x+y=24\}[x/x-1] = \{x \geq 1 \wedge y \geq 1 \wedge x+y=25\}$

$x=x-1$

$\{x\geq 0 \wedge y \geq 0 \wedge x+y=23\}\ [y/y-1] = \{x\geq 0 \wedge y \geq 1 \wedge x+y=24\}$

$y=y-1$

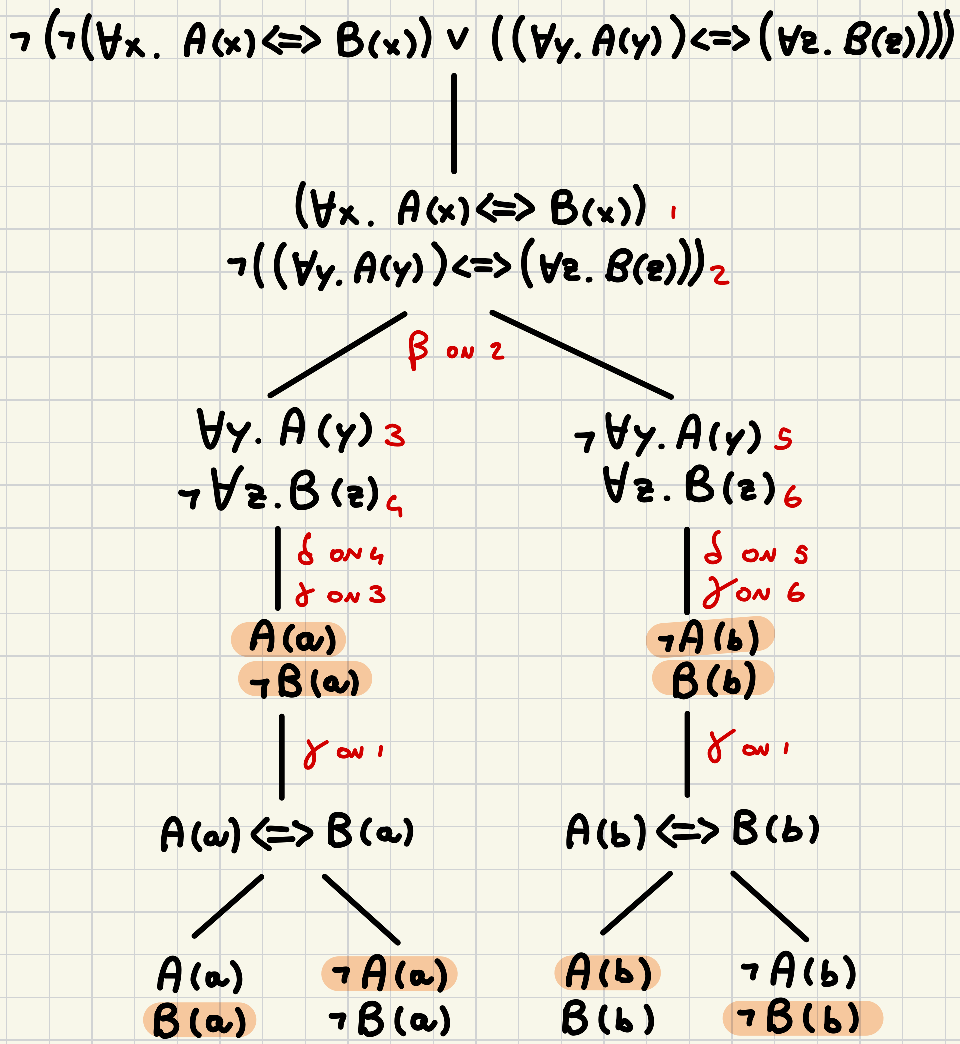
$\{x\geq 0 \wedge y \geq 0 \wedge x+y=23\}$

$\{x>0 \wedge y \geq 0 \wedge x+y=23)\} \supset \{x \geq 1 \wedge y \geq 1 \wedge x+y=25\}$? ✗

$(x\geq 0 \wedge y \geq 0 \wedge x+y=23)$ IS NOT AN INVARIANT

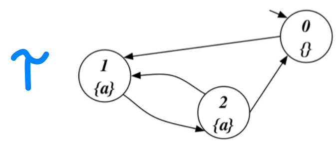
Exercise 5. Check whether the following FOL formula is valid, by using tableaux:

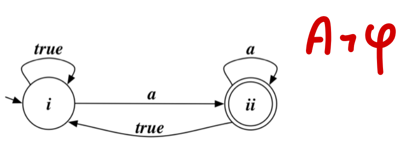
$$(\forall x.(A(x) \equiv B(x))) \supset ((\forall y.A(y)) \equiv (\forall z.B(z)))$$



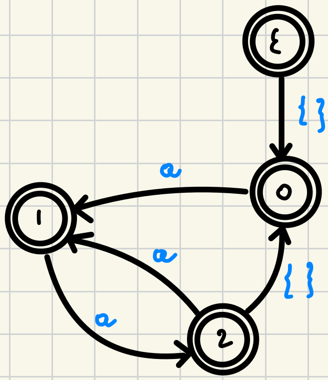
THE FOL FORMULA IS VALID BECAUSE ALL BRANCHES ARE CLOSED

Exercise 6 (optional). [1] Model check the LTL formula $\Diamond\Box\neg a$ against the following transition system, by considering that the Büchi automaton for $\neg(\Diamond\Box\neg a)$ is the one below:

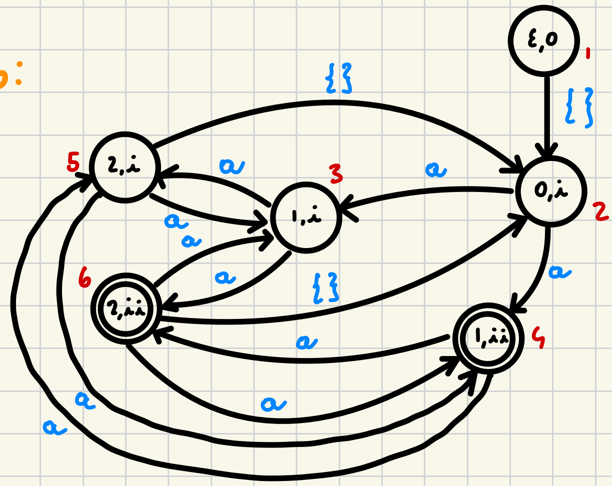




A_Υ:



$A_\Upsilon \wedge A_{\neg\varphi}$:



$$\nu X.\mu Y\,(F \wedge \langle NEXT\rangle X \vee \langle NEXT\rangle Y)$$

$$[X_0] = \{1,2,3,4,5,6\}$$

$$[X_1] = [\mu Y\,(F \wedge \langle NEXT\rangle X_0 \vee \langle NEXT\rangle Y)]$$

$$[Y_0] = \emptyset$$

$$[Y_1] = [F] \cap PREE(NEXT, X_0) \cup PREE(NEXT, Y_0) =$$

$$= \{4,6\} \cap \{1,2,3,4,5,6\} \cup \emptyset = \{4,6\}$$

$$[Y_2] = [F] \cap PREE(NEXT, X_0) \cup PREE(NEXT, Y_1) =$$

$$= \{4,6\} \cap \{1,2,3,4,5,6\} \cup \{2,3,4,5,6\} = \{2,3,4,5,6\}$$

$$[Y_3] = [F] \cap PREE(NEXT, X_0) \cup PREE(NEXT, Y_2) =$$

$$= \{4,6\} \cap \{1,2,3,4,5,6\} \cup \{1,2,3,4,5,6\} = \{1,2,3,4,5,6\}$$

$$[Y_4] = [F] \cap PREE(NEXT, X_0) \cup PREE(NEXT, Y_3) =$$

$$= \{4,6\} \cap \{1,2,3,4,5,6\} \cup \{1,2,3,4,5,6\} = \{1,2,3,4,5,6\}$$

$$[Y_3] = [Y_4] = [X_1] = \{1,2,3,4,5,6\}$$

$$[X_0] = [X_1] = \{1,2,3,4,5,6\}$$

$s_1 \in [\nu X.\mu Y\,(F \wedge \langle NEXT\rangle X \vee \langle NEXT\rangle Y)] = \{1,2,3,4,5,6\}$? YES!

SO $(A_\Upsilon \wedge A_{\neg\varphi}) \neq \emptyset \rightarrow \Upsilon \not\models \varphi$