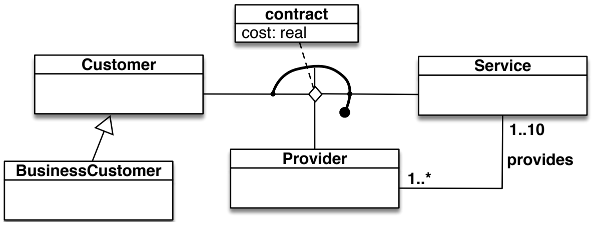
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

Formal Methods - Final Test A – December 21, 2017

(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
c3
c4

$BCustumers$
b1
b2
b3

$Services$
s1
s2
s3

$Provider$
p1
p2

$provides$

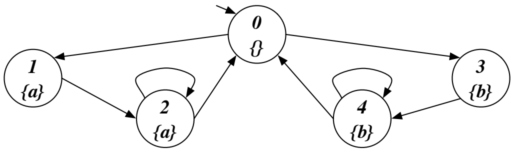
p1	s1
p1	s2
p1	s3
p2	s2

$contacts/cost$

c1	s1	p1	90.0
c1	s2	p1	80.0
c1	s3	p1	50.0
b2	s1	p2	170,0
b2	s2	p2	100,0

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) Check that, for every provider x and service y involved in a contract, provider x does provide service y.
    (b) Return those customers that have contracts only for services provided by $p1$.
    (c) Return those customers that have a contract for all services.

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



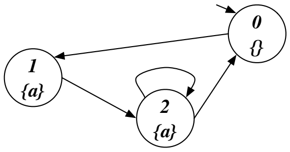
Exercise 4. Check whether the Hoare triple below is correct, by using $(x \geq 0 \wedge y \geq 0 \wedge x + y = 23)$ as invariant:

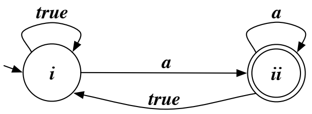
$$\{x = 23 \wedge y = 0\}\ \texttt{while(x>0) do (x=x-1; y:= y+1)}\ \{y = 23\}$$

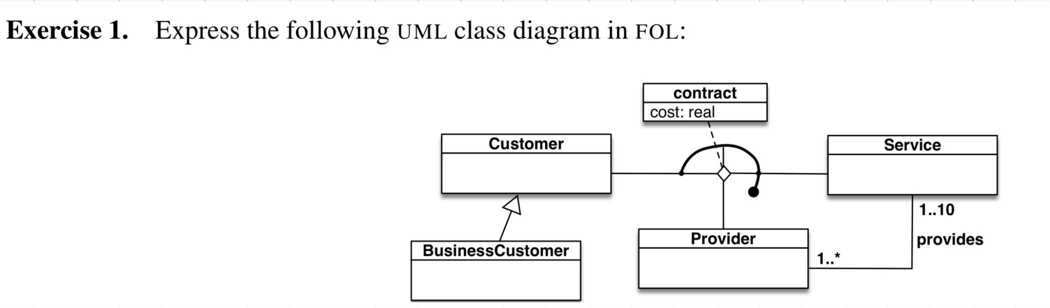
Exercise 5. Check whether the following FOL formula is valid, by using tableaux:

$$(\forall x.P(x) \wedge \forall x.Q(x)) \equiv \forall x.(P(x) \wedge Q(x))$$

Exercise 6 (optional). 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:







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

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

$CON(x, y, z)$

$COST(x, y, z, w)$

$PROV(x, y)$

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

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

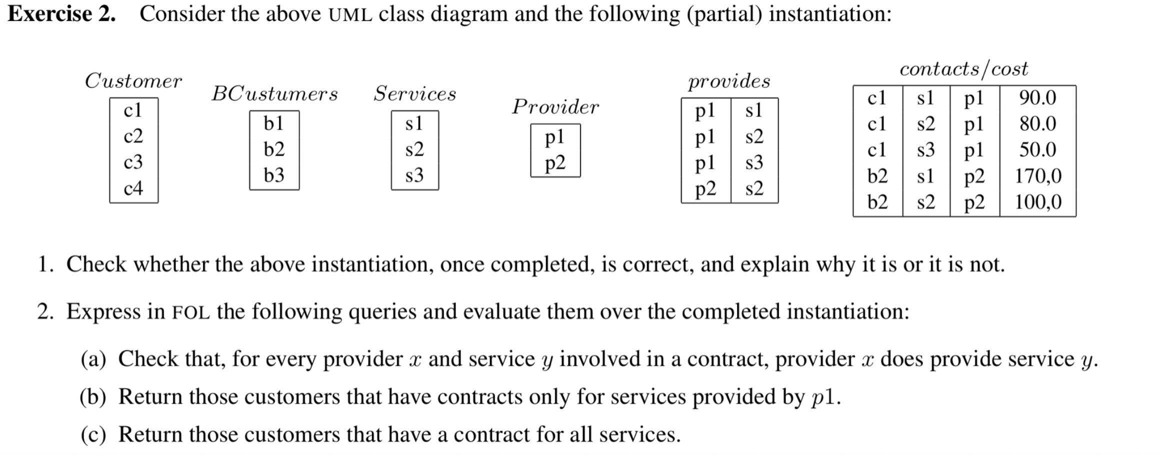
$\forall x, y, z, w.\ COST(x, y, z, w) \supset CON(x, y, z) \wedge REAL(w)$

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

$\forall x.\ P(x) \supset 1 \leq \#\{y \mid PROV(x, y)\} \leq 10$

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

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



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

Customer
c1
c2
c3
c4

BCustumers
b1
b2
b3

Services
s1
s2
s3

Provider
p1
p2

provides

p1	s1
p1	s2
p1	s3
p2	s2

contacts/cost

c1	s1	p1	90.0
c1	s2	p1	80.0
c1	s3	p1	50.0
b2	s1	p2	170,0
b2	s2	p2	100,0

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) Check that, for every provider x and service y involved in a contract, provider x does provide service y.
   (b) Return those customers that have contracts only for services provided by $p1$.
   (c) Return those customers that have a contract for all services.

1) $C = \{c_1, c_2, c_3, c_4, b_1, b_2, b_3\}$

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

p_1, p_2 ARE PROVIDERS → CARDINALS OK!

s_1, s_2, s_3 ARE SERVICES

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

c_1, b_2 ARE CUSTOMERS

p_1, p_2 ARE PROVIDERS → CARDINALS OK!

s_1, s_2, s_3 ARE SERVICES

2) a. $\forall c,p,s.\ CON(c,s,p) \supset PROV(p,s)$

$\{FALSE\}$

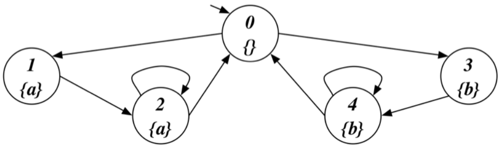
b. $C(x) \wedge \exists s,p.\ CON(x,s,p) \wedge \forall s,p.\ (CON(x,s,p) \supset PROV(p_1,s))$

$\{c_1\}$

c. $\forall s.\ C(x) \wedge (S(s) \supset \exists p\ CON(x,s,p))$

$\{c_1\}$

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



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

$[X_0] = \{0,1,2,3,4\}$

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

$[Y_0] = \phi$

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

$= (\{1,2\} \cap \{0,1,2,3,4\}) \cup (\{3,4\} \cap \phi) = \{1,2\}$

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

$= (\{1,2\} \cap \{0,1,2,3,4\}) \cup (\{3,4\} \cap \{0,1,2\}) = \{1,2\}$

$[Y_1] = [Y_2] = [X_1] = \{1,2\}$

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

$[Y_0] = \phi$

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

$= (\{1,2\} \cap \{1\}) \cup (\{3,4\} \cap \phi) = \{1\}$

$[Y_2] = ([a] \cap PREA(NEXT, X_1)) \cup ([b] \cap PREE(NEXT, Y_1)) =$

$= (\{1,2\} \cap \{1\}) \cup (\{3,4\} \cap \{0\}) = \{1\}$

$[Y_1] = [Y_2] = [X_2] = \{1\}$

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

$[Y_0] = \phi$

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

$(\{1,2\} \cap \phi) \cup (\{3,4\} \cap \phi) = \phi$

$[Y_0] = [Y_1] = [X_3] = \phi$

$[X_4] = [\mu Y.((a \wedge [NEXT]X_3) \vee (b \wedge \langle NEXT \rangle Y))]$

$[Y_0] = \phi$

$[Y_1] = ([a] \cap PREA(NEXT, X_3)) \cup ([b] \cap PREE(NEXT, Y_0)) =$

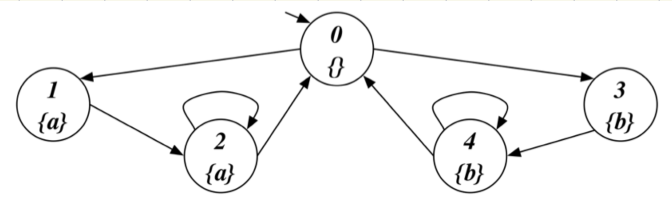
$(\{1,2\} \cap \phi) \cup (\{3,4\} \cap \phi) = \phi$

$[Y_0] = [Y_1] = [X_4] = \phi$

$[X_3] = [X_4] = \phi$

$s_0 \in [\nu X. \mu Y. ((a \wedge [NEXT]X) \vee (b \wedge \langle NEXT \rangle Y))] = \phi$? No!

b) $AF(\underbrace{EG(\underbrace{a \supset \underbrace{AX\, \underbrace{EX \neg a}_{\alpha}}_{\beta}}_{\gamma})}_{\delta})$ with ε under the whole formula



$[\alpha] = [EX \neg a] = [\langle NEXT \rangle \neg a] = PREE(NEXT, \neg a) = \{0,2,3,4\} = [\alpha]$

$[\beta] = [AX\, \alpha] = [[NEXT]\alpha] = PREA(NEXT, \alpha) = \{1,2,3,4\} = [\beta]$

$[\gamma] = [a \supset \beta] = [\neg a] \cup [\beta] = \{0,3,4\} \cup \{1,2,3,4\} = \{0,1,2,3,4\} = [\gamma]$

$[\delta] = [EG\, \gamma] = [\nu Z. \gamma \wedge \langle NEXT \rangle Z]$

$[Z_0] = \{0,1,2,3,4\}$

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

$= \{0,1,2,3,4\} \cap \{0,1,2,3,4\} = \{0,1,2,3,4\}$

$[Z_0] = [Z_1] = [\delta] = \{0,1,2,3,4\}$

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

$[Z_0] = \phi$

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

$= \{0,1,2,3,4\} \cup \phi = \{0,1,2,3,4\}$

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

$= \{0,1,2,3,4\} \cup \{0,1,2,3,4\} = \{0,1,2,3,4\}$

$[Z_1] = [Z_2] = [\varepsilon] = \{0,1,2,3,4\}$

$\mathcal{T}\, s_0 \models \varepsilon$? → $s_0 \in [\varepsilon] = \{0,1,2,3,4\}$? YES!

I

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

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

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\. $(x \leq 0 \wedge (x \geq 0 \wedge y \geq 0 \wedge x+y=23)) \supset y=23$

$(x=0 \wedge y \geq 0 \wedge x+y=23) \supset y=23$ ✓

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

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

$\{x \geq 0 \wedge y \geq -1 \wedge x+y=22\}[x/x-1] = \{x \geq 1 \wedge y \geq -1 \wedge x+y=23\}$

$x=x-1;$

$\{x \geq 0 \wedge y \geq 0 \wedge x+y=23\}[y/y+1] = \{x \geq 0 \wedge y \geq -1 \wedge x+y=22\}$

$y=y+1;$

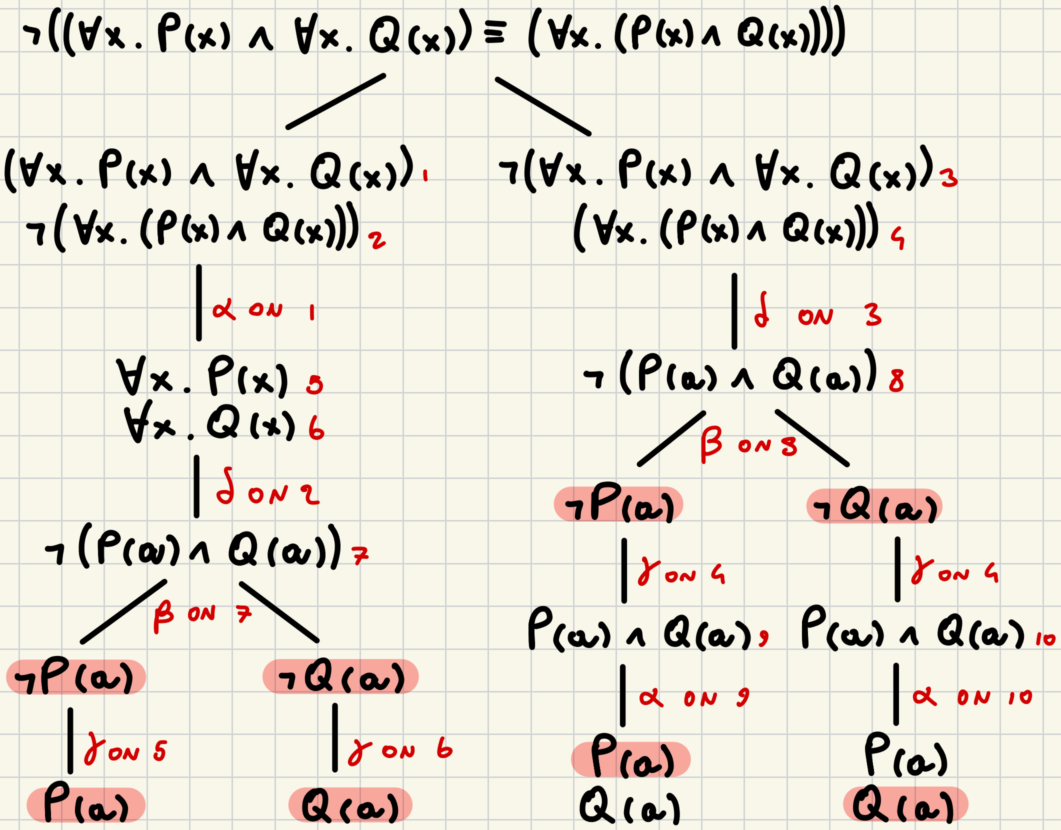
$\{x \geq 0 \wedge y \geq 0 \wedge x+y=23\}$

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

$(x \geq 0 \wedge y \geq 0 \wedge x+y=23)$ IS AN INVARIANT

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

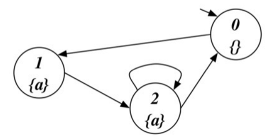
$$(\forall x.P(x) \wedge \forall x.Q(x)) \equiv \forall x.(P(x) \wedge Q(x))$$

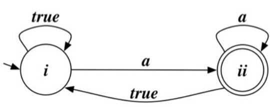


SINCE ALL BRANCHES ARE CLOSED, THE FORMULA IS VALID

Exercise 6 (optional). 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:

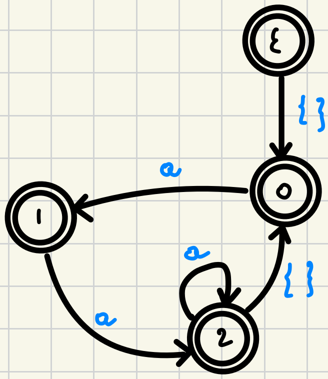
Υ



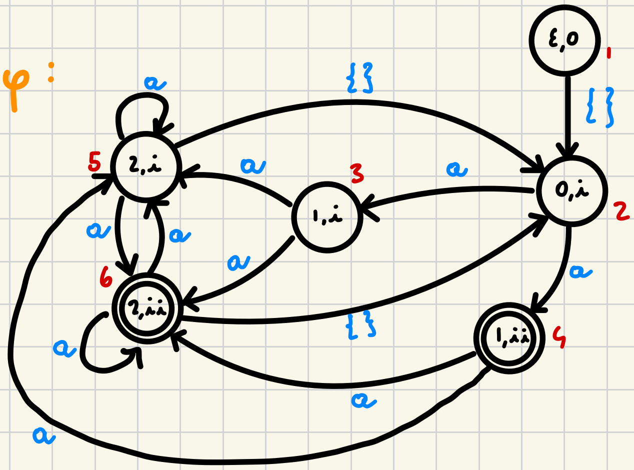


$A_{\neg\varphi}$

A_{Υ} :



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



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

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

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

$[Y_0]=\phi$

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

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

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

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

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

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

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

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

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

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

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

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