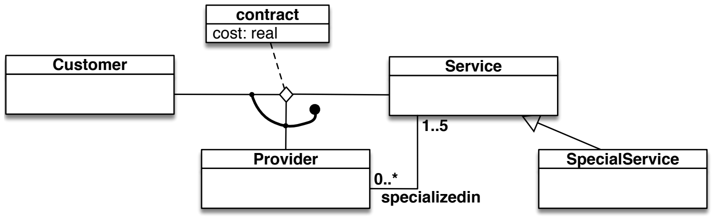
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

Formal Methods – June 17, 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
c3
c4

$Service$
s1
s2
s3

$SpecialService$
ss1
ss2

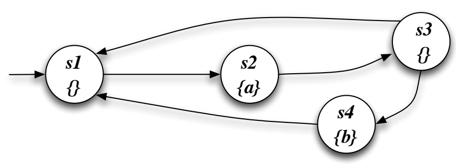
$Provider$
p1
p2

$specializedin$	
p1	s1
p1	s2
p1	s3
p2	ss1
p2	ss2

$contacts/cost$			
c1	p1	s1	90.0
c1	p2	s2	80.0
c2	p1	s1	50.0
c3	p2	ss1	170,0
c2	p2	ss2	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) Return those providers that have contracts with at least two customers.
   (b) Return those providers that have contracts only services they are specialized in.
   (c) Return those providers that have contracts all services they are specialized in.
   (d) Check whether there exists a customer with contracts for all services.

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



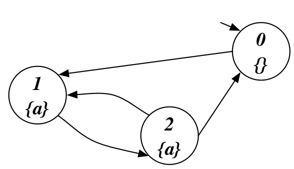
Exercise 4. Check whether CQ q_1 is contained in CQ q_2, reporting canonical DBs and homomorphism:

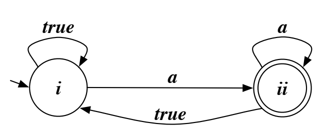
$$
\begin{array}{lcl}
q_1() & \leftarrow & edge(r,g), edge(g,b), edge(b,r). \\
q_2() & \leftarrow & edge(x,y), edge(y,z), edge(z,x), edge(z,v), edge(v,w), edge(w,z).
\end{array}
$$

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

$$(\forall x.\forall y.P(x,y) \supset Q(x)) \equiv (\forall x.(\exists y.P(x,y)) \supset Q(x))$$

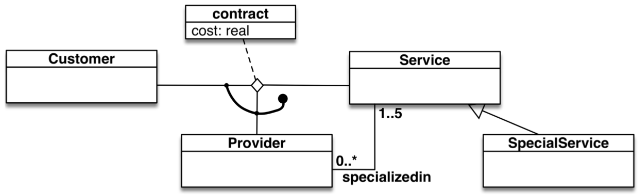
Exercise 6 (optional). [1] Model check the LTL formula $\Diamond\Box\neg a$ against the following transition system, by considering that the Büchi automaton for $\neg(\Diamond\Box\neg a)$ is the one below:





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

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



$C(x)$, $P(x)$, $S(x)$, $SS(x)$

$CON(x,y,z)$

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

$SPECIN(x,y)$

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

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

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

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

$\forall x.\ P(x) \supset 1 \leq \#\{y \mid SPECIN(x,y)\} \leq 5$

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

$\forall x.\ SS(x) \supset S(x)$

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

Customer

c1
c2
c3
c4

Service

s1
s2
s3

SpecialService

ss1
ss2

Provider

p1
p2

specializedin

p1	s1
p1	s2
p1	s3
p2	ss1
p2	ss2

contacts/cost

c1	p1	s1	90.0
c1	p2	s2	80.0
c2	p1	s1	50.0
c3	p2	ss1	170,0
c2	p2	ss2	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) Return those providers that have contracts with at least two customers.
   (b) Return those providers that have contracts only services they are specialized in.
   (c) Return those providers that have contracts all services they are specialized in.
   (d) Check whether there exists a customer with contracts for all services.

1) $S = \{s_1, s_2, s_3, ss_1, ss_2\}$

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

p_1, p_2 ARE PROVIDERS
$s_1, s_2, s_3, ss_1, ss_2$ ARE SERVICES → CARDINALS ARE OK!

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

c_1, c_2, c_3 ARE CUSTOMERS
p_1, p_2 ARE PROVIDERS
s_1, s_2, ss_1, ss_2 ARE SERVICES → CARDINALS ARE OK!

2) a. $\exists y, y', z. \; P(x) \wedge CON(y,x,z) \wedge CON(y',x,z) \wedge y \neq y'$

$\{p_1, p_2\}$

b. $\forall c, s. \; (P(x) \wedge CON(c,x,s)) \supset SPECIN(x,s)$

$\{p_1\}$

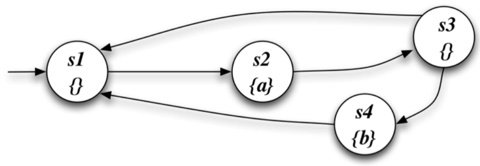
c. $\forall s. \; (P(x) \wedge SPECIN(x,s)) \supset \exists c \; CON(c,x,s)$

$\{p_2\}$

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

$\{\}$

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



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

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

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

$[Y_0] = \phi$

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

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

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

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

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

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

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

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

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

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

$[Y_0] = \phi$

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

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

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

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

$[Y_3] = ([a] \cap PREE(NEXT, X_1)) \cup ([\neg b] \cap PREE(NEXT, Y_2)) =$

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

$[Y_4] = ([a] \cap PREE(NEXT, X_1)) \cup ([\neg b] \cap PREE(NEXT, Y_3)) =$

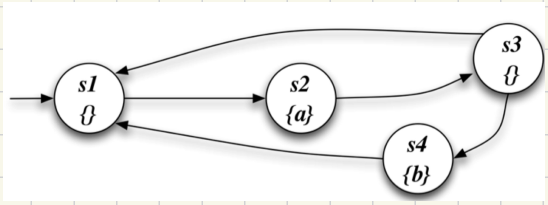
$= (\{2\} \cap \{1,2,3,4\}) \cup (\{1,2,3\} \cap \{1,2,3,4\}) = \{1,2,3\}$

$[Y_3] = [Y_4] = [X_2] = \{1,2,3\}$

$[X_1] = [X_2] = \{1,2,3\}$

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

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



$[\alpha] = [EG\,\neg b] = [\nu Z. \neg b \wedge \langle NEXT \rangle Z]$

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

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

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

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

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

$[Z_1] = [Z_2] = [\alpha] = \{1,2,3\}$

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

$[Z_0] = \emptyset$

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

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

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

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

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

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

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

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

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

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

$[\gamma] = [AF\ a] = [\mu Z\ a \vee [NEXT] Z]$

$[Z_0] = \phi$

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

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

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

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

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

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

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

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

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

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

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

$[\varepsilon] = [AG\ \delta] = [\nu Z.\ \delta \wedge [NEXT] Z]$

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

$[Z_1] = [\delta] \cap PREA(NEXT, Z_0) = \{1,2,3\} \cap \{1,2,3,4\} = \{1,2,3\}$

$[Z_2] = [\delta] \cap PREA(NEXT, Z_1) = \{1,2,3\} \cap \{1,2,4\} = \{1,2\}$

$[Z_3] = [\delta] \cap PREA(NEXT, Z_2) = \{1,2,3\} \cap \{1,4\} = \{1\}$

$[Z_4] = [\delta] \cap PREA(NEXT, Z_3) = \{1,2,3\} \cap \{4\} = \phi$

$[Z_5] = [\delta] \cap PREA(NEXT, Z_4) = \{1,2,3\} \cap \phi = \phi$

$[Z_4] = [Z_5] = [\varepsilon] = \phi$

$T_{s_1} \models \varepsilon\ ? \rightarrow s_1 \in [\varepsilon] = \phi\ ?$ **NO!**

Exercise 4. Check whether CQ q_1 is contained in CQ q_2, reporting canonical DBs and homomorphism:

$$\begin{aligned} q_1() &\leftarrow edge(r,g), edge(g,b), edge(b,r). \\ q_2() &\leftarrow edge(x,y), edge(y,z), edge(z,x), edge(z,v), edge(v,w), edge(w,z). \end{aligned}$$

CHECK WHETHER $q_1() \subseteq q_2()$

BUILD CANONICAL INTERPRETATION

$\mathcal{I}_{q_1}$:

$\Delta^{\mathcal{I}_{q_1}}: \{r, g, b\}$

$EDGE^{q_1}: \{\langle r,g\rangle, \langle g,b\rangle, \langle b,r\rangle\}$

$\mathcal{I}_{q_2}$:

$\Delta^{\mathcal{I}_{q_2}}: \{x, y, z, v, w\}$

$EDGE^{q_2}: \{\langle x,y\rangle, \langle y,z\rangle, \langle z,x\rangle, \langle z,v\rangle, \langle v,w\rangle, \langle w,z\rangle\}$

QUERY ANSWERING

$\mathcal{I}_{q_1}() \models q_2()$?

$\alpha(x) = ? \rightarrow \alpha(x) = r$
$\alpha(y) = ? \rightarrow \alpha(y) = g$
$\alpha(z) = ? \rightarrow \alpha(z) = b$
$\alpha(v) = ? \rightarrow \alpha(v) = r$
$\alpha(w) = ? \rightarrow \alpha(w) = g$

$\mathcal{I}_{q_1,\alpha} \models q_2()$ YES, SINCE

$\mathcal{I}_{q_1,\alpha} \models EDGE(x,y)$ $\quad \mathcal{I}_{q_1,\alpha} \models EDGE(y,z)$ $\quad \mathcal{I}_{q_1,\alpha} \models EDGE(z,x)$

$\mathcal{I}_{q_1,\alpha} \models EDGE(z,v)$ $\quad \mathcal{I}_{q_1,\alpha} \models EDGE(v,w)$ $\quad \mathcal{I}_{q_1,\alpha} \models EDGE(w,z)$

HOMOMORPHISM

$h(x) = \alpha(x) = r$
$h(y) = \alpha(y) = g$
$h(z) = \alpha(z) = b$
$h(v) = \alpha(v) = r$
$h(w) = \alpha(w) = g$

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

$$(\forall x.\forall y.P(x,y) \supset Q(x)) \equiv (\forall x.(\exists y.P(x,y)) \supset Q(x))$$

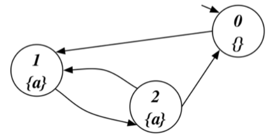
$\neg(\forall x,y.\ P(x,y) \supset Q(x)) \equiv (\forall x.(\exists y.P(x,y)) \supset Q(x))$

- $\forall x,y.\ P(x,y) \supset Q(x)$ 1
  $\neg(\forall x.(\exists y.P(x,y)) \supset Q(x))$ 2
  - $\exists x\ \neg(\exists y.P(x,y) \supset Q(x))$ 5
  - δ on 5
  - $\neg(\exists y.\ P(a,y) \supset Q(a))$ 6
  - α on 6
  - $\exists y.P(a,y)$ 7
    $\neg Q(a)$
  - δ on 7
  - $P(a,b)$
  - γ on 1
  - $P(a,b) \supset Q(a)$ 8
  - β on 8
    - $\neg P(a,b)$
    - $Q(a)$
- $\neg(\forall x,y.\ P(x,y) \supset Q(x))$ 3
  $\forall x.(\exists y.P(x,y)) \supset Q(x)$ 4
  - δ on 3
  - $\neg(P(a,b) \supset Q(a))$ 9
  - $P(a,b)$
    $\neg Q(a)$
  - γ on 4
  - $\exists y.\ P(a,y) \supset Q(a)$ 10
  - β on 10
    - $\neg\exists y.P(a,y)$ 11
      - γ on 11
      - $\neg P(a,b)$
    - $Q(a)$

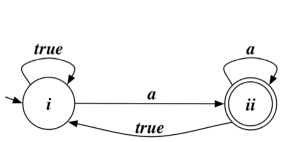
SINCE ALL BRANCHES ARE CLOSED THE FORMULA IS VALID

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:

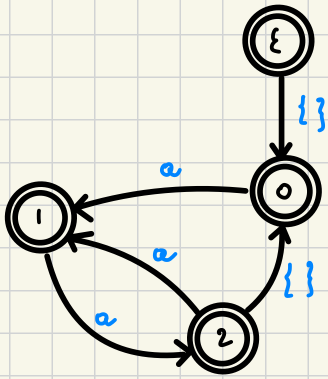
Υ



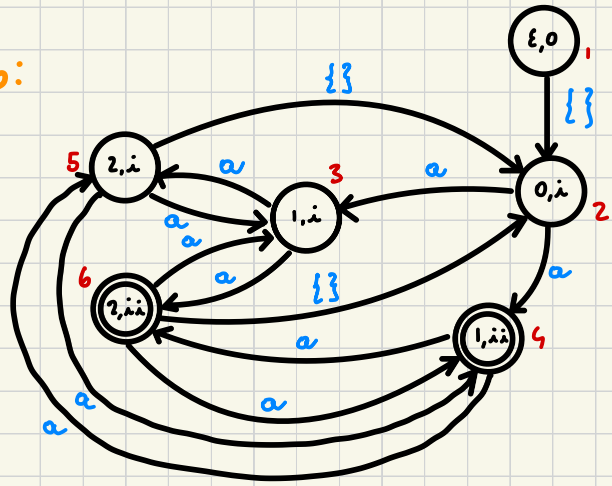
$A_{\neg\varphi}$



A_Υ:



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



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

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

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

$[Y_0] = \emptyset$

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

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

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

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

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

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

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

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

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

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

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

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