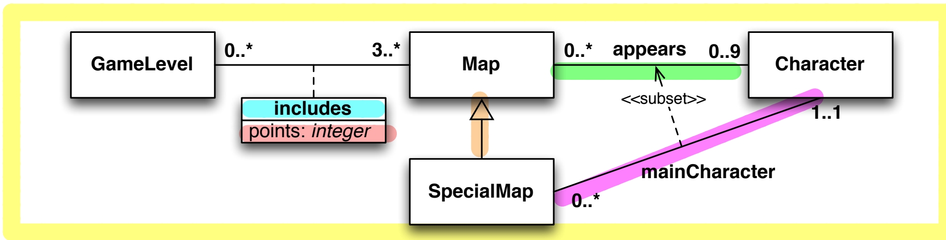
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

Formal Methods – Jan. 25, 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.

Map
artica
bush

$SpecialMap$
city
desert

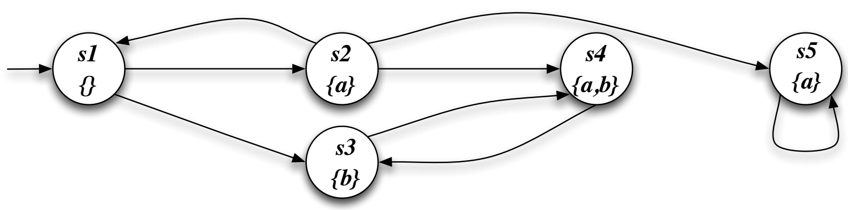
$Character$
adrian
bob
charline

$appaears$	
adrian	artica
adrian	bush
adrian	desert
bob	city
charline	artica

$mainCharacter$	
adrian	city
charline	desert

1. Check whether the instantiation (once completed) is correct (and explain why it is or it is not).
2. Express in FOL and evaluate the following queries:
   (a) Return the maps with at least 3 distinct characters.
   (b) Return the characters that appear in maps only as main characters.
   (c) Check if there exists a map where all characters appears.

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



Exercise 4. Check whether the following Hoare triple is correct, using as *invariant* $(i + j = 9)$.

```
{i=0 AND j=9}  while(i<10) do (i:= i+1; j=j-1)  {j<0}
```

Exercise 5. Given the following conjunctive queries:

```
q1(x) :- edge(x,y), edge(y,y), edge(x,z), edge(y,z), edge(z,y).
q2(x) :- edge(x,y), edge(y,z), edge(x,v), edge(v,z), edge(v,y).
```

check whether $q1$ is contained into $q2$, explaining the technique used and, in case of containment, showing the homomorphism between the canonical databases.

1) ALPHABET: $G(X)$, $M(X)$, $SM(X)$, $C(X)$, includes (X,Y) Integer (X)

ISA: $\forall x \; SM(X) \supset M(X)$

mainchoracter: $\forall xy \; mc(x,y) \supset C(x) \wedge SM(y)$

$\forall y \; SM(y) \supset 1 \leq \#\{x \mid mc(x)\} \leq 1$

$\forall xy \; mc(x,y) \supset opp(x,y)$

opposes: $\forall xy \; opp(x,y) \supset C(x) \wedge M(y)$

$\forall y \; M(y) \supset \#\{x \mid opp(x,y)\} \leq 9$

includes: $\forall xy \; inc(x,y) \supset G(x) \wedge M(y)$

$\forall x \; G(x) \supset 3 \leq \#\{y \mid inc(x,y)\}$

$\forall xy \; inc(x,y) \supset 1 \leq \#\{z \mid points(x,y,z)\} \leq 1$

points: $\forall xyz \; points(x,y,z) \supset inc(x,y) \wedge Integer(z)$

2) The completed instantiation (merge mc with opp table) is correct because makes all axioms true.

- $\exists x x' x'' \; opp(x,y) \wedge opp(x',y) \wedge opp(x'',y) \wedge x \neq x' \wedge x \neq x'' \wedge x' \neq x''$

$\Rightarrow \{\emptyset\}$

- $\forall y \; opp(x,y) \supset mc(x,y)$

$\Rightarrow \{\emptyset\}$

- $\exists y \forall x \; C(x) \supset opp(x,y)$

$\Rightarrow \{\emptyset\}$

4) $I = \{i + J = 9\}$

$P = \{i = 0 \wedge J = 9\}$

$Q = \{J < 0\}$

$\delta = \{i = i+1 ; J = J-1\}$

$G = \{i < 10\}$

- Check $P \supset I$

$i=0 \wedge J=9 \supset i+J=9$ ✓

- Check $\neg G \wedge I \supset Q$

$i \geq 10 \wedge i+J=9 \supset J<0$ ✓ $i=10$ $J=-1$

- Check $G \wedge I \supset wp(\delta, I)$

$i<10 \wedge i+J=9 \supset wp(\delta, I) \longrightarrow$

$i<10 \wedge i+J=9 \supset i+J=9$ ✓

$\{i+1+J-1=9\}$

$i=i+1$

$\{i+J-1=9\}$

$J=J-1$

$\{i+J=9\}$

I is an invariant so the Hoare triple is correct!

3) $\nu X \mu Y ((a \wedge \langle - \rangle X) \vee [-]Y)$

$[X_0] = S$

$[X_1] = \mu Y ((a \wedge \langle - \rangle X) \vee [-]Y) = S$ } → greatest fixpoint

$[Y_{10}] = \emptyset$

$[Y_{11}] = ([a] \cap PreE(-, [X_0])) \cup PreA(-, [Y_{10}])$

$= (\{2,4,5\} \cap \{S\}) \cup \{\emptyset\} = \{2,4,5\}$

$[Y_{12}] = ([a] \cap PreE(-, [X_0])) \cup PreA(-, [Y_{11}])$

$= \{2,4,5\} \cap \{3,5\} = \{2,3,4,5\}$

$[Y_{13}] = ([a] \cap PreE(-, [X_0])) \cup PreA(-, [Y_{11}])$

$= \{2,4,5\} \cup \{1,2,3,4,5\} = S$ least fixpoint

Initial state in solution $\longrightarrow \mathcal{T} \models \phi$

CTL : $EF\underbrace{(\neg a \supset \overbrace{EX \underbrace{AG b}_{\alpha}}^{\beta})}_{\gamma}$

$\alpha = \nu X\, b \wedge [-]X = \{3,4,5\}$

$[X_0] = S$

$[X_1] = [b] \cap PreA(-, [X_0])$

$= \{3,4,5\} \cap S = \{3,4,5\}$

$[X_1] = [b] \cap PreA(-, [X_1])$

$= \{3,4,5\} \cap \{2,3,4,5\} = \{3,4,5\}$ greatest fixpoint

$\beta = \langle - \rangle \alpha = PreE(-, \{3,4,5\}) = S$

$\gamma = a \vee \beta = \{2,4,5\} \cup \{S\} = S$

$EF\, \gamma = \mu X (\gamma \vee \langle - \rangle X) = \{S\}$

$[X_0] = \emptyset$

$[X_1] = S \cup PreE(-, [X_0]) = S$ least fixpoint

Initial state in solution $\longrightarrow \mathcal{T} \models \phi$

5) $q_1 \subseteq q_2$?

- Freeze free variables (x and x_2)
- Build canonical interpretation

$$I_{q_1} = \begin{cases} \Delta^{I_{q_1}} = \{x, y, z\} \\ x^{I_{q_1}} = x \\ E = \{(x,y)(y,y)(x,z)(y,z)(z,y)\} \end{cases}$$

$$I_{q_2} = \begin{cases} \Delta^{I_{q_2}} = \{x, y, z, v\} \\ x_2^{I_{q_2}} = x_2 \\ E = \{(x,y)(y,z)(x,v)(v,z)(v,y)\} \end{cases}$$

$h(x_2) = x$

$h(x_2, y_2) = (x, ?) \rightarrow h(y_2) = y$

$h(y_2, z_2) = (y, ?) \rightarrow h(z_2) = z$

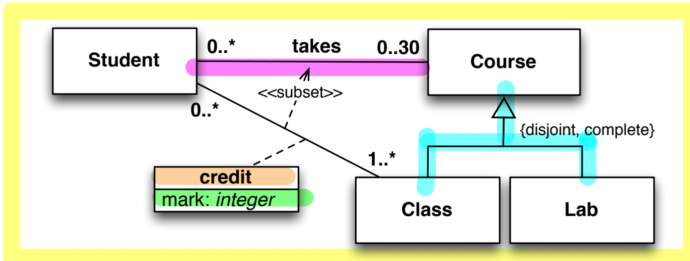
$h(x_2, v_2) = (x, ?) \rightarrow h(v_2) = z$

$h(v_2, z_2) = (z, z)$ x

There is no homomorphism $\rightarrow q_1 \not\subseteq q_2$

SAPIENZA Università di Roma – MSc. in Engineering in Computer Science
Formal Methods – Feb. 13, 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.

Student

peter
paul
mary
jane

Class

calculus
AI
FM
algorithms

Lab

IoT lab
db lab
hacking lab

credit/mark

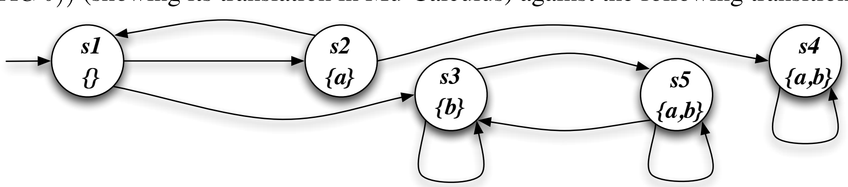
peter	algorithm	30
paul	calculus	27
mary	algorithms	28
mary	AI	30
jane	FM	30
jane	algorithms	30

takes

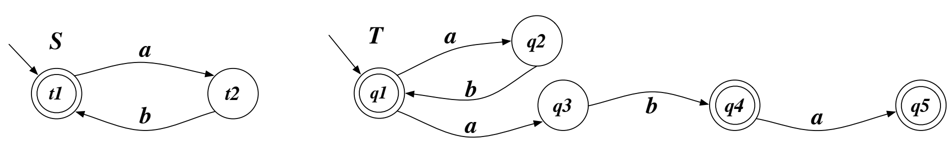
peter	IoT lab
paul	IoT lab
mary	FM
jane	db lab
jane	hacking lab
jane	IoT lab

1. Check whether the instantiation (once completed) is correct (and explain why it is or it is not).
2. Express in FOL and evaluate the following queries:
   (a) Return students that have taken at least 3 courses.
   (b) Return students that have taken only classes.
   (c) Check if there exists a student that has taken all labs.
   (d) Check if there is a student that has taken all classes, but not for credit.

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



Exercise 4. Consider the following two transition systems:



Write the definition of bisimilarity and compute the bisimilarity relation for the two transition systems.

Exercise 5. Given the following conjunctive queries:

```
q1(x) :- edge(x,y), edge(y,z), edge(z,x).
q2(x) :- edge(x,y), edge(x,w), edge(y,z), edge(z,x), edge(z,v), edge(v,y), edge(v,w), edge(w,z).
```

check whether $q1$ is contained into $q2$, explaining the technique used and, in case of containment, showing the homomorphism between the canonical databases.

1) ALPHABET : $s(x)$, $c(x)$, $cl(x)$, $L(x)$, $credit(x,y)$, $mark(x,y,z)$, $Integer(x)$

ISA : $\forall x\ C(x) \supset CL(x) \vee L(x)$

$\forall x\ CL(x) \supset \neg L(x)$

$\forall x\ CL(x) \supset C(x)$

$\forall x\ L(x) \supset C(x)$

$\rightarrow$ maybe redundant, IDK

TAKES : $\forall xy\ takes(x,y) \supset S(x) \wedge C(y)$

$\forall x\ S(x) \supset \#\{y \mid takes(x,y)\} \leq 30$

CREDIT : $\forall x,y\ credit(x,y) \supset S(x) \wedge CL(y)$

$\forall x\ S(x) \supset 1 \leq \#\{y \mid credit\ y\}$

$\forall xy\ credit(x,y) \supset 1 \leq \#\{z \mid mark(x,y,z)\} \geq 1$

$\forall xy\ credit(x,y) \supset takes(x,y)$

MARK : $\forall xyz\ mark(x,y,z) \supset credit(x,y) \wedge Integer(z)$

2) Completed instantiation (add table for Course unifying class and Lab and add missing line in "takes" from "credit" eg Petor - algorithm) is correct because all axioms are true.

- $\exists yy'y''\ takes(x,y) \wedge take(x,y') \wedge takes(x,y'') \wedge y \neq y' \wedge y \neq y'' \wedge y' = y''$
  $\Rightarrow \{Jone\}$
- $\forall y\ takes(x,y) \supset CL(y)$
  $\Rightarrow \{Mary\}$
- $\exists x \forall y\ L(y) \supset takes(x,y)$
  $\Rightarrow \{Jone\}$
- $\exists x \forall y\ CL(y) \supset takes(x,y) \wedge \neg credit(x,y)$
  $\Rightarrow \{\emptyset\}$

5) $q_1 \subseteq q_2$?

- Freeze free variables (x)
- Build canonical interpretation of q_1 and q_2

$$I_{q_1} = \begin{cases} \Delta^{I_{q_1}} = \{x, y, z\} \\ x^{I_{q_1}} = x \\ E^{I_{q_1}} = \{(x,y), (y,z), (z,x)\} \end{cases}$$

$$I_{q_2} = \begin{cases} \Delta^{I_{q_2}} = \{x,y,z,v,w\} \\ x^{I_{q_2}} = x \\ E^{I_{q_2}} = \{(x,y), (x,w), (y,z), (z,x), (z,v), (v,y), (v,w), (w,z)\} \end{cases}$$

- Check if $I_{q_1} \models I_{q_2}$ $\longrightarrow$ find homomorphism from I_{q_2} to I_{q_1}

- $h(x_2) = x_1$
- $h(x_2,y_2) = (x_1, ?) \rightarrow h(y_2) = y_1$
- $h(x_2,w_2) = (x_1, ?) \rightarrow h(w_2) = y_1$
- $h(y_2,z_2) = (y_1, ?) \rightarrow h(z_1) = z_1$
- $h(z_2,x_2) = (z_1, x_1)$ ✓
- $h(z_2,v_2) = (z_1, ?) \longrightarrow h(v_2) = x_1$
- $h(v_2,y_2) = (x_1, y_1)$ ✓

- $h(v_2,w_2) = (x,y)$ ✓
- $h(w_2,z_2) = (y,z)$ ✓

Exists an homomorphism

$\Rightarrow q_1 \subseteq q_2$

3) $\nu X \mu Y((a \wedge [-]X) \vee [-]Y)$

$[X_0] = S$

$[X_1] = \mu Y((a \wedge [-]X) \vee [-]Y) = \{2,4,5\}$

$[Y_{10}] = \emptyset$

$[Y_{11}] = ([a] \cap preA(-,[X_0])) \cup preA(-,[Y_{10}])$

$= (\{2,5,4\} \cap \{S\}) \cup \{\emptyset\} = \{2,5,4\}$

$[Y_{12}] = ([a] \cap preA(-,[X_0])) \cup preA(-,[Y_{11}])$ → least fixpoint

$= \{2,5,4\} \cup \{4\} = \{2,5,4\}$

$[X_2] = \mu Y((a \wedge [-]X) \vee [-]Y = \{4\}$

$[Y_{20}] = \emptyset$

$[Y_{21}] = ([a] \cap preA(-,[X_1])) \cup preA(-,[Y_{20}])$

$= (\{2,4,5\} \cap \{4\}) \cup \{\emptyset\} = \{4\}$

$[Y_{22}] = ([a] \cap preA(-,[X_1])) \cup preA(-,[Y_{21}])$ → least fixpoint

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

→ greatest fixpoint

$[X_3] = \mu Y((a \wedge [-]X) \vee [-]Y = \{4\}$

$[Y_{30}] = \emptyset$

$[Y_{31}] = ([a] \cap preA(-,[X_2])) \cup preA(-,[Y_{30}])$

$= (\{2,4,5\} \cap \{4\}) \cup \{\emptyset\} = \{4\}$

$[Y_{32}] = ([a] \cap preA(-,[X_2])) \cup preA(-,[Y_{31}])$ → least fixpoint

$= (\{2,4,5\} \cap \{4\}) \cup \{4\} = \{4\}$

Initial state not in solution → $\tau \not\models \phi$

CTL: $EF(\overbrace{\neg a \supset (\underbrace{\overbrace{EX\, a}^{\gamma} \wedge \underbrace{EX\, \overbrace{AG\, b}^{\alpha}}_{\beta}}_{\delta})}^{\omega})$

$\alpha = \nu X\, b \wedge [-]X = \{3,4,5\}$

$[X_0] = S$

$[X_1] = [b] \cap preA(-,[X_0])$

$= \{3,4,5\} \cap S = \{3,4,5\}$

$[X_2] = [b] \cap preA(-,[X_1])$ → greatest fixpoint

$= \{3,4,5\} \cap \{3,4,5\} = \{3,4,5\}$

$\beta = \langle - \rangle \alpha = preE(-,[\alpha]) = S$

$\gamma = \langle - \rangle a = preE(-,[a]) = S$

$\delta = S \cap S = S$

$\omega = a \vee S = S$

$EF(\omega) = \mu X\, \omega \vee [-]X = S$

$[X_0] = \emptyset$

$[X_1] = [\omega] \cup preA(-,[X_0])$

$= S \cup \emptyset = S$ → least fixpoint

Initial state in solution → $\tau \models \phi$

4) Two transition system are bisimilar if:

- locally they look equal
- each action done on one of them can be done also on the second one

R_0 = cartesian product = $\{(t_1,q_1),(t_1,q_2),(t_1,q_3),(t_1,q_4),(t_1,q_5),(t_2,q_1),(t_2,q_2),(t_2,q_3)(t_2,q_4)(t_2,q_5)\}$

R_1 = remove pairs that violate local condition on final state

$= \{(t_1,q_1)(t_1,q_4)\cancel{(t_1,q_5)}\cancel{(t_2,q_1)}(t_2,q_2)(t_2,q_3)\cancel{(t_2,q_4)}\cancel{(t_2,q_5)}\}$

R_2 = remove actions that can be done only on one of the two states

$= \{(t_1,q_1)\cancel{(t_1,q_4)}(t_2,q_2)\cancel{(t_2,q_3)}\}$

R_3 = remove pairs that lead to pairs no more in the list

$= \{(t_1,q_1)(t_2,q_2)\}$

R_4 = same $= \{(t_1,q_1)(t_2,q_2)\}$ → greatest fixpoint

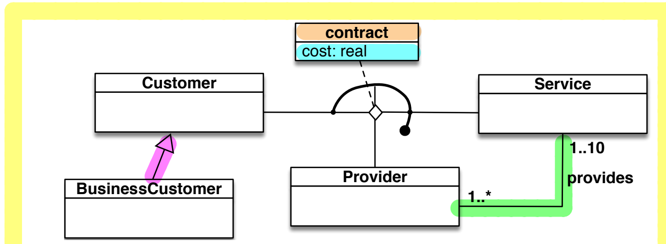
(t_1,q_1) belong to greatest fixpoint ⟶ S and T are bisimilar

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

Formal Methods - Final Test B – 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

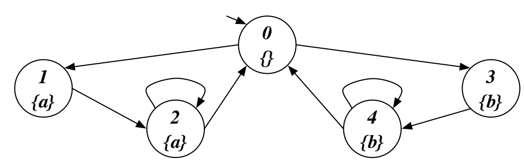
$Provider$
p1
p2

$provides$	
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 $p2$.
   (c) Return those customers that have a contract for with all providers.

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



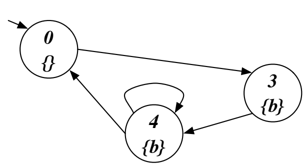
Exercise 4. Check whether the Hoare triple below is correct, by using $(x \geq 0 \wedge y \geq 0 \wedge x + y = 31)$ as invariant:

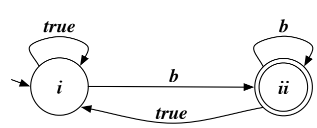
$$\{x = 31 \wedge y = 0\}\ \texttt{while(x>0) do (x=x-1; y:= y+1)}\ \{y = 31\}$$

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

$$(\exists x.P(x) \vee \exists x.Q(x)) \equiv \exists x.(P(x) \vee Q(x))$$

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





1) ALPHABET: $C(x)$, $B(x)$, $P(x)$, $S(x)$, $contr(x,y,z)$, $cost(x,y,z,w)$, $Real(x)$

ISA: $\forall x\ B(x) \supset C(x)$

PROVIDES: $\forall xy\ prov(x,y) \supset P(x) \wedge S(y)$

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

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

CONTRACT: $\forall xyz\ contr(x,y,z) \supset C(x) \wedge S(y) \wedge P(z)$

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

$\forall xyz\ contr(x,y,z) \supset 1 \leq \#\{w \mid cost(x,y,z,w)\} \geq 1$

COST: $\forall xyzw\ cost(x,y,z,w) \supset contr(x,y,z) \wedge Real(w)$

2) Completed instantiation is correct because all axioms are true

- $\forall xy\ contr(z,y,x) \supset prov(x,y)$

  $\Rightarrow$ false $[contr(b_2, s_1, p_2)$ but not $prov(p_2, s_1)]$
- $\exists yz\ contr(x,y,z) \supset prov(p_2, y)$

  $\Rightarrow \{\emptyset\}$
- $\exists z \forall y\ S(y) \supset contr(x,y,z)$

  $\Rightarrow \{\emptyset\}$

5) $\neg[(\exists x P(x) \vee \exists x Q(x)) \equiv \exists x (P(x) \vee Q(x))]$

Left branch:

$\exists x P(x) \vee \exists x Q(x)$

$\neg(\exists x (P(x) \vee Q(x)))$

- $\exists x P(x)$ → $P(\alpha)$ × → $\neg(P(\alpha) \vee Q(\beta))$ → × $\neg P(\alpha)$, $\neg Q(\beta)$
- $\exists x Q(x)$ → $Q(\beta)$ × → $\neg(P(\alpha) \vee Q(\beta))$ → $\neg P(\alpha)$, $\neg Q(\beta)$ ×

Right branch:

$\neg(\exists x P(x) \vee \exists x Q(x))$

$\exists x (P(x) \vee Q(x))$

→ $P(\alpha) \vee Q(\alpha)$

- $P(\alpha)$ × → $\neg\exists P(x)$, $\neg\exists Q(x)$ → $\neg Q(\alpha)$, $\neg P(\alpha)$ ×
- $Q(\alpha)$ × → $\neg\exists P(x)$, $\neg\exists Q(x)$ → $\neg Q(\alpha)$ ×, $\neg P(\alpha)$

$\neg\Gamma$ unsat $\Rightarrow \Gamma$ valid

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

$[X_0] = S$

$[X_1] = \mu Y((b \wedge [-]X) \vee (a \wedge \langle - \rangle Y)) = \{3,4\}$

$[Y_{10}] = \emptyset$

$[Y_{11}] = ([b] \cap preA(-,[X_0])) \cup ([a] \cap preE(-,[Y_{10}]))$

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

$[Y_{12}] = ([b] \cap preA(-,[X_0])) \cup ([a] \cap preE(-,[Y_{11}]))$

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

$[X_2] = \mu Y((b \wedge [-]X) \vee (a \wedge \langle - \rangle Y)) = \{3\}$

$[Y_{20}] = \emptyset$

$[Y_{21}] = ([b] \cap preA(-,[X_1])) \cup ([a] \cap preE(-,[Y_{20}]))$

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

$[Y_{22}] = ([b] \cap preA(-,[X_1])) \cup ([a] \cap preE(-,[Y_{21}]))$ least fixpoint

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

$[X_3] = \mu Y((b \wedge [-]X) \vee (a \wedge \langle - \rangle Y)) = \emptyset$ greatest fixpoint

$[Y_{30}] = \emptyset$

$[Y_{31}] = ([b] \cap preA(-,[X_2])) \cup ([a] \cap preE(-,[Y_{30}]))$

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

Initial state not in solution $\rightarrow T \not\models \Phi$

CTL: $EF(\overbrace{AG(\underbrace{a \supset \overbrace{EX\, \underbrace{AX\, \neg a}_{\alpha}}^{\beta}}_{\gamma})}^{\delta})$

$\alpha = [-]\neg a = \{3,4\}$

$\beta = \langle - \rangle \alpha = \{0,3,4\}$

$\gamma = \neg a \vee \beta = \{0,3,4\} \cup \{0,3,4\} = \{0,3,4\}$

$\delta = \nu X\ \delta \wedge [-]X = \emptyset$

$[X_0] = \{S\}$

$[X_1] = [\delta] \cap preA(-,[X_0])$

$= \{0,3,4\} \cap \{S\} = \{0,3,4\}$

$[X_2] = [\delta] \cap preA(-,[X_1])$

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

$[X_3] = [\delta] \cap preA(-,[X_2])$

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

$[X_4] = [\delta] \cap pre(-,[X_3])$

$= \{3,4\} \cap \{\emptyset\} = \emptyset$ greatest fixpoint

$EF(\delta) = \mu X\ \delta \vee \langle - \rangle X = \emptyset$

$[X_0] = \emptyset$

$[X_1] = [\delta] \cup preE(-,[X_0])$

$= \emptyset \cup \emptyset$ least fixpoint

Initial state not in solution $\rightarrow T \not\models \Phi$

4) $I = \{x \geq 0 \wedge y \geq 0 \wedge x+y = 31\}$

$P = \{x = 31 \wedge y = 0\}$

$G = \{x > 0\}$

$\delta = \{x = x-1 \,;\, y = y+1\}$

$Q = \{y = 31\}$

- Check $P \supset I$

$x = 31 \wedge y = 0 \supset x \geq 0 \wedge y \geq 0 \wedge x+y = 31$ ✓

- Check $\neg G \wedge I \supset Q$

$\underbrace{x \leq 0 \wedge x \geq 0}_{x=0} \wedge y \geq 0 \wedge x+y = 31 \supset y = 31$ ✓

- Check $\{G \wedge I\}\, \delta\, \{I\} = G \wedge I \supset Wp(\delta, I)$

$x > 0 \wedge x \geq 0 \wedge y \geq 0 \wedge x+y = 31 \supset Wp(\delta, I)$ →

$x > 0 \wedge x \geq 0 \wedge y \geq 0 \wedge x+y = 31 \supset x \geq 1 \wedge y \geq -1 \wedge x+y = 31$ ✓

$\{x \geq 1 \wedge y \geq -1 \wedge x+y = 31\}$

$x = x-1$

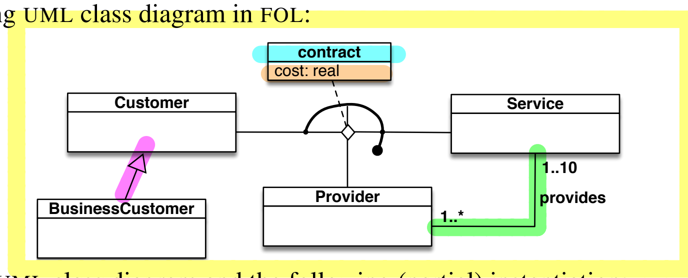
$\{x \geq 0 \wedge y \geq -1 \wedge x+y = 30\}$

$y = y+1$

$\{x \geq 0 \wedge y \geq 0 \wedge x+y = 31\}$

I is an invariant → the hoare triple is correct!

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

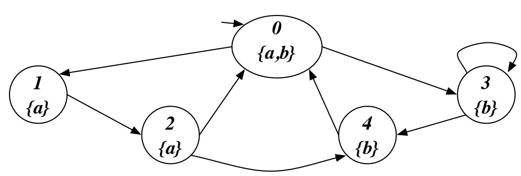
$Provider$
p1
p2

$provides$	
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 whether there is a customer with contract with two providers for the same service.
   (b) Return those customers that have contracts only for one service.
   (c) Return those customers that have a contracts with the same provider for all their services.

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



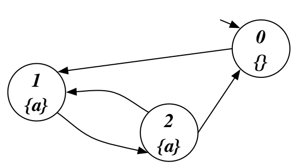
Exercise 4. Check whether CQ q_1 is contained in CQ q_2, reporting canonical DBs and homomorphism:

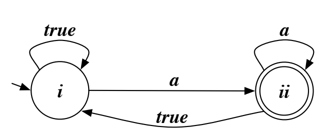
$$\begin{array}{lcl} q_1(x_r) & \leftarrow & e(x_r, x_g), e(x_g, x_b), e(x_b, x_r). \\ q_2(x) & \leftarrow & e(x, y), e(y, z), e(z, x), e(z, v)e(v, w), e(w, z). \end{array}$$

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

$$(\forall x.P(x) \supset Q(x)) \supset (\exists x.P(x) \supset \exists x.Q(x))$$

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.*

1) Alphabet: $C(x)$, $B(x)$, $P(x)$, $S(x)$, $real(x)$
$contr(x,y,z)$
$cost(x,y,z,w)$

ISA: $\forall x\, B(x) \supset C(x)$

PROVIDES: $\forall x,y\ provides(x,y) \supset P(x) \wedge S(y)$
$\forall x\ P(x) \supset (1 \leq \#\{y \mid provides(x,y)\} \leq 10$
$\forall y\ S(x) \supset (1 \leq \#\{x \mid provides(x,y)\})$

CONTRACT: $\forall x,y,z\ contr(x,y,z) \supset C(x) \wedge S(y) \wedge P(z)$
$\forall x,y,z,z'\ contr(x,y,z) \wedge contr(x,y,z') \supset z = z'$
$\forall x,y,z\ contr(x,y,z) \supset (1 \leq \#\{w \mid cost(x,y,z,w)\} \leq 1)$

COST: $\forall x,y,z,w\ cost(x,y,z,w) \supset contr(x,y,z) \wedge real(w)$

2) Instantiation is correct because satisfies all axioms in Γ

- $\exists y,z,z'\ contr(x,y,z) \wedge contr(x,y,z') \wedge z \neq z'$
  No need to check $C(x)$, $S(y)$, $P(z)$ alone because they are implied in $cont(x,y,z)$
  $\Rightarrow \{\emptyset\}$
- $\exists y,z\ contr(x,y,z) \wedge [\forall y y'\ \exists z\ contr(x,y,z) \wedge \exists z'\ contr(x,y',z') \supset y = y']$
  $\Rightarrow \{\emptyset\}$
- $\exists p\ \forall y\ \exists z\ contr(x,y,z) \supset contr(x,y,p)$
  $\Rightarrow \{c_1, b_2\}$

5) $\neg((\forall x\, P(x) \supset Q(x)) \supset (\exists x\, P(x) \supset \exists x\, Q(x)))$ $[\neg(\alpha \supset \beta)]$

$\cancel{\forall x\, P(x) \supset Q(x)}$
$\cancel{\neg(\exists x\, P(x) \supset \exists x\, Q(x))}$ $[\neg(\alpha \supset \beta)]$

$\cancel{\exists x\, P(x)}$
$\cancel{\neg\exists x\, Q(x)}$

$P(\alpha)$ × — we need to generate a clash so we need a $\neg P(\alpha)$ $\longrightarrow$ useless to expand $\neg\exists x Q(x)$!

$P(\alpha) \supset Q(\alpha)$

$\neg P(\alpha)$ × | $Q(\alpha)$ ×

$\neg Q(\alpha)$ ×

$\neg\Gamma$ is unsat. $\longrightarrow$ Γ is valid!

3) $\nu X \mu Y ((a \wedge [-]X) \vee (b \wedge [-]Y))$

$[X_0] = S$

$[X_1] = \mu Y((a \wedge [-]X) \vee (b \wedge [-]Y)) = \{s_0, s_1, s_2, s_4\}$

$[Y_{10}] = \emptyset$

$[Y_{11}] = (a \wedge [-]X) \vee (b \wedge [-]Y)$

$= ([a] \cap PreA(-, [X_0]) \cup ([b] \cap PreA(-[Y_{10}])$

$= (\{s_0, s_1, s_2\} \cap \{s_0, s_1, s_2, s_3, s_4\}) \cup (\{s_0, s_3, s_4\}) \cap \{\emptyset\}) = \{s_0, s_1, s_2\}$

$[Y_{12}] = (([a] \cap PreA(-, [X_0])) \cup ([b] \cap PreA(-[Y_{11}]))$

$= \{s_0, s_1, s_2\} \cup \{s_4\} = \{s_0, s_1, s_2, s_4\}$

$[Y_{13}] = (([a] \cap PreA(-, [X_0]) \cup ([b] \cap PreA(-, [Y_{12}]))$ — least fixpoint

$= \{s_0, s_1, s_2\} \cup \{s_4\} = \{s_0, s_1, s_2, s_4\}$

$[X_2] = \mu Y((a \wedge [-]X) \vee (b \wedge [-]Y)) = \{s_1, s_2\}$

$[Y_{20}] = \emptyset$

$[Y_{21}] = (a \wedge [-]X_1) \vee (b \wedge [-]Y_{20})$

$= ([a] \cap PreA(-, [X_1])) \cup ([b] \cap PreA(-, [Y_{20}])$

$= (\{s_0, s_1, s_2\} \cap \{s_1, s_2, s_4\}) \cup (\{s_0, s_3, s_4\} \cap \{\emptyset\}) = \{s_1, s_2\}$

$[Y_{22}] = ([a] \cap PreA(-, [X_1])) \cup ([b] \cap PreA(-, [Y_{21}]))$ — least fixpoint!

$= \{s_1, s_2\} \cup \{s_1\} = \{s_1, s_2\}$

$[X_3] = \mu Y((a \wedge [-]X) \vee (b \wedge [-]Y)) = \{s_1\}$

$[Y_{30}] = \emptyset$

$[Y_{31}] = (a \wedge [-]X_2) \vee (b \wedge [-]Y_{30})$

$= ([a] \cap PreA(-, [X_2])) \cup ([b] \cap PreA(-, [Y_{30}]))$

$= (\{s_0, s_1, s_2\} \cap \{s_1\}) \cup (\{s_0, s_3, s_4\} \cap \{\emptyset\}) = \{s_1\}$

$[Y_{32}] = ([a] \cap PreA(-, [X_2])) \cup ([b] \cap PreA(-, [Y_{31}]))$ — least fixpoint

$= \{s_1\} \cup \{\emptyset\} = \{s_1\}$

$[X_4] = \mu Y((a \wedge [-]X) \vee (b \wedge [-]Y)) = \{\emptyset\}$ greatest fixpoint

$[Y_{40}] = \emptyset$

$[Y_{41}] = (a \wedge [-]X_3) \vee (b \wedge [-]Y_{40})$

$= ([a] \cap PreA(-, [X_3]) \cup ([b] \cap PreA(-, [Y_{40}]))$

$= (\{s_0, s_1, s_2\} \cap \{\emptyset\}) \cup (\{s_0, s_3, s_4\} \cap \{\emptyset\}) = \{\emptyset\}$ least fixpoint

Initial stage not in solution $\Rightarrow \mathcal{T} \nvDash \phi$

CTL: $AF(\overbrace{EG(\overbrace{a \supset \underbrace{EX\,\underbrace{AXb}_{\alpha}}_{\beta}}^{\gamma})}^{\sigma})$

$\alpha = AXb = [-]b = PreA(-,[b]) = \{s_2, s_3, s_4\}$

$\beta = EX\alpha = \langle - \rangle \alpha = PreE(-,[\alpha]) = \{s_0, s_1, s_2, s_3\}$

$\gamma = a \supset \beta = \neg a \vee \beta = \{s_3, s_4\} \cup \{s_0, s_1, s_2, s_3\} = S$

$\sigma = EG\gamma = \nu X\, \gamma \wedge \langle - \rangle X$

$[X_0] = S$

$[X_1] = [\gamma] \cap PreE(-,[X_0]) = S \cap S = \{S\}$ fixpoint

$AF\sigma = \mu X\, \sigma \vee [-]X$

$[X_0] = \emptyset$

$[X_1] = [\sigma] \cup PreA(-,[X_0]) = \{S\}$ fixpoint

Initial state in solution $\Rightarrow \mathcal{T} \models \phi$

4) $q_1 \subseteq q_2$?

- Freeze free variables (x_r and x)
- Build canonical interpretation of q_1 and q_2

$$I_{q_1} = \begin{cases} \Delta^{I_{q_1}} = \{x_r, x_g, x_b\} \\ x_r^{I_{q_1}} = x_r \\ E^{I_{q_1}} = \{(x_r, x_g), (x_g, x_b), (x_b, x_r)\} \end{cases}$$

$$I_{q_2} = \begin{cases} \Delta^{I_{q_2}} = \{x, y, z, v, w\} \\ x^{I_{q_2}} = x \\ E^{I_{q_2}} = \{(x,y), (y,z), (z,x), (z,v), (v,w), (w,z)\} \end{cases}$$

- Check if $I_{q_1} \models q_2 \longrightarrow$ find homomorphism from I_{q_2} to I_{q_1}

On order, check all $e \in E^{I_{q_2}}$

- $h(x) = x_r$ because constants
- $h(x,y) = (x_r, ?) \longrightarrow$ find an e starting with x_r ✓ $\longrightarrow (x_r, x_g) \longrightarrow h(y) = x_g$
- $h(y,z) = (x_g, ?) \longrightarrow$ again ✓ $\longrightarrow (x_g, x_b) \longrightarrow h(z) = x_b$
- $h(z,x) = (x_b, x_r) \longrightarrow$ is present in $E^{I_{q_1}}$ ✓
- $h(z,v) = (x_b, ?) \longrightarrow$ find e starting with x_b ✓ $\longrightarrow (x_b, x_r) \longrightarrow h(v) = x_r$
- $h(v,w) = (x_r, ?) \longrightarrow$ ... ✓ $\longrightarrow (x_r, x_g) \longrightarrow h(w) = x_g$
- $h(w,z) = (x_g, x_b) \longrightarrow$ is present in $E^{I_{q_1}}$ ✓

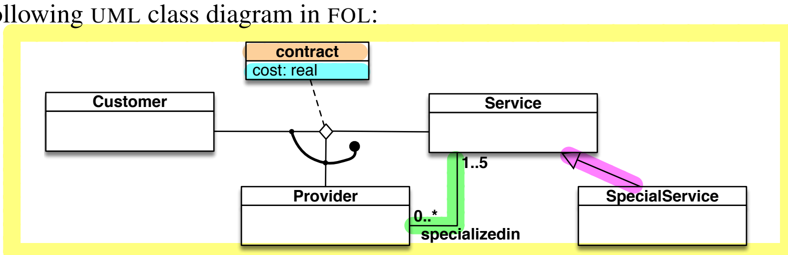
Exists an homomorphism $\Rightarrow q_1 \subseteq q_2$

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

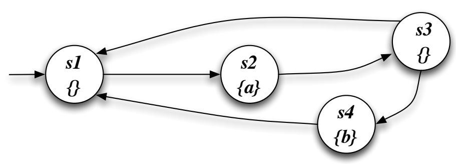
p1	s1
p1	s2
p1	s3
p2	ss1
p2	ss2

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



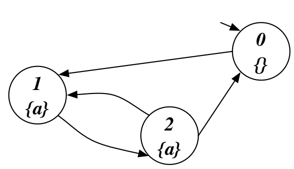
Exercise 4. Check whether CQ q_1 is contained in CQ q_2, reporting canonical DBs and homomorphism:

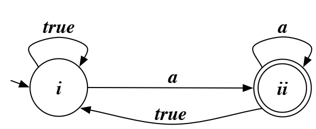
$$q_1() \leftarrow edge(r,g), edge(g,b), edge(b,r).$$
$$q_2() \leftarrow edge(x,y), edge(y,z), edge(z,x), edge(z,v), edge(v,w), edge(w,z).$$

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.*

1) ALPHABET: $c(x)$, $s(x)$, $p(x)$, $ss(x)$, $contr(x,y,z)$, $cost(x,y,z,w)$, $Red(x)$

ISA: $\forall x\ ss(x) \supset s(x)$

SPECIALIZED IN: $\forall x,y\ spec(x,y) \supset P(x) \wedge s(x)$

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

CONTRACT: $\forall x,y,z\ contr(x,y,z) \supset c(x) \wedge P(y) \wedge s(z)$

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

$\forall x,y,z\ contr(x,y,z) \supset 1 \leq \#\{w \mid cost(x,y,z,w)\} \leq 1$

COST: $\forall x,y,z,w\ cost(x,y,z,w) \supset contr(x,y,z) \wedge Red(w)$

2) The completed instantiation is correct because all axioms are made true.

- $\exists x,x',z\ contr(x,y,z) \wedge contr(x',y,z) \wedge \neg(x = x')$
  $\Rightarrow \{P_1, P_2\}$
- $\forall x \exists z\ contr(x,y,z) \supset spec(y,z)$
  $\Rightarrow \{P_1\}$
- $\forall y\ spec(x,y) \supset \exists z\ contr(x,y,z)$
  $\Rightarrow \{P_2\}$
- $\exists y \forall z\ s(z) \supset contr(x,y,z)$
  $\Rightarrow \{\emptyset\}$

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

Left branch:

$\forall x \forall y\ P(x,y) \supset Q(x)$

$\neg[\forall x\ (\exists y\ P(x,y)) \supset Q(x)]$

$\downarrow$

$\neg[(\exists y\ P(\alpha,y)) \supset Q(\alpha)]$

$\downarrow$

$\exists y\ P(\alpha,y)$

$\neg Q(\alpha)$ ×

$\downarrow$

$P(\alpha,\beta)$ ×

$\downarrow$

$\forall y\ P(\alpha,y) \supset Q(\alpha)$

$\downarrow$

$P(\alpha,\beta) \supset Q(\alpha)$

$\swarrow \quad \searrow$

$\neg P(\alpha,\beta)$ × $\quad Q(\alpha)$ ×

Right branch:

$\neg[\forall x \forall y\ P(x,y) \supset Q(x)]$

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

$\downarrow$

$\neg[\forall y\ P(\alpha,y) \supset Q(x)]$

$\downarrow$

$\neg[P(\alpha,\beta) \supset Q(x)]$

$\downarrow$

$P(\alpha,\beta)$ ×

$\neg Q(\alpha)$ ×

$\downarrow$

$\exists y\ P(\alpha,y) \supset Q(\alpha)$

$\swarrow \quad \searrow$

$\neg \exists y\ P(\alpha,y)$ $\quad Q(\alpha)$ ×

$\downarrow$

$\neg P(\alpha,\beta)$ ×

3) $\nu X \mu Y((a \wedge \langle - \rangle X) \vee (\neg b \wedge \langle - \rangle Y))$

$[X_0] = S$

$[X_1] = \mu Y((a \wedge \langle - \rangle X) \vee (\neg b \wedge \langle - \rangle Y)) = \{s_1, s_2, s_3\}$

$[Y_{10}] = \{\emptyset\}$

$[Y_{11}] = (a \wedge \langle - \rangle X_0) \vee (\neg b \wedge \langle - \rangle Y_{10})$

$= ([a] \wedge preE(-,[X_0])) \vee ([\neg b] \wedge preE(-,[Y_{10}]))$

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

$[Y_{12}] = ([a] \wedge preE(-,[X_0])) \vee ([\neg b] \wedge preE(-,[Y_{11}]))$

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

$[Y_{13}] = ([a] \wedge preE(-,[X_0])) \vee ([\neg b] \wedge preE(-,[Y_{12}]))$

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

$[Y_{14}] = ([a] \wedge preE(-,[X_0])) \vee ([\neg b] \wedge preE(-,[Y_{13}]))$

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

least fixpoint

greatest fixpoint

$[X_2] = \mu Y((a \wedge \langle - \rangle X) \vee (\neg b \wedge \langle - \rangle Y)) = \{s_1, s_2, s_3\}$

$[Y_{20}] = \{\emptyset\}$

$[Y_{21}] = (a \wedge \langle - \rangle X_1) \vee (\neg b \wedge \langle - \rangle Y_{20})$

$= ([a] \wedge preE(-,[X_1])) \vee ([\neg b] \wedge preE(-,[Y_{20}]))$

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

$[Y_{22}] = ([a] \wedge preE(-,[X_1]) \vee ([\neg b] \wedge preE(-,[Y_{21}]))$

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

$[Y_{23}] = ([a] \wedge preE(-,[X_1])) \vee ([\neg b] \wedge preE(-,[Y_{22}]))$

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

$[Y_{24}] = ([a] \wedge preE(-,[X_1])) \vee ([\neg b] \wedge preE(-,[Y_{23}]))$

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

least fixpoint

Initial state in solution $\rightarrow \mathcal{T} \models \Phi$

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

$\alpha = \mu X\ a \vee [-]X = S$

$[X_0] = \emptyset$

$[X_1] = [a] \cup preA(-,[X_0])$

$= \{s_2\} \cup \emptyset = \{s_2\}$

$[X_2] = [a] \cup preA(-,[X_1])$

$= \{s_2\} \cup \{s_1\} = \{s_1, s_2\}$

$[X_3] = [a] \cup preA(-,[X_2])$

$= \{s_2\} \cup \{s_1, s_4\} = \{s_1, s_2, s_4\}$

$[X_4] = [a] \cup preA(-,[X_3])$

$= \{s_2\} \cup \{s_1, s_3, s_4\} = S$ least fixpoint

$\beta = \mu X\ b \vee \langle - \rangle X$ $= \{s_4\}$

$[X_0] = \emptyset$

$[X_1] = [b] \cup PreE(-, [X_0])$

$= \{s_4\} \cup \emptyset = \{s_4\}$

$[X_2] = [b] \cup PreE(-, [X_1])$

$= \{s_4\} \cup \{s_3\} = \{s_3, s_4\}$

$[X_3] = [b] \cup Pre(-, [X_2])$

$= \{s_4\} \cup \{s_2, s_3\} = \{s_2, s_3, s_4\}$

$[X_4] = [b] \cup PreE(-, [X_3])$

$= \{s_4\} \cup \{s_1, s_2, s_3\} = S$ → least fixpoint

$\gamma = \nu X\ \neg b \wedge \langle - \rangle X$

$[X_0] = S$

$[X_1] = [\neg b] \cap PreE(-, [X_0])$

$= \{s_1, s_2, s_3\} \cap \{S\} = \{s_1, s_2, s_3\}$

$[X_2] = [\neg b] \cap PreE(-, [X_1])$

$= \{s_1, s_2, s_3\} \cap S = \{s_1, s_2, s_3\}$

→ greatest fixpoint

$AG(\alpha \wedge \beta \wedge \gamma) = AG(\gamma) = \nu X\ [\gamma] \wedge [-]X$

$[X_0] = S$

$[X_1] = [\gamma] \cap PreA(-, [X_0])$

$= \{s_1, s_2, s_3\} \cap \{S\} = \{s_1, s_2, s_3\}$

$[X_2] = [\gamma] \cap PreA(-, [X_1])$

$= \{s_1, s_2, s_3\} \cap \{s_1, s_2, s_4\} = \{s_1, s_2\}$

$[X_3] = [\gamma] \cap PreA(-, [X_2])$

$= \{s_1, s_2, s_3\} \cap \{s_1\} = \{s_1\}$

$[X_4] = [\gamma] \cap Pre(-, [X_3])$

$= \{s_1, s_2, s_3\} \cap \{\emptyset\} = \{\emptyset\}$ least fixpoint

Initial state not in solution → $T \not\models \phi$

4) $q_1 \subseteq q_2$?

- Freeze free variables (none)
- Build canonical interpretation I_{q_1} and I_{q_2}

$$I_{q_1} = \begin{cases} \Delta^{I_{q_1}} = \{r, g, b\} \\ E^{I_{q_1}} = \{(r,g), (g,b), (b,r)\} \end{cases}$$

$$I_{q_2} = \begin{cases} \Delta^{I_{q_2}} = \{x, y, z, v, w\} \\ E^{I_{q_2}} = \{(x,y), (y,z), (z,x), (z,v), (v,w), (w,z)\} \end{cases}$$

- Check if $I_{q_1} \models I_{q_2}$ — find homomorphism from I_{q_2} to I_{q_1}

$- h(x) = r$ at random

$- h(x,y) = (r,?) \rightarrow h(y) = g$

$- h(y,z) = (g,?) \rightarrow h(z) = b$

$- h(z,x) = (b,r) \rightarrow$ ok

$- h(z,v) = (b,?) \rightarrow h(v) = r$

$- h(v,w) = (r,?) \rightarrow h(w) = g$

$- h(w,z) = (g,b) \rightarrow$ ok

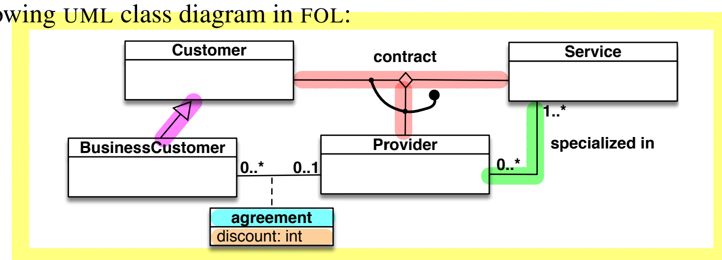
Homomorphism exists $\Rightarrow q_1 \subseteq q_2$

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

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

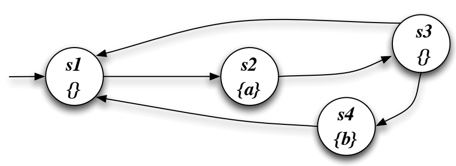
$Service$
s1
s2
s3
s4
s5

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



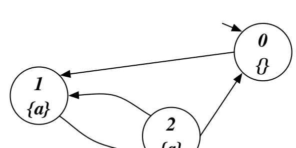
Exercise 4. Check whether the Hoare triple below is correct, by using $(x \geq 0 \wedge y \geq 0 \wedge x + y = 23)$ as invariant:

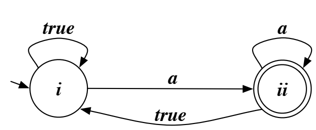
$$\{x = 23 \wedge y = 0\}\ \texttt{while(x>0) do (x=x-1; y:= y+1)}\ \{y = 23\}$$

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

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

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.*

1) Alphabet: $c(x)$, $B(x)$, $P(x)$, $S(x)$, $contr(x,y,z)$, $agr(x,y)$, $discount(x,y,z)$

ISA: $\forall x\, B(x) \supset C(x)$

SPECIALIZED: $\forall x,y\ spec(x,y) \supset P(x) \wedge S(y)$

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

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

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

AGREEMENT: $\forall x,y\ agr(x,y) \supset B(x) \wedge P(y)$

$\forall x\ B(x) \supset \#\{y \mid agr(x,y)\} \leq 1$

$\forall x,y\ agr(x,y) \supset 1 \leq \#\{z \mid disc(x,y,z)\} \leq 1$

DISCOUNT: $\forall x,y,z\ disc(x,y,z) \supset agr(x,y) \wedge Int(z)$

2) The completed instantiation (chose ISA) is correct because all axioms of Γ are made true

- $\exists y y'\ spec(x,y) \wedge spec(x,y') \wedge y \neq y'$
  $\Rightarrow \{p_1, p_2\}$
- $\forall y\ \exists z\ contr(x,y,z) \supset agr(x,y)$
  $\Rightarrow \{\emptyset\}$
- $\forall y\ agr(x,y) \supset \exists z\ contr(x,y,z)$
  $\Rightarrow \{b_1\}$
- $\exists y\ \forall z\ S(z) \supset contr(x,y,z)$ $\qquad \forall z\ S(z) \supset \exists y\ contr(x,y,z)$
  $\Rightarrow \{\emptyset\}$

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

$\forall x\,(A(x) \equiv B(x))$
$\neg((\forall y A(y)) \equiv (\forall z B(z)))$

$\forall y A(y)$ $\neg \forall z B(z)$	$\neg \forall y A(y)$ $\forall z B(z)$
$\neg B(a)$	$\neg A(b)$
$A(a)$	$B(b)$
$A(a)$, $B(a)$ ✗ $\quad$ $\neg A(a)$, $\neg B(a)$ ✗	$A(b)$, $B(b)$ ✗ $\quad$ $\neg A(b)$, $\neg B(b)$ ✗

$\neg\Gamma$ unsat $\longrightarrow$ Γ is valid!

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

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

$[X_1] = \mu Y ((a \wedge \langle - \rangle X) \vee ([-]\neg b \wedge \langle - \rangle Y)) = \{s_1, s_2, s_4\}$

$[Y_{10}] = \{\emptyset\}$

$[Y_{11}] = ((a \wedge \langle - \rangle X_0) \vee ([-]\neg b \wedge \langle - \rangle Y_{10})) =$

$(([a] \cap preE(-,[X_0])) \cup (preA(-,[\neg b]) \cap preE(-,[Y_{10}]))$

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

$[Y_{12}] = (([a] \cap preE(-,[X_0])) \cup (preA(-,[\neg b]) \cap preE(-,[Y_{11}])) =$

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

$[Y_{13}] = (([a] \cap preE(-,[X_0])) \cup (preA(-,[\neg b]) \cap preE(-,[Y_{12}])) =$

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

$[Y_{14}] = (([a] \cap preE(-,[X_0])) \cup (preA(-,[\neg b]) \cap preE(-,[Y_{13}])) =$

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

least fixpoint!

$[X_2] = \mu Y ((a \wedge \langle - \rangle X) \vee ([-]\neg b \wedge \langle - \rangle Y)) = \{\emptyset\}$

$[Y_{20}] = \{\emptyset\}$

$[Y_{21}] = ((a \wedge \langle - \rangle X_1) \vee ([-]\neg b \wedge \langle - \rangle Y_{20})) =$

$(([a] \cap preE(-,[X_1])) \cup (preA(-,[\neg b]) \cap preE(-,[Y_{20}])) =$

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

least fixpoint!

greatest fixpoint

$[X_3] = \mu Y ((a \wedge \langle - \rangle X) \vee ([-]\neg b \wedge \langle - \rangle Y)) = \{\emptyset\}$

$[Y_{30}] = \{\emptyset\}$

$[Y_{31}] = ((a \wedge \langle - \rangle X_2) \vee ([-]\neg b \wedge \langle - \rangle Y_{30})) =$

$(([a] \cap preE(-,[X_2])) \cup (preA(-,[\neg b]) \cap preE(-,[Y_{30}])) =$

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

least fixpoint

Initial state not in solution ($\{\emptyset\}$) $\rightarrow T \not\models \Phi$ (Φ = μ-calculus formula)

CTL: $EG(AFa \wedge (\underbrace{EFb}_{\beta} \vee \underbrace{AG\neg b}_{\alpha}))$

$\alpha = \nu X\ \neg b \wedge [-]X = \{\emptyset\}$

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

$[X_1] = \neg b \wedge [-]X_0 = [\neg b] \cap preA(-,[X_0]) = \{s_1, s_2, s_3\} \cap \{s_1, s_2, s_3, s_4\} = \{s_1, s_2, s_3\}$

$[X_2] = [\neg b] \cap preA(-,[X_1]) = \{s_1, s_2, s_3\} \cap \{s_1, s_2, s_4\} = \{s_1, s_2\}$

$[X_3] = [\neg b] \cap preA(-,[X_2]) = \{s_1, s_2, s_3\} \cap \{s_1, s_4\} = \{s_1\}$

$[X_4] = [\neg b] \cap preA(-,[X_3]) = \{s_1, s_2, s_3\} \cap \{s_4\} = \emptyset$ fixpoint! (X_5 will be $\emptyset$)

$\beta = \mu X\ b \vee \langle - \rangle X = \{s_1, s_2, s_3, s_4\}$

$[X_0] = \emptyset$

$[X_1] = [b] \cup preE(-,X_0) = \{s_4\} \cup \{\emptyset\} = \{s_4\}$

$[X_2] = [b] \cup preE(-,X_1) = \{s_4\} \cup \{s_3\} = \{s_3, s_4\}$

$[X_3] = [b] \cup preE(-,X_2) = \{s_4\} \cup \{s_2, s_3\} = \{s_2, s_3, s_4\}$

$[X_4] = [b] \cup preE(-,X_3) = \{s_4\} \cup \{s_1, s_2, s_3\} = \{s_1, s_2, s_3, s_4\}$ fixpoint! (X_5 will be equal $/S$)

$EG(AFa \wedge (S \vee \emptyset)) = EG(AFa \wedge S) = EG(AFa)$ because $\wedge S \rightarrow \cap S \rightarrow$ intersection with all states is meaningless.

$AF\,a = \mu X . a \vee [-]X$ $= \{S\}$

$[X_0] = \emptyset$

$[X_1] = [a] \cup PreA(-, X_0) = \{S_2\}$

$[X_2] = [a] \cup PreA(-, X_1) = \{S_2\} \cup \{S_1\} = \{S_1, S_2\}$

$[X_3] = [a] \cup PreA(-, X_2) = \{S_2\} \cup \{S_1, S_4\} = \{S_1, S_2, S_4\}$

$[X_4] = [a] \cup PreA(-, X_3) = \{S_2\} \cup \{S_1, S_3, S_4\} = \{S\}$ fixpoint

$EG(AF\,a) = EG(S) = \nu X . S \wedge \langle - \rangle X$ $= \{S\}$

$[X_0] = S$

$[X_1] = \{S\} \cup Pre(-, [X_0]) = \{S\}$ fixpoint

Initial state in solution $\rightarrow T \not\models \phi$

4) $I = \{x \geq 0 \wedge y \geq 0 \wedge \; x + y = 23\}$

$P = \{x = 23 \wedge y = 0\}$

$Q = \{y = 23\}$

$\delta = \{x = x - 1;\; y = y + 1\}$

$G = \{x > 0\}$

- check $P \supset I$

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

- check $\neg g \wedge I \supset Q$

$\underbrace{x \leq 0 \wedge x \geq 0}_{x = 0} \wedge y \geq 0 \wedge x + y = 23 \supset y = 23$ ✓

- check $\{g \wedge I\}\, \delta\, \{I\} = g \wedge I \supset wp(\delta, I)$

$x > 0 \wedge x \geq 0 \wedge y \geq 0 \wedge x + y = 23 \quad \supset wp(\delta, I)$

$\hookrightarrow x > 0 \wedge x \geq 0 \wedge y \geq 0 \wedge x + y = 23 \supset x - 1 \geq 0 \wedge y + 1 \geq 0 \wedge x + y = 23$

$\{x - 1 \geq 0 \wedge y + 1 \geq 0 \wedge x + y = 23\}$

$x = x - 1$

$\{x \geq 0 \wedge y + 1 \geq 0 \wedge x + y + 1 = 23\}$

$y = y + 1$

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

I is an invariant so the Hoare triple is correct!