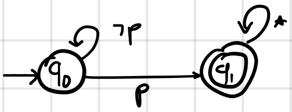
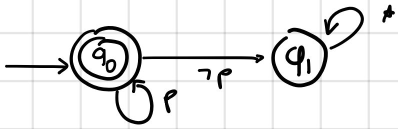
Ex From LTL to (G)NBA

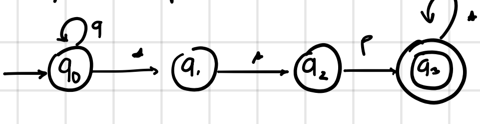
- Fp



- Gp

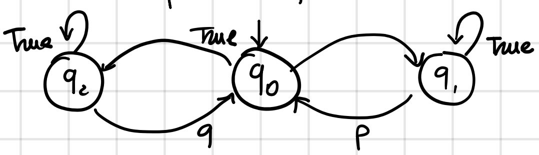


- $q\,U\,(XXp)$



- $G(p \to Fq)$

- $GFp \wedge GFq$



$F_1 = \{q_1\}$
$F_2 = \{q_2\}$

LTL model checking algorithms takes :
- a model T
- a formula φ

and returns
- YES if $T \models \varphi$
- NO and a counter example if $T \not\models \varphi$

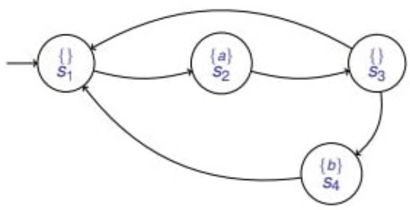
Consider a model T and an LTL property φ
$T \models \varphi$ if $\forall$ paths π of T it holds that $\pi \models \varphi$ namely if $\pi \in \mathcal{L}(\varphi)$

$$\to T \models \varphi \Leftrightarrow \mathcal{L}(T) \subseteq \mathcal{L}(\varphi)$$
$$\Leftrightarrow \mathcal{L}(T) \cap \overline{\mathcal{L}(\varphi)} = \emptyset$$
$$\Leftrightarrow \mathcal{L}(T) \cap \mathcal{L}(\neg\varphi) = \emptyset$$

① construct N_T automaton from LTS
② construct $N_{\neg\varphi}$ automaton from LTL formula
③ construct product automaton $N_{T,\neg\varphi} = N_T \otimes N_{\neg\varphi}$
④ Solve nonempiteness problem $\mathcal{L}(N_{T,\neg\varphi}) \overset{?}{\neq} \emptyset$

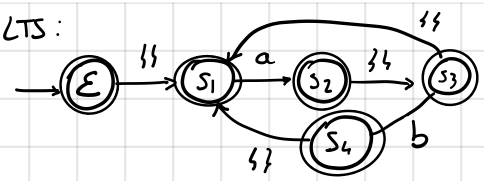
$\left.\right\}$ YES if $\mathcal{L}(N_{T,\neg\varphi}) = \emptyset$
NO otherwise

Ex.



$Xa \wedge (G(b \to Xa)) \wedge Fa$

LTS :

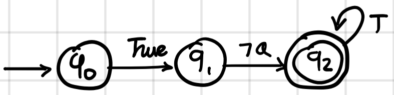


LTL : $\varphi = Xa \wedge (G(b \to Xa)) \wedge Fa$

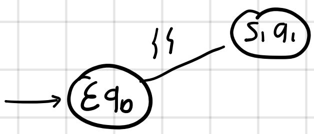
$\to \neg\varphi = \varphi_1 \vee \varphi_2 \vee \varphi_3 = \neg Xa \vee \neg G(b \to Xa) \vee \neg Fa$
$= X\neg a \vee (b \wedge \neg Xa) \vee G\neg a$

We just need one of φ_1, φ_2 and φ_3 to be "true"

- φ_1 :

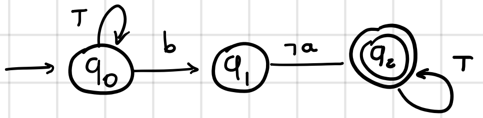


Product (LTS always accepting !) :

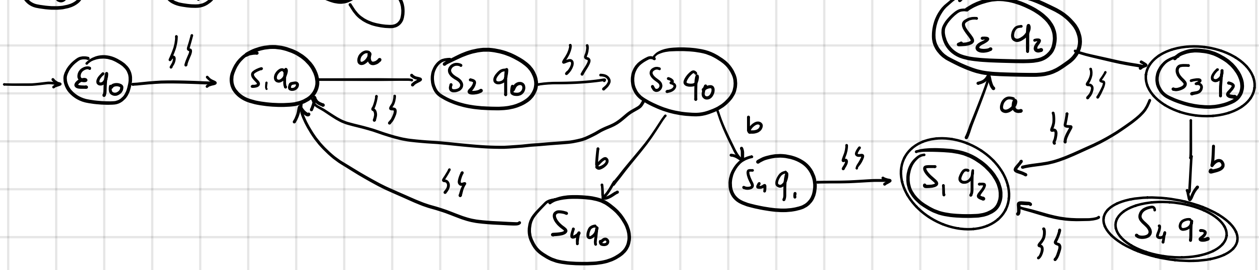


From s_1 we move only with "a"
From q_1 we move only with "¬a"
$\longrightarrow$ STUCK $\longrightarrow$ empty

• φ_2



Product:



$B = \{(s_1 q_2), (s_2 q_2), (s_3 q_2), (s_4 q_2)\}$

Recurrent Reachability:

$Buchi(B) = \nu Y\,(Reach(B \wedge \langle next \rangle Y))$ $\qquad [Reach(F) = \mu Z(F \vee \langle next \rangle Z)]$

$= \nu Y \mu Z((B \wedge \langle next \rangle Y) \vee \langle next \rangle Z)$

Y_0 = all states

$Z_0 = \emptyset$

$Z_1 = (B \cap \langle next \rangle Y_0) \cup \langle next \rangle Z_0 = \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2\} \cup \{\text{all states} \setminus \varepsilon q_0\} = \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2\}$

$Z_2 = (B \cap \langle next \rangle Y_0) \cup \langle next \rangle Z_1 = \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2\} \cup \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2, s_4 q_1\} = \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2, s_4 q_1$

$Z_3 = (B \cap \langle next \rangle Y_0) \cup \langle next \rangle Z_2 = \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2\} \cup \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2, s_4 q_1, s_3 q_0\}$

$= \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2, s_4 q_1, s_3 q_0\}$

$Z_4 = (B \cap \langle next \rangle Y_0) \cup \langle next \rangle Z_3 = \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2, s_4 q_1, s_3 q_0, s_2 q_0\}$

$Z_5 = (B \cap \langle next \rangle Y_0) \cup \langle next \rangle Z_4 = \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2, s_4 q_1, s_3 q_0, s_2 q_0, s_1 q_0\}$

$Z_6 = (B \cap \langle next \rangle Y_0) \cup \langle next \rangle Z_5 = \{s_1 q_2, s_2 q_2, s_3 q_2, s_4 q_2, s_4 q_1, s_3 q_0, s_2 q_0, s_1 q_0, \varepsilon q_0, s_4 q_0\}$

$Z_7 = (B \cap \langle next \rangle Y_0) \cup \langle next \rangle Z_6 = Z_6$ l.f.p.

$Y_1 = Y_0$ g.f.p.

$\Longrightarrow G(b \rightarrow Xa)$ is false in LTS $\longrightarrow \varphi$ not satisfied in LTS

Ex Check whether CQ q_1 is contained in CQ q_2 exploiting canonical DBs and homomorphism

$q_1 \leftarrow edge(r,g), edge(g,b), edge(b,r)$

$q_2 \leftarrow edge(x,y), edge(y,z), edge(z,v), edge(v,w), edge(w,z)$

There are no free variable → no need to freeze them!

I_{q_1} = canonical DB of q_1

e	
r	g
g	b
b	r

For second query we need to guess assignments for existencial variables α

We start from $\alpha(x)$ and we assign to it (at random) r

$\alpha(X)=r$

$\rightarrow edge(x,y) = edge(r,y)$

we check on canonical DB of q_1 a predicate starting with r and "guess" $\alpha(y)$: only row starting with r has a g at second place

$\alpha(y)=g$

We do the same for $edge(y,z)$. $\alpha(y)=g$, there is only [g b] → $g(z)=b$

$edge(z,x) \longrightarrow edg(b,r)$ that is in canonical DB ✓

$edge(z,v)$, $\alpha(z)=b \longrightarrow g(v)=r$

$edge(v,w)$, $\alpha(v)=r \longrightarrow g(w)=g$

$edge(w,z) \longrightarrow edge(g,b)$ is in canonical DB ✓

Satisfy assignment of existencial variables.

I_{q_2}

e	
x	y
y	z
z	x
z	v
v	w
w	z

Finding homomorphism means extend assignment to constants. But in our case there arent.

So? Nothing to do

$h = \hat{\alpha} = \alpha$

└ α on constants

To check homomorphism we need to check that

$h(c^{I_{q_1}}) = h(c^{I_{q_2}})$ $\forall$ constansts

but since we dont have ... is true

$(x,y) \in e^{I_{q_2}} \Rightarrow h(x),h(y) \in e^{I_{q_1}}$

how to check? Simply use assignments: $h(x)h(y) \rightarrow [r\ g]$

$[r\ g]$ is $e^{I_{q_1}}$ ✓

Do fo every entry in $e^{I_{q_2}}$. They should be all true, mistakes otherwise.

Ex Check whether the following FOL formula is valid using tableaux:

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

Tableaux can only solve satisfiability problems, not validity

$\rightarrow$ negate the formula and check unsatisfiability

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

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

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

$\downarrow \qquad [\neg(\alpha \supset \beta)]$

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

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

$\downarrow$

$P(\alpha)$ ×

we need to generate a clash so we need a $\neg P(\alpha)$

$\rightarrow$ useless to expand $\neg \exists x Q(x)$!

$\downarrow$

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

$\neg P(\alpha)$ × $\qquad Q(\alpha)$ ×

$\qquad\qquad \downarrow$

$\qquad\qquad \neg Q(\alpha)$ ×

Ex Check if valid using tableaux and if not exhibit an interpretation that is a counter example

$$\neg((\forall x\, P(x) \lor Q(x)) \equiv (\forall x\, P(x) \lor \forall x\, Q(x)))$$

$[\neg \alpha \equiv \beta]$

Left branch:

$\cancel{\forall x\, P(x) \lor Q(x)}$

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

$\downarrow$

$\cancel{\neg \forall x\, P(x)}$

$\cancel{\neg \forall x\, Q(x)}$

$\downarrow$

$\neg P(\alpha)$ ×

$\downarrow$

$\neg Q(\beta)$

$\downarrow$

$P(\alpha) \lor Q(\alpha)$

$P(\alpha)$ × $\qquad Q(\alpha)$

$\neq Q(\beta)$

no clash!

Right branch:

$\cancel{\forall x\, P(x) \lor \forall x\, Q(x)}$

$\cancel{\neg(\forall x P(x) \lor Q(x))}$

$\downarrow$

$\neg(P(c) \lor Q(c))$

$\downarrow$

$\neg P(c)$ ×

$\neg Q(c)$ ×

$\forall x P(x) \qquad \forall x\, Q(x)$

$\downarrow \qquad\qquad \downarrow$

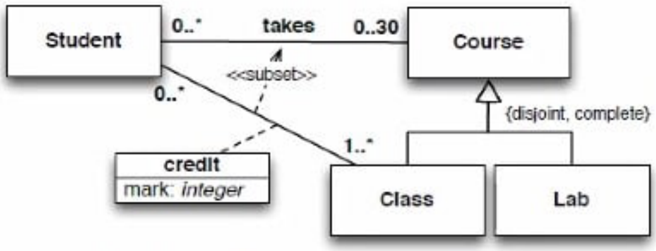
$P(c)$ × $\qquad Q(c)$ ×

Δ^I = all constants = $\{\alpha, \beta\}$ [only of first branch]

$P^I = \{\beta\}$

$Q^I = \{\alpha\}$

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.

①

$St(x)$, $Course(x)$, $Class(x)$, $Lab(x)$, $takes(x,y)$, $credit(x,y)$, $mark(x,y,z)$, $int(x)$

$\forall x,y\ takes(x,y) \supset St(x) \land Course(y)$ — takes
$\forall x\ St(x) \supset \#\{y \mid takes(x,y)\} \leq 30$ → $1 \leq \ldots \leq 30$ to be more precise, but logic will do for us.

$\forall x,y\ credit(x,y) \supset St(x) \land class(y)$ — credit
$\forall x\ St(x) \supset 1 \leq \#\{y \mid credit(x,y)\}$
$\forall x,y\ Credit(x,y) \supset takes(x,y)$

$\forall x,y,z\ mark(x,y,z) \supset credit(x,y) \land int(z)$ — mark
$\forall x,y\ credit(x,y) \supset \exists z\ mark(x,y,z)$
$\forall x,y\ credit(x,y) \supset \forall z,z'\ mark(x,y,z) \land mark(x,y,z') \supset z = z'$

$\forall x\ Class(x) \supset Course(x)$ — ISA
$\forall x\ Lab(x) \supset Course(x)$
$\forall x\ Class(x) \supset \neg Lab(x)$ [OR viceversa] — disjoint
$\forall x\ Course(x) \supset Class(x) \lor Lab(x)$ — complete

②

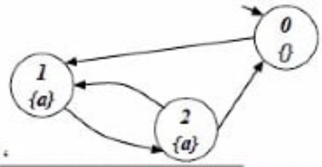
1. Use CHASE algorithm (apply/check ISA on instantiation 1 time more than the max lenght of ISA chain in diagram (1 in our case))
Instantiation is correct (every class and lab is also a course, create the table)

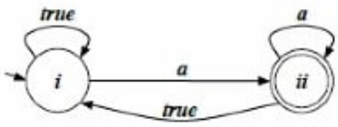
2.

- $\exists y_1, y_2, y_3\ St(x) \land takes(x,y_1) \land takes(x,y_2) \land takes(x,y_3) \land y_1 \neq y_2 \land y_1 \neq y_3 \land y_2 \neq y_3$
- $St(x) \land \forall\ takes(x,y) \supset class(y)$
- $\exists x.\ St(x) \land \forall y\ Lab(y) \supset takes(x,y)$
- $\exists x.\ St(x) \land \forall y\ Class(y) \supset (takes(x,y) \land \neg Credit(x,y))$

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:

[T] $\mapsto$





$\leftarrow [A_{\neg\Diamond\Box\neg a}]$

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

$\forall$ traces of T $\supset$ traces satisfy $\Diamond\Box\neg a$

$\forall t \in \mathcal{L}(A_T) \Rightarrow t \in \mathcal{L}(A_{\Diamond\Box\neg a})$

$\hookrightarrow \exists t \in \mathcal{L}(A_T) \wedge t \notin \mathcal{L}(A_{\Diamond\Box\neg a})$

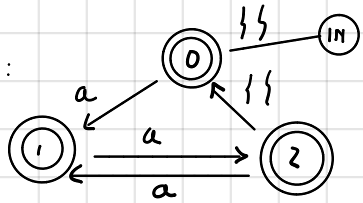
$\hookrightarrow$ find complementary $\overline{A_{\Diamond\Box\neg a}}$

We must check emptyness of $A_T \wedge \overline{A_{\Diamond\Box\neg a}}$

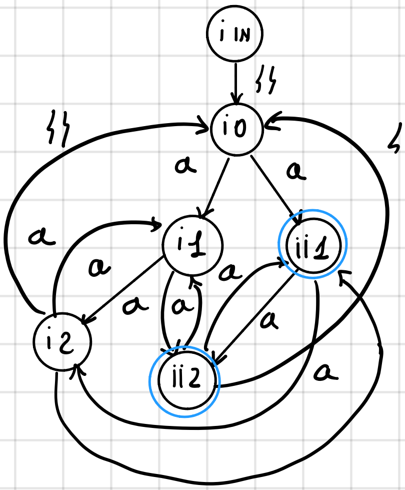
$\exists t \in \mathcal{L}(A_T) \wedge t \in \mathcal{L}(A_{\neg(\Diamond\Box\neg a)})$

check emptyness of $A_T \wedge A_{\neg(\Diamond\Box\neg a)}$

A_T :



$A_T \wedge A_{\neg\phi}$



Non emptyness:

$\nu X\, \mu Y (Acc \wedge \langle - \rangle X) \vee \langle - \rangle Y$

X_0 = All states

$X_1 = \mu Y (Acc \wedge \langle - \rangle X_0) \vee \langle - \rangle Y$ = All states $\rightarrow$ greatest fixpoint

$[Y_{10}] = \emptyset$

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

$= \{ii1, ii2\} \cup \emptyset = \{ii1, ii2\}$

$[Y_{12}] = \{ii1, ii2\} \cup PreE(-,[Y_{11}])$

$= \{ii1, ii2\} \cup \{i0, i1, i2, ii1, ii2\} = \{i0, i1, i2, ii1, ii2\}$

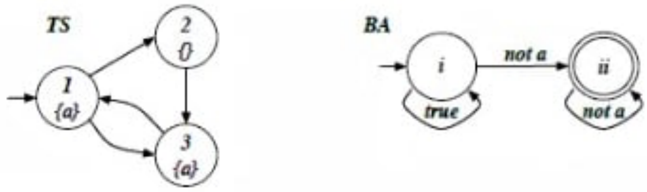
$[Y_{13}] = \{ii1, ii2\} \cup PreE(-,[Y_{12}])$

= All states   least fixpoint

Not empty! $\Rightarrow \exists t .\ t$ is generated by $T \wedge t \models \neg(\Box\Diamond\neg a)$

$\Rightarrow T \not\models \phi$

Exercise 5. Consider the transition system TS below. Model check the LTL formula $\Box\Diamond a$, by considering that the Büchi automaton BA for $\neg\Box\Diamond a$ (i.e., $\Diamond\Box\neg a$) is the one below:



$\forall t.\ t \text{ of } T \supset t \models \phi$

$\mathcal{L}(T) \subseteq \mathcal{L}(\phi)$

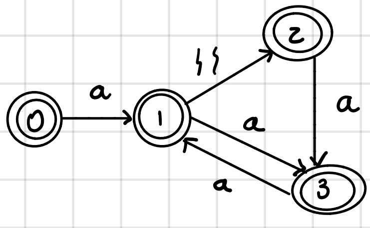
$\mathcal{L}(T) \cap \mathcal{L}(\neg\phi) = \emptyset$

$\mathcal{L}(A_T) \cap \mathcal{L}(A_{\neg\phi}) = \emptyset$

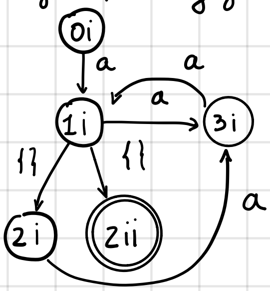
$\mathcal{L}(A_T \wedge A_{\neg\phi}) = \emptyset$

① Build A_T:
- all states are final
- add "input node" (0)
- move "actions" on edges (a and {})

$\Rightarrow$



② Build $A_T \wedge \boxed{A_{\neg\phi}}$ → given:
- run both automatons from "input" and "i" (0i)
- final state if final in both automatons



3) Check non-emptyness using "magic formula"

→ final state

$\nu X \mu Y (Acc \wedge \langle - \rangle X) \vee \langle - \rangle Y$

$[X_0] = S$

$[X_1] = \mu Y (Acc \wedge \langle - \rangle X) \vee \langle - \rangle Y$ = $\emptyset$ greatest fixpoint

$[Y_{10}] = \emptyset$

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

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

Empty! $\Rightarrow \neg\exists\, t \in T \wedge t \models \neg\Box\Diamond a \Rightarrow T \models \phi$

General rule: if initial state (0i) • is NOT in fixpoint → $T \models \phi$ $(\mathcal{L}(N_{T,\neg\phi}) = \emptyset)$

• is in fixpoint → $T \not\models \phi$ $(\mathcal{L}(N_{T,\neg\phi}) \neq \emptyset)$

RECAP RULES & μ-calculus CONVERSIONS

α rules

$$\frac{\phi \wedge \psi}{\begin{array}{c}\phi\\ \psi\end{array}} \qquad \frac{\neg(\phi \vee \psi)}{\begin{array}{c}\neg\phi\\ \neg\psi\end{array}} \qquad \frac{\neg(\phi \supset \psi)}{\begin{array}{c}\phi\\ \neg\psi\end{array}}$$

$\neg\neg$-Elimination

$$\frac{\neg\neg\phi}{\phi}$$

β rules

$$\frac{\phi \vee \psi}{\phi \mid \psi} \qquad \frac{\neg(\phi \wedge \psi)}{\neg\phi \mid \neg\psi} \qquad \frac{\phi \supset \psi}{\neg\phi \mid \psi}$$

Branch Closure

$$\frac{\begin{array}{c}\phi\\ \neg\phi\end{array}}{X}$$

$$\frac{\phi \equiv \psi}{\begin{array}{c|c}\phi & \neg\phi\\ \psi & \neg\psi\end{array}} \qquad \frac{\neg(\phi \equiv \psi)}{\begin{array}{c|c}\phi & \neg\phi\\ \neg\psi & \psi\end{array}}$$

$$\frac{\exists x\ \phi(x)}{\phi(c)} \qquad \frac{\neg\forall x\ \phi(x)}{\neg\phi(c)}$$

c = fresh constant = new constant not previously appearing in tableaux

$$\frac{\neg\exists x\ \phi(x)}{\neg\phi(t)} \qquad \frac{\forall x\ \phi(x)}{\phi(t)}$$

t = any term = not fresh

CTL $\longrightarrow$ μ-calculus

CTL	μ-calculus
p	p
$\vee, \wedge, \rightarrow$	$\vee, \wedge, \rightarrow$
$EX\varphi$	$\langle next \rangle t(\varphi)$
$AX\varphi$	$[next]\, t(\varphi)$
$EF\varphi$	$\mu Z\ t(\varphi) \vee \langle next \rangle Z$
$AF\varphi$	$\mu Z\ \ t(\varphi) \vee [next]\, Z$
$EG\varphi$	$\nu Z\ \ t(\varphi) \wedge \langle next \rangle Z$
$AG\varphi$	$\nu Z\ \ t(\varphi) \wedge [next]\, Z$
$\varphi EU\psi$	$\mu Z.\ t(\psi) \wedge (t(\varphi) \wedge \langle next \rangle Z)$
$\varphi AU\psi$	$\mu Z\ t(\psi) \vee (t(\varphi) \wedge [next]\, Z)$

$E \longrightarrow$ has always $\langle - \rangle$
$A \longrightarrow$ has always $[-]$

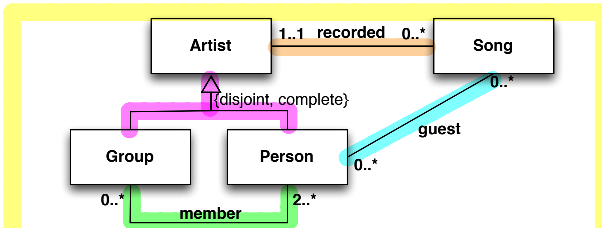
$F \longrightarrow \mu \ \ldots \ \vee \ \ldots$
$G \longrightarrow \nu \ \ldots \ \wedge \ldots$

Note: $A \supset B \longrightarrow \neg A \vee B$

Formal Methods – July 25, 2016

(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.

Group

Be
RS

Person

John
Paul
George
Ringo
Mick
Keith

member

John	Be
Paul	Be
George	Be
Ringo	Be
Mick	RS
Keith	RS

Song

I wanna be your man (original)
I wanna be your man (cover)

recorded

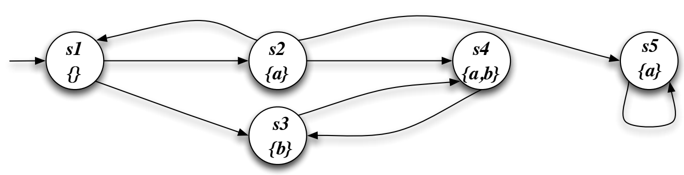
RS	I wanna be your man (original)
Be	I wanna be your man (cover)

guest

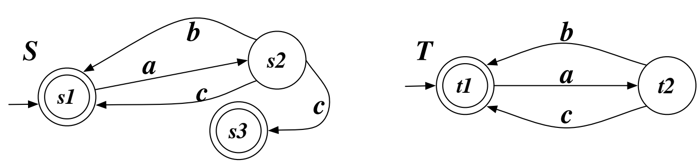
John	I wanna be your man (original)
Paul	I wanna be your man (original)

1. Check whether the above 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 groups to with more that 3 members.
   (b) Return person that are guest of all songs that they, or group they are member of, did not recorded.
   (c) Check whether there are no songs recoded by groups whose members also participated as guests to the song.

Exercise 3. Model check the Mu-Calculus formula $\nu X.\mu Y.((b \wedge \langle next\rangle X) \vee \langle next\rangle Y)$ and the CTL formula $EG(AX(\neg a \vee AFb))$ (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. Check whether the following Hoare triple is correct, using as *invariant* $i \leq 10$.

```
{i=0} while(i<10) do i:= i+1 {i=10}
```

1) ALPHABET: $A(x), G(x), P(x), S(x)$, $member(x,y)$, $guest(x,y)$, $recorded(x,y)$

ISA: $\forall x \; A(x) \supset G(x) \vee P(x)$

$\forall x \; G(x) \supset \neg P(x)$

$\forall x \; G(x) \supset A(x)$

$\forall x \; P(x) \supset A(x)$

member: $\forall xy \; member(x,y) \supset G(x) \wedge P(y)$

$\forall x \; G(x) \supset 2 \leq \#\{y \mid member(x,y)\}$

guest: $\forall xy \; guest(x,y) \supset P(x) \wedge S(y)$

recorded: $\forall xy \; recorded(x,y) \supset A(x) \wedge S(y)$

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

2) 1. To check if instantiation is correct, we apply chase algorithm untill we reach a fixpoint (no more modifications possible)

$I_0 = \emptyset$

$I_1 = I$

$I_2 = I_1 \cup \{group \cup person\}$ = create Artist table

$I_3 = I_2 \cup \emptyset = I_2$ fixpoint (complete instantiation)

The complete instantiation is correct because all axioms are made true.

2. $-\exists y y' y'' \; member(x,y) \wedge member(x,y') \wedge member(x,y'') \wedge \neg(y=y') \wedge \neg(y'=y'') \wedge \neg(y=y'')$

$\Rightarrow \{Be\}$

$- \quad P(x) \wedge \forall y \; guest(x,y) \supset \neg recorded(x,y) \vee (\forall z \; member(z,x) \supset recorded(z,y))$

$\Rightarrow \{Paul, John\}$

$- \quad \neg \exists xyz \; recorded(x,y) \wedge G(x) \supset \exists z \; member(x,z) \wedge guest(z,y)$

$\Rightarrow \{\emptyset\}$

4) Two transition systems are bisimilar if:

- locally they look equal
- each action that can be done on one can also be done on the other.

R_0 = cartesion product $= \{(s_1,t_1)(s_1,\cancel{t_2})(s_2,\cancel{t_1})(s_2,t_2)(s_3,t_1)(s_3,\cancel{t_2})\}$

R_1 = remove pairs that violate local conditions on final states

$= \{(s_1,t_1)(s_2,t_2)(s_3,\cancel{t_1})\}$

R_2 = remove pairs that allow action only on one of the two states

$= \{(s_1,t_1)(s_2,t_2)\}$

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

$= \{(s_1,t_1)(s_2 t_2)\}$

$(s_1 t_1)$ belongs to gfp $\longrightarrow$ S and T are bisimilar

5) $P = \{i = 0\}$
$Q = \{i = 10\}$
$\delta = \{i = i+1\}$
$G = \{i < 10\}$
$I = \{i \leq 10\}$

- Check if $P \supset I$
  $i = 0 \supset i \leq 10$ ✓
- Check $\neg G \wedge I \supset Q$
  $i \leq 10 \wedge i \leq 10 \supset i = 10$ ✓ $(i = 10)$
- Check $G \wedge I \supset Wp(\delta, I)$
  $i < 10 \wedge i \leq 10 \supset \quad i \leq 9$ ✓ $(i = 9)$
  $i = i+1$
  $i \leq 10$

I is an invariant $\longrightarrow$ the Hoare triple is correct!

3) $\nu X \mu Y((b \wedge \langle - \rangle X) \vee \langle - \rangle Y)$
$[X_0] = S$
$[X_1] = \mu Y((b \wedge \langle - \rangle X) \vee \langle - \rangle Y) = \{1, 2, 3, 4\}$
$[Y_{10}] = \emptyset$
$[Y_{11}] = ([b] \cap PreE(-, [X_0])) \cup PreE(-, [Y_{10}])$
$= (\{3, 4\} \cap S) \cup \{\emptyset\} = \{3, 4\}$
$[Y_{12}] = ([b] \cap PreE(-, [X_0])) \cup PreE(-, [Y_{11}])$
$= \{3, 4\} \cup \{1, 2, 3, 4\} = \{1, 2, 3, 4\}$
$[Y_{13}] = ([b] \cap PreE(-, [X_0])) \cup PreE(-, [Y_{12}])$ → least fixpoint
$= \{3, 4\} \cup \{1, 2, 3, 4\} = \{1, 2, 3, 4\}$
$[X_2] = \mu Y((b \wedge \langle - \rangle X) \vee \langle - \rangle Y) = \{1, 2, 3, 4\}$ greatest fixpoint
$[Y_{20}] = \emptyset$
$[Y_{21}] = ([b] \cap PreE(-, [X_1])) \cup PreE(-, [Y_{20}])$
$= (\{3, 4\} \cap \{1, 2, 3, 4\}) \cup \{\emptyset\} = \{3, 4\}$
$[Y_{22}] = ([b] \cap PreE(-, [X_1])) \cup PreE(-, [Y_{21}])$
$= \{3, 4\} \cup \{1, 2, 3, 4\} = \{1, 2, 3, 4\}$
$[Y_{23}] = ([b] \cap PreE(-, [X_1])) \cup PreE(-, [Y_{22}])$ → least fixpoint
$= \{3, 4\} \cup \{1, 2, 3, 4\} = \{1, 2, 3, 4\}$

Initial state in solution (greatest fixpoint) $\longrightarrow \mathcal{T} \models \phi$

$$EG(\underbrace{AX(\overbrace{\neg a \vee \underbrace{AFb}_{\alpha}}^{\beta})}_{\gamma})$$

$\alpha = AFb = \mu X\ b \vee [-]X \quad = \{3,4\}$

$[X_0] = \emptyset$

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

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

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

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

$\Big\} \to$ least fixpoint

$\beta = \neg a \vee \alpha \quad = \{1,3,4\}$

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

$\gamma = AX\ \beta = [-]\beta = preA(-, [\beta]) = \{3,4\}$

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

$[X_0] = S$

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

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

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

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

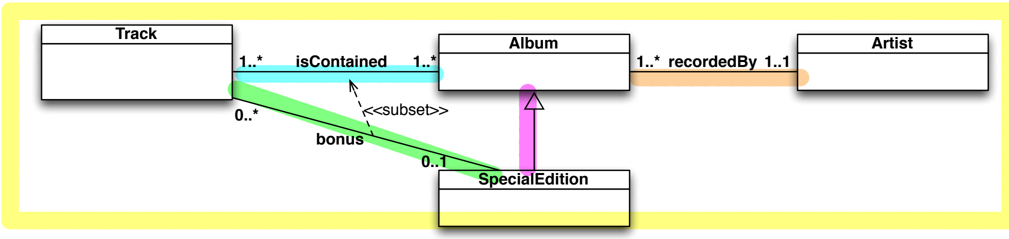
$\Big\} \to$ greatest fixpoint

Initial states doesnt belong to solution (greatest fixpoint) $\longrightarrow \mathcal{T} \not\models \phi$

Formal Methods - Final Test B – December 16, 2016

(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.

$Track$

t1
t2
t3
t4
t5
t6

$Album$

a1
a2
a3

$SpEd$

s1
s2

$Artist$

bt
rs

$isContained$

t1	a1
t2	a1
t3	a1
t1	a2
t4	a2
t5	a2
t5	a3

$bonus$

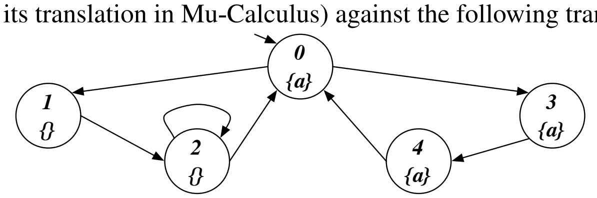
t5	s1
t6	s2

$recordedBy$

a1	bt
a2	bt
a3	rs
s1	rs
s2	bt

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 the tracks that are contained in an album and a special edition of the same artist.
   (b) Return those artist that have recorded only albums that are not special editions.
   (c) Check if there is a track appearing in all special editions.

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



Exercise 4. Consider the following two transition systems:

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

Exercise 5. Compute the certain answers to the following CQs over the following incomplete database (naive tables), and discuss how you obtained the result:

$$q() \leftarrow lives(x, y), incountry(y, z) \qquad q(x, z) \leftarrow lives(x, y), incountry(y, z)$$

$lives$

$person$	$city$
$null_0$	$null_1$
$null_2$	$null_3$
$null_4$	$null_5$
mary	$null_5$

$incountry$

$city$	$country$
$null_1$	IT
$null_3$	$null_6$
$null_5$	JP

1) ALPHABET: $T(x)$, $A(x)$, $Art(x)$, $S(x)$, $bonus(x,y)$, $contained(x,y)$, $recorded(x,y)$

ISA: $\forall x \; S(x) \supset A(x)$

BONUS: $\forall xy \; bonus(x,y) \supset T(x) \land S(y)$

$\forall x \; T(x) \supset \#\{y \mid bonus(x,y)\} \leq 1$

$\forall xy \; bonus(x,y) \supset contained(x,y)$

CONTAINED: $\forall xy \; contained(x,y) \supset T(x) \land A(y)$

$\forall x \; T(x) \supset 1 \leq \#\{y \mid contained(x,y)\}$

$\forall y \; A(y) \supset 1 \leq \#\{x \mid contained(x,y)\}$

RECORDED: $\forall xy \; recorded(x,y) \supset A(x) \land Art(y)$

$\forall x \; A(x) \supset 1 \leq \#\{y \mid recorded(x,y)\} \leq 1$

$\forall y \; Art(y) \supset 1 \leq \#\{x \mid recorded(x,y)\}$

2) Complete instantiation (merge Album with SE tables and Contained with Bonus) is correct because all axioms are made true

- $\exists y y' z z' \; bonus(x,y) \land contained(x,y') \land recorded(y,z) \land recorded(y',z) \land z = z'$
  $\Rightarrow \{t_5\}$
- $\forall x \; recored(x,y) \supset \neg S(x)$
  $\Rightarrow \{\emptyset\}$
- $\exists x \; \forall y \; S(y) \supset bonus(x,y)$
  $\Rightarrow \{\emptyset\}$

4) Two transition systems are bisimilar if:
- locally they look equal
- each action done on one of them can be done also on second one

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

R_1 = remove pairs that violate local condition on final states
$= \{(t_1,q_1)(t_2,q_2)(\cancel{t_2,q_3})\}$

R_2 = remove pairs that can "accept" action only on one of the two states
$= \{(t_1,q_1)(t_2,q_2)\}$

R_3 = remove pairs that lead to pairs no more in the list $\Big\} \rightarrow$ greatest fixpoint
$= \{(t_1,q_1)(t_2,q_2)\}$

(t_1,q_1) belongs to gfp $\longrightarrow$ T and Q are bisimilar

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

$[X_0] = S$

$[X_1] = \mu Y((\neg a \wedge \langle - \rangle X) \vee ([-]Y)) = \{1,2\}$

$[Y_{10}] = \emptyset$

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

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

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

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

$[X_2] = \mu Y((\neg a \wedge \langle - \rangle X) \vee ([-]Y)) = \{1,2\}$

$[Y_{20}] = \emptyset$

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

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

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

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

→ greatest fixpoint

Initial state not in solution $\longrightarrow \mathcal{T} \not\models \phi$

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

$\alpha = [-]a = PreA(-,[a]) = \{3,4\}$

$\beta = EX\alpha = \langle - \rangle \alpha = PreE(-,\{3,4\}) = \{0,3\}$

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

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

$[X_0] = S$

$[X_1] = \{0,1,2,3\} \cap PreA(-,[X_0]) = \{0,1,2,3\}$

$[X_2] = \{0,1,2,3\} \cap PreA(-,[X_1]) = \{0,1,2\}$

$[X_3] = \{0,1,2,3\} \cap PreA(-,[X_2]) = \{1,2\}$

$[X_4] = \{0,1,2,3\} \cap PreA(-,[X_3]) = \{1\}$

$[X_5] = \{0,1,2,3\} \cap PreA(-,[X_4]) = \emptyset$

$EF\ \emptyset = \mu X\ \emptyset \vee \langle - \rangle X$

$[X_0] = \emptyset$

$[X_1] = \emptyset \cup \emptyset = \emptyset$

Initial state not in solution $\longrightarrow \mathcal{T} \not\models \phi$

⑤ $q() \leftarrow lives(x,y), incountry(y,z)$
- Evaluate query on DB as it was complete : True (eg $\{(null_0, null_1, IT)\}$)
- Remove null tuples : nothing to do since it is a boolean query

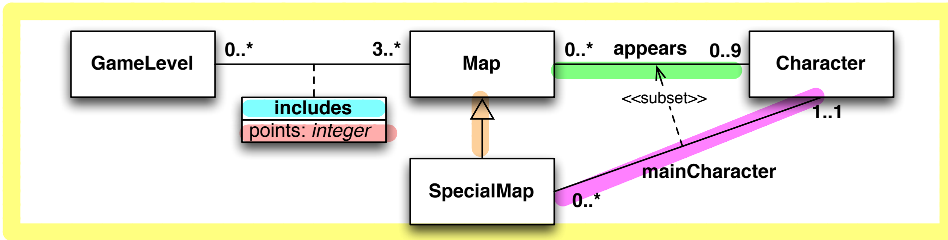
$q(x,z) \leftarrow lives(x,y), incountry(y,z)$
- Evaluate query on DB as it was complete : $\{(null_0, IT), (null_2, null_6), (null_4, JP), (mary, JP)$
- Remove null tuples : $\{(mary, JP)\}$

We remove tuples because the certain answer is constitued by tuples of constants.

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

$appaears$

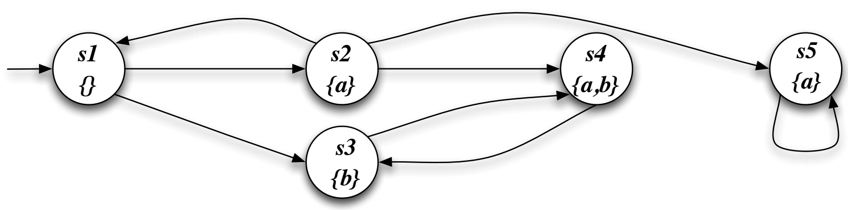
adrian	artica
adrian	bush
adrian	desert
bob	city
charline	artica

$mainCharacter$

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

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

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

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

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 $\longrightarrow T \models \phi$

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 $\longrightarrow T \models \Phi$

5)

1) Freeze free variables

$q_1(a) = e(a,y)\ e(y,y)\ e(a,z)\ e(y,z)\ e(z,y)$

$q_2(a) - e(a,y)\ e(y,z)\ e(a,v)\ e(v,z)\ e(v,y)$

2) Canonical interpretations

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

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

3) Find homomorphism from I_{q_2} to I_{q_1} [CM77 theorem]

$h(a) = a$

$h(a,y) = (a,?) \rightarrow h(y) = y$

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

$h(a,v) = (a,?) \rightarrow h(v) = z$

$h(v,z) = (z,y)$ ✓

$h(v,y) = (z,y)$ ✓

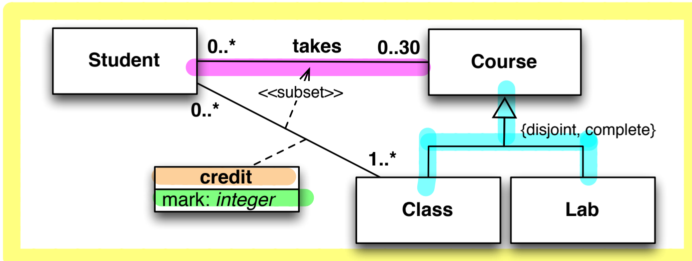
Homomorphism exists $\Longrightarrow q_1 \subseteq q_2$

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

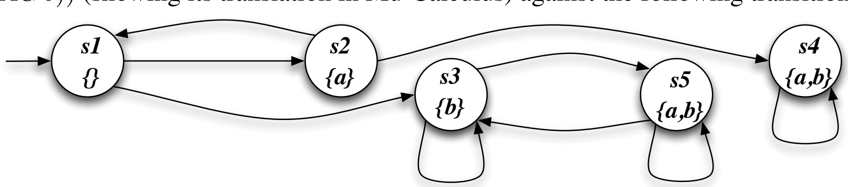
peter	algorithm	30
paul	calculus	27
mary	algorithms	28
mary	AI	30
jane	FM	30
jane	algorithms	30

takes

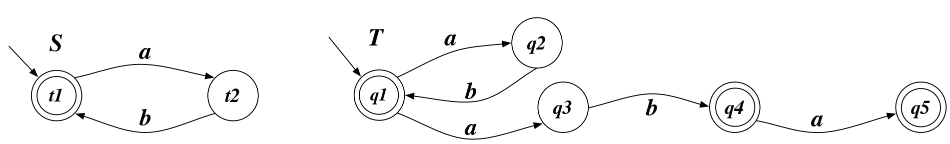
peter	IoT lab
paul	IoT lab
mary	FM
jane	db lab
jane	hacking lab
jane	IoT lab

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

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

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

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

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 Peter - algorithm) is correct because all axioms are true.

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

5) $q_1 \subseteq q_2$?

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

$$I q_1 = \begin{cases} \Delta^{Iq_1} = \{x, y, z\} \\ x^{Iq_1} = x \\ E^{Iq_1} = \{(x,y), (y,z), (z,x)\} \end{cases}$$

$$I q_2 = \begin{cases} \Delta^{Iq_2} = \{x, y, z, v, w\} \\ x^{Iq_2} = x \\ E^{Iq_2} = \{(x,y), (x,w), (y,z), (z,x), (z,v), (v,y), (v,w), (w,z)\} \end{cases}$$

- Check if $Iq_1 \models Iq_2 \longrightarrow$ find homomorphism from Iq_2 to Iq_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

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

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

$[Y_{20}] = \emptyset$

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

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

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

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

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

$[Y_{30}] = \emptyset$

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

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

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

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

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

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

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

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

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

$\delta = S \cap S = S$

$\omega = a \vee S = S$

$EF(\omega) = \mu X\, \omega \vee \langle - \rangle X = S$

$[X_0] = \emptyset$

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

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

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

4) Two tronsition system ore bisimilor if:
- locolly they look equol
- each oction done on one of them con be done olso on the second one

R_0 = cortesion 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 poirs thot violote locol condition on finol stote
$= \{(t_1,q_1)(t_1,q_4)\cancel{(t_1,q_5)}\cancel{(t_2,q_1)}(t_2,q_2)(t_2,q_3)\cancel{(t_2,q_4)}\cancel{(t_2,q_5)}\}$

R_2 = remove octions thot con be done only on one of the two stotes
$= \{(t_1,q_1)\cancel{(t_1,q_4)}(t_2,q_2)\cancel{(t_2,q_3)}\}$

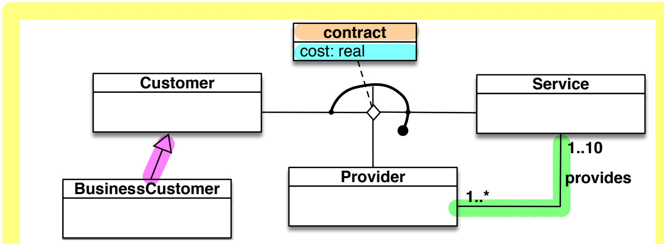
R_3 = remove poirs thot leod to poirs no more in the list
$= \{(t_1,q_1)(t_2,q_2)\}$

R_4 = some $= \{(t_1,q_1)(t_2,q_2)\}$ → greotest fixpoint

(t_1,q_1) belong to greotest fixpoint $\longrightarrow$ S ond T ore bisimilor

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

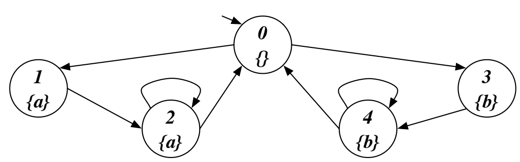
$Provider$
p1
p2

$provides$	
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:



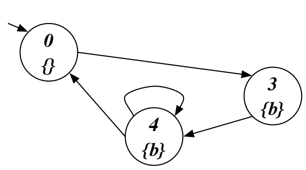
Exercise 4. Check whether the Hoare triple below is correct, by using $(x \geq 0 \wedge y \geq 0 \wedge x + y = 31)$ as invariant:

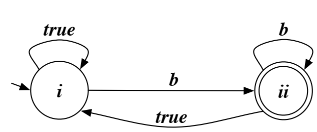
$$\{x = 31 \wedge y = 0\}\ \texttt{while(x>0) do (x=x-1; y:= y+1)}\ \{y = 31\}$$

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

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

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

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

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

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

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

$[X_0] = S$

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

$[Y_{10}] = \emptyset$

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

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

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

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

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

$[Y_{20}] = \emptyset$

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

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

$[Y_{22}] = ([b] \cap PreA(-,[X_1])) \cup ([a] \cap PreE(-,[Y_{21}]))$ → 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 → $T \not\models \varphi$

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 → $T \not\models \varphi$

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 $\{G \wedge I\}\ \delta\ \{I\} = G \wedge I \supset wp(\delta, I)$

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

$\{x \geq 1 \wedge y \geq -1 \wedge x+y = 31\}$
$x = x-1$
$\{x \geq 0 \wedge y \geq -1 \wedge x+y = 30\}$
$y = y+1$
$\{x \geq 0 \wedge y \geq 0 \wedge x+y = 31\}$

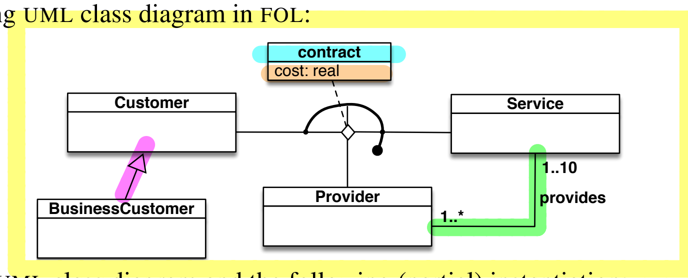
$x > 0 \wedge x \geq 0 \wedge y \geq 0 \wedge x+y = 31 \supset x \geq 1 \wedge y \geq -1 \wedge x+y = 31$ ✓

I is an invariant → the hoare triple is correct!

Formal Methods – January 18, 2018

(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

$provides$

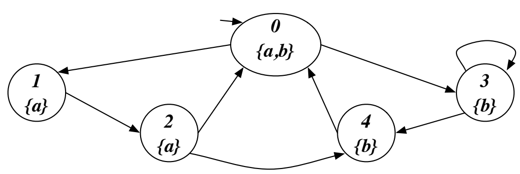
p1	s1
p1	s2
p1	s3
p2	s2

$contacts/cost$

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 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:



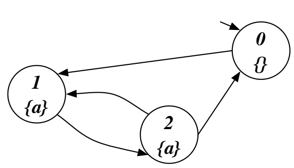
Exercise 4. Check whether CQ q_1 is contained in CQ q_2, reporting canonical DBs and homomorphism:

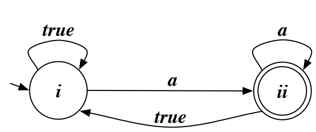
$$
\begin{array}{lcl}
q_1(x_r) & \leftarrow & e(x_r, x_g), e(x_g, x_b), e(x_b, x_r). \\
q_2(x) & \leftarrow & e(x, y), e(y, z), e(z, x), e(z, v)e(v, w), e(w, z).
\end{array}
$$

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

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

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

$\downarrow$

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

$\downarrow$

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

$\downarrow$

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

$\neg P(\alpha)$ × $\qquad$ $Q(\alpha)$ ×

$\qquad\qquad\qquad\qquad \downarrow$

$\qquad\qquad\qquad\qquad \neg Q(\alpha)$ ×

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

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

$[X_0] = S$

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

$[Y_{10}] = \emptyset$

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

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

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

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

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

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

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

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

$[Y_{20}] = \emptyset$

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

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

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

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

$= \{s_1,s_2\} \cup \{s_1\} = \{s_1,s_2\}$ least fixpoint!

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

$[Y_{30}] = \emptyset$

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

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

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

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

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

$[X_4] = \mu Y((a \wedge [-]X) \vee (b \wedge [-]Y)) = \{\emptyset\}$ 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 $\Rightarrow T \not\models \phi$

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

$\alpha = AXb = [-]b = PreA(-,[b]) = \{s_2, s_3, s_4\}$
$\beta = EX\alpha = \langle - \rangle \alpha = PreE(-,[\alpha]) = \{s_0, s_1, s_2, s_3\}$
$\gamma = a \supset \beta = \neg a \vee \beta = \{s_3, s_4\} \cup \{s_0, s_1, s_2, s_3\} = S$
$\sigma = EG\gamma = \nu X\, \gamma \wedge \langle - \rangle X$
$[X_0] = S$
$[X_1] = [\gamma] \cap PreE(-,[X_0]) = S \cap S = \{S\}$ fixpoint

$AF\sigma = \mu X\, \sigma \vee [-]X$
$[X_0] = \emptyset$
$[X_1] = [\sigma] \cup PreA(-,[X_0]) = \{S\}$ fixpoint

Initial state in solution $\Rightarrow T \models \phi$

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 $E^{I_{q_1}}$ ✓

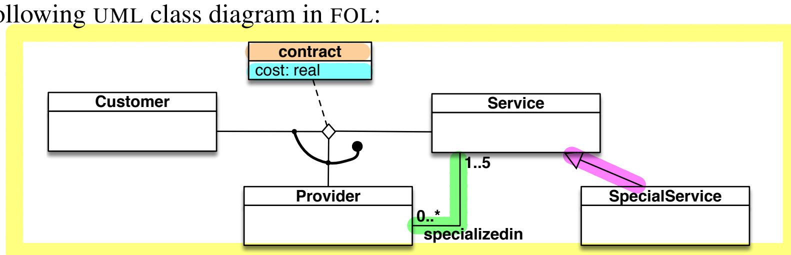
Exists an homomorphism $\Rightarrow q_1 \subseteq q_2$

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

$specializedin$

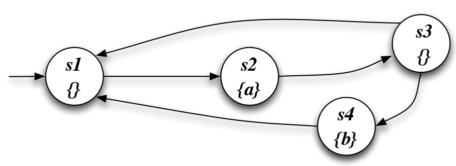
p1	s1
p1	s2
p1	s3
p2	ss1
p2	ss2

$contacts/cost$

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



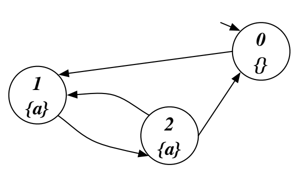
Exercise 4. Check whether CQ q_1 is contained in CQ q_2, reporting canonical DBs and homomorphism:

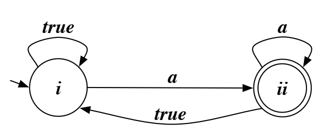
$$q_1() \leftarrow edge(r,g), edge(g,b), edge(b,r).$$
$$q_2() \leftarrow edge(x,y), edge(y,z), edge(z,x), edge(z,v), edge(v,w), edge(w,z).$$

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: $c(x)$, $s(x)$, $p(x)$, $ss(x)$, $contr(x,y,z)$, $cost(x,y,z,w)$, $Real(x)$

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

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

Left branch:

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

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

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

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

$\neg Q(\alpha)$ ×

$P(\alpha,\beta)$ ×

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

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

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

Right branch:

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

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

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

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

$P(\alpha,\beta)$ ×

$\neg Q(\alpha)$ ×

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

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

$\neg P(\alpha,\beta)$ ×

All branches clash $\Rightarrow$ Unsat $\neg\phi$ $\quad \models \phi$ valid

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

$$
\begin{aligned}
[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\} \\
&\quad [Y_{10}] = \{\emptyset\} \\
&\quad [Y_{11}] = (a \wedge \langle - \rangle X_0) \vee (\neg b \wedge \langle - \rangle Y_{10}) \\
&\quad\quad = ([a] \wedge PreE(-,[X_0])) \vee ([\neg b] \wedge PreE(-,[Y_{10}])) \\
&\quad\quad = (\{s_2\} \cap \{S\}) \cup (\{s_1, s_2, s_3\} \cap \{\emptyset\}) = \{s_2\} \\
&\quad [Y_{12}] = ([a] \wedge PreE(-,[X_0])) \vee ([\neg b] \wedge PreE(-,[Y_{11}])) \\
&\quad\quad = (\{s_2\} \cap \{S\}) \cup (\{s_1, s_2, s_3\} \cap \{s_1\}) = \{s_1, s_2\} \\
&\quad [Y_{13}] = ([a] \wedge PreE(-,[X_0])) \vee ([\neg b] \wedge PreE(-,[Y_{12}])) \\
&\quad\quad = \{s_2\} \cup (\{s_1, s_2, s_3\} \cap \{s_1, s_3, s_4\}) = \{s_1, s_2, s_3\} \\
&\quad [Y_{14}] = ([a] \wedge PreE(-,[X_0])) \vee ([\neg b] \wedge PreE(-,[Y_{13}])) \\
&\quad\quad = \{s_2\} \cup (\{s_1, s_2, s_3\} \cap \{S\}) = \{s_1, s_2, s_3\} \quad \text{least fixpoint} \\
[X_2] &= \mu Y((a \wedge \langle - \rangle X) \vee (\neg b \wedge \langle - \rangle Y)) = \{s_1, s_2, s_3\} \quad \text{greatest fixpoint} \\
&\quad [Y_{20}] = \{\emptyset\} \\
&\quad [Y_{21}] = (a \wedge \langle - \rangle X_1) \vee (\neg b \wedge \langle - \rangle Y_{20}) \\
&\quad\quad = ([a] \wedge PreE(-,[X_1])) \vee ([\neg b] \wedge PreE(-,[Y_{20}])) \\
&\quad\quad = (\{s_2\} \cap \{S\}) \cup (\{s_1, s_2, s_3\} \cap \{\emptyset\}) = \{s_2\} \\
&\quad [Y_{22}] = ([a] \wedge PreE(-,[X_1]) \vee ([\neg b] \wedge PreE(-,[Y_{21}])) \\
&\quad\quad = \{s_2\} \cup (\{s_1, s_2, s_3\} \cap \{s_1\} = \{s_1, s_2\} \\
&\quad [Y_{23}] = ([a] \wedge PreE(-,[X_1])) \vee ([\neg b] \wedge PreE(-,[Y_{22}])) \\
&\quad\quad = \{s_2\} \cup (\{s_1, s_2, s_3\} \cap \{s_1, s_3, s_4\}) = \{s_1, s_2, s_3\} \\
&\quad [Y_{24}] = ([a] \wedge PreE(-,[X_1])) \vee ([\neg b] \wedge PreE(-,[Y_{23}])) \\
&\quad\quad = \{s_2\} \cup (\{s_1, s_2, s_3\} \cap \{S\} = \{s_1, s_2, s_3\} \quad \text{least fixpoint}
\end{aligned}
$$

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

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

$$
\begin{aligned}
\alpha &= \mu X\, a \vee [-]X = S \\
&[X_0] = \emptyset \\
&[X_1] = [a] \cup PreA(-,[X_0]) \\
&\quad = \{s_2\} \cup \emptyset = \{s_2\} \\
&[X_2] = [a] \cup PreA(-,[X_1]) \\
&\quad = \{s_2\} \cup \{s_1\} = \{s_1, s_2\} \\
&[X_3] = [a] \cup PreA(-,[X_2]) \\
&\quad = \{s_2\} \cup \{s_1, s_4\} = \{s_1, s_2, s_4\} \\
&[X_4] = [a] \cup PreA(-,[X_3]) \\
&\quad = \{s_2\} \cup \{s_1, s_3, s_4\} = S \quad \text{least fixpoint}
\end{aligned}
$$

$\beta = \mu X\ b \vee \langle - \rangle X$ $= \{S_4\}$

$[X_0] = \emptyset$

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

$= \{S_4\} \cup \emptyset = \{S_4\}$

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

$= \{S_4\} \cup \{S_3\} = \{S_3, S_4\}$

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

$= \{S_4\} \cup \{S_2, S_3\} = \{S_2, S_3, S_4\}$

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

$= \{S_4\} \cup \{S_1, S_2, S_3\} = S$ $\rightarrow$ least fixpoint

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

$[X_0] = S$

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

$= \{S_1, S_2, S_3\} \cap \{S\} = \{S_1, S_2, S_3\}$

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

$= \{S_1, S_2, S_3\} \cap S = \{S_1, S_2, S_3\}$ $\rightarrow$ greatest fixpoint

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

$[X_0] = S$

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

$= \{S_1, S_2, S_3\} \cap \{S\} = \{S_1, S_2, S_3\}$

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

$= \{S_1, S_2, S_3\} \cap \{S_1, S_2, S_4\} = \{S_1, S_2\}$

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

$= \{S_1, S_2, S_3\} \cap \{S_1, S_4\} = \{S_1\}$

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

$= \{S_1, S_2, S_3\} \cap \{\emptyset\} = \{S_4\}$ least fixpoint

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

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

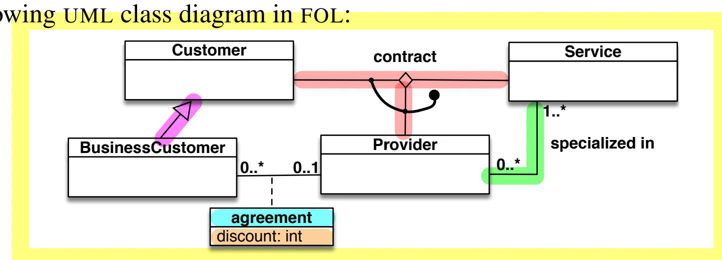
Homomorphism exists $\Rightarrow q_1 \subseteq q_2$

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

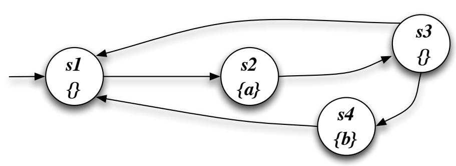
$Service$
s1
s2
s3
s4
s5

$specializedin$	
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:



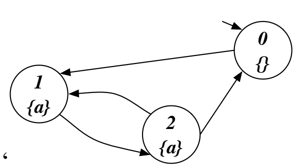
Exercise 4. Check whether the Hoare triple below is correct, by using $(x \geq 0 \wedge y \geq 0 \wedge x + y = 23)$ as invariant:

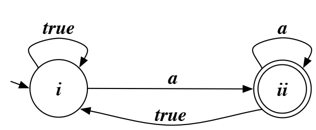
$$\{x = 23 \wedge y = 0\} \; \texttt{while(x>0) do (x=x-1; y:= y+1)} \; \{y = 23\}$$

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

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

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

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

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

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

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

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

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

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

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

$\forall x\,(A(x) \equiv B(x))$

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

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

$A(a)$	$\neg A(a)$	$A(b)$	$\neg A(b)$
$B(a)$	$\neg B(a)$	$B(b)$	$\neg B(b)$
×	×	×	×

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

greatest fixpoint

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$[X_0] = \emptyset$

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

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

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

$[X_4] = [b] \cup \text{preE}(-, X_3) = \{s_4\} \cup \{s_1, s_2, s_3\} = \{s_1, s_2, s_3, s_4\}$ 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 $\rightarrow T \nvDash \phi$

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 $P \supset I$

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

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

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

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

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

$x = x - 1$

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

$y = y + 1$

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

I is an invariant so the Hoare triple is correct!