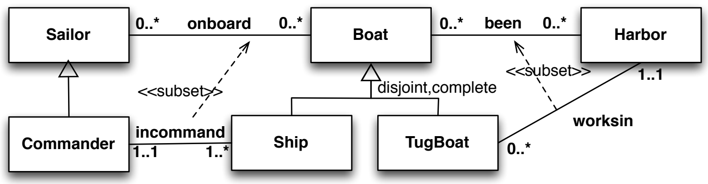
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

Formal Methods – January 12, 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.

$Sailors$

Dustin
Lubber
Rusty

$Commander$

Alice
Jim

$Ship$

Constitution
Enterprise

$TugBoat$

Bumpy
Lumpy

$Harbor$

Genoa
Calais
Piraeus

$onboard$

Dustin	Constitution
Rusty	Bumpy

$incommand$

Alice	Constitution
Jim	Enterprise

$been$

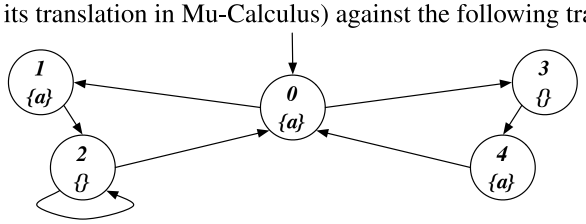
Constitution	Genoa
Constitution	Calais
Constitution	Piraeus
Bumpy	Calais

$worksin$

Bumby	Calais
Lumpy	Calais

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 sailors that have been on board of a boat which has been in a harbor where a tag boat works in.
   (b) Check whether there exists a harbor in which there have been at least two tag boats.
   (c) Return the sailors that have been in all harbors.

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



Exercise 4. Check whether the following Hoare triple is correct, using as *invariant* $(0 \leq i \;\wedge\; 0 \leq j \;\wedge\; i + j \leq 5)$.

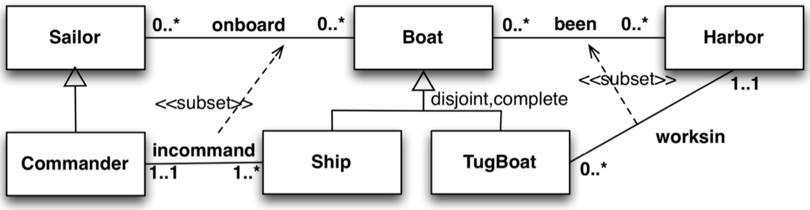
```
{i=0 AND j=5}      while(i<5) do (j=j-1; i:= i+1)      {j=0}
```

Exercise 5. Given the following boolean conjunctive queries (with a constant):

```
q1() :- e(a,y),e(y,y),e(y,a)
q2() :- e(a,y),e(y,z),e(z,w),e(w,w),e(w,z),e(z,y),e(y,a)
```

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

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



$S(x)$, $B(x)$, $H(x)$, $C(x)$, $SH(x)$, $TB(x)$
$ONBOARD(x,y)$
$INCOMMAND(x,y)$
$BEEN(x,y)$
$WORKSIN(x,y)$

$\forall x,y.\ ONBOARD(x,y) \supset S(x) \wedge B(y)$

$\forall x,y.\ BEEN(x,y) \supset B(x) \wedge H(y)$

$\forall x,y.\ INCOMMAND(x,y) \supset C(x) \wedge SH(y)$
$\forall x.\ C(x) \supset \exists y.\ INCOMMAND(x,y)$
$\forall y.\ SH(y) \supset 1 \leq \#\{x \mid INCOMMAND(x,y)\} \leq 1$
$\forall x,y\ \ INCOMMAND(x,y) \supset ONBOARD(x,y)$

$\forall x,y\ \ WORKSIN(x,y) \supset TB(x) \wedge H(y)$
$\forall x.\ TB(x) \supset \exists y.\ WORKSIN(x,y)$
$\forall x,y.\ WORKSIN(x,y) \supset BEEN(x,y)$

$\forall x.\ C(x) \supset S(x)$
$\forall x.\ SH(x) \supset B(x)$
$\forall x.\ TB(x) \supset B(x)$
$\forall x.\ SH(x) \supset \neg TB(x)$
$\forall x.\ B(x) \supset SH(x) \vee TB(x)$

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

Sailors

Dustin
Lubber
Rusty

Commander

Alice
Jim

Ship

Constitution
Enterprise

TugBoat

Bumpy
Lumpy

Harbor

Genoa
Calais
Piraeus

onboard

Dustin	Constitution
Rusty	Bumpy

incommand

Alice	Constitution
Jim	Enterprise

been

Constitution	Genoa
Constitution	Calais
Constitution	Piraeus
Bumpy	Calais

worksin

Bumby	Calais
Lumpy	Calais

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 sailors that have been on board of a boat which has been in a harbor where a tag boat works in.
   (b) Check whether there exists a harbor in which there have been at least two tag boats.
   (c) Return the sailors that have been in all harbors.

1) S = { DUST, LUB, RUST, AL, JIM }   B = { COST, ENT, BUM, LUM }

ONBOARD = { .... (AL, COST), (JIM ENT) }
BEEN = { .... (LUM, CAL) }

$\forall x, y.\ ONBOARD(x,y) \supset S(x) \wedge B(y)$

D, R ARE SAILORS
COST, BUM ARE BOATS → CARDINALS OK!

$\forall x, y.\ BEEN(x,y) \supset B(x) \wedge H(y)$

COST, BUN ARE BOATS
GEN, CAL, PIR ARE HARBOR → CARDINALS OK!

$\forall x, y.\ INCOMMAND(x,y) \supset C(x) \wedge SH(y)$

AL, JIM ARE COMMANDER
COST, ENT ARE SHIPS → CARDINALS OK!

$\forall x, y\ WORKSIN(x,y) \supset TB(x) \wedge H(y)$

BUM, LUM ARE TB
CAL IS A HARBOR → CARDINALS OK!

2) a. $\exists s, h, t.\ S(x) \wedge ONBOARD(x, s) \wedge BEEN(s, h) \wedge WORKSIN(t, h)$

{ RUSTY, DUSTIN }

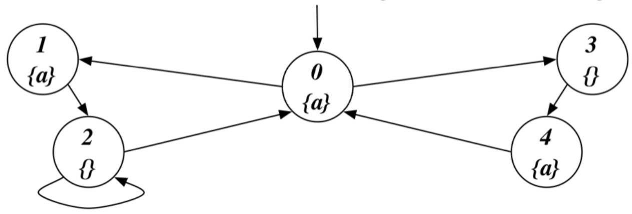
b. $\exists h, t, t'.\ HARBOR(h) \wedge WORKSIN(t, h) \wedge WORKSIN(t', h) \wedge t \neq t'$

{ FALSE }

c. $S(x) \wedge \forall h.\ (H(h) \supset \exists b.\ (ONBOARD(x, b) \wedge BEEN(b, h)))$

{ DUSTIN }

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



1) $\nu X.\mu Y.((a \wedge [NEXT]X) \vee ([NEXT]Y))$

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

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

$[Y_0] = \emptyset$

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

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

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

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

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

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

$[Y_2] = [Y_3] = [X_1] = \{0,1,3,4\}$

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

$[Y_0] = \emptyset$

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

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

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

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

$[Y_3] = ([a] \cap PREA(NEXT, X_1)) \cup PREA(NEXT, Y_2) =$

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

$[Y_2] = [Y_3] = [X_2] = \{0,3,4\}$

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

$[Y_0] = \phi$

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

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

$[Y_2] = ([a] \cap PREA(NEXT, X_2)) \cup PREA(NEXT, Y_1) =$

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

$[Y_3] = ([a] \cap PREA(NEXT, X_2)) \cup PREA(NEXT, Y_2) =$

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

$[Y_2] = [Y_3] = [X_3] = \{3,4\}$

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

$[Y_0] = \phi$

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

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

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

$[X_5] = [\mu Y.((a \wedge [NEXT]X_4) \vee ([NEXT]Y))]$

$[Y_0] = \phi$

$[Y_1] = ([a] \cap PREA(NEXT, X_4)) \cup PREA(NEXT, Y_0) =$

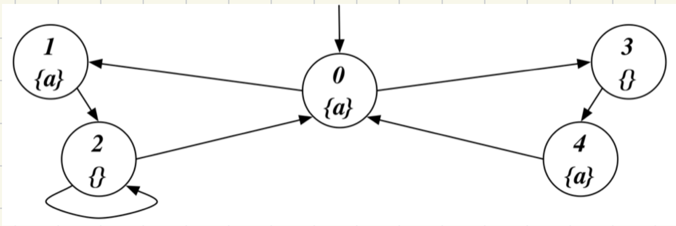
$= (\{0,1,4\} \cap \phi) \cup \phi = \phi$

$[Y_0] = [Y_1] = [X_5] = \phi$

$[X_4] = [X_5] = \phi$

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

2) $\underbrace{EF\,(\underbrace{AG\,(\underbrace{a \supset \underbrace{EX\,\underbrace{EX\,\neg a}_{\alpha}}_{\beta}}_{\gamma})}_{\delta})}_{\varepsilon}$



$[\alpha] = [EX\ \neg a] = [\langle NEXT \rangle \neg a] = PREE\,(NEXT, \neg a) = \{0, 1, 2\} = [\alpha]$

$[\beta] = [EX\ \alpha] = [\langle NEXT \rangle\ \alpha] = PREE\,(NEXT, \alpha) = \{0, 1, 2, 4\} = [\beta]$

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

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

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

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

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

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

$[\varepsilon] = [EF\ \delta] = [\mu Z.\, \delta \cup \langle NEXT \rangle\, Z]$

$[Z_0] = \phi$

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

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

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

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

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

$T_{s_0} \in \varepsilon\ ? \rightarrow s_0 \in [\varepsilon] = \{0, 1, 2, 3, 4\}\ ?$ YES!

Exercise 4. Check whether the following Hoare triple is correct, using as *invariant* $(0 \le i \wedge 0 \le j \wedge i + j \le 5)$.

I

P — g — δ — Q

```
{i=0 AND j=5}        while(i<5) do (j=j-1; i:= i+1)        {j=0}
```

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

1. $\{i=0 \wedge j=5\} \supset (0 \le i \wedge 0 \le j \wedge i+j \le 5)$ ✓

2. $\{i \ge 5 \wedge (0 \le i \wedge 0 \le j \wedge i+j \le 5)\} \supset j=0$

$\{i \ge 5 \wedge 0 \le j \wedge i+j \le 5)\} \supset j=0$ ✓

3. $\{i<5 \wedge (0 \le i \wedge 0 \le j \wedge i+j \le 5)\}\ j=j-1;\ i:=i+1\ \{0 \le i \wedge 0 \le j \wedge i+j \le 5\}$

$\{0 \le i < 5 \wedge 0 \le j \wedge i+j \le 5\} \supset wp(j=j-1; i=i+1)\{0 \le i \wedge 0 \le j \wedge i+j \le 5\}$

$\{-1 \le i \wedge 0 \le j \wedge i+j \le 5\}[j/j-1] = \{-1 \le i \wedge 1 \le j \wedge i+j \le 5\}$
$j=j-1;$
$\{0 \le i \wedge 0 \le j \wedge i+j \le 5\}[i/i+1] = \{-1 \le i \wedge 0 \le j \wedge i+j \le 5\}$
$i=i+1;$
$\{0 \le i \wedge 0 \le j \wedge i+j \le 5\}$

$\{0 \le i < 5 \wedge 0 \le j \wedge i+j \le 5\} \supset \{-1 \le i \wedge 1 \le j \wedge i+j \le 5\}$?

$\{0 \le i < 5 \wedge 0 \le j \wedge i+j \le 5\}$ IS NOT AN INVARIANT

$j \ge 0 \not\supset j \ge 1$

Exercise 5. Given the following boolean conjunctive queries (with a constant):

```
q1() :- e(a,y),e(y,y),e(y,a)
q2() :- e(a,y),e(y,z),e(z,w),e(w,w),e(w,z),e(z,y),e(y,a)
```

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

$q_1 \subseteq q_2$?

BUILD CANONICAL INTERPRETATION

$I_{q_1()}$: $\Delta^{I_{q_1}} : \{a, y\}$

$e^{q_1} : \{\langle a,y\rangle, \langle y,y\rangle, \langle y,a\rangle\}$

$I_{q_2()}$: $\Delta^{I_{q_2}} : \{a, y, z, w\}$

$e^{q_2} : \{\langle a,y\rangle, \langle y,z\rangle, \langle z,w\rangle, \langle w,w\rangle, \langle w,z\rangle, \langle z,y\rangle, \langle y,a\rangle\}$

QUERY ANSWERING

$I_{q_1()} \models I_{q_2()}$?

$\alpha(a) = ? \rightarrow \alpha(a) = a$
$\alpha(y) = ? \rightarrow \alpha(y) = y$
$\alpha(z) = ? \rightarrow \alpha(z) = a$
$\alpha(w) = ? \rightarrow \alpha(w) = y$

$I_{q_1}, \alpha() \models q_2()$ YES!

HOMOMORPHISM

$h(a) = \alpha(a) = a$
$h(y) = \alpha(y) = y$
$h(z) = \alpha(z) = a$
$h(w) = \alpha(w) = y$

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

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

$(z,w) \in e^{q_2()} \Rightarrow (h(z), h(w)) \in e^{q_1()}$

$(w,w) \in e^{q_2()} \Rightarrow (h(w), h(w)) \in e^{q_1()}$

$(w,z) \in e^{q_2()} \Rightarrow (h(w), h(z)) \in e^{q_1()}$

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

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