Exam 2019 – 07 – 12

Roberto Sorce

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

Alphabet:

C(x), P(x), S(x), BC(x), contract(x, y, z), agreement(x, y) , specializedIn(x, y), discount(x, y, z)

Axioms:

Forall x, y. Agreement(x, y) implies BC(x) and P(y) typing

Forall x. BC(x) implies C(x) ISA

Forall x. BC(x) implies Forall y, y'. Agreement(x, y) and Agreement (x, y') implies y=y' Multiplicity (EXPLICIT FORM)

Forall x. BC(x) implies 0 <= # {y | Agreement(x, y)} <= 1 Multiplicity (IMPLICIT SHORT FORM)

Forall x, y, z. discount(x, y, z) implies Agreement(x, y) and Integer(z) Typing

Forall x, y. Agreement(x, y) implies 1 <= # {z | discount(x, y, z)} <= 1 Multiplicity (IMPLICIT FORM)

Exists z. Discount(x, y, z) AND (Forall z, z'. Discount(x, y, z) AND Discount(x, y, z') implies z = z') Multiplicity (EXPLICIT FORM)

Forall x, y. SpecializedIn(x, y) implies P(x) and s(y) Typing

Forall x. P(x) implies 1 <= #{Y | SpecializedIn(x, y)} Multiplicity (IMPLICIT FORM)

Forall x, y, z. Contract(x, y, z) implies C(x) and P(y) and s(Z) Typing
ì
Forall x, y, z, z'. Contract(x, y, z) and Contract(x, y, z') implies z=z' Foreign key constraint

Exercise 2.

1. The above instantiation is incomplete. Customer must be modified, by adding also the BusinessCustomers in its table, because there is an ISA relation between BC and Customer. The new resulting table will be the following:

   Customer = {c1, c2, b1, b2}

2. **(a)** Return those providers that are specialized in at least two services.

   P(x) and Exists y, y'. specializedIn(x, y) and SpecializedIn(x, y') AND y != y'
   ~~Conjunctive Query: there are only AND conjunctions~~

OR
P(x) and Exists y. SpecializedIn(x, y) and Exists y’. SpecializedIn(x, y’) and y != y’

(b) Return those Business customers that have contracts only with providers with whom they have an agreement.

NB: ONLY means FORALL

BC(x) and Forall y.(Exists z. Contract(x, y, z) implies Agreement(x, y))

(c) Return those business customers that have contracts with all providers with whom they have an agreement.

BC(x) and Forall y. Agreement(x, y) implies Exists z. Contract(x, y, z)

(d) Check if there exists a customer with contracts for all services.

Exists x. C(x) and Forall y. S(z) implies Exists y. Contract(x, y, z)

NOTE: C(x), P(y), S(z)

Exercise 3. Model checking. Mu-Calculus

Model check the Mu-Calculus formula NuX.MuY.((a AND <next>X) OR ([next] NOT b AND <next>Y)) and the CTL formula EG(AFa AND (EFb OR AG NOT b)). Show the transition in Mu-calculus against the following transition system.

1. **Model check the formula $\nu X.\, \mu Y.((a \wedge \langle next \rangle X) \vee ([next] \neg b \wedge \langle next \rangle Y))$**

$$\Phi = \nu X. \mu Y. ((a \wedge \langle next \rangle X) \vee ([next] \neg b \wedge \langle next \rangle Y))$$

$[| X_0 |] = \{S1, S2, S3, S4\}$
$[| X_1 |] = [| \mu Y.((a \wedge \langle next \rangle X_0) \vee ([next] \neg b \wedge \langle next \rangle Y)) |]$

$[| y_0 |] = \{\}$
$[| Y_1 |] = [|(a \wedge \langle next \rangle X_0) \vee ([next] \neg b \wedge \langle next \rangle Y_0) |] =$

$= [|a|] \wedge PreE(next, [|X_0|]) \vee PreA(next, [|\neg b|]) \wedge PreE(next, [|Y_0|]) =$

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

$[| Y_2 |] = [|(a \wedge \langle next \rangle X_0) \vee ([next] \neg b \wedge \langle next \rangle Y_1) |] =$

$= [|a|] \wedge PreE(next, [|X_0|]) \vee PreA(next, [|\neg b|]) \wedge PreE(next, [|Y_1|]) =$

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

$[|\ Y_3\ |] = [|(a \land \langle next\rangle X_0) \lor ([next]\ \neg b \land \langle next\rangle Y_2)\ |] =$

$= [|a|] \land PreE(next, [|X_0|]) \lor PreA(next, [|\neg b|]) \land PreE(next, [|Y_2|]) =$

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

$\cancel{[|\ Y_4\ |] = [|(a \land \langle next\rangle X_0) \lor ([next]\ \neg b \land \langle next\rangle Y_3)\ |] =}$

$\cancel{= [|a|] \land PreE(next, [|X_0|]) \lor PreA(next, [|\neg b|]) \land PreE(next, [|Y_3|]) =}$

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

Found a LFP -> $[|y_2|] = [|y_3|] =$ {1, 2}

$[|\ X_1\ |] = [|y_3|] = [|y_4|] = \{1, 2\}$

$[|\ X_2\ |] = [|\ \mu Y.((a \land \langle next\rangle X_1) \lor ([next]\ \neg b \land \langle next\rangle Y))\ |]$

$[|\ y_{00}\ |] = \{\}$
$[|\ Y_{11}\ |] = [|(a \land \langle next\rangle X_1) \lor ([next]\ \neg b \land \langle next\rangle Y_{00})\ |] =$

$= [|a|] \land PreE(next, [|X_1|]) \lor PreA(next, [|\neg b|]) \land PreE(next, [|Y_{00}|]) =$

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

$[|\ Y_{22}\ |] = [|(a \land \langle next\rangle X_1) \lor ([next]\ \neg b \land \langle next\rangle Y_{11})\ |] =$

$= [|a|] \land PreE(next, [|X_1|]) \lor PreA(next, [|\neg b|]) \land PreE(next, [|Y_{11}|]) =$

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

Found a LFP -> $[|\ X_2\ |] = [|y_{11}|] = [|y_{22}|] = \{\ \}$

$[|\ X_3\ |] = [|\ \mu Y.((a \land \langle next\rangle X_2) \lor ([next]\ \neg b \land \langle next\rangle Y))\ |]$

$[|\ y_{00}\ |] = \{\}$
$[|\ Y_{11}\ |] = [|(a \land \langle next\rangle X_2) \lor ([next]\ \neg b \land \langle next\rangle Y_{00})\ |] =$

$= [|a|] \land PreE(next, [|X_2|]) \lor PreA(next, [|\neg b|]) \land PreE(next, [|Y_{00}|]) =$

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

$[|\ X_3\ |] = [|\ y_{00}\ |] = [|\ y_{11}\ |] = \{\ \}$
$[|\ X_2\ |] = [|\ X_3\ |] = [|\ y_{11}\ |] = \{\ \}$
Is Φ True in Transition system? ---> NO: Initial state of the transition system is contained in the extension of Φ?

S1 $\in [|\ \Phi\ |]$? NO

2. Decompose CTL Formula:

Use these operands: $\wedge \vee \cup \cap \neg$ $\boldsymbol{\mu}$ $\boldsymbol{\nu}$ $\boldsymbol{\alpha}$ $\boldsymbol{\beta}$ $\boldsymbol{\gamma}$ $\boldsymbol{\delta}$

α = AG NOT b = NuX. $\neg$b $\wedge$ [next] X
β = EFb OR alpha = MuX. b $\vee$ <next>X $\vee$ t(Alpha)
γ = AFa AND Beta = MuX. a $\vee$ [next]X $\wedge$ t(Beta)
δ = EG Gamma = NuX. [| t(Gamma) |] $\wedge$ <next> X

[|Alpha|] = [| AG NOT b |] = [| NuX. NOT b $\wedge$ [next]X |] =
[|X_0|] = {1, 2, 3, 4}
[|X_1|] = [| NOT b $\wedge$ [next]X_0 |] = [| NOT b |] $\cap$ PreA(next, [| X_0 |]) =
{1, 2, 3} $\cap$ {1, 2, 3, 4} = {1, 2, 3}

[|X_2|] = [| NOT b $\wedge$ [next]X_1 |] = [| NOT b |] $\cap$ PreA(next, [| X_1 |]) =
{1, 2, 3} $\cap$ {1, 2, 3} = {1, 2, 3}

[|X1|] = [|X2|] -> GFP = {1, 2, 3}

[|Beta|] = [| EFb $\vee$ alpha |] = [| MuX. b $\vee$<next>X |] U [| Alpha |] =
[|X_0|] = {}
[|X_1|] = [| b $\vee$<next>X_0 |] U [| Alpha |] = [| b |] U PreE(next, [| X_0 |]) U [| Alpha |] =
{4} U {} U {1, 2, 3} = {1, 2, 3, 4}

[|X_2|] = [| b $\vee$<next>X_1 |] U [| Alpha |] = [| b |] U PreE(next, [| X_1 |]) U [| Alpha |] =
{4} U {1, 2, 3, 4} U {1, 2, 3} = {1, 2, 3, 4}

~~**[|X_3|] = [| b $\vee$<next>X_2 |] U [| Alpha |] = [| b |] U PreE(next, [| X_2 |]) U [| Alpha |] =**~~
~~**{4} U {1, 2, 3, 4} U {1, 2} = {1, 2, 3, 4}**~~

[|X_1|] = [|X_2|] -> LFP = {1, 2, 3, 4}

[| Gamma |] = [| AFa AND Beta |] = [| MuX. a $\vee$[next]X |] $\cap$ [| Beta |] =
[|X_0|] = {}
[|X_1|] = [| a $\vee$[next]X_0 |] $\cap$ [| Beta |] = [| a |] U PreA(next, [| X_0 |]) $\cap$ [| Beta |] =
{2} U {} $\cap$ {1, 2, 3, 4} = {2}

[|X_2|] = [| a $\vee$[next]X_1 |] $\cap$ [| Beta |] = [| a |] U PreA(next, [| X_1 |]) $\cap$ [| Beta |] =
{2} U {} $\cap$ {1, 2, 3, 4} = {2}

~~**[|X_3|] = [| a $\vee$[next]X_2 |] $\cap$ [| Beta |] = [| a |] U PreA(next, [| X_2 |]) $\cap$ [| Beta |] =**~~
~~**{2} U {1} $\cap$ {1, 2, 3, 4} = {1, 2}**~~
[|X_1|] = [|X_2|] -> LFP = {2}

[| Delta|] = [| EG Gamma |] = [| NuX. gamma ∧ <next>X |] =

[|X_0|] = {1, 2, 3, 4}

[|X_1|] = [|gamma ∧ <next>X_0 |] = [| gamma |] ∩ PreE(next, [| X_0 |]) =
{2} ∩ {1, 2, 3, 4} = {2}

[|X_2|] = [|gamma ∧ <next>X_1 |] = [| gamma |] ∩ PreE(next, [| X_1 |]) =
{1, 2} ∩ {} = {}

[|X_3|] = [|gamma ∧ <next>X_2 |] = [| gamma |] ∩ PreE(next, [| X_2 |]) =
{1, 2} ∩ {3, 4} = {}

~~**[|X_4|] = [|gamma ∧ <next>X_3 |] = [| gamma |] ∩ PreE(next, [| X_3 |]) =**~~
~~**{1, 2} ∩ {} = {}**~~

[|X_2|] = [|X_2|] -> GFP = {}

Is Delta True in TS? TS ⊨ Delta?

1 ∈ [| Delta |] ? NO Initial state of TS is not present in the extension of Delta. The formula is false in this transition system.

Exercise 4. Check wether the Hoare triple below is correct, by using (x >= 0 && y >= 0 && x+y = 23) as an invariant:

{ x=23 && y=0} while (x>0) do (x=x-1; y= y+1) {y = 23}

PRE(P) g Delta(S) POST(Q)

Check the candidate invariant (x >= 0 && y >= 0 && x+y = 23):
Check if the three condition hold to prove that the Hoare triple holds

1. P => I
2. {g AND I} Delta {I}
3. I AND not g => Q

Solve:

1. P=>I

   P: X=23 && Y=0: I: (x >= 0 && y >= 0 && x+y = 23)
   SATISFIED

2. {g AND I} Delta {I}

   Check the WP(Delta, I) => WP (x=x-1 AND y= y+1 AND x+y=23)

   Delta: { x=x-1 && y= y+1 }

   I: (x >= 0 && y >= 0 && x+y = 23)

I AND g => WP?

(x >= 0 && y >= 0 && x+y = 23) AND (x>0) => (x=x-1 AND y= y+1 AND x+y=23)
NOT SATISFIED: I is NOT an Invariant and the Hoare triple do not hold with this invariant

3. Check if the invariant exits the loop:

   I AND Not g => Q

   (x >= 0 && y >= 0 && x+y = 23) && (X<=0) => {y=23}
   SATISFIED