Formal Methods – January 25, 2017

Roberto Sorce

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

Alphabet: GameLevel(x), Map(x), SpecialMap(x), Character(x), Includes(x, y), Points(x, y, z), Appears(x, y), MainCharacter(x, y)

Axioms:

Forall x, y. Includes(x, y) implies GameLevel(x) and Map(y) Typing

Forall x, y, z Points(x, y, z) implies Includes(x, y) and Integer(z)

Forall x, y. Includes(x, y) implies 1 <= #{z|Points(x, y, z)} <= 1

Forall x, y. Includes(x, y) implies Exists z. Points(x, y, z) and (Forall z, z'. Points(x, y, z) and Points(x, y, z') implies z=z')

Forall x. GameLevel(x) implies 3 <= #{ y|Includes(x, y)}

Forall x. GameLevel(x) implies (Forall x, y, y', y''. Includes(x, y) and Includes(x, y') and Includes(x, y'') implies y!= y' and y' != y'')

Forall x. SpecialMap(x) implies Map(x)

Forall x, y. appears(x, y) implies Map(x) and Character(y)

Forall x. MainCharacter(x, y) implies SpecialMap(x) and Character(y)

Forall x, y. MainCharacter(x, y) implies Appears(x, y)

Forall x. Map(x) implies #{y|Appears(x, y) } <= 9

Forall x. SpecialMap(x) implies 1 <= #{y|MainCharacter(x, y)}<= 1

Exercise 2.

1. Check whether the above instantiation, once completed, is correct, and explain why it is or it is not.

The instantiation is not complete, to be completed, it is required to apply a chase procedure for ISA and Subset relations and constraints. All the instances of SpecialMap must be included in Map table because there is an ISA relation between them, while all the instances of mainCharachter must be included in Appears table. The correct and complete instantiation is the following:

Express in FOL and evaluate the following queries:

(a) Return the maps with at least 3 distinct characters.

Map(x) and Exists y. Appears(x, y) and Exists. Y'. appears(x, y') and Exists y''. Appears(x y'') and y != y' and y' != y''

(b) Return the characters that appear in maps only as main characters.

Character(x) and forall x, y. Appears(x, y) implies MainCharacter(x, y)

(c) Check if there exists a map where all characters appears.

Exists x. Map(x) and forall y. Character(y) implies Appears(x, y)

Exercise 3. Model check the Mu-Calculus formula νX.μY.((a ∧ ⟨next⟩X) ∨ [next]Y) and the CTL formula EF(¬a ⊃ EXAGb) (showing its translation in Mu-Calculus) against the following transition system:

Φ = νX.μY.((a ∧ ⟨next⟩X) ∨ [next]Y)

$[|X_0|] = \{1, 2, 3, 4, 5\}$
$[|X_1|]$ = [| μY.((a ∧ ⟨next⟩X) ∨ [next]Y) |]
$[|Y_{00}|] = \{\}$

$[|Y_{01}|]$ = [| (a ∧ ⟨next⟩X_0) ∨ [next]Y_{00}) |] = [| a |] inter PreE(next, X_0) U PreA(next, Y_{00}) =

{2, 4, 5} INTER {1, 2, 3, 4, 5} U {} = {2, 4, 5}

$[|Y_{02}|]$ = [| (a ∧ ⟨next⟩X_0) ∨ [next]Y_{01}) |] = [| a |] inter PreE(next, X_0) U PreA(next, Y_{01}) =

{2, 4, 5} INTER {1, 2, 3, 4, 5} U {3, 5} = {2, 3, 4, 5}

$[|Y_{03}|]$ = [| (a ∧ ⟨next⟩X_0) ∨ [next]Y_{02}) |] = [| a |] inter PreE(next, X_0) U PreA(next, Y_{02}) =

{2, 4, 5} INTER {1, 2, 3, 4, 5} U {1, 3, 4, 5} = {1, 2, 3, 4, 5}

$[|Y_{04}|]$ = [| (a ∧ ⟨next⟩X_0) ∨ [next]Y_{03}) |] = [| a |] inter PreE(next, X_0) U PreA(next, Y_{03}) =

{2, 4, 5} INTER {1, 2, 3, 4, 5} U {1, 3, 4, 5} = {1, 2, 3, 4, 5}

$[|Y_{04}|] = [|Y_{03}|]$ -> Found a LFP = {1, 2, 3, 4, 5}

$[|X_1|] = [|X_0|]$ -> Found a GFP = {1, 2, 3, 4, 5}

1 in Phi?
1 in $[|X_1|]$? Yes, initial state of TS is included in the extension of X_1, hence Phi is valid in TS

TS models Phi

Decomposing CTL formula EF(¬a ⊃ EX AGb)

Alpha = AGb
Beta = EX Alpha
Gamma = ¬a ⊃ Beta
Delta = EF(Gamma)

T(Alpha) = νX. b AND [Next]X
T(Beta) = <Next> T(alpha)
T(Gamma) = a OR T(Beta))
T(Delta) = μX. T(Gamma) OR <Next>X

[|Alpha|] = [| νX. b AND [Next]X |]
[|X_0|] = {1, 2, 3, 4, 5}
[|X_1|] = [| b AND [Next]X_0 |] = [| b |] inter PreA(next, [|X_0|]) =
= {3, 4} inter {1, 2, 3, 4, 5} = {3, 4}
[|X_2|] = [| b AND [Next]X_1 |] = [| b |] inter PreA(next, [|X_1|]) =
= {3, 4} inter {3, 4} = {3, 4}
[|X_2|] = [|X_1|] -> Found GFP = {3, 4}

[| Beta |] = [| <Next> Alpha|] = PreE(next, [|Alpha|]) = {1, 2, 3, 4}
[|Gamma|] = [|a|] OR [|Beta|] = {2, 4} U {1, 2, 3, 4} = {1, 2, 3, 4}
[|Delta|] = [| μX. T(Gamma) OR <Next>X |] =
[|X_0|] = { }
[|X_1|] = [|Gamma |] OR PreE(next, X_0) = {1, 2, 3, 4} U { } = {1, 2, 3, 4}
[|X_2|] = [|Gamma |] OR PreE(next, X_1) = {1, 2, 3, 4} U { 1, 2, 3, 4 } = {1, 2, 3, 4}
[|X_2|] = [|X_1|] -> LFP = {1, 2, 3, 4}

1 in [|Delta|]? Yes, initial state of TS is contained in the extension of Delta.

TS models [|Delta|]

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}

{P} g Delta (S) {Q}

1. **P => I, Setting up I**
   {i=0 AND j=9} => (i + j = 9) -> SATISFIED

2. **{I AND g} S {I}**

   I AND G => WP(delta, I): Abstraction characterization, P is stronger than the weakest Precondition
   Compute the WP(S, I):

   (i+1 + j-1 = 9)

   Delta: (i:= i+1; j=j-1)

   I: (i + j = 9)

   (i + j = 9) AND (I <10) => (i+1 + j-1 = 9) SATISFIED

3.{I} AND {Not g} => {Q} , Exit condition

(i + j = 9) AND {i >= 10} => j < 0 SATISFIED

All the properties are satisfied, hence the Hoare triple holds.

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.

We want to check if q1(x) subseteq q2(x), in order to check the containment, we must transform the containment into an evaluation, "Freezing the free variables", substituting the free variables with fresh constants with the same value to obtain Boolean conjunctive queries:

Forall I, c models Iq1 => q2(c)

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

Building the canonical DB of Iq1:

$Iq1 = \{Delta^{Iq1}, E, C\}$
E = {(c, y),(y, y),(c, z),(y, z),(z, y)}
C = c

Tabula form DBIq1
{(c, y),
(y, y),
(c, z),
(y, z),
(z, y)}

Check whether q2 is True in Iq1: Guess an assignment function alpha for all the fixed variables of q2.

Alpha(y) = y
Alpha(z) = y
Alpha(v) = z

This is a satisfying assignment.

Alpha(y, z) = (y, y) in EIq1
Alpha(v, z) = (z, y) in EIq1
Alpha(v, y) = (z, y) in EIq1

Check homomorphism:
Check if the two following properties are satisfied:

X, y in DeltaIq2

$$H(c^I) = H(c^J)$$

$$(h(x), h(y)) \text{ in } C^J$$

From CM theorem: Iq1 models q2(c) iff Exists h. Iq2 -> Iq1

Building the canonical Interpretation of q2
Iq2 = {DeltaIq2, E, c}
E = {(c,y), (y,z), (c,v), (v,z), (v,y)}

C = c

H(c) = C
H(y) = Alpha(y) = (y)
H(z) = Alpha(z) = (y)
H(v) = Alpha(v) = (z)

(c, y) in EIq2 -> (h(c), h(y)) = (c, y) in EIq1
(y, z) in EIq2 -> (h(y), h(z)) = (y, y) in EIq1
(c, v) in EIq2 -> (h(c), h(v)) = (c, z) in EIq1
(v, z) in EIq2 -> (h(v), h(z)) = (z, y) in EIq1
(v, y) in EIq2 -> (h(v), h(y)) = (z, y) in EIq1