SAPIENZA Universita` di Roma – MSc. in Engineering in Computer Science Formal Methods – Feb. 13, 2017
Roberto Sorce
(Time to complete the test: 2 hours)

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

Alphabet: Student(x), Course(x), Class(x), Lab(x), Takes(x, y), Credit(x, y), Mark(x, y, z)

Axioms:

Forall x, y. Takes(x, y) implies Student(x) and Course(y)
Forall x, y. Credit(x, y) implies Student(x) and Class(y)
Forall x, y. Credit(x, y) implies Takes(x, y)
Forall x, y, z. Mark(x, y, z) implies Credit(x, y) and Integer(z)

Forall x. Class(x) implies Course(x) ISA GENERALIZATION
Forall x. Lab(x) implies Course(x) ISA GENERALIZATION
Forall x. Class(x) implies Not Lab(x) DISJOINTNESS
Forall x. Course(x) implies Class(x) OR Lab(x) COMPLETENESS

Forall x. Student(x) implies 1 <= #{y|Takes(x, y)} <= 30
Forall x. Student(x) implies 1 <= #{y|Credit(x, y)} <= 30
Forall x, y. Credit(x, y) implies Exists z. Mark(x, y, z) and (Forall z, z'. Mark(x, y, z) and Mark(x, y, z') implies z=z')

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

1. **Check whether the instantiation (once completed) is correct (and explain why it is or it is not).**

   The above instantiation is not complete, in order to complete the instantiation, we must apply a chase procedure for ISA relations and subset constraints. To complete the instantiation there must be a Class table that includes all the elements of Class and Lab, because there is an ISA relation between these classes. Also, all the instances of Credit table must be included in the Takes relation, because there is a subset constraint. The complete instantiation is the following:

2. Express in FOL and evaluate the following queries:

(a) Return students that have taken at least 3 courses.

Student(x) and Exists y, y', y''. Takes(x, y) and Takes(x, y') and Takes(x, y'') and y!= y' and y'!= y''

{jane, mary}

(b) Return students that have taken only classes.

Student(x) and Forall y. takes(x, y) implies Class(y)

{Mary}

(c) Check if there exists a student that has taken all labs.

Exists x. Student(x) and Forall y. Lab(y) implies Takes(x, y)

{jane}

(d) Check if there is a student that has taken all classes, but not for credit.

Exists x. Student(x) and Forall y. Class(y) implies Takes(x, y) and Not Credit(x, y)

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 $\wedge$ EXAG b)) (showing its translation in Mu-Calculus) against the following transition system:

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

$[|X_0|] = \{1, 2, 3, 4, 5\}$

$[|X_1|] = [|\ \mu Y.((a \wedge [next]X) \vee [next]Y)\ |]$

$[|Y00|] = \{\ \}$

$[|Y01|] = [|\ (a \wedge [next]X) \vee [next]Y00\ |] =$

= [|a|] inter PreA(next, X0) U PreA(next, Y00) =

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

[|Y02|] = [| (a ∧ [next]X) ∨ [next]Y01 |] =

= [|a|] inter PreA(next, X0) U PreA(next, Y01) =

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

[|Y02|] = [|Y01|] = {2, 4, 5}

[|X_2|] = [| μY.((a ∧ [next]X1) ∨ [next]Y) |]

[|Y10|] = { }

[|Y11|] = [| (a ∧ [next]X1) ∨ [next]Y10 |] =

= [|a|] inter PreA(next, X1) U PreA(next, Y10) =

= {2, 4, 5} inter {4} U {} = {4}

[|Y12|] = [| (a ∧ [next]X1) ∨ [next]Y01 |] =

= [|a|] inter PreA(next, X1) U PreA(next, Y11) =

= {2, 4, 5} inter {4} U {4} = {4}

[|Y12|] = [|Y11|] = {4}

[|X_3|] = [| μY.((a ∧ [next]X2) ∨ [next]Y) |]

[|Y20|] = { }

[|Y21|] = [| (a ∧ [next]X2) ∨ [next]Y20 |] =

= [|a|] inter PreA(next, X2) U PreA(next, Y20) =

= {2, 4, 5} inter {4} U {} = {4}

[|Y22|] = [| (a ∧ [next]X2) ∨ [next]Y21 |] =

= [|a|] inter PreA(next, X2) U PreA(next, Y20) =

= {2, 4, 5} inter {4} U {4} = {4}

[|Y22|] = [|Y21|] - > LFP {4}

[|X3|] = [|X2|] -> GFP {4}

1 in [|Phi|]? No, initial state of TS is not contained in the extension of Phi. Phi is not true in TS, TS does not model PHI.

CTL formula EF (¬a ⊃ (EX a ∧ EX AG b))

Alpha = AG b
Beta = EX alpha
Gamma = EX a
Delta = Gamma and Beta
Epsilon = ¬a ⊃ (Gamma)
Zeta = EF (Delta)

T(alpha) = NuX. b And [Next]X
T(Beta) = <Next>alpha
T(Gamma) = <Next> a
T(Delta) = T(Gamma) and T(Beta)
T(Epsilon) = a OR Gamma
T(Zeta) = MuX. Epsilon OR <Next>X

[|ALPHA|] = [| NuX. 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, 5} Inter {1, 2, 3, 4, 5} = {3, 4, 5}
[|x_2|] = [| b And [Next]X_1 |] = [| b |] Inter PreA(next, X_1) =
= {3, 4, 5} Inter {3, 4, 5} = {3, 4, 5}

[|x_2|] = [|x_1|] = {3, 4, 5}

[|Beta|] = [|<Next>alpha |] = PreE(next, [|Alpha|]) = {1, 2, 3, 4, 5}

[|Gamma|] = [| <Next> a |] = PreE(next, [|a|]) = {1, 2, 3, 4, 5}

[|Delta|] = [|Beta|] inter [|Gamma|] = {1, 2, 3, 4, 5}

[| Epsilon |] = [|a OR Gamma|] = {2, 4, 5} U {1, 2, 3, 4, 5} = {1, 2, 3, 4, 5}

[|Zeta|] = [|MuX. Epsilon OR <Next>X|]=

[| X_0 |] = {}

[| X_1 |] = [|Epsilon OR <Next>X |] = [|Epsilon|] U PreE(next, X_0) =

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

[| X_2 |] = [|Epsilon OR <Next>X1 |] = [|Epsilon|] U PreE(next, X_1) =

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

[| X_2 |] = [| X_1 |] = {1, 2, 3, 4, 5}

1 in [| X_2 |]? Yes, the formula is True in TS, initial state S1 IS CONTAINED IN [| X_2 |].

TS MODELS [| X_2 |]

Exercise 4. Consider the following two transition systems:

DEFINITION OF BISIMILARITY:

R0= {(t1, q1), (t1, q2), (t1, q3), (t1, q4), (t1, q5), (t2, q1), (t2, q2), (t2, q3), (t2, q4), (t2, q5)}

R1 = {(t1, q1), (t1, q4), (t1, q5), (t2, q2), (t2, q3)}
R2 = {(t1, q1), (t2, q2), (t2, q3)}
R3 = {(t1, q1), (t2, q2)}
R4 = {(t2, q2)}
R5 = {}
R6 = {}

R6 = R5 -> GFP = {} No states are bisimilar, in particular S And T are not Bisimilar

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.

Check if q1(x) subseteq q2(x), how? Checking the Evaluation.

Recognition problem:

Forall I, alpha models Forall x. q1(x) implies q2(x) VALID

Where I is the interpretation, and alpha is the assignment function.

In order to evaluate, we must freeze the free variables to obtain boolean conjunctive queries. Introducing fresh constants.

From CM theorem, we are *Reducing* the query containment into a query evaluation.

q1(c) subseteq q2(c) iff Iq1(c) models q2(c)

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

Building the DB of the canonical Interpretation of q1(c), Iq1(c)

Iq1(c) = {Delta, e, C}
Delta = {c, y, z}
E = {(c,y), (y,z), (z,c)}
C = c

DB Iq1(c) = { (c,y),
(y,z),
(z,c) }
Check if Iq1(c) models q2(c). Guess an assignment function alpha for q2(c) s.t. is true in Iq1(c).

Alpha(y) = y
Alpha(w) = y
Alpha(z) = z
Alpha(v) = c

This is a Satisfying assignment.

From CM theorem, Homorphism:

Iq1(c) models q2(c) iff Exists h. Iq2(c) $\rightarrow_h$ Iq1(c)

To check homomorphism: building Iq2(c)
Iq2(c) = {Delta, e, C}
Delta = {c, y, w, z, v}
E = {(c,y), (c,w), (y,z), (z,c), (z,v), (v,y), (v,w), (w,z)}
C = c

DB Iq2(c) = {(c,y),
(c,w),
(y,z),
(z,c),
(z,v),
(v,y),
(v,w),
(w,z) }

To check the homomorphism, we have to map all the elements of Iq2(c) in Iq1(c)

H(c) = c
H(y) = alpha(y) =y
H(w) = alpha(w) = y
H(v) = alpha(v) = c
H(z) = alpha(z) = z

Check if the homomorphism is true. Check if the relation is maintained by the mapping.

(c,y) in Iq2(c) -> (h(c), h(y)) = (c, y) in Iq1(c)
(c,w) in Iq2(c) -> (h(c), h(w)) = (c, y) in Iq1(c)
(y,z) in Iq2(c) -> (h(y), h(z)) = (y, z) in Iq1(c),
(z,c) in Iq2(c) -> (h(c), h(y)) = (z, c) in Iq1(c),
(z,v) in Iq2(c) -> (h(c), h(y)) = (z, c) in Iq1(c),
(v,y) in Iq2(c) -> (h(c), h(y)) = (c, y) in Iq1(c),
(v,w) in Iq2(c) -> (h(c), h(y)) = (c, y) in Iq1(c),
(w,z) in Iq2(c) -> (h(c), h(y)) = (y, z) in Iq1(c)