SAPIENZA Universita` di Roma – MSc. in Engineering in Computer Science Formal Methods - Final Test B – December 21, 2017

Roberto Sorce

(Time to complete the test: 2 hours)

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

Alphabet: Customer(x), Provider(y), Service(z), BusinessCustomer(x), Contract(x, y, z), Cost(x, y, z, w), Provides(X, y)

Axioms:

Forall x. BusinessCustomer(x) implies Customer(x) ISA

Forall x, y, z. Contract(X, Y, Z) implies Customer(x) and Provider(y) and Service(z) TYPING

Forall x, y, z, w Cost(x, y, z, w) implies Contract(X, Y, Z) and Real(w) TYPING

Forall x, y, z Contract(x, y, z) implies 1 <= #{w|cost(x, y, z, w)} <= 1 MULTIPLICITY (EXPLICIT)

Exists w. Cost(x, y, z, w) and (Forall w, w'. Cost(x, y, z, w) And Cost(x, y, z, w') implies w=w') MULTIPLICITY (IMPLICIT)

Forall x, y, Y' z. Contract(X, Y, Z) AND Contract(x, y' z) implies y=y' KEY

Forall x, y. Provides(x, y) implies Provider(x) and Service(y)

Forall x. Provider(x) implies 1 <= #{y | provides(x, y)} <= 10 MULTIPLICITY (EXPLICIT)

Forall x. Service(x) implies 1 <= #{y | provides(y, x)} MULTIPLICITY (EXPLICIT)

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

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:**

   The above instantiation is not correct: In order to adjust the instantiation, all the instances of Business Customers must be also in Customer's table. Another error is reported in contracts/cost table, in which S1 is provided by Provider 2, but providers tables does not show this relation.
   The resulting tables corrected are the followings:

   Customer:= {c1, c2, c3, c4, b1, b2, b3}

Provides := {(p1, s1), (p1, s2), (p1, s3), (p2, s1), (p2, s1)}

2.

(a) Check that, for every provider x and service y involved in a contract, provider x does provide service y.

Forall x, y. (Exists z. Contract(x, y, z) implies Provides(x, y))

(b) Return those customers that have contracts only for services provided by p2.

~~C(x) and Forall x, y. Provides(x, y) implies x=p2 and Exists z.Contract(x, y, z)~~

Customer(x) and Forall z.(Exists y. contract(x, y, z)) implies Provides(p2, z)

(c) Return those customers that have a contract for with all providers.

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

Customer(x) and Forall y. P(y) implies Exists z. Contract(x, y, z)

Cus

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

$\Phi = \nu X.\mu Y.((b \land [next]X) \lor (a \land \langle next\rangle Y)) =$

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

$[|X_1|] = \mu Y.((b \land [next]X_0) \lor (a \land \langle next\rangle Y)) = \{3\}$

$[|Y_0|] = \{\}$

$[|Y_1|] = (b \land [next]X_0) \lor (a \land \langle next\rangle Y_0) =$

$= [|b|]$ inter $PreA(next, X_0)$ U $[|a|]$ inter $PreE(next, Y_0) =$

$= \{3, 4\}$ inter $\{1, 3\}$ U $\{1, 2\}$ inter $\{\} = \{3\}$

$[|Y_2|] = (b \land [next]X_0) \lor (a \land \langle next\rangle Y_1) =$

$= [|b|]$ inter $PreA(next, X_0)$ U $[|a|]$ inter $PreE(next, Y_1) =$

= {3, 4} inter {1, 3} U {1, 2} inter {0} = {3}

$[|Y_1|] = [|Y_2|] = \{3\}$

$[|X_2|] = \mu Y.((b \wedge [next]X_1) \vee (a \wedge \langle next \rangle Y)) = \{\ \}$

$[|Y_{00}|] = \{\}$

$[|Y_{01}|] = (b \wedge [next]X_1) \vee (a \wedge \langle next \rangle Y_{00}) =$

$= [|b|]$ inter $PreA(next, X_1)$ U $[|a|]$ inter $PreE(next, Y_{00}) =$

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

$[|Y_{02}|] = (b \wedge [next]X_1) \vee (a \wedge \langle next \rangle Y_{01}) =$

$= [|b|]$ inter $PreA(next, X_1)$ U $[|a|]$ inter $PreE(next, Y_{01}) =$

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

$[|Y_{01}|] = [|Y_{02}|] = \{\}$

$[|X_3|] = \mu Y.((b \wedge [next]X_2) \vee (a \wedge \langle next \rangle Y)) = \{\ \}$

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

$[|Y_{11}|] = (b \wedge [next]X_2) \vee (a \wedge \langle next \rangle Y_{10}) =$

$= [|b|]$ inter $PreA(next, X_2)$ U $[|a|]$ inter $PreE(next, Y_{10}) =$

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

$[|Y_{12}|] = (b \wedge [next]X_2) \vee (a \wedge \langle next \rangle Y_{11}) =$

$= [|b|]$ inter $PreA(next, X_2)$ U $[|a|]$ inter $PreE(next, Y_{11}) =$

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

$[|Y_{11}|] = [|Y_{12}|] = \{\}$

$[|X_2|] = [|X_3|] = \{\}$

1 in $[|X_3|]$? No, Initial state of transition system is not present in the extension of X_3

Decompose CTL formula $EF(AG(a \supset EXAX\neg a))$

Alpha = AX ¬a
Beta = EX ALPHA
Gamma = a ⊃ BETA
Delta = AG(Gamma)
Theta = EF(Delta)

T(alpha) = [Next] ¬a = PreA(next,[| ¬a |])
T(Beta) = <Next> T(alpha) = PreE(next, [| T(alpha)|])
T(Gamma) = a ⊃ T(BETA) = a U [| Beta |]
T(Delta) = νX. T(Gamma) ∧ [Next] X = [| T(Gamma) |] inter PreA(next, [|X|])

T(Theta) = μX. T(Delta) ∨ <Next> X = [| T(Delta) |] U PreE(next, [|X|])

T(CTL FORMULA) = μX.νX. a ⊃ <Next> [Next] ¬a ∧ [Next] X ∨ <Next> X

[|Alpha|] = [| AX ¬a |] = [| [Next] ¬a |] = PreA(next, [| ¬a |]) = {3}

[|Beta|] = [| EX ALPHA |] = [| <Next> alpha |] = PreE(next, [| alpha |]) = {0}

[|Gamma|] = [| a ⊃ BETA |] = [|a|] U [|Beta|] = {1, 2} U {0} = {0, 1, 2}

[|Delta|] = [|AG (Gamma)|] = [| νX. Gamma ∧ [Next] X |] = { }
- **[|X_0|] = {0, 1, 2, 3, 4}**
- **[|X_1|] = [| Gamma |] inter PreA(next, X_0) = {0, 1, 2} inter {1, 3} = {1}**
- **[|X_2|] = [| Gamma |] inter PreA(next, X_1) = {0, 1, 2} inter {} = {}**
- **[|X_3|] = [| Gamma |] inter PreA(next, X_2) = {0, 1, 2} inter {} = {}**

[|Theta|] = [| EF(Delta) |] = [| μX. Delta ∨ <Next> X |] = { }
- **[|X_0|] = { }**
- **[|X_1|] = [|Delta|] U PreE(next, X_0) = {} U {} ={}**
- **[|X_2|] = [|Delta|] U PreE(next, X_1) = {} U {} ={}**

1 in [|Theta|]? No, Initial state is not in the extension of Theta.

Exercise 4.
Check whether the Hoare triple below is correct, by using (x ≥ 0 ∧ y ≥ 0 ∧ x + y = 31) as invariant:
{x = 31∧y = 0} 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:
(∃x.P (x) ∨ ∃x.Q(x)) ≡ ∃x.(P (x) ∨ Q(x))

UNSAT => VALID

Exercise 6.

Check Nonemptiness
Starting from initial state, check if there exists a path that infinitely arrives in a final state.

Eventually always final

νX.μY ((final and <next>X) OR (<next>Y))

[|X_0|] = { (init,i), (0, i), (3, ii), (4, ii)}

[|X_1|] = [|μY ((final and <next>X) OR (<next>Y))|]

[|Y_{00}|] = { }

[|Y_{01}|] = [| ((final and <next>X_0) OR (<next>Y_{00})) |] =

= [|final |] inter PreE(next, [|X_0|]) U PreE(next, [|Y_{00}|]) =

= { (3, ii), (4, ii) } inter { (init,i), (0, i), (3, ii), (4, ii)} U { } = { (3, ii), (4, ii) }

[|Y_{02}|] = [| ((final and <next>X_0) OR (<next>Y_{01})) |] =

= [|final |] inter PreE(next, [|X_0|]) U PreE(next, [|Y_{01}|]) =

= { (3, ii), (4, ii) } inter { (init,i), (0, i), (3, ii), (4, ii)} U

{ (0, i), (3, ii), (4, ii) } = { (0, i), (3, ii), (4, ii) }

[|Y_{03}|] = [| ((final and <next>X_0) OR (<next>Y_{02})) |] =

= [|final |] inter PreE(next, [|X_0|]) U PreE(next, [|Y_{02}|]) =

= { (3, ii), (4, ii) } inter { (init,i), (0, i), (3, ii), (4, ii)} U

{ (init,i), (0, i), (3, ii), (4, ii) } = { (init,i), (0, i), (3, ii), (4, ii) }

[|Y_{04}|] = [|Y_{03}|] -> LFP

I can't develop any further, because all the states of the domain have been reached in the extension of Y_{03}, hence [|Y_{04}|] = [|Y_{03}|] -> I found a LFP.

[|X_1|] = [|X_0|] -> GFP

I can't develop any further, because all the states of the domain have been reached in the extension of Y_{03}, hence [|X_1|] = [|X_1|] -> I found a GFP.

(Init, i) in [|X_1|]? YES, initial state of automaton is contained in the extension of X1.

Ts models phi(LTL)?

Ts models Not phi(LTL), hence Ts not models phi(LTL)