SAPIENZA Universita` di Roma – MSc. in Engineering in Computer Science Formal Methods - Final Test A – 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), BusinessCustomer(x), Provider(x), Service(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. Provides(x, y) implies Provider(x) and Service(y) TYPING

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)

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 FORM)

Forall x, y, y' z. Contract(x, y, z) and Contract(x, y', z) implies y=y'

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.

The above instantiation is not correct. The instantiation does not take into account business customers as customers. To complete the instantiation we must add all the instances of BC also into the Customer's Table:

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

Another error is in the contracts/cost table, in which the service1 is provided by Provider1, but is not referenced anywhere in other tables. We must insert in the providers table also {(p2, s1)}.

2.Express in FOL the following queries and evaluate them over the completed instantiation:

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

(b) Return those customers that have contracts only for services provided by p1.

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

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

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

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

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

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

$[|Y_1|] = [|\ (a \wedge [next]X_0) \vee (b \wedge \langle next\rangle Y_0)\ |] = \{1\}$

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

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

$[|Y_2|] = [| (a \wedge [next]X_1) \vee (b \wedge \langle next\rangle Y_1) |] = \{1\}$

$[|a|]$ inter preA(next, $[|X_1|]$) U $[|b|]$ inter PreE(next, $[|Y_1|]$) =

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

Found a LFP -> {1}

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

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

$[|Y_{11}|] = [| (a \wedge [next]X_1) \vee (b \wedge \langle next\rangle Y_{10}) |] =$

$[|a|]$ inter preA(next, $[|X_1|]$) U $[|b|]$ inter PreE(next, $[|Y_{10}|]$) =

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

Found a LFP -> { }

$[|X_3|] = [|\mu Y.((a \wedge [next]X_1) \vee (b \wedge \langle next\rangle Y))|] =$

$[|Y_{20}|] = \{ \}$

$[|Y_{21}|] = [| (a \wedge [next]X_2) \vee (b \wedge \langle next\rangle Y_{20}) |] =$

$[|a|]$ inter preA(next, $[|X_2|]$) U $[|b|]$ inter PreE(next, $[|Y_{20}|]$) =

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

Found a LFP -> { }
Found a GFP -> { } -> $[|X_2|] = [|X_3|]$

Is 1 in $[|X_3|]$? NO, initial state of ts is not in the extension of $[|\Phi|]$
$[|\Phi\ |] = \{ \}$
The formula is FALSE in the Transition System.

Decomposition of CTL formula AF(EG(a ⊃ AX EX¬a)):

Alpha = EX ¬a
Beta = AX alpha
Gamma = a ⊃ Beta
Delta = EG(Gamma)
Theta = AF(Delta)

Translation of CTL formula in Mu-Calculus:

T(alpha) = <Next> ¬a
T(Beta) = [Next]Alpha
T(Gamma) = ¬a ∨ Beta
T(Delta) = νX. Gamma ∧ <next>X
T(Theta) = μX. Delta ∨ [next]X

[|Alpha|] = [| <Next> ¬a |] = PreE(next, [| ¬a |]) = {0, 2, 3, 4}
[|Beta|] = [| [Next]Alpha |] = PreA(next, [|Alpha|]) = {1, 3}
[|Gamma|] = [|¬a ∨ Beta|] = [| ¬a |] U [|Beta|] = {0, 3, 4} U {1, 3} = {0, 1, 3, 4}
[|Delta|] = [|νX. Gamma ∧ <next>X|] =

[|X_0|] = {0 ,1, 2, 3, 4}
[|X_1|] = [| Gamma ∧ <next>X_0 |] = [|Gamma|] inter PreE(next, [|X_0|]) =
{0, 1, 3, 4} inter {0, 1, 2, 3, 4} = {0, 1, 3, 4}

[|X_2|] = [| Gamma ∧ <next>X_1 |] = [|Gamma|] inter PreE(next, [|X_1|]) =
{0, 1, 3, 4} inter {0, 1, 2, 3, 4} = {0, 1, 3, 4}

Found a GFP -> [|X_1|] = [|X_2|] = {0, 1, 3, 4}

[|Theta|] = [| μX. Delta ∨ [next]X |] = {0, 1, 3, 4}

[|X_0|] = { }
[|X_1|] = [|Delta ∨ [next]X_o |] = [|Delta|] U PreA(next, [|X_0|]) =
{0, 1, 3, 4} U {} = {0, 1, 3, 4}

[|X_2|] = [|Delta ∨ [next]X_1 |] = [|Delta|] U PreA(next, [|X_1|]) =
{0, 1, 3, 4} U {3} = {0, 1, 3, 4}

Found a GFP -> [|X_1|] = [|X_2|] = {0, 1, 3, 4}

1 in [|Theta|]? Yes, Initial state of transition system is in the extension of theta, hence the formula is valid in this transition system.