Formal Methods – January 18, 2018
Roberto Sorce
Exercise 1. Express the following UML class diagram in FOL:

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

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 (IMPLICIT)

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

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 (IMPLICIT FORM)

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 (EXPLICIT FORM)

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

Exercise 2.

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

   The above instantiation is not complete, in order to be completed, let's apply a chase procedure for ISAs and subset constraints, to obtain a complete instantiation **I**. All the instances of **BusinessCustomer** must be also in the **Customer**'s table.
   The new resulting completed instantiation with the correct Customer table is the following:

   Customer := {c1, c 2, c3, c3, b1, b2, b3}

   Also, the **contracts/costs** table reports that service **S1** is provided by provider **P2**, but it is not defined in Provides table.

   ~~A possible solution is to add in **Provides** table the service **S1** provided by **P2**~~

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

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

(a) Check whether there is a customer with contract with two providers for the same service.

   Exists x. C(x) and Forall y, y', z, z'. contract(x, y, z) and contract(x, y', z') implies z=z'

(b) Return those customers that have contracts only for one service.

   C(x) and Exists y, z, z'. contract(x, y, z) and Contract(x, y, z') and z=z'

(c) Return those customers that have a contracts with the same provider for all their services.

   C(x) and forall z. S(z) implies Exists y, y'. contract(x, y, z) and contract(x, y', z) and y=y'

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

1.

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

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

$[|X_1|] = \mu Y.((a \wedge [next]X) \vee (b \wedge [next]Y)) = \{1\}$

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

$[|Y_1|] = [| (a \wedge [next]X_0) \vee (b \wedge [next]Y_0) |] =$

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

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

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

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

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

Found a fixpoint -> $[|Y_1|] = [|Y_2|] = \{1\}$

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

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

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

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

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

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

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

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

Found a LFP -> $[|Y_{01}|] = [|Y_{02}|] = \{\}$

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

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

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

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

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

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

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

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

Found a LFP -> $[|Y_{11}|] = [|Y_{12}|] = \{\}$

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

Is Initial state of the Transition system in [|X3|]? NO

2.

CTL formula AF(EG(a ⊃ EX AXb))

ALPHA = AX b

BETA = EX alpha

GAMMA = a ⊃ beta

DELTA = EG(GAMMA)

THETA = AF(DELTA)

T(ALPHA) = [NEXT] X b

T(BETA) = <NEXT> X T(ALPHA)

T(GAMMA) = Not a ∨ T(beta)

T(DELTA) = νX. T(GAMMA) ∧ <NEXT>X

T(THETA) = μX. T(DELTA) ∨ [NEXT] X

[|alpha|] = [|[NEXT] X b |] = preA(next, [|b|]) = preA(next, {0, 3, 4}) = {3, 4}

[|Beta|] = [| <next>X alpha |] = PreE(next, [| alpha |]) = PreE(next, {3, 4}) = {0, 2, 3}
[|GAMMA|] = [| a ⊃ Beta|] = {0, 1, 2} U {0, 2, 3} = {0, 1, 2, 3}

[|DELTA|] = [| νX. T(GAMMA) ∧ <NEXT>X |] = {0, 1, 2, 3}

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

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

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

Found a LFP -> [| X_1|] = [| X_2|] = {0, 1, 2, 3}

[|THETA|] = [| μX. T(DELTA) ∨ [NEXT] X |] =

[| X_0 |] = {}

[| X_1 |] = [| DELTA ∨ [NEXT] X_0 |] = [| DELTA |] ∨ preA(next, X_0) =
= (0, 1, 2, 3) U {} = {0, 1, 2, 3}

[| X_2 |] = [| DELTA ∨ [NEXT] X_1 |] = [| DELTA |] ∨ preA(next, X_1) =
= (0, 1, 2, 3) U {1, 4} = {0, 1, 2, 3, 4}

[| X_3 |] = [| DELTA ∨ [NEXT] X_2 |] = [| DELTA |] ∨ preA(next, X_2) =
= (0, 1, 2, 3) U {1, 4} = {0, 1, 2, 3, 4}

Found a LFP -> [| X_2 |] = [| X_3 |] = {0, 1, 2, 3, 4}

Is theta true in TS? Yes

1 in [| THETA |]

Exercise 4.
Check whether CQ q1 is contained in CQ q2, reporting canonical DBs and homomorphism:

q1(xr) ← e(xr, xg), e(xg, xb), e(xb, xr).
q2(x) ← e(x, y), e(y, z), e(z, x), e(z, v)e(v, w), e(w, z).

We want to check if q1(xr) subseteq q2(x)

We must transform the containment into an evaluation:

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

Freeze all the free variables of q1. Introducing fresh constants to have Boolean queries.

q1(c) ← e(c, xg), e(xg, xb), e(xb, c).

q2(c) ← e(c, y), e(y, z), e(z, c), e(z, v)e(v, w), e(w, z).

Build the DB Iq1(c):

Iq1(c) := {Delta^{Iq1}, E ^{Iq1}, c ^{Iq1}} Composed by Domain, Edges(tuples) Constants
Delta^{Iq1} := {c, Xg, Xb} Domain of interest: i.e. All the terms that occurs in the query
E ^{Iq1} := {(c, Xg), (Xg, Xb), (Xb, c)} List of edges: i.e. All the tuples of the query
c ^{Iq1} := c constants are mapped to constants

Tabula form of Iq1(c):
{(c, Xg),
(Xg, Xb),
(Xb, c)}

Check if q2 is True in q1: Guess an assignment alpha for all the fixed variables of q2.
First I consider the more constrained atoms

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

This is a Satisfying assignment.
CM theorem guarantees that this is an Homomorphism. And also from CM theorem:

Iq1(c) models Iq2(c) iff Iq2(c) implies Iq1(c)

To check the Homomorphism, we must assure that the two following conditions are satisfied:

1. **$H(c^I) = C^J$**
2. **$(H(x), h(y))$ in c^J**

Check the homomorphism, mapping each tuple of Iq2(c) to Iq1(c):
Building the CANONICAL DB Iq2(c):

Iq2(c) := {$Delta^{Iq2}$, E^{Iq2}, c^{Iq2}} Composed by Domain, Edges(tuples) Constants
$Delta^{Iq2}$:= {c, Y, Z, V, W} Domain of interest: i.e. All the terms that occurs in the query
E^{Iq2} := {(c, Y), (Y, Z), (Z, c), (Z, V), (V, W), (W, Z)} List of edges: i.e. All the tuples of the query
c^{Iq2} := c constants are mapped to constants, constants preserve Interpretation.

Tabula form of Iq2(c):
{(c, Y),
(Y, Z),
(Z, c),
(Z, V),
(V, W),
(W, Z)}

H(c) = H(c^{Iq2}) = alpha(c) = c
H(y) = alpha(y) = Xg
H(z) = alpha(z) = Xb
H(v) = alpha(v) = c
H(w) = alpha(w) = Xg

Check if the homomorphism is True, checking if the relation is maintained by the mapping:

(c, Y) in C^J IMPLIES (h(c), h(Y)) IN C^I
(Y, Z) in C^J IMPLIES (h(Y), h(Z)) IN C^I
(Z, c) in C^J IMPLIES (h(Z), h(c)) IN C^I
(Z, V) in C^J IMPLIES (h(Z), h(V)) IN C^I
(V, W) in C^J IMPLIES (h(V), h(W)) IN C^I
(W, Z) in C^J IMPLIES (h(W), h(Z)) IN C^I

All the properties are satisfied and the homomorphism is TRUE.

Formal Methods – January 18, 2018

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

Alphabet:

Axioms: