SAPIENZA Universita` di Roma – MSc. in Engineering in Computer Science Formal Methods - Final Test – June, 26 2020

Roberto Sorce

(Time to complete the test: 2:30 hours)

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

Alphabet: Course(x), Student(y), BScStudent(x), MScStudent(x), Professor(z), Exam(x, y, z), Mark(x, y, z, w), Supervises(x, y)

Axioms:

Forall x. BScStudent(x) implies Student(x) ISA
Forall x. MScStudent(x) implies Student(x) ISA
Forall x. BScStudent(x) implies not MScStudent(x) DISJOINTNESS
Forall x. Student(x) implies BScStudent(x) OR MScStudent(x) COMPLETENESS
Forall x, y. Supervises(x, y) implies Professor(x) and MScStudent(y)
Forall x. Professor(x) implies 1<= #{y|supervises(x, y)}
Forall x. MScStudent(x) implies 0 <= #{y|supervises(y, x)} <=1

Forall x, y, z. Exam(x, y, z) implies Course(x) and Student(y) and Professor(z)
Forall x, y, z, w. Mark(x, y, z, w) implies Exam(x, y, z) and Integer(w)
Forall x, y, z, z'. Exam(x, y, z) and Exam(x, y, z') implies z=z' KEY

Forall x, y, z. Exam(x, y, z) implies 1 <= #{w|Mark(x, y, z, w)}<= 1

Exists Exam(x, y, z, w) and (Forall w, w'. Exam(x, y, z) and Exam(x, y, z, w') implies w=w') MULTIPLICITY EXPLICIT FORM

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, it does not contain Student table. In order to fix the instantiation, we must add the Student table and insert all the instances of BScStudent and MScStudent, because there is an ISA relation between these classes. The resulting table is the following:

Student:= {sb1, sb2, sm1, sm2, sm3}

All other constraints are not violated. The instantiation is now complete.

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

Exercise 3.
1.Model check the Mu-Calculus formula $\nu X.\mu Y.((a \wedge [next]X) \vee \langle next\rangle Y)$
2.Model check (by translating in Mu-Calculus) the CTL formula: $EG(a \wedge AFa)$

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

$[|X_0|] = \{0, 1, 2, 3, 4\}$
$[|X_1|] = [|\ \mu Y.((a \wedge [next]X_0) \vee \langle next\rangle Y)\ |] =$
$[|Y_0|]= \{\ \}$
$[|Y_1|] = [|\ (a \wedge [next]X_0) \vee \langle next\rangle Y_0)\ |] =$
$[|a|]$ inter $PreA(next, [|X_0|])$ U $PreE(next, [|Y_0|]) =$

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

$[|Y_2|] = [|\ (a \wedge [next]X_0) \vee \langle next\rangle Y_1)\ |] =$
$[|a|]$ inter $PreA(next, [|X_0|])$ U $PreE(next, [|Y_1|]) =$

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

$[|Y_3|] = [|\ (a \wedge [next]X_0) \vee \langle next\rangle Y_2)\ |] =$
$[|a|]$ inter $PreA(next, [|X_0|])$ U $PreE(next, [|Y_2|]) =$

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

Found a LFP -> $[|Y_2|] = [|Y_3|] = \{0, 1, 3, 4\}$

$[|X_2|] = [|\ \mu Y.((a \wedge [next]X_1) \vee \langle next\rangle Y)\ |] =$
$[|Y_{00}|]= \{\ \}$
$[|Y_{01}|] = [|\ (a \wedge [next]X_1) \vee \langle next\rangle Y_{00})\ |] =$
$[|a|]$ inter $PreA(next, [|X_1|])$ U $PreE(next, [|Y_{00}|]) =$

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

$[|Y_{02}|] = [|\ (a \wedge [next]X_1) \vee \langle next\rangle Y_{01})\ |] =$
$[|a|]$ inter PreA(next, $[|X_1|]$) U PreE(next, $[|Y_{01}|]$) =

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

$[|Y_{03}|] = [|\ (a \wedge [next]X_1) \vee \langle next\rangle Y_{02})\ |] =$
$[|a|]$ inter PreA(next, $[|X_1|]$) U PreE(next, $[|Y_{02}|]$) =

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

$[|Y_{04}|] = [|\ (a \wedge [next]X_1) \vee \langle next\rangle Y_{03})\ |] =$
$[|a|]$ inter PreA(next, $[|X_1|]$) U PreE(next, $[|Y_{03}|]$) =

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

Found a LFP -> $[|Y_{03}|] = [|Y_{04}|]$ = {0, 3, 4}

$[|X_3|] = [|\ \mu Y.((a \wedge [next]X_2) \vee \langle next\rangle Y)\ |] =$
$[|Y_{10}|]$= { }
$[|Y_{11}|] = [|\ (a \wedge [next]X_2) \vee \langle next\rangle Y_{11})\ |] =$
$[|a|]$ inter PreA(next, $[|X_2|]$) U PreE(next, $[|Y_{11}|]$) =

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

$[|Y_{12}|] = [|\ (a \wedge [next]X_2) \vee \langle next\rangle Y_{12})\ |] =$
$[|a|]$ inter PreA(next, $[|X_2|]$) U PreE(next, $[|Y_{12}|]$) =

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

$[|Y_{13}|] = [|\ (a \wedge [next]X_2) \vee \langle next\rangle Y_{13})\ |] =$
$[|a|]$ inter PreA(next, $[|X_2|]$) U PreE(next, $[|Y_{13}|]$) =

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

$[|Y_{14}|] = [|\ (a \wedge [next]X_2) \vee \langle next\rangle Y_{14})\ |] =$
$[|a|]$ inter PreA(next, $[|X_2|]$) U PreE(next, $[|Y_{14}|]$) =

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

Found LFP $[|X_2|] = [|x_3|]$ = { 0, 3, 4 }

Φ = **{ 0, 3, 4 }**
1 in [| Φ |]? No, initial state of transition system is not present in the extension of Φ , Hence the formula is False in this transition system.

Decompose the CTL formula: EG(a ∧ AFa)

Alpha = AFa
Beta = a ∧ alpha
Gamma = EG(Beta)

Translation of CTL formula:

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

[|Alpha|] = [| μX. a ∨ [next]X |] =
[| X_0 |] = { }
[| X_1 |] = [| a ∨ [next] X_0 |] = [| a |] U PreA(next, [| X_0 |]) =
= {0, 1, 4} U {} = {0, 1, 4}

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

[| X_3 |] = [| a ∨ [next] X_2 |] = [| a |] U PreA(next, [| X_2 |]) =
= {0, 1, 4} U {3, 4} = {0, 1, 3, 4}

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

[|Beta|] = [| a |] ∧ [| alpha |] = {0, 1, 4} inter {0, 1, 3, 4} = {0, 1, 4}
[|Gamma|] = [|νX. Beta ∧ <Next>X|] =
[| X_0 |] ={0, 1, 2, 3, 4}
[| X_1 |] = [| Beta|] inter PreE(next, [| X_0 |]) =
= {0, 1, 4} inter {0, 1, 2, 3, 4} = {0, 1, 4}

[| X_2 |] = [| Beta|] inter PreE(next, [| X_1 |]) =
= {0, 1, 4} inter {0, 3, 4} = {0, 4}

[| X_3 |] = [| Beta|] inter PreE(next, [| X_2 |]) =
= {0, 1, 4} inter {3, 4} = {4}

$[|X_4|] = [|\text{ Beta}|] \text{ inter PreE}(\text{next}, [|X_3|]) =$
$= \{0, 1, 4\} \text{ inter } \{3\} = \{\ \}$

$[|X_5|] = [|\text{ Beta}|] \text{ inter PreE}(\text{next}, [|X_4|]) =$
$= \{0, 1, 4\} \text{ inter } \{\ \} = \{\ \}$

[|Gamma|] = { }

CTL Formula = { }

Is 1 in [|Gamma|]? No, initial state of TS is not present in the extension of Gamma, hence, the formula is not valid in the TS. CTL formula is false in this TS

Exercise 4. Compute the *weakest precondition* for getting x=y executing the following program:

Evaluation semantics:

Computing the weakest precondition, regressing the Post condition Q from the bottom to the top of the execution of program:

{P} S {Q} iff P => WP(S, Q)

Note, Hoare logic is concerned only about partial correctness, it does not consider termination. If termination and post condition is achieved, producing the right result, then total correctness is achieved. Termination in this case is irrelevant, because there are no while loops.

WP(Delta, Q) -> WP(Delta, {x=y}) => {y=5}

{x=y} ->
{y:=5;}

X:=10;
{ (y > 10 and x+5=0) OR (y<=10 and x=2y) } ->

- ➔ { (y > 10 and 10+5 = 0) OR (y<=10 and 10=2y) }
- ➔ { (y > 10 and 15=0) OR (y<=10 and y=5) }
- ➔ FALSE OR TRUE

If (y >10) then {
{x=y} -> {x + y + 5 = y} -> { x + 5 = y - y} -> {x + 5 = 0} FALSE
x = x+y;
{x=y} -> {x = y-5} -> {y = x + 5}
y = y-5;

{x=y}
}
{x=y} -> {x-y=y} -> { x = 2y }
else x = x-y;

{x=y}

Alpha implies not (Beta)