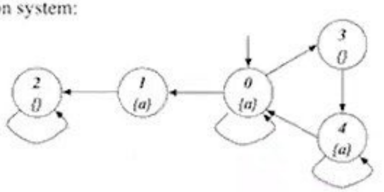
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

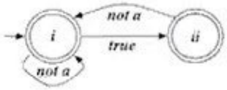
Formal Methods – June 17, 2024

(Time to complete the test online: 2:00 hours)

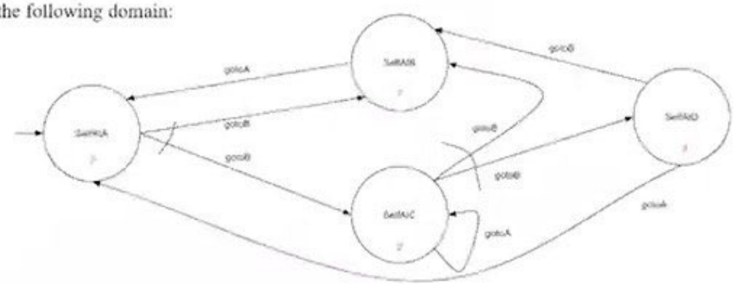
Part 1. Consider the following transition system:



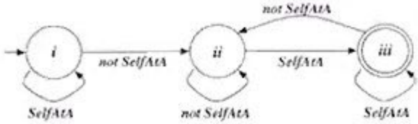
- **Exercise 1.1:** Model check the Mu-Calculus formula: $\nu X.\mu Y.((a \wedge \langle next \rangle X) \vee \langle next \rangle Y)$
- **Exercise 1.2:** Model check the CTL formula $AF(a \wedge AXa)$, by translating it in Mu-Calculus.
- **Exercise 1.3:** Model check the LTL formula $\Diamond(a \wedge \bigcirc a)$, by considering that the Büchi automaton for $\neg\Diamond(a \wedge \bigcirc a))$ is the one below:



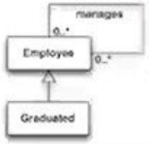
Part 2 Consider the following domain:



- **Exercise 2.1:** Synthesize a strategy (a plan) for realizing the LTLf formula $\Diamond(\neg SelfAtA \wedge \Diamond(SelfAtA \wedge \bullet false))$, by considering that the corresponding DFA is the one below:

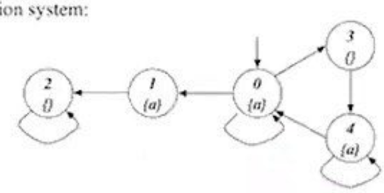


Part 3 Consider the following simple UML class diagram, and express in FOL the following boolean queries (stating which ones are CQs):

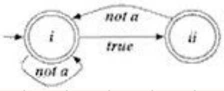


1. *There exists a graduated employee that manages at least one graduated employee.*
2. *There exists a graduated employee that manages at least two graduated employees.*
3. *There exists a graduated employee that manages an employee who graduated and an employee who is not graduated.*
4. *There exists an employee that manages only graduated employees.*
5. *There exists an employee that manages all graduated employees.*

Part 1. Consider the following transition system:



- **Exercise 1.1:** Model check the Mu-Calculus formula: $\nu X.\mu Y.((a \wedge \langle next \rangle X) \vee \langle next \rangle Y)$
- **Exercise 1.2:** Model check the CTL formula $AF(a \wedge AXa)$, by translating it in Mu-Calculus.
- **Exercise 1.3:** Model check the LTL formula $\Diamond(a \wedge \bigcirc a)$, by considering that the Büchi automaton for $\neg\Diamond(a \wedge \bigcirc a))$ is the one below:



1) $\varphi = \nu X.\mu Y((a \wedge \langle NEXT \rangle X) \vee \langle NEXT \rangle Y)$

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

$[X_1] = [\mu Y((a \wedge \langle NEXT \rangle X_0) \vee \langle NEXT \rangle Y)] =$

$[Y_0] = \phi$

$[Y_1] = ([a] \cap PREE(NEXT, X_0)) \cup PREE(NEXT, Y_0) =$

$= (\{0,1,4\} \cap \{0,1,2,3,4\}) \cup \phi = \{0,1,4\}$

$[Y_2] = ([a] \cap PREE(NEXT, X_0)) \cup PREE(NEXT, Y_1) =$

$= (\{0,1,4\} \cap \{0,1,2,3,4\}) \cup \{0,3,4\} = \{0,1,3,4\}$

$[Y_3] = ([a] \cap PREE(NEXT, X_0)) \cup PREE(NEXT, Y_2) =$

$= (\{0,1,4\} \cap \{0,1,2,3,4\}) \cup \{0,3,4\} = \{0,1,3,4\}$

$[Y_2] = [Y_3] = [X_1] = \{0,1,3,4\}$

$[X_2] = [\mu Y((a \wedge \langle NEXT \rangle X_1) \vee \langle NEXT \rangle Y)] =$

$[Y_0] = \phi$

$[Y_1] = ([a] \cap PREE(NEXT, X_1)) \cup PREE(NEXT, Y_0) =$

$= (\{0,1,4\} \cap \{0,3,4\}) \cup \phi = \{0,4\}$

$[Y_2] = ([a] \cap PREE(NEXT, X_1)) \cup PREE(NEXT, Y_1) =$

$= (\{0,1,4\} \cap \{0,3,4\}) \cup \{0,3,4\} = \{0,3,4\}$

$[Y_3] = ([a] \cap PREE(NEXT, X_1)) \cup PREE(NEXT, Y_2) =$

$= (\{0,1,4\} \cap \{0,3,4\}) \cup \{0,3,4\} = \{0,3,4\}$

$[Y_2] = [Y_3] = [X_2] = \{0,3,4\}$

$[X_3] = [\mu Y\, ((a \wedge \langle NEXT \rangle X_2) \vee \langle NEXT \rangle Y)] =$

$[Y_0] = \emptyset$

$[Y_1] = ([a] \cap PREE(NEXT, X_2)) \cup PREE(NEXT, Y_0) =$

$= (\{0,1,4\} \cap \{0,3,4\}) \cup \emptyset = \{0,4\}$

$[Y_2] = ([a] \cap PREE(NEXT, X_2)) \cup PREE(NEXT, Y_1) =$

$= (\{0,1,4\} \cap \{0,3,4\}) \cup \{0,3,4\} = \{0,3,4\}$

$[Y_3] = ([a] \cap PREE(NEXT, X_2)) \cup PREE(NEXT, Y_2) =$

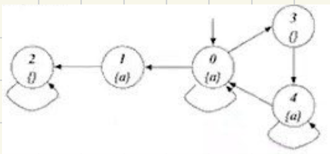
$= (\{0,1,4\} \cap \{0,3,4\}) \cup \{0,3,4\} = \{0,3,4\}$

$[Y_2] = [Y_3] = \boxed{[X_3] = \{0,3,4\}}$

$\boxed{[X_2] = [X_3] = \{0,3,4\}}$

$s_0 \in [\varphi] = \{0,3,4\}$? YES!

2) $AF(\underbrace{\underbrace{a \wedge \underbrace{AX\, a}_{\alpha}}_{\beta}}_{\gamma})$



$[\alpha] = [AX\, a] = [[NEXT]\, a] = PREA(NEXT, a) = \boxed{\{3,4\} = [\alpha]}$

$[\beta] = [a \wedge \alpha] = [a] \cap [\alpha] = \{0,1,4\} \cap \{3,4\} = \boxed{\{4\} = [\beta]}$

$[\gamma] = [AF\, \beta] = [\mu Z.\, \beta \vee [NEXT]\, Z]$

$[Z_0] = \emptyset$

$[Z_1] = [\beta] \cup PREA(NEXT, Z_0) =$

$= \{4\} \cup \emptyset = \{4\}$

$[Z_2] = [\beta] \cup PREA(NEXT, Z_1) =$

$= \{4\} \cup \{3\} = \{3,4\}$

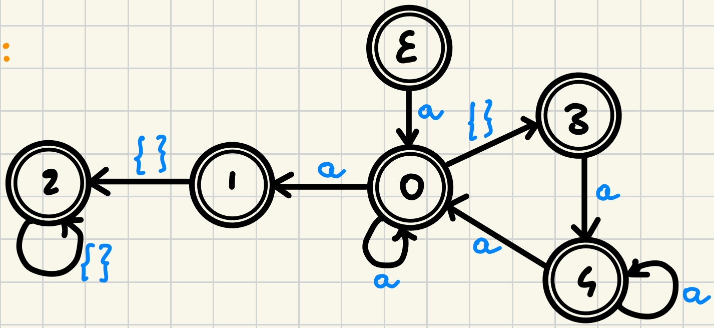
$[Z_3] = [\beta] \cup PREA(NEXT, Z_2) =$

$= \{4\} \cup \{3\} = \{3,4\}$

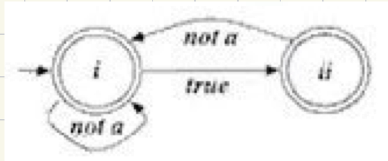
$[Z_2] = [Z_3] = \boxed{[\gamma] = \{3,4\}}$

$\Upsilon s_0 \in \gamma$? $\rightarrow$ $s_0 \in [\gamma] = \{3,4\}$? NO!

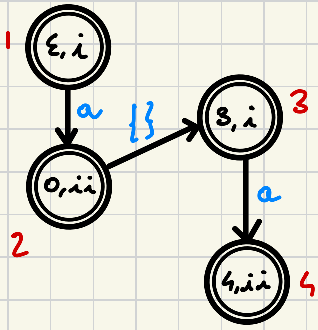
3) A_γ :



$A_{\neg\varphi}$:



$A_\gamma \cap A_{\neg\varphi}$:



$\nu X.\mu Y.(F \wedge \langle NEXT \rangle X \vee \langle NEXT \rangle Y)$

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

$[X_1] = [\mu Y.(F \wedge \langle NEXT \rangle X_0 \vee \langle NEXT \rangle Y)] =$

$[Y_0] = \emptyset$

$[Y_1] = [F] \cap PREE(NEXT, X_0) \cup PREE(NEXT, Y_0) =$

$= \{1,2,3,4\} \cap \{1,2,3,4\} \cup \emptyset = \{1,2,3,4\}$

$[Y_2] = [F] \cap PREE(NEXT, X_0) \cup PREE(NEXT, Y_1) =$

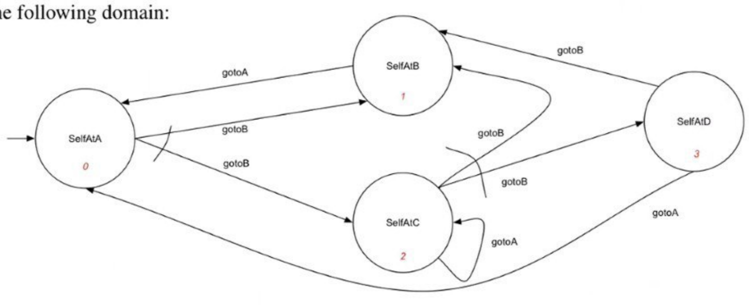
$= \{1,2,3,4\} \cap \{1,2,3,4\} \cup \{1,2,3\} = \{1,2,3,4\}$

$[Y_1] = [Y_2] = [X_1] = \{1,2,3,4\}$

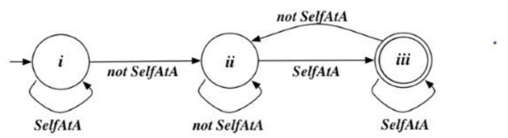
$[X_0] = [X_1] = \{1,2,3,4\}$

$s_1 \in [\nu X.\mu Y.(F \wedge \langle NEXT \rangle X \vee \langle NEXT \rangle Y)] = \{1,2,3,4\}$? YES!

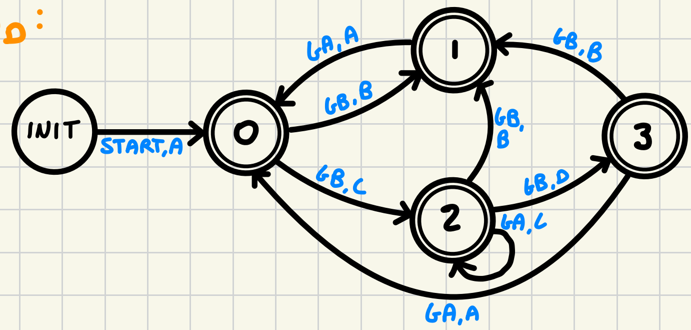
Part 2 Consider the following domain:



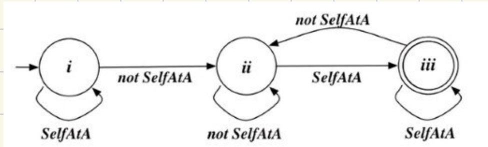
- **Exercise 2.1:** Synthesize a strategy (a plan) for realizing the LTLf formula $\Diamond(\neg SelfAtA \wedge \Diamond(SelfAtA \wedge \bullet false))$, by considering that the corresponding DFA is the one below:



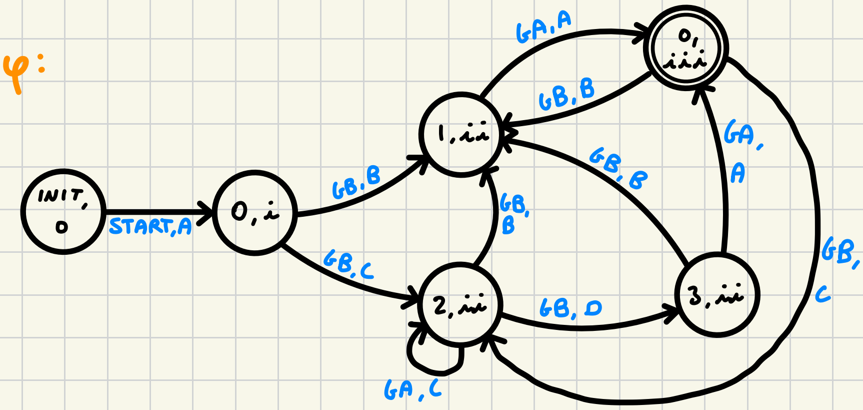
A_D:



A_φ:



$A_D \cap A_\varphi$:



$W_0 = \{(0, iii)\}$

$W_1 = W_0 \cup PREADV(W_0) = \{(0, iii), (1, ii), (3, ii)\}$

$W_2 = W_1 \cup PREADV(W_1) = \{(0, iii), (1, ii), (3, ii), (2, ii)\}$

$W_3 = W_2 \cup PREADV(W_2) = \{(0, iii), (1, ii), (3, ii), (2, ii), (0, i)\}$

$W_4 = W_3 \cup PREADV(W_3) = \{(0, iii), (1, ii), (3, ii), (2, ii), (0, i), (INIT, 0)\}$

$W_5 = W_4 \cup PREADV(W_4) = \{(0, iii), (1, ii), (3, ii), (2, ii), (0, i), (INIT, 0)\}$

$W_4 = W_5$

$W(\text{INIT}, 0) = \{\text{START}\}$ $\quad$ $W(1, ii) = \{GA\}$

$W(0, i) = \{GB\}$ $\quad$ $W(3, ii) = \{GA\}$

$W(2, ii) = \{GB\}$ $\quad$ $W(0, iii) = \text{WIN}$

$W_c(\text{INIT}, 0) = \text{START}$ $\quad$ $W_c(1, ii) = GA$

$W_c(0, i) = GB$ $\quad$ $W_c(3, ii) = GA$

$W_c(2, ii) = GB$ $\quad$ $W_c(0, iii) = \text{WIN}$

$$T = (2^X, S, S_0, \rho, W_c)$$

$$S = \{(\text{INIT}, 0), (0, i), (2, ii), (1, ii), (3, ii), (0, iii)\}$$

$$S_0 = \{(\text{INIT}, 0)\}$$

$$\rho(s, x) = \delta(s, (W_c(s), x))$$

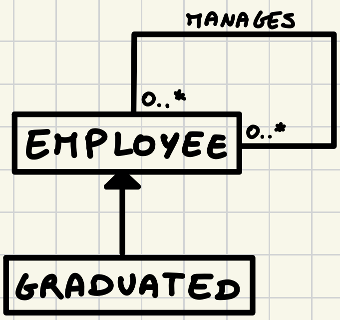
EX: $\rho((0, i), B) = \delta((0, i), (GB, B)) = (1, ii)$

T RECOGNIZE THE STRATEGY

Part 3 Consider the following simple UML class diagram, and express in FOL the following boolean queries (stating which ones are CQs):

1. *There exists a graduated employee that manages at least one graduated employee.*
2. *There exists a graduated employee that manages at least two graduated employees.*
3. *There exists a graduated employee that manages an employee who graduated and an employee who is not graduated.*
4. *There exists an employee that manages only graduated employees.*
5. *There exists an employee that manages all graduated employees.*

A QUERY IS A CQ IF IT CONTAINS ONLY "$\exists$ + $\wedge$", AND NOT "$\neg$, $\neq$, $\supset$, $\forall$, $\vee$".



1. $\exists x, y.\ G(x) \wedge G(y) \wedge \text{MANAGES}(x, y)$ ✓
2. $\exists x, y, y'.\ G(x) \wedge G(y) \wedge G(y') \wedge \text{MANAGES}(x, y) \wedge \wedge\ \text{MANAGES}(x, y') \wedge y \neq y'$ ✗
3. $\exists x, y, z.\ G(x) \wedge G(y) \wedge \neg G(z) \wedge \text{MANAGES}(x, y) \wedge \wedge\ \text{MANAGES}(x, z)$ ✗
4. $\exists x.\ E(x) \wedge \forall y.\ (\text{MANAGES}(x, y) \supset G(y))$ ✗
5. $\exists x.\ E(x) \wedge \forall y.\ (G(y) \supset \text{MANAGES}(x, y))$ ✗