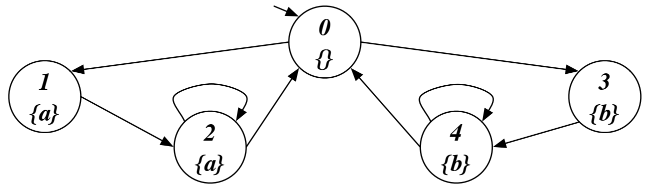
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

Formal Methods – September 15, 2023

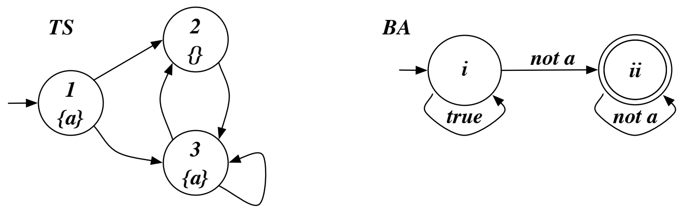
(Time to complete the test: 2:00 hours)

Part 1. Consider the following transition system:

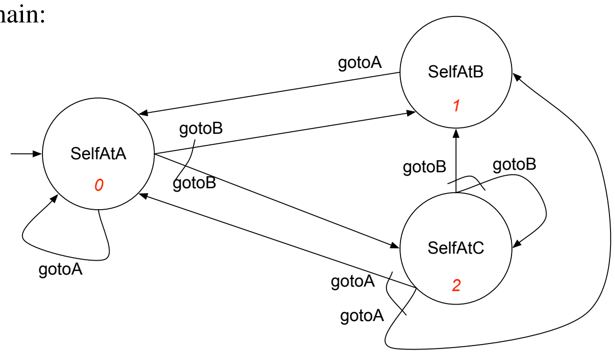


- **Exercise 1.1:** Model check the Mu-Calculus formula: $\nu X.\mu Y.((a \wedge [next]X) \vee (b \wedge \langle next \rangle Y))$
- **Exercise 1.2:** Model check the CTL formula $AF(EG(a \supset AXEX\neg a))$, by translating it in Mu-Calculus.

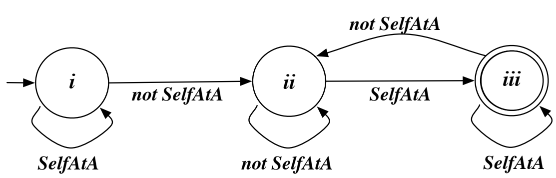
Part 2 Consider the transition system TS below. Model check the LTL formula $\Box\Diamond a$, by considering that the Büchi automaton BA for $\neg\Box\Diamond a$ (i.e., $\Diamond\Box\neg a$) is the one below:



Part 3 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:



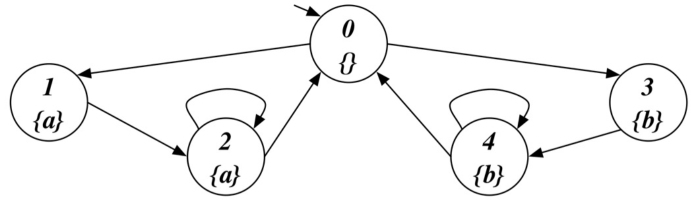
Part 4 (optional) Consider the following program:

```
while (x<10) do x := x + 1
```

Compute its *execution* and *final state*, starting from an *initial state* where $x = 9$, by using:

1. *Evaluation Semantics*;
2. *Transition Semantics*.

Part 1. Consider the following transition system:



- **Exercise 1.1:** Model check the Mu-Calculus formula: $\nu X.\mu Y.((a \wedge [next]X) \vee (b \wedge \langle next \rangle Y))$
- **Exercise 1.2:** Model check the CTL formula $AF(EG(a \supset AXEX\neg a))$, by translating it in Mu-Calculus.

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

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

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

$$[Y_0] = \emptyset$$

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

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

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

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

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

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

$$[Y_0] = \emptyset$$

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

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

$$[Y_2] = ([a] \cap PREA(NEXT, X_1)) \cup ([b] \cap PREE(NEXT, Y_0)) =$$

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

$$[Y_1] = [Y_2] = [X_2] = \{1\}$$

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

$$[Y_0] = \emptyset$$

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

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

$$[Y_0] = [Y_1] = [X_3] = \emptyset$$

$[X_4] = [\mu Y. ((a \wedge [NEXT]X_3) \vee (b \wedge \langle NEXT \rangle Y))]$

$[Y_0] = \emptyset$

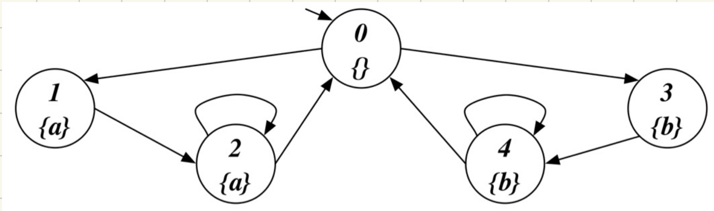
$[Y_1] = ([a] \cap PREA(NEXT, X_3)) \cup ([b] \cap PREE(NEXT, Y_0)) =$

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

$[Y_0] = [Y_1] = [X_4] = \emptyset$

$[X_3] = [X_4] = \emptyset$

2) $\underbrace{AF(\underbrace{EG(\underbrace{a \supset \underbrace{AX \underbrace{EX \neg a}_{\alpha}}_{\beta}}_{\gamma})}_{\delta})}_{\varepsilon}$



$[\alpha] = [EX \neg a] = [\langle NEXT \rangle \neg a] = PREE(NEXT, \neg a) = \{0,2,3,4\} = [\alpha]$

$[\beta] = [AX\, \alpha] = [[NEXT]\, \alpha] = PREA(NEXT, \alpha) = \{1,2,3,4\} = [\beta]$

$[\gamma] = [a \supset \beta] = [\neg a] \cup [\beta] = \{0,3,4\} \cup \{1,2,3,4\} = \{0,1,2,3,4\} = [\gamma]$

$[\delta] = [EG\, \gamma] = [\nu Z. \gamma \wedge \langle NEXT \rangle Z]$

$[Z_0] = \{0,1,2,3,4\}$

$[Z_1] = [\gamma] \cap PREE(NEXT, Z_0) =$

$= \{0,1,2,3,4\} \cap \{0,1,2,3,4\} = \{0,1,2,3,4\}$ $[Z_0] = [Z_1] = [\delta] = \{0,1,2,3,4\}$

$[\varepsilon] = [AF\, \delta] = [\mu Z. \delta \vee [NEXT] Z]$

$[Z_0] = \emptyset$

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

$= \{0,1,2,3,4\} \cup \emptyset = \{0,1,2,3,4\}$

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

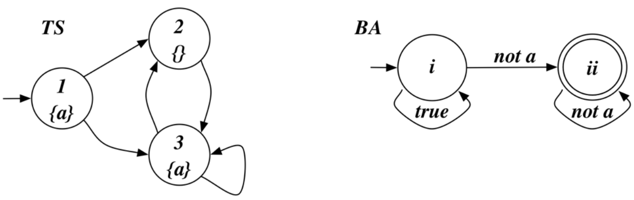
$= \{0,1,2,3,4\} \cup \{0,1,2,3,4\} = \{0,1,2,3,4\}$

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

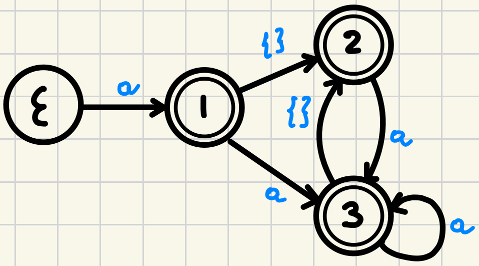
$= \{0,1,2,3,4\} \cup \{0,1,2,3,4\} = \{0,1,2,3,4\}$

$[Z_2] = [Z_3] = [\varepsilon] = \{0,1,2,3,4\}$ $s_0 \in [\varepsilon] = ?$ YES!

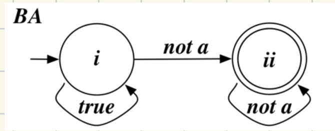
Part 2 Consider the transition system TS below. Model check the LTL formula $\Box\Diamond a$, by considering that the Büchi automaton BA for $\neg\Box\Diamond a$ (i.e., $\Diamond\Box\neg a$) is the one below:



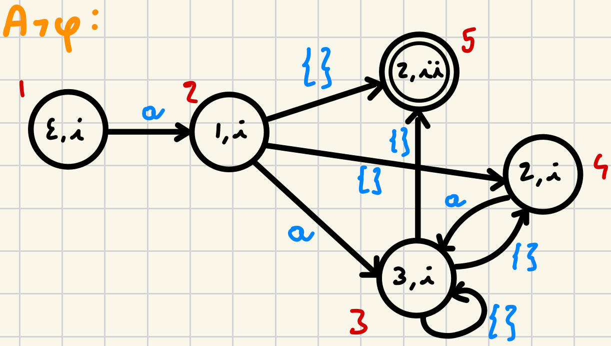
A_T:



$A_{\neg\varphi}$:



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



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

$[X_0] = \{1,2,3,4,5\}$

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

$[Y_0] = \emptyset$

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

$= \{5\} \cap \{1,2,3,4\} \cup \emptyset = \emptyset$

$[Y_0] = [Y_1] = [X_1] = \emptyset$

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

$[Y_0] = \emptyset$

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

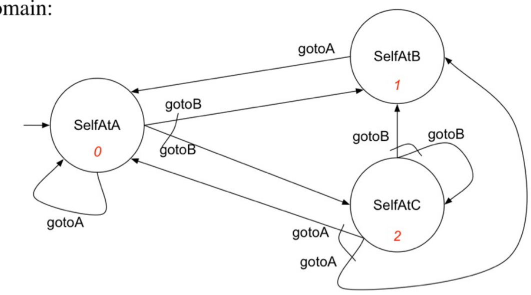
$= \{5\} \cap \emptyset \cup \emptyset = \emptyset$

$[Y_0] = [Y_1] = [X_2] = \emptyset$

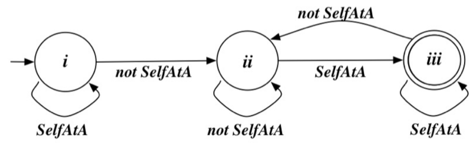
$[X_1] = [X_2] = \emptyset$

$s_1 \in [\varphi] = \emptyset$? NO!

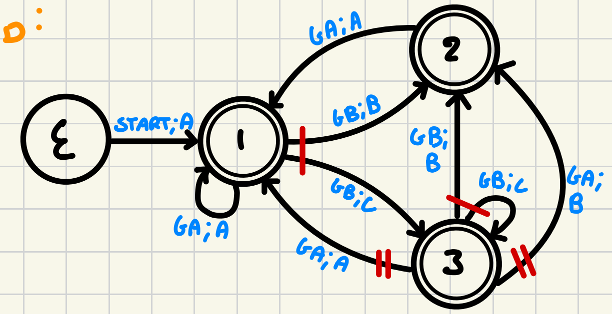
Part 3 Consider the following domain:



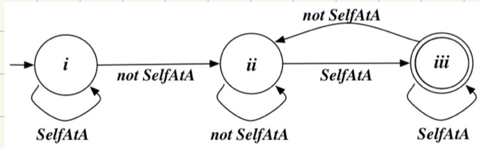
- **Exercise 2.1:** Synthesize a strategy (a plan) for realizing the LTLf formula $\Diamond(\neg SelfAtA \land \Diamond(SelfAtA \land \bullet false))$, by considering that the corresponding DFA is the one below:



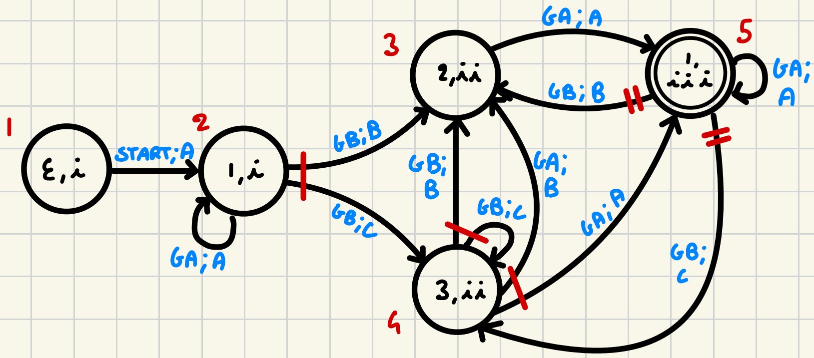
A_D:



A_φ:



$A_D \times A_\varphi$



$W_0 = \{5\}$

$W_1 = W_0 \cup PREADV(W_0) = \{3, 5\}$

$W_2 = W_1 \cup PREADV(W_1) = \{3, 4, 5\}$

$W_3 = W_2 \cup PREADV(W_2) = \{2, 3, 4, 5\}$

$W_4 = W_3 \cup PREADV(W_3) = \{1, 2, 3, 4, 5\}$

$W_5 = W_4 \cup PREADV(W_4) = \{1, 2, 3, 4, 5\}$

$W_4 = W_5$

$W(1) = \{START\}$
$W(2) = \{GB\}$
$W(3) = \{GA\}$
$W(4) = \{GA, GB\}$
$W(5) = WIN$

$W_c(1) = START$
$W_c(2) = GB$
$W_c(3) = GA$
$W_c(4) = GA$
$W_c(5) = WIN$

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

$S = \{1, 2, 3, 4, 5\}$

$S_0 = \{1\}$

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

Part 4 (optional) Consider the following program:

```
while (x<10) do x := x + 1
```

Compute its *execution* and *final state*, starting from an *initial state* where $x = 9$, by using:

1. *Evaluation Semantics*;
2. *Transition Semantics*.

1) $S_0 = \{x=9\}$

$$\dfrac{\text{WHILE}\ (x<10)\ \text{DO}\ x:=x+1,\ S_0 \to S_F}{\dfrac{(x = x+1, S_0) \to S_1}{\text{TRUE}} \wedge \dfrac{(\text{WHILE}\ (x<10)\ \text{DO}\ x:=x+1,\ S_1) \to S_F}{\text{TRUE}}}$$

$S_1 = S_F = \{x=10\}$

2) FIRST STEP

$$\dfrac{(\text{WHILE}\ (x<10)\ \text{DO}\ x:=x+1,\ S_0) \to (d_1, S_1)}{\dfrac{x=x+1,\ S_0 \to (\varepsilon, S_1)}{\text{TRUE}}}$$

$S_1 = \{x=10\}$

SECOND STEP

$$\dfrac{\varepsilon;\ \text{WHILE}\ (x<10)\ \text{DO}\ x:=x+1,\ S_1 \to (d_2, S_2)}{\text{TRUE}}$$

$S_F = S_2 = S_1 = \{x=10\}$