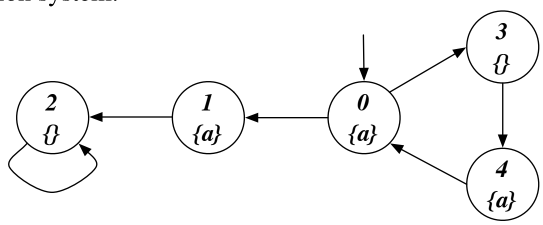
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

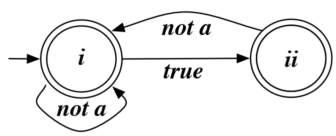
Formal Methods – February 16, 2023

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

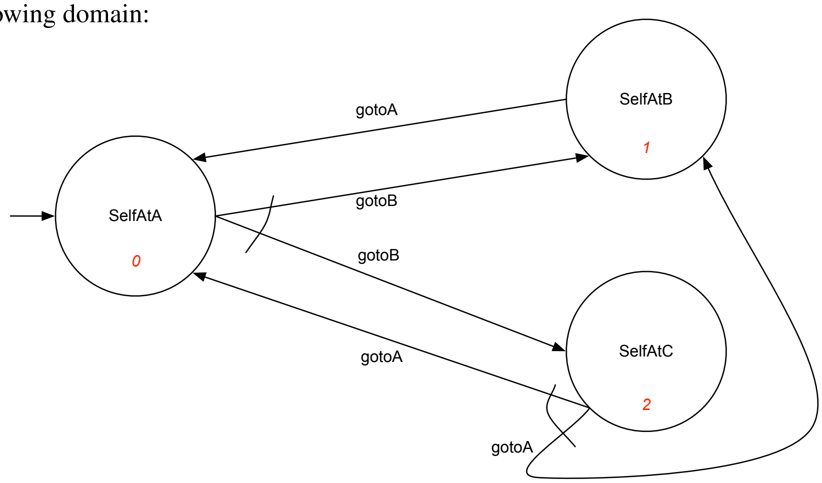
Part 1. Consider the following transition system:



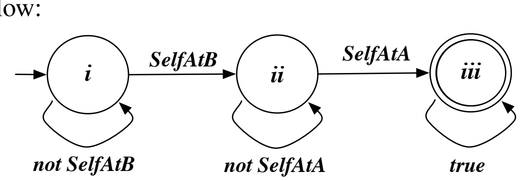
- **Exercise 1.1:** Model check the Mu-Calculus formula: $\nu X.\mu Y.((a \wedge \langle next\rangle X) \vee \langle next\rangle Y)$
- **Exercise 1.2:** Model check the CTL formula $AF(a \wedge AXa)$, by translating it in Mu-Calculus.
- **Exercise 1.3:** Model check the LTL formula $\Diamond(a \wedge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

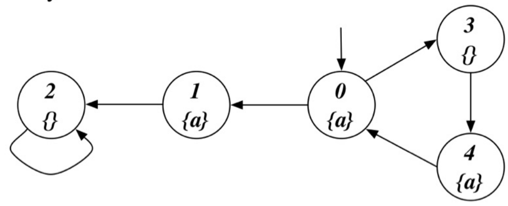


Part 3 Consider the notion of invariant of a while-loop.

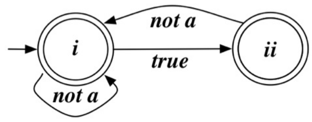
- **Exercise 3.1:** Check whether the following Hoare triple is correct, using as *invariant* $i \leq 10$.

$\{i = 0\}$ `while (i<10) do (tmp := i; tmp := tmp +1; i:= tmp)` $\{i = 10\}$

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

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

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

$[Y_0] = \emptyset$

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

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

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

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

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

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

$[Y_4] = [Y_3] = [X_1] = \{0,1,3,4\}$

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

$[Y_0] = \emptyset$

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

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

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

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

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

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

$[Y_4]=[Y_3]=[X_2]=\{0,3,4\}$

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

$[Y_0]=\phi$

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

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

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

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

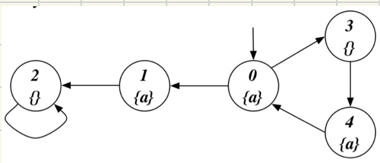
$[Y_3]=([a]\cap PREE(NEXT, X_2))\cup PREE(NEXT, Y_2)=$

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

$[Y_4]=[Y_3]=[X_3]=\{0,3,4\}$

$[X_2]=[X_3]=\{0,3,4\}$ $\qquad\qquad$ $s_0\in[\varphi]=?$ YES!

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



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

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

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

$[Z_0]=\phi$

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

$=\{4\}\cup\phi=\{4\}$

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

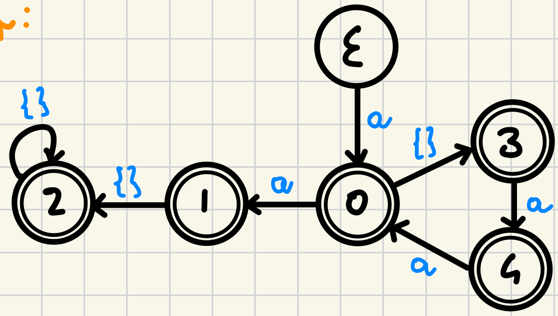
$=\{4\}\cup\{3\}=\{3,4\}$

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

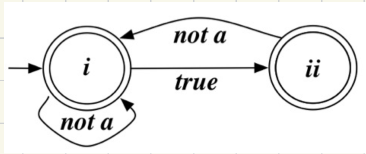
$=\{4\}\cup\{3\}=\{3,4\}$

$[Z_2]=[Z_3]=[\gamma]=\{3,4\}$ $\qquad\qquad$ $s_0\in[\gamma]=?$ NO!

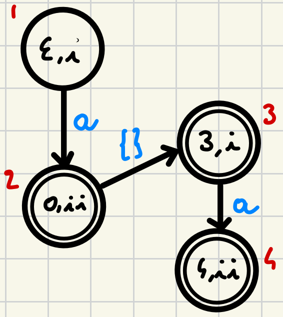
3) A_φ:



$A_{\neg\varphi}$:



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



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

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

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

$$[Y_0] = \emptyset$$

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

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

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

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

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

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

$$[Y_2] = [Y_3] = [X_1] = \{1,2,3\}$$

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

$$[Y_0] = \emptyset$$

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

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

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

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

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

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

$$[Y_4] = [F] \cap PREE(NEXT, X_1) \cup PREE(NEXT, Y_3) =$$

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

$$[Y_3] = [Y_4] = [X_2] = \{1,2\}$$

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

$$[Y_0] = \emptyset$$

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

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

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

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

$$[Y_0] = \emptyset$$

$$[Y_1] = [F] \cap PREE(NEXT, X_3) \cup PREE(NEXT, Y_0) =$$

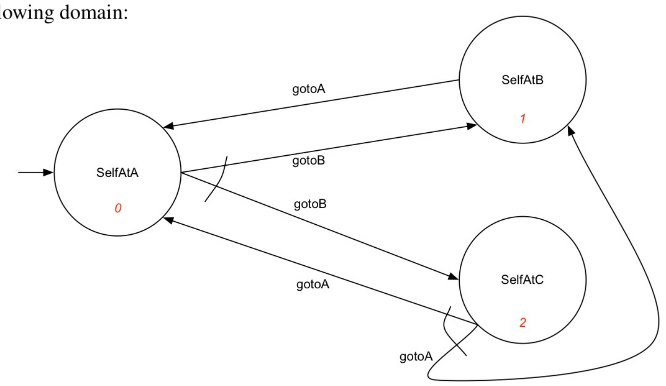
$$= \{2,3,4\} \cap \emptyset \cup \emptyset = \emptyset$$

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

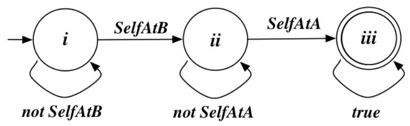
$$[X_3] = [X_4] = \emptyset$$

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

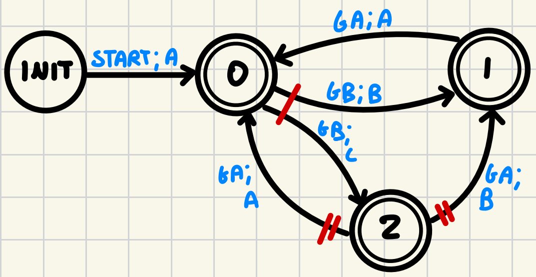
Part 2 Consider the following domain:



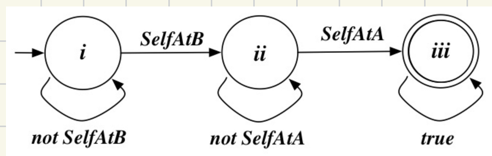
- **Exercise 2.1:** Synthesize a strategy (a plan) for realizing the LTLf formula $\Diamond(SelfAtB \wedge \Diamond(SelfAtA))$, by considering that the corresponding DFA is the one below:



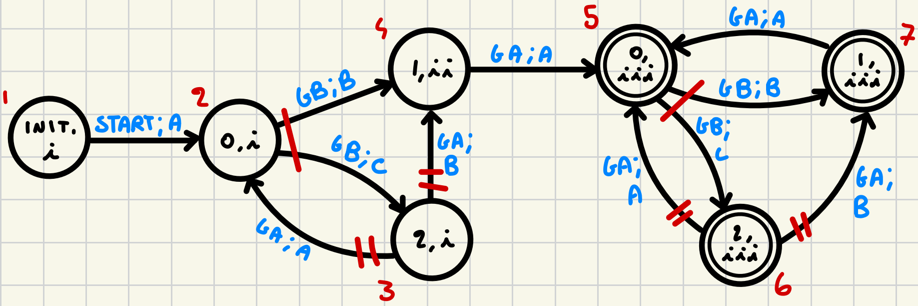
A_D:



A_φ:



$A_D \times A_\varphi$:



$W_0 = \{5, 6, 7\}$

$W_1 = W_0 \cup PREADV(W_0) = \{4, 5, 6, 7\}$

$W_2 = W_1 \cup PREADV(W_1) = \{4, 5, 6, 7\}$

$W_1 = W_2$

THERE IS NO STRATEGY

Part 3 Consider the notion of invariant of a while-loop.

- **Exercise 3.1:** Check whether the following Hoare triple is correct, using as *invariant* $\overset{I}{i \leq 10}$.

$$\overset{P}{\{i = 0\}}\ \texttt{while}\ \overset{g}{\texttt{(i<10)}}\ \texttt{do}\ \overset{\delta}{\texttt{(tmp := i; tmp := tmp +1; i:= tmp)}}\ \overset{Q}{\{i = 10\}}$$

1. $P \supset I$
2. $\neg g \wedge I \supset Q$
3. $\{g \wedge I\}\ \delta\ \{I\}$

1. $\{i=0\} \supset i \leq 10$ ✓

2. $i \geq 10 \wedge i \leq 10 \supset i = 10$ ✓

3. $\{i<10 \wedge i \leq 10\}(tmp := i;\ tmp := tmp+1;\ i := tmp)\ \{i \leq 10\}$

$\{i<10 \wedge i \leq 10\} \supset wp(tmp := i;\ tmp := tmp+1;\ i := tmp)\ \{i \leq 10\}$

$\{tmp \leq 9\}[tmp/i] = \{i \leq 9\}$
$tmp := i;$
$\{tmp \leq 10\}[tmp/tmp+1] = \{tmp \leq 9\}$
$tmp := tmp+1;$
$\{i \leq 10\}[i/tmp] = \{tmp \leq 10\}$
$i := tmp;$
$\{i \leq 10\}$

$\{i<10 \wedge i \leq 10\} \supset \{i \leq 9\}$? ✓

$i \leq 10$ IS AN INVARIANT