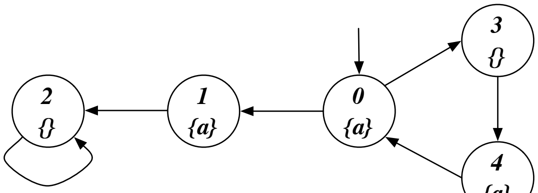
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

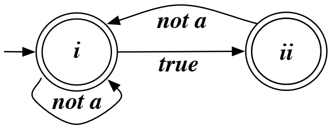
Formal Methods – February 16, 2023

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

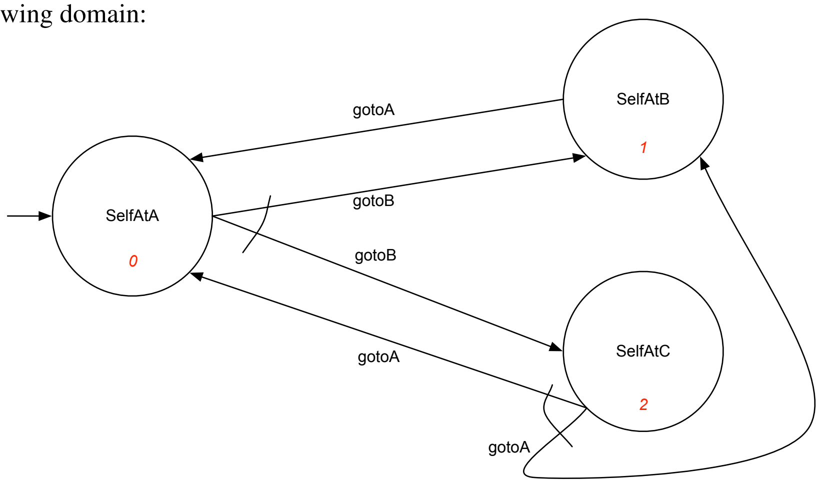
Part 1. Consider the following transition system:



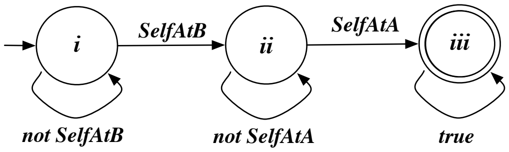
- **Exercise 1.1:** Model check the Mu-Calculus formula: $\nu X.\mu Y.((a \land \langle next\rangle X) \lor \langle next\rangle Y)$
- **Exercise 1.2:** Model check the CTL formula $AF(a \land AXa)$, by translating it in Mu-Calculus.
- **Exercise 1.3:** Model check the LTL formula $\Diamond(a \land \bigcirc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



Part 2 Consider the following domain:



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

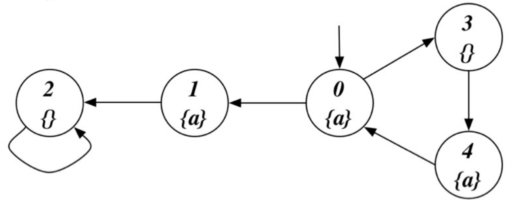


Part 3 Consider the notion of invariant of a while-loop.

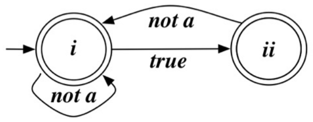
- **Exercise 3.1:** Check whether the following Hoare triple is correct, using as *invariant* $i \leq 10$.

$\{i = 0\}$ `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) $\varphi = \nu X.\mu Y.((a \wedge \langle NEXT \rangle X) \vee \langle NEXT \rangle Y)$

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

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

$[Y_0] = \phi$

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

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

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

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

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

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

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

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

$[Y_0] = \phi$

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

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

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

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

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

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

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

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

$[Y_0] = \phi$

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

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

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

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

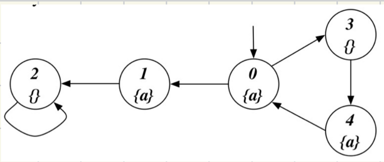
$[Y_3] = ([a] \cap PREE(NEXT, X_2)) \cup PREE(NEXT, Y_2) =$

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

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

$[X_2] = [X_3] = \{0,3,4\}$ $S_0 \in [\varphi] = ?$ YES!

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



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

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

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

$[Z_0] = \phi$

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

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

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

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

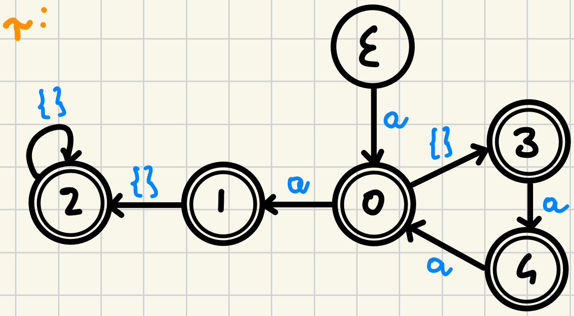
$[Z_3] = [\beta] \cup PREA(NEXT, Z_2) =$

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

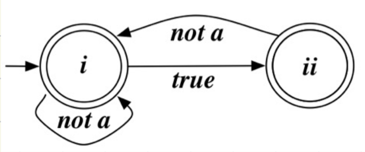
$S_0 \in [\gamma] = ?$ NO!

$[Z_4] = [Z_3] = [\gamma] = \{3,4\}$

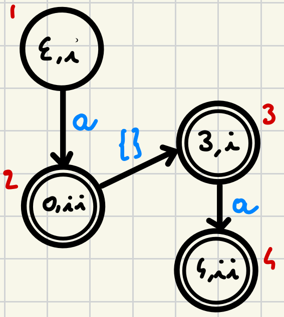
3) A_φ:



$A_{\neg\varphi}$:



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



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

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

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

$$[Y_0] = \emptyset$$

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

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

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

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

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

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

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

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

$$[Y_0] = \emptyset$$

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

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

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

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

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

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

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

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

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

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

$[Y_0] = \phi$

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

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

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

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

$[Y_0] = \phi$

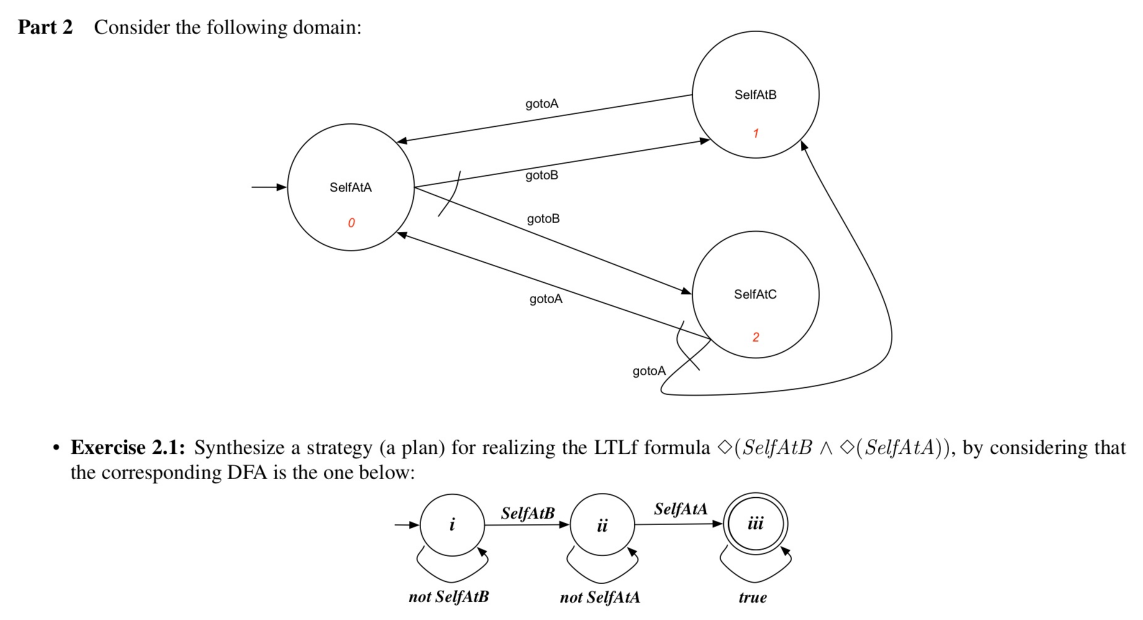
$[Y_1] = [F] \cap PREE(NEXT, X_3) \cup PREE(NEXT, Y_0) =$

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

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

$[X_3] = [X_4] = \phi$

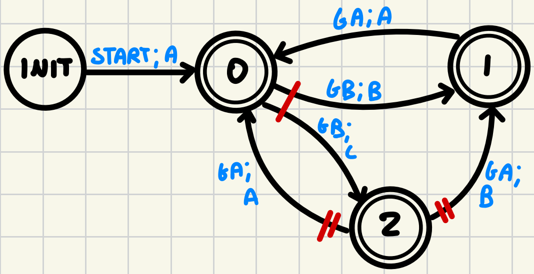
$s_1 \in [\varphi] = ?$ NO!



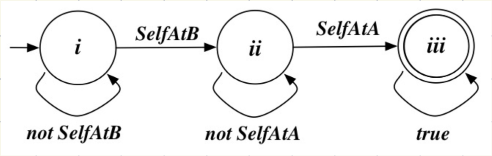
Part 2 Consider the following domain:

- **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:

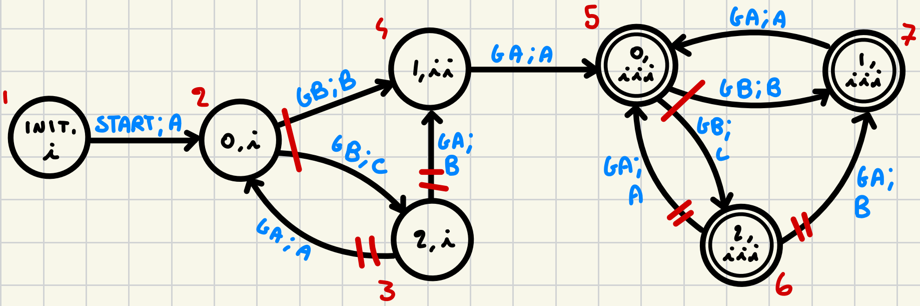
A_D:



A_φ:



$A_D \times A_\varphi$:



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

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

$W_2 = W_1 \cup \text{PREADV}(W_1) = \{2,3,4,5,6,7\}$

$W_3 = W_2 \cup \text{PREADV}(W_2) = \{1,2,3,4,5,6,7\}$

$W_4 = W_3 \cup \text{PREADV}(W_3) = \{1,2,3,4,5,6,7\}$

$W_3 = W_4$

$w(1) = \{\text{START}\}$
$w(2) = \{\text{GB}\}$
$w(3) = \{\text{GA}\}$
$w(4) = \{\text{GA}\}$
$w(5) = \text{WIN}$
$w(6) = \text{WIN}$
$w(7) = \text{WIN}$

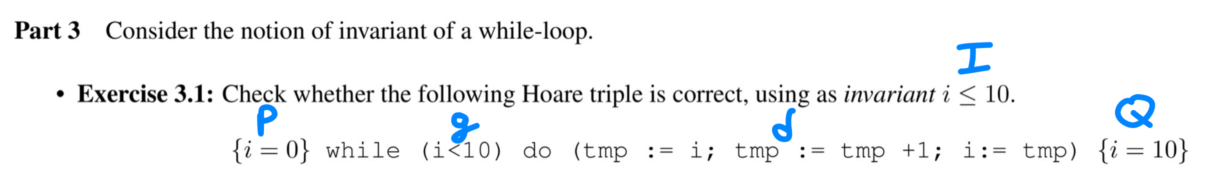
$w_c(1) : \text{START}$
$w_c(2) : \text{GB}$
$w_c(3) : \text{GA}$
$w_c(4) = \text{GA}$
$w_c(5) = \text{WIN}$
$w_c(6) = \text{WIN}$
$w_c(7) = \text{WIN}$

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

$S = \{1,2,3,4,5,6,7\}$

$S_0 = \{1\}$

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



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* $\overset{I}{i \le 10}$.

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

1. $P \supset I$ 1. $\{i=0\} \supset i \le 10$ ✓

2. $\neg g \wedge I \supset Q$ 2. $i \ge 10 \wedge i \le 10 \supset i = 10$ ✓

3. $\{g \wedge I\}\ \delta\ \{I\}$

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

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

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

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

$i \le 10$ IS AN INVARIANT