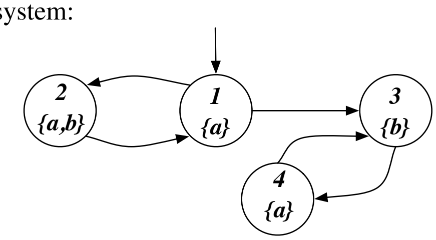
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

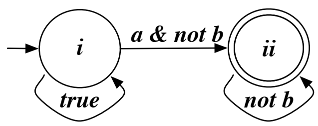
Formal Methods – January 26, 2023

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

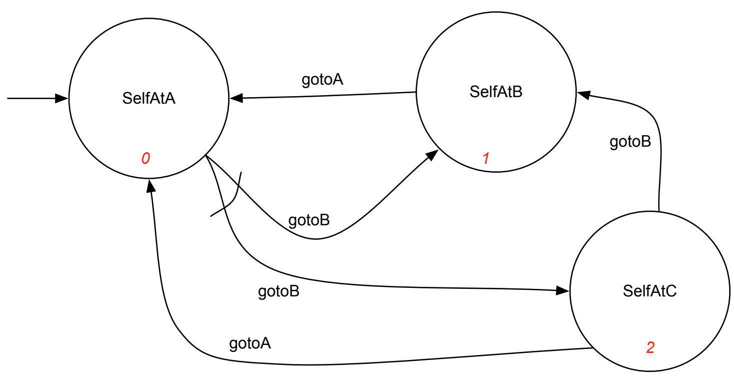
Part 1. Consider the following transition system:



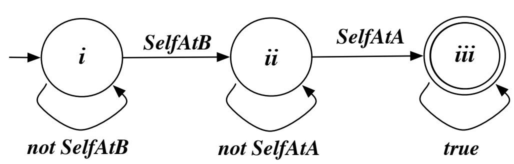
- **Exercise 1.1:** Model check the Mu-Calculus formula: $\nu X.\mu Y.(((a \wedge b) \wedge [next]X) \vee [next]Y)$.
- **Exercise 1.2:** Model check the CTL formula $EF(AG(\neg(a \wedge b)))$, by translating it in Mu-Calculus.
- **Exercise 1.3:** Model check the LTL formula $\Box(a \supset \Diamond b)$, by considering that the Büchi automaton for $\neg(\Box(a \supset \Diamond b))$ 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:

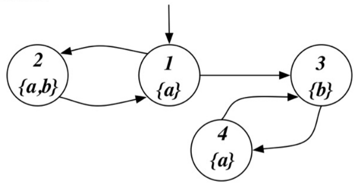


Part 3 Consider the notion of weakest precondition of a program.

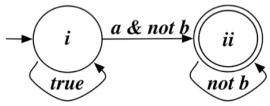
- **Exercise 3.1:** Compute the weakest precondition for getting $\{x = y\}$ by executing the following program:

```
x := y + 1;
if (x > 0 & y >= 0) then {
  x := y - x;
  y := x - y
}
else if (x > 0) then
  x := x - y
```

Part 1. Consider the following transition system:



- **Exercise 1.1:** Model check the Mu-Calculus formula: $\nu X.\mu Y.(((a \wedge b) \wedge [next]X) \vee [next]Y)$.
- **Exercise 1.2:** Model check the CTL formula $EF(AG(\neg(a \wedge b)))$, by translating it in Mu-Calculus.
- **Exercise 1.3:** Model check the LTL formula $\Box(a \supset \Diamond b)$, by considering that the Büchi automaton for $\neg(\Box(a \supset \Diamond b))$ is the one below:



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

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

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

$[Y_0] = \emptyset$

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

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

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

$= ((\{1,2,4\} \cap \{2,3\}) \cap \{1,2,3,4\}) \cup \emptyset = \{2\}$ $\quad [Y_1] = [Y_2] = [X_1] = \{2\}$

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

$[Y_0] = \emptyset$

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

$= ((\{1,2,4\} \cap \{2,3\}) \cap \emptyset) \cup \emptyset = \emptyset$ $\quad [Y_0] = [Y_1] = [X_2] = \emptyset$

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

$[Y_0] = \emptyset$

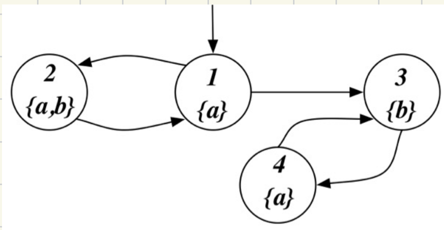
$[Y_1] = (([a] \cap [b]) \cap PREA(NEXT, X_2)) \cup PREA(NEXT, Y_0) =$

$= ((\{1,2,4\} \cap \{2,3\}) \cap \emptyset) \cup \emptyset = \emptyset$ $\quad [Y_0] = [Y_1] = [X_3] = \emptyset$

$[X_2] = [X_3] = \emptyset$

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

2) $\underbrace{EF(\underbrace{AG(\underbrace{\neg(a\wedge b)}_{\alpha}))}_{\beta}}_{\gamma}$



$[\alpha] = [\neg(a\wedge b)] = [\neg a \vee \neg b] = [\neg a] \cup [\neg b] = \{3\} \cup \{1,4\} = \{1,3,4\} = [\alpha]$

$[\beta] = [AG\ \alpha] = [\nu Z.\ \alpha \wedge [NEXT]\, Z]$

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

$[Z_1] = [\alpha] \cap PREA(NEXT, Z_0) =$

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

$[Z_2] = [\alpha] \cap PREA(NEXT, Z_1) =$

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

$[Z_3] = [\alpha] \cap PREA(NEXT, Z_2) =$

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

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

$[\gamma] = [EF\ \beta] = [\mu Z.\ \beta \vee \langle NEXT\rangle Z]$

$[Z_0] = \emptyset$

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

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

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

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

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

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

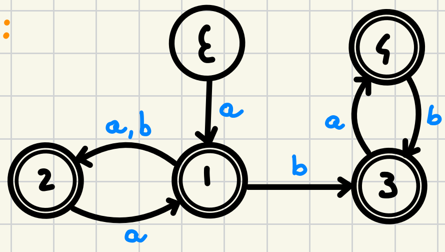
$[Z_4] = [\beta] \cup PREE(NEXT, Z_3) =$

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

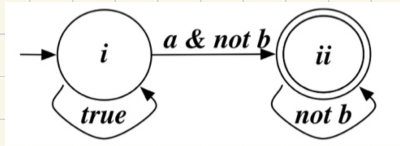
$[Z_3] = [Z_4] = [\gamma] = \{1,2,3,4\}$

$\Upsilon s_1 \in \gamma$? $\rightarrow$ $s_1 \in [\gamma] = \{1,2,3,4\}$? YES!

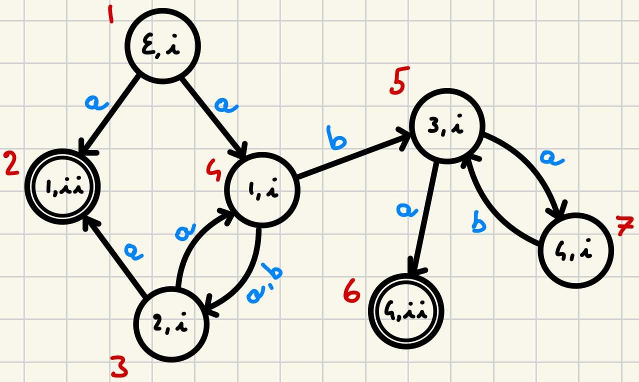
3) A_γ:



$A_{\neg\varphi}$:



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



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

$[X_0] = \{1,2,3,4,5,6,7\}$

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

$[Y_0] = \phi$

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

$= \{2,6\} \cap \{1,3,4,5,7\} \cup \phi = \phi$

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

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

$[Y_0] = \phi$

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

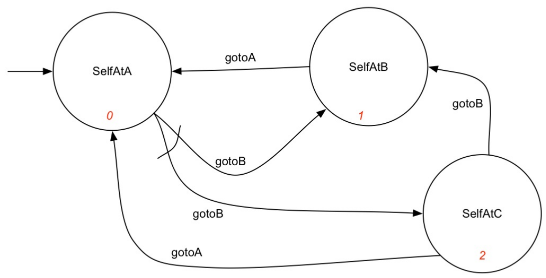
$= \{2,6\} \cap \phi \cup \phi = \phi$

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

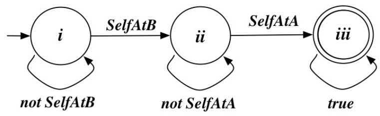
$[X_1] = [X_2] = \phi$

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

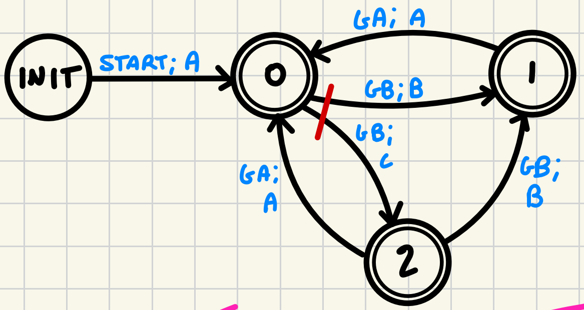
Part 2 Consider the following domain:



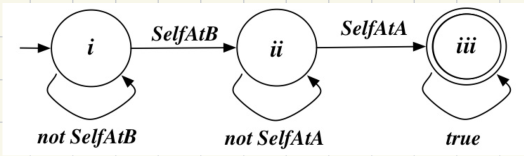
- **Exercise 2.1:** Synthesize a strategy (a plan) for realizing the LTLf formula $\Diamond(SelfAtB \wedge \Diamond(SelfAtA))$, by considering that the corresponding DFA is the one below:



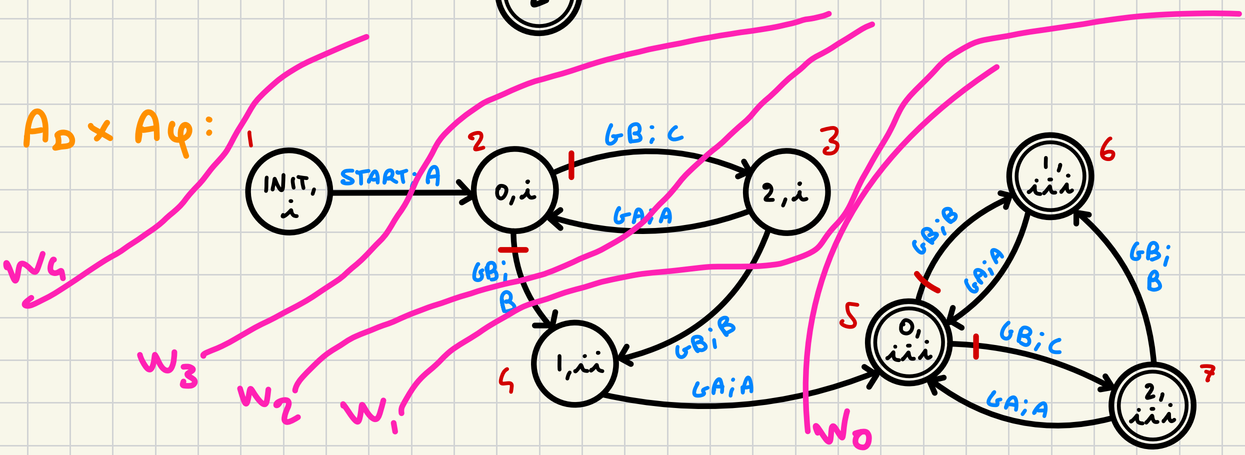
A_D:



A_φ:



$A_D \times A_\varphi$:



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

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

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

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

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

$W_5 = W_4 \cup PREADV(W_4) = \{1, 2, 3, 4, 5, 6, 7\}$

$W_4 = W_5$

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

$w_c(1) = START$
$w_c(2) = GB$
$w_c(3) = GB$
$w_c(4) = GA$
$w_c(5) = WIN$
$w_c(6) = WIN$
$w_c(7) = WIN$

$T = (2^X, S, s_0, \rho, w_c)$

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

$s_0 = \{1\}$

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

$w_c =$

Part 3 Consider the notion of weakest precondition of a program.

- **Exercise 3.1:** Compute the weakest precondition for getting $\{x = y\}$ by executing the following program:

```
x := y + 1;
if (x > 0 & y >= 0) then {
  x := y - x;
  y := x - y
}
else if (x > 0) then
  x := x - y
```

$y=0$

$\{*\}[x/y+1] = \{(y>-1 \wedge y \geq 0 \wedge y=0) \vee ((y \leq -1 \vee y<0) \wedge y>-1 \wedge y=1)\}$

$x = y+1;$

$* \{((x>0 \wedge y \geq 0) \wedge y=0) \vee ((x \leq 0 \vee y<0) \wedge x>0 \wedge x=2y)\}$

IF $(x>0 \wedge y \geq 0)$ THEN {

$\{y=0\}[x/y-x] = \{y=0\}$

$x = y-x;$

$\{x=y\}[y/x-y] = \{y=0\}$

$y = x-y;$

$\{x=y\}$

}

ELSE IF $(x>0)$ THEN

$\{x=y\}[x/x-y] = \{x=2y\}$

$x = x-y;$

$\{x=y\}$

$$wp(\delta, x=y) = y=0$$