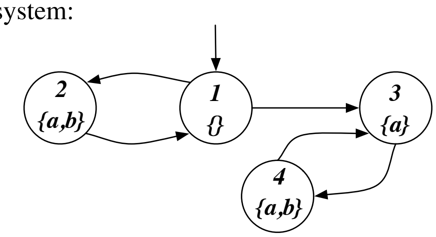
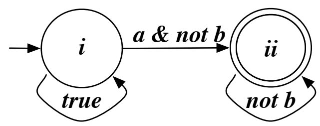
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

Formal Methods

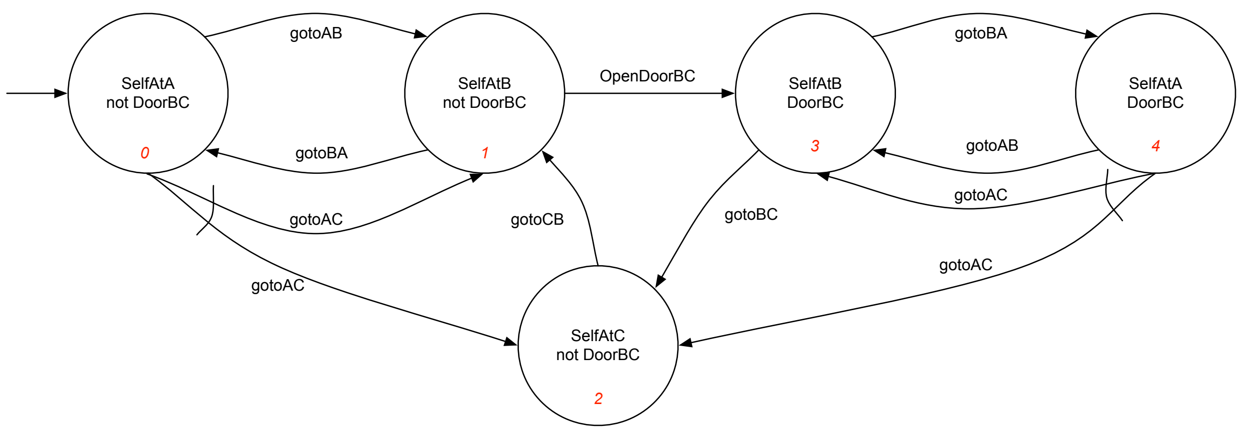
Part 1. Consider the following transition system:



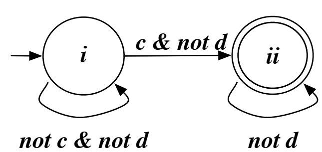
- **Exercise 1.1:** Model check the CTL formula $EG(b \supset EXAFa)$, by translating it in Mu-Calculus.
- **Exercise 1.2:** Model check the LTL formula $\Box(a \supset \Diamond b)$, by considering that the Büchi automaton for $\neg(\Box(a \supset \Diamond b))$ is the one below:



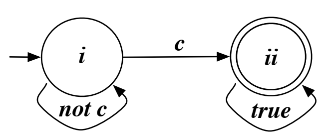
Part 2 Consider the following domain:



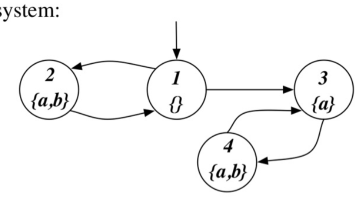
- **Exercise 2.1:** Model check the LTLf formula $\Box(\neg DoorBC) \supset \Box(\neg SelfAtC)$, by considering that the DFA for $\neg(\Box(\neg DoorBC) \supset \Box(\neg SelfAtC)$ is the one below:



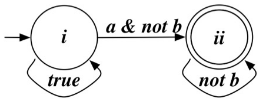
- **Exercise 2.2:** Synthesize a strategy (a plan) for realizing the LTLf formula $\Diamond(SelfAtC)$, by considering that the DFA for $\Diamond(SelfAtC)$ is the one below:



Part 1. Consider the following transition system:



- **Exercise 1.1:** Model check the CTL formula $EG(b \supset EXAFa)$, by translating it in Mu-Calculus.
- **Exercise 1.2:** 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) $$\underbrace{EG(\underbrace{b \supset \underbrace{EX\underbrace{AF\,a}_{\alpha}}_{\beta}}_{\gamma})}_{\delta}$$

$$[\alpha] = [AF\,a] = [\mu Z.\ a \vee [NEXT]Z]$$

$$[Z_0] = \emptyset$$

$$[Z_1] = [a] \cup PREA(NEXT, Z_0) =$$
$$= \{2,3,4\} \cup \emptyset = \{2,3,4\}$$

$$[Z_2] = [a] \cup PREA(NEXT, Z_1) =$$
$$= \{2,3,4\} \cup \{1,3,4\} = \{1,2,3,4\}$$

$$[Z_3] = [a] \cup PREA(NEXT, Z_2) =$$
$$= \{2,3,4\} \cup \{1,2,3,4\} = \{1,2,3,4\}$$

$$[Z_2] = [Z_3] = [\alpha] = \{1,2,3,4\}$$

$$[\beta] = [EX\,\alpha] = [\langle NEXT\rangle \alpha] = PREE(NEXT, \alpha) = \{1,2,3,4\} = [\beta]$$

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

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

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

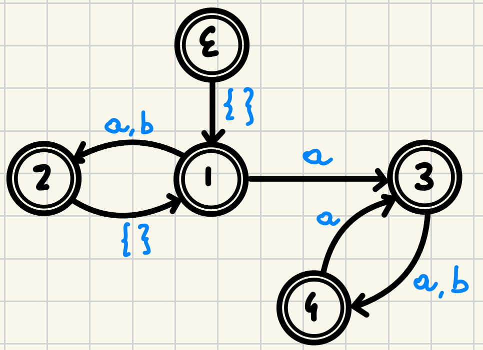
$$[Z_1] = [\gamma] \cap PREE(NEXT, Z_0) =$$
$$= \{1,2,3,4\} \cap \{1,2,3,4\} = \{1,2,3,4\}$$

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

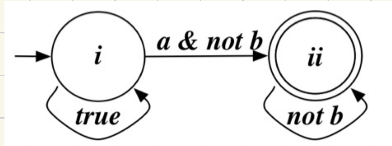
$s_1 \in \delta$? → $s_1 \in [\delta] = \{1,2,3,4\}$? YES!

2)

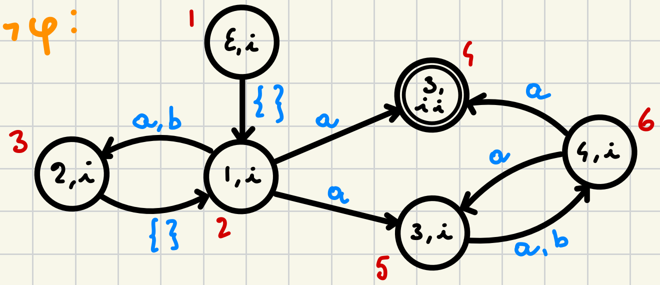
A_γ:



$A_{\neg\varphi}$:



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



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

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

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

$$[Y_0] = \phi$$

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

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

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

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

$$[Y_0] = \phi$$

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

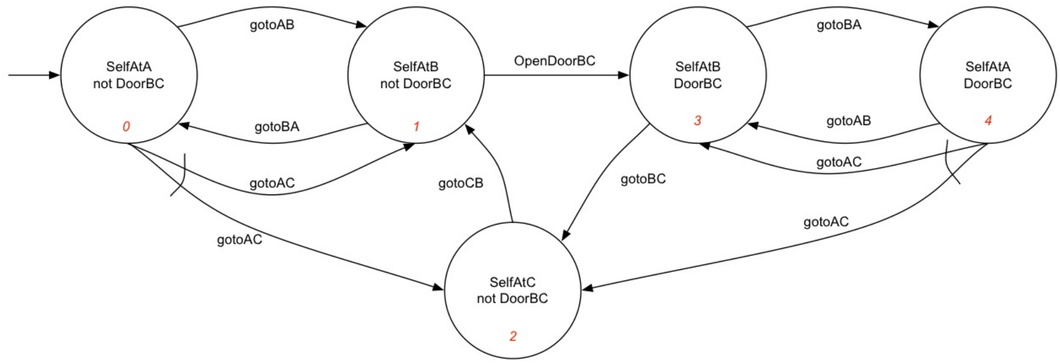
$$= \{4\} \cap \phi = \phi$$

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

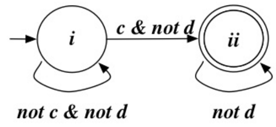
$$[X_1] = [X_2] = \phi$$

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

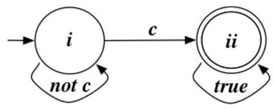
Part 2 Consider the following domain:



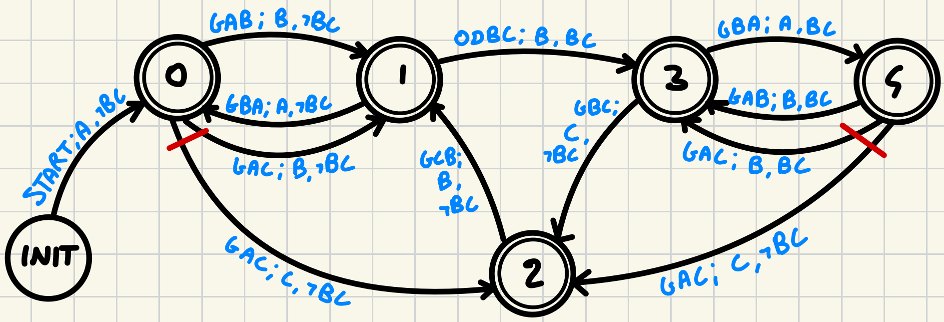
- **Exercise 2.1:** Model check the LTLf formula $\square(\neg DoorBC) \supset \square(\neg SelfAtC)$, by considering that the DFA for $\neg(\square(\neg DoorBC) \supset \square(\neg SelfAtC))$ is the one below:



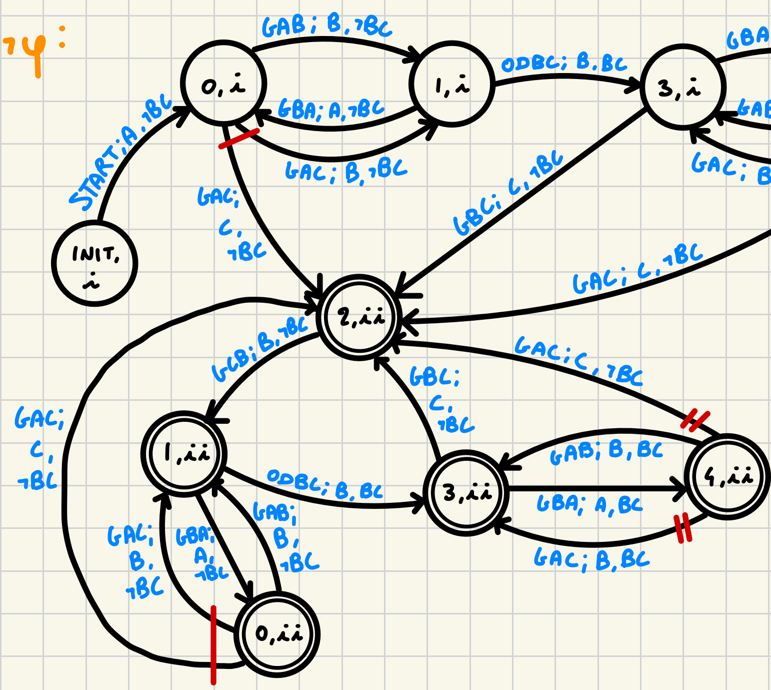
- **Exercise 2.2:** Synthesize a strategy (a plan) for realizing the LTLf formula $\diamond(SelfAtC)$, by considering that the DFA for $\diamond(SelfAtC)$ is the one below:



1) A_D:

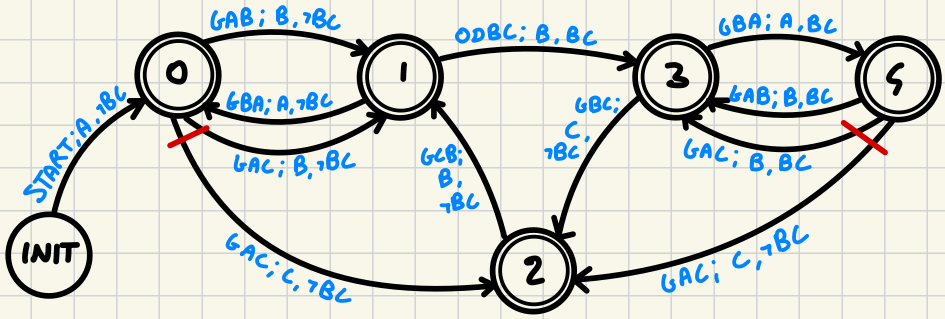


$A_D \times A_{\neg\varphi}$:

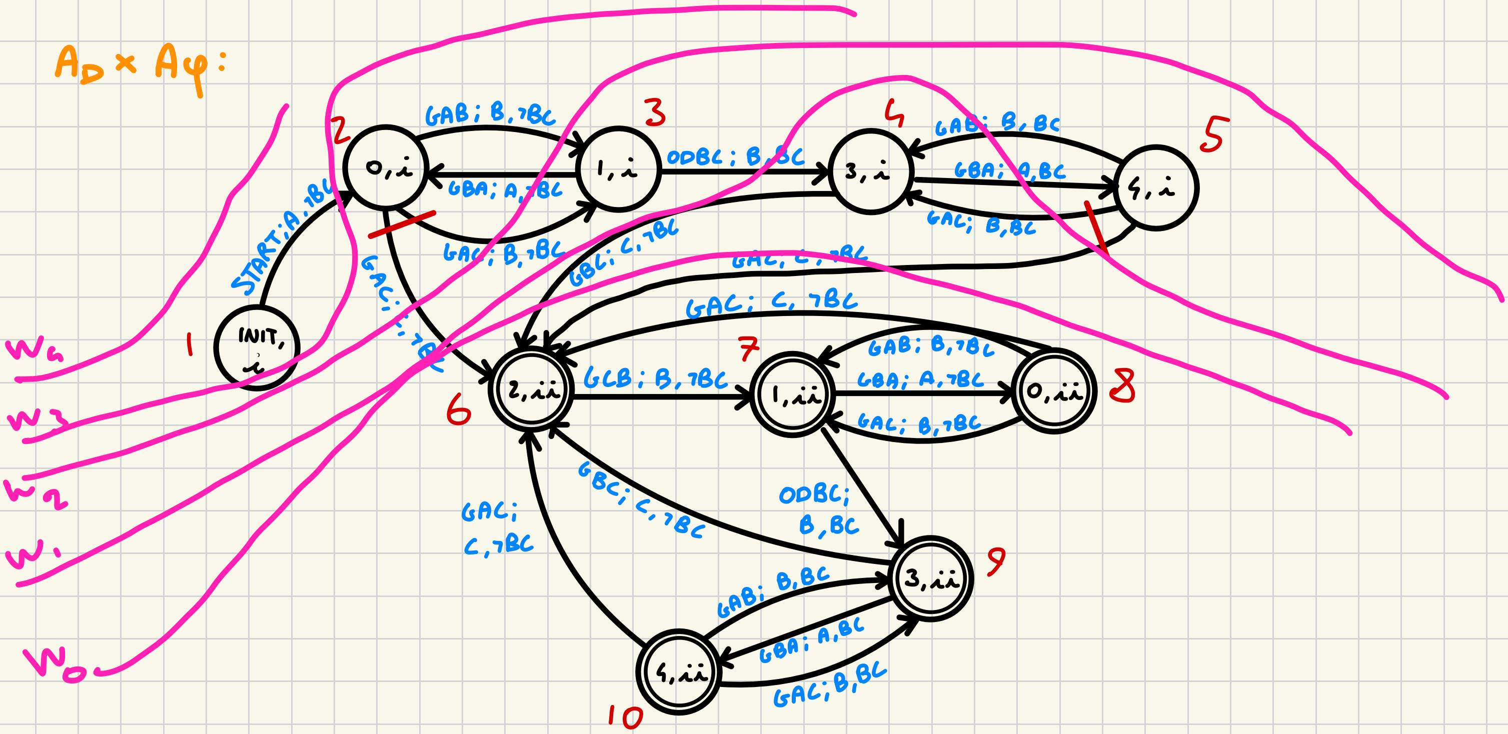


SINCE THERE EXIST A PATH FROM THE INIT TO A FINAL STATE, $\neg\phi$ IS SATISFIABLE AND SO ϕ IS NOT SAT.

2) A_D:



$A_D \times A_\varphi$:



$W_0 = \{6, 7, 8, 9, 10\}$

$W_1 = W_0 \cup \text{PREADV}(W_0) = \{4, 6, 7, 8, 9, 10\}$

$W_2 = W_1 \cup \text{PREADV}(W_1) = \{3, 4, 5, 6, 7, 8, 9, 10\}$

$W_3 = W_2 \cup \text{PREADV}(W_2) = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$W_4 = W_3 \cup \text{PREADV}(W_3) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$W_5 = W_4 \cup \text{PREADV}(W_4) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$W_4 = W_5 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$W(1) = \{\text{START}\}$	$W_c(1) = \text{START}$
$W(2) = \{\text{GAB}, \text{GAC}\}$	$W_c(2) = \text{GAC}$
$W(3) = \{\text{ODBC}\}$	$W_c(3) = \text{ODBC}$
$W(4) = \{\text{GBC}\}$	$W_c(4) = \text{GBC}$
$W(5) = \{\text{GAB}, \text{GAC}\}$	$W_c(5) = \text{GAC}$
$W(6) = \text{WIN}$	$W_c(6) = \text{WIN}$
$W(7) = \text{WIN}$	$W_c(7) = \text{WIN}$
$W(8) = \text{WIN}$	$W_c(8) = \text{WIN}$
$W(9) = \text{WIN}$	$W_c(9) = \text{WIN}$
$W(10) = \text{WIN}$	$W_c(10) = \text{WIN}$

$T = (2^X, S, s_0, p, W_c)$

$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$s_0 = \{1\}$

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

$W_c =$