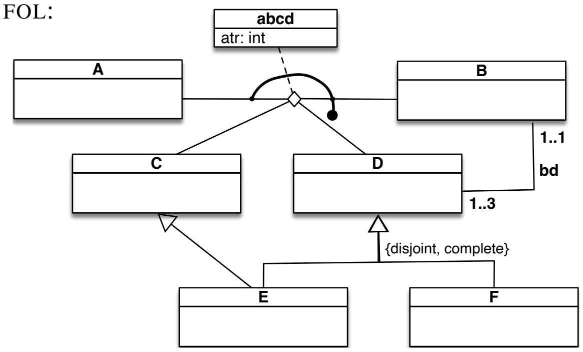
SAPIENZA Università di Roma – MSc. in Engineering in Computer Science

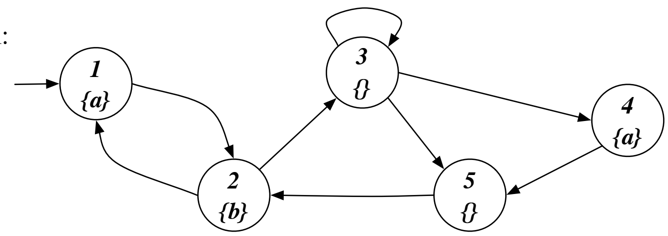
Formal Methods – June 26, 2025

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

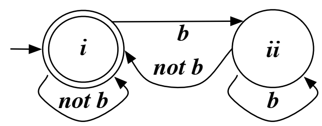
Exercise 1 Express the following UML class diagram in FOL:



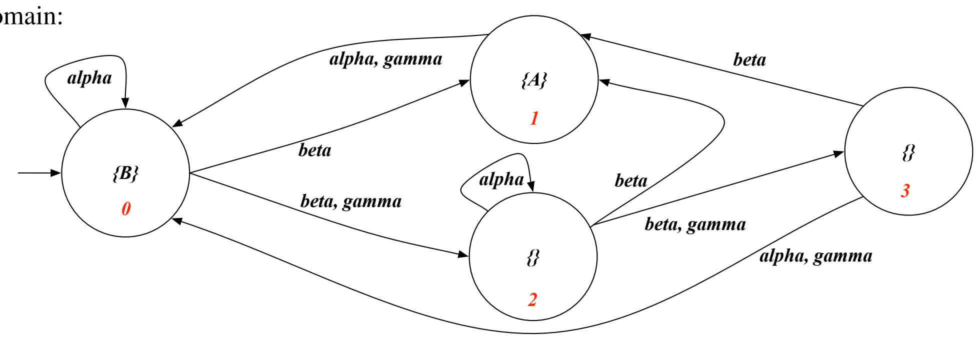
Exercise 2 Consider the following transition system:



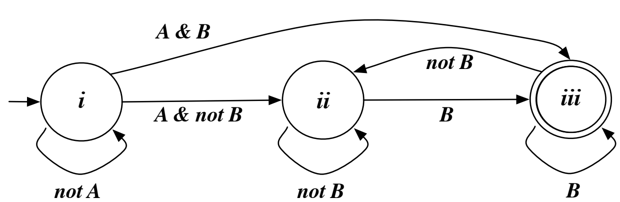
- **Exercise 2.1:** Model check the Mu-Calculus formula: $\nu X.\mu Y.((a \land [next]X) \lor (b \land \langle next \rangle Y))$
- **Exercise 2.2:** Model check the CTL formula $EF(EG(a \land EXb))$, by translating it in Mu-Calculus.
- **Exercise 2.3** Model check the CTL formula $AF(AG(a \supset AXb))$, by translating it in Mu-Calculus.
- **Exercise 2.4:** Model check the LTL formula $\Diamond\Box(b)$, by considering that the Büchi automaton for $\neg\Diamond\Box(b)$ (i.e., $\Box\Diamond(\neg b)$) is:



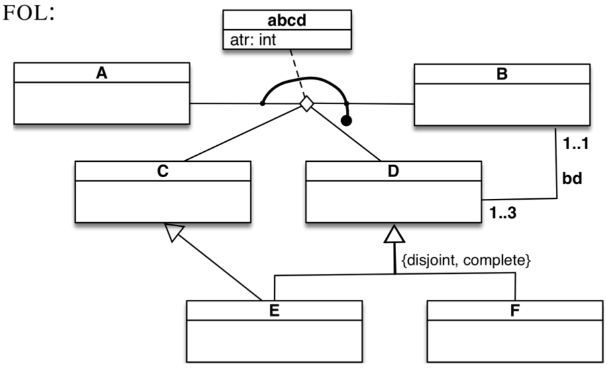
Exercise 3 Consider the following domain:



Synthesize a strategy (a plan) for realizing the LTL$_f$ formula $\Diamond(A \land \Diamond(B \land \bullet false))$, by considering that the corresponding DFA is:



Exercise 1 Express the following UML class diagram in FOL:



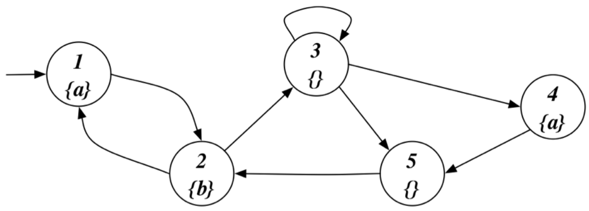
$A(x)$, $B(x)$, $C(x)$, $D(x)$, $E(x)$, $F(x)$, $INT(x)$
$ABCD(x, y, z, w)$
$ATR(x, y, z, w, t)$
$BD(x, y)$

$\forall x, y, z, w.\ ABCD(x, y, z, w) \supset A(x) \wedge B(y) \wedge C(z) \wedge D(w)$
$\forall x, y, z, z', w, w'.\ ABCD(x, y, z, w) \wedge ABCD(x, y, z', w') \supset z = z' \wedge w = w'$
$\forall x, y, z, w, t.\ ATR(x, y, z, w, t) \supset ABCD(x, y, z, w) \wedge INT(t)$
$\forall x, y, z, w.\ ABCD(x, y, z, w) \supset 1 \leq \#\{t \mid ATR(x, y, z, w, t)\} \leq 1$

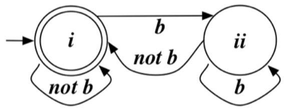
$\forall x, y.\ BD(x, y) \supset B(x) \wedge D(y)$
$\forall x.\ B(x) \supset 1 \leq \#\{y \mid BD(x, y)\} \leq 3$
$\forall y.\ D(y) \supset 1 \leq \#\{x \mid BD(x, y)\} \leq 1$

$\forall x.\ E(x) \supset D(x) \wedge C(x) \wedge \neg F(x)$
$\forall x.\ F(x) \supset D(x)$
$\forall x.\ D(x) \supset E(x) \vee F(x)$

Exercise 2 Consider the following transition system:



- **Exercise 2.1:** Model check the Mu-Calculus formula: $\nu X.\mu Y.((a \wedge [next]X) \vee (b \wedge \langle next \rangle Y))$
- **Exercise 2.2:** Model check the CTL formula $EF(EG(a \wedge EXb))$, by translating it in Mu-Calculus.
- **Exercise 2.3** Model check the CTL formula $AF(AG(a \supset AXb))$, by translating it in Mu-Calculus.
- **Exercise 2.4:** Model check the LTL formula $\Diamond\Box(b)$, by considering that the Büchi automaton for $\neg\Diamond\Box(b)$ (i.e., $\Box\Diamond(\neg b)$) is:



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

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

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

$[Y_0] = \emptyset$

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

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

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

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

$[Y_3] = ([a] \cap PREA(NEXT, X_0)) \vee ([b] \cap PREE(NEXT, Y_2)) =$

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

$[Y_2] = [Y_3] = [X_1] = \{1,2,4\}$

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

$[Y_0] = \emptyset$

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

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

$[Y_2] = ([a] \cap PREA(NEXT, X_1)) \vee ([b] \cap PREE(NEXT, Y_1)) =$

$= (\{1,4\} \cap \{1,5\}) \cup (\{2\} \cap \{2\}) = \{1,2\}$

$[Y_3] = ([a] \cap PREA(NEXT, X_1)) \vee ([b] \cap PREE(NEXT, Y_2)) =$

$= (\{1,4\} \cap \{1,5\}) \cup (\{2\} \cap \{1,2,5\}) = \{1,2\}$

$[Y_2] = [Y_3] = [X_2] = \{1,2\}$

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

$[Y_0] = \phi$

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

$= (\{1,4\} \cap \{1,5\}) \cup (\{2\} \cap \phi) = \{1\}$

$[Y_2] = ([a] \cap PREA(NEXT, X_2)) \vee ([b] \cap PREE(NEXT, Y_1)) =$

$= (\{1,4\} \cap \{1,5\}) \cup (\{2\} \cap \{2\}) = \{1,2\}$

$[Y_3] = ([a] \cap PREA(NEXT, X_2)) \vee ([b] \cap PREE(NEXT, Y_2)) =$

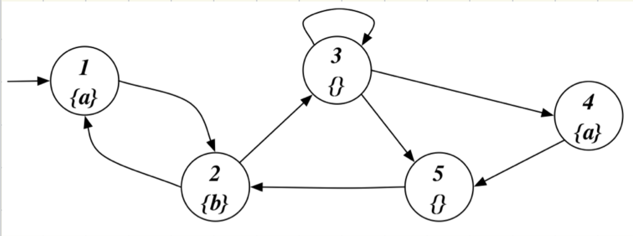
$= (\{1,4\} \cap \{1,5\}) \cup (\{2\} \cap \{1,2,5\}) = \{1,2\}$

$[Y_2] = [Y_3] = [X_3] = \{1,2\}$

$[X_2] = [X_3] = \{1,2\}$

$s_1 \in [\varphi] = \{1,2\}$? YES!

2) $EF(EG(\underbrace{a \wedge \underbrace{EX\, b}_{\alpha}}_{\beta})_{\gamma})_{\delta}$



$[\alpha] = [EX\, b] = [\langle NEXT \rangle b] = PREE(NEXT, b) = \{1,5\} = [\alpha]$

$[\beta] = [a \wedge \alpha] = [a] \cap [\alpha] = \{1,4\} \cap \{1,5\} = \{1\} = [\beta]$

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

$[Z_0] = \{1,2,3,4,5\}$

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

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

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

$= \{1\} \cap \{2\} = \emptyset$

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

$= \{1\} \cap \emptyset = \emptyset$

$[Z_2] = [Z_3] = [\gamma] = \emptyset$

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

$[Z_0] = \emptyset$

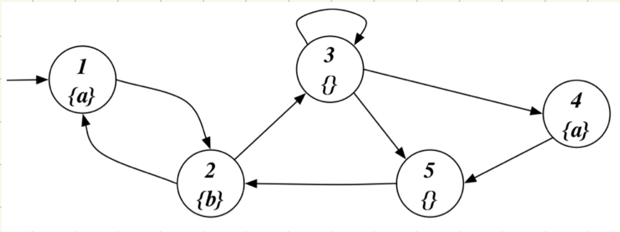
$[Z_1] = [\gamma] \cup PREE(NEXT, Z_0) =$

$= \emptyset \cup \emptyset = \emptyset$

$[Z_0] = [Z_1] = [\delta] = \emptyset$

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

3) $\underbrace{AF(\underbrace{AG\,(\underbrace{a \supset \underbrace{AXb}_{\alpha}}_{\beta})}_{\gamma})}_{\delta}$



$[\![\alpha]\!] = [\![AX\,b]\!] = [\![[NEXT]\,b]\!] = \mathrm{PREA}(NEXT, b) = \{1,5\} = [\![\alpha]\!]$

$[\![\beta]\!] = [\![a \supset \alpha]\!] = [\![\neg a]\!] \cup [\![\alpha]\!] = \{2,3,5\} \cup \{1,5\} = \{1,2,3,5\} = [\![\beta]\!]$

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

$[\![Z_0]\!] = \{1,2,3,4,5\}$

$[\![Z_1]\!] = [\![\beta]\!] \cap \mathrm{PREA}(NEXT, Z_0) =$

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

$[\![Z_2]\!] = [\![\beta]\!] \cap \mathrm{PREA}(NEXT, Z_1) =$

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

$[\![Z_3]\!] = [\![\beta]\!] \cap \mathrm{PREA}(NEXT, Z_2) =$

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

$[\![Z_4]\!] = [\![\beta]\!] \cap \mathrm{PREA}(NEXT, Z_3) =$

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

$[\![Z_5]\!] = [\![\beta]\!] \cap \mathrm{PREA}(NEXT, Z_4) =$

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

$[\![Z_4]\!] = [\![Z_5]\!] = [\![\gamma]\!] = \phi$

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

$[\![Z_0]\!] = \phi$

$[\![Z_1]\!] = [\![\gamma]\!] \cup \mathrm{PREA}(NEXT, Z_0) =$

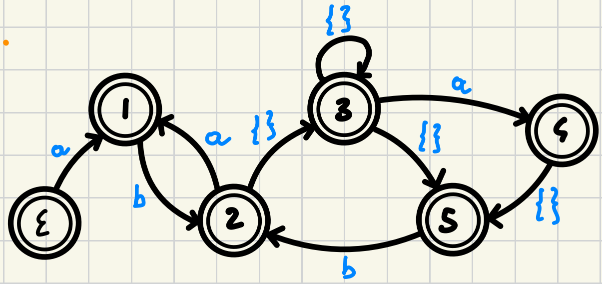
$= \phi \cup \phi = \phi$

$[\![Z_0]\!] = [\![Z_1]\!] = [\![\delta]\!] = \phi$

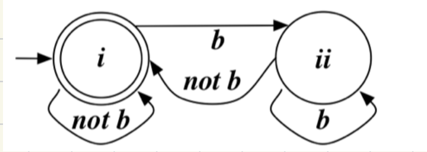
$\Upsilon_{s_1} \in [\![\delta]\!] = \phi$? **NO!**

4)

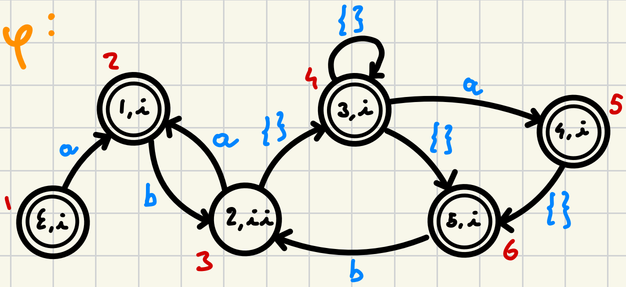
A_γ:



$A_{\neg\varphi}$:



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



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

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

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

$[Y_0] = \emptyset$

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

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

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

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

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

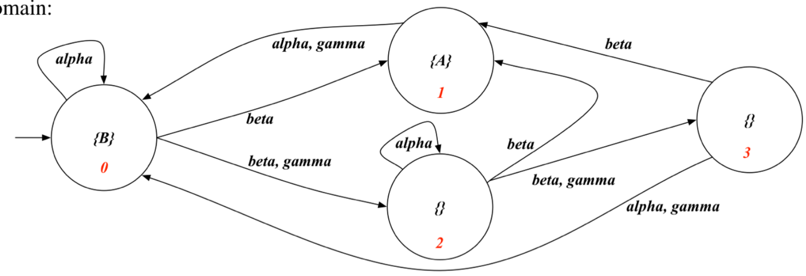
$= \{1,2,4,5,6\} \cap \{1,2,3,4,5,6\} \cup \{1,2,3,4,5,6\} = \{1,2,3,4,5,6\}$

$[Y_2] = [Y_3] = [X_1] = \{1,2,3,4,5,6\}$

$[X_1] = [X_2] = \{1,2,3,4,5,6\}$

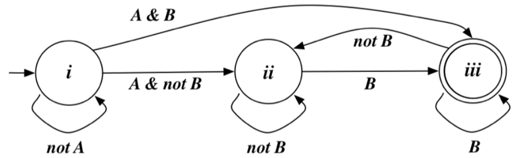
$s_1 \in [\varphi] = \{1,2,3,4,5,6\}$? YES!

Exercise 3 Consider the following domain:

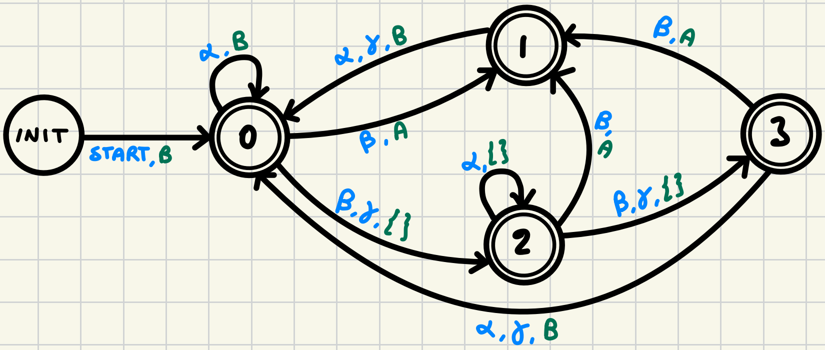


Synthesize a strategy (a plan) for realizing the LTL_f formula $\Diamond(A \wedge \Diamond(B \wedge \bullet false))$, by considering that the corresponding DFA is:

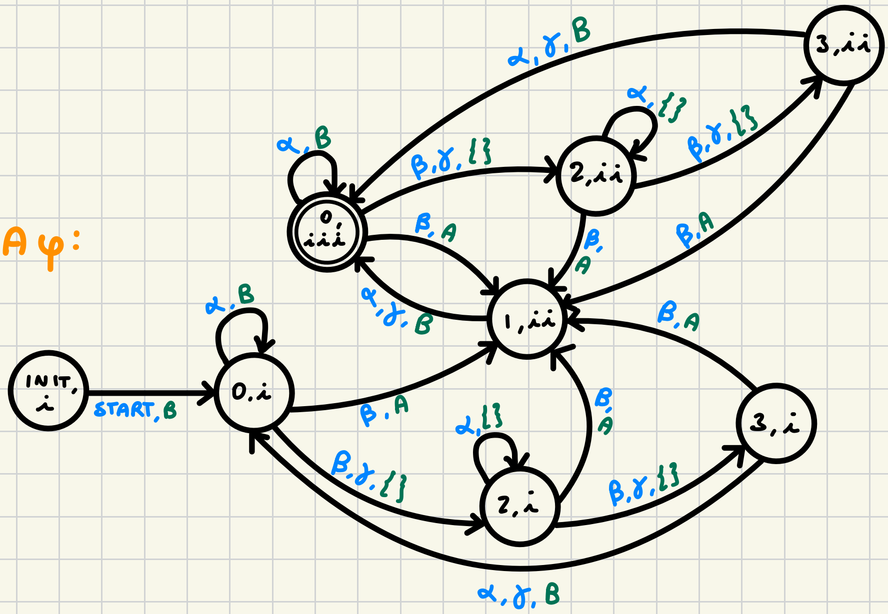
$A\varphi$



A_D:



$A_D \times A\varphi$:



$W_0 = \{(0, iii)\}$

$W_1 = W_0 \cup \text{PREADV}(W_0) = \{(0, iii), (1, ii), (3, ii)\}$

$W_2 = W_1 \cup \text{PREADV}(W_1) = \{(0, iii), (1, ii), (3, ii), (2, ii), (3, i)\}$

$W_3 = W_2 \cup \text{PREADV}(W_2) = \{(0, iii), (1, ii), (3, ii), (2, ii), (3, i), (2, i)\}$

$W_4 = W_3 \cup \text{PREADV}(W_3) = \{(0, iii), (1, ii), (3, ii), (2, ii), (3, i), (2, i), (0, i)\}$

$W_5 = W_3 \cup \text{PREADV}(W_3) = \{(0, iii), (1, ii), (3, ii), (2, ii), (3, i), (2, i), (0, i), (\text{INIT}, i)\}$

$W_6 = W_5 \cup \text{PREADV}(W_5) = \{(0, iii), (1, ii), (3, ii), (2, ii), (3, i), (2, i), (0, i), (\text{INIT}, i)\}$

$W_5 = W_6$

$$
\begin{aligned}
W(\text{INIT}, i) &= \{\text{START}\} \\
W(0,i) &= \{\beta, \gamma\} \\
W(2,i) &= \{\beta, \gamma\} \\
W(3,i) &= \{\beta\} \\
W(2,ii) &= \{\beta, \gamma\} \\
W(3,ii) &= \{\alpha, \gamma\} \\
W(1,ii) &= \{\alpha, \gamma\} \\
W(0,iii) &= \text{WIN}
\end{aligned}
$$

$$
\begin{aligned}
W_c(\text{INIT}, i) &= \text{START} \\
W_c(0,i) &= \beta, \gamma \\
W_c(2,i) &= \beta, \gamma \\
W_c(3,i) &= \beta \\
W_c(2,ii) &= \beta \\
W_c(3,ii) &= \alpha, \gamma \\
W_c(1,ii) &= \alpha, \gamma \\
W_c(0,iii) &= \text{WIN}
\end{aligned}
$$

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

$$S = \{(\text{INIT}, i), (0,i), (2,i), (3,i), (2,ii), (3,ii), (1,ii), (0,iii)\}$$

$$s_0 = \{(\text{INIT}, i)\}$$

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