COL:750/7250

Foundations of Automatic Verification

Instructor: Priyanka Golia

Course Webpage

https://priyanka-golia.github.io/teaching/COL-750-COL7250/index.html

CTL Syntax

F, F_1 = True |

p (atomic proposition) |

$F_1 \wedge F, F_1 \vee F, F \rightarrow F_1, F_1 \leftrightarrow F$ |

$\neg F$ |

$\forall \mathbf{N}\ F \mid \forall \Box F \mid \forall \Diamond F \mid \forall (F\ \mathbf{U}\ F_1) \mid$

$\exists \mathbf{N}\ F \mid \exists \Box F \mid \exists \Diamond F \mid \exists (F\ \mathbf{U}\ F_2)$

$\exists \Diamond \Box F$ Not a WWF!!

$\exists \Diamond (\mathbf{N}\ F)$ Not a WWF!!

CTL : Semantics

Semantics with respect to a given Kripke Structure M

Let $\pi = s_0, s_1, s_2, \ldots$ $\pi(i) = s_i$ State at i^{th} level. $\pi^i = s_i, s_{i+1}, s_{i+2}, \ldots$ Suffix of π

$< M, s_o > \models p$ Iff $p \in L(s_o)$ $< M, s_i > \models p$ Iff $p \in L(s_i)$

$< M, s_i > \models \forall \mathbf{N}\, F_1$ Iff $\forall \pi \in \{s_i, s_{i+1}, s_{i+2}, \ldots, \}$ $< M, s_{i+1} > \models F_1$

$< M, s_i > \models \exists \mathbf{N}\, F_1$ Iff $\exists \pi \in \{s_i, s_{i+1}, s_{i+2}, \ldots, \}$ $< M, s_{i+1} > \models F_1$

$< M, s_i > \models \forall \Box F_1$ Iff $\forall \pi \in \{s_i, s_{i+1}, s_{i+2}, \ldots, \}$ $\forall j \geq i, < M, s_j > \models F_1$

$< M, s_i > \models \exists \Box F_1$ Iff $\exists \pi \in \{s_i, s_{i+1}, s_{i+2}, \ldots, \}$ $\forall j \geq i, < M, s_j > \models F_1$

$< M, s_i > \models \forall \Diamond F_1$ Iff $\forall \pi \in \{s_i, s_{i+1}, s_{i+2}, \ldots, \}$ $\exists j \geq i, < M, s_j > \models F_1$

$< M, s_i > \models \exists \Diamond F_1$ Iff $\exists \pi \in \{s_i, s_{i+1}, s_{i+2}, \ldots, \}$ $\exists j \geq i, < M, s_j > \models F_1$

CTL : Semantics

Semantics with respect to a given Kripke Structure M

Let $\pi = s_0, s_1, s_2, \ldots$ $\pi(i) = s_i$ State at i^{th} level. $\pi^i = s_i, s_{i+1}, s_{i+2}, \ldots$ Suffix of π

$< M, s_o > \models p$ Iff $p \in L(s_o)$ $< M, s_i > \models p$ Iff $p \in L(s_i)$

$< M, s_i > \models \forall(F \textbf{ U } F_1)$ Iff $\forall \pi \in \{s_i, s_{i+1}, s_{i+2}, \ldots, \}$

$\exists j \geq i, < M, s_j > \models F_1 \ \& \ \forall \ i \leq k < j, < M, s_k > \models F$

$< M, s_i > \models \exists \ (F \textbf{ U } F_1)$ Iff $\exists \pi \in \{s_i, s_{i+1}, s_{i+2}, \ldots, \}$

$\exists j \geq i, < M, s_j > \models F_1 \ \& \ \forall \ i \leq k < j, < M, s_k > \models F$

CTL :Examples

Safety: "something bad will never happen"

$$\neg(\exists \Diamond p) \equiv \forall \Box \neg p$$

Reactor_temp is never going to be above 1000.

$$\forall \Box \neg (ReactorTemp > 1000)$$

If car takes left, then immediately car should not take right.

$$\forall \Box \neg (left \ \wedge \ \exists \, \mathbf{N} \ right)$$

$$\neg \exists \Diamond \neg (left \ \wedge \ \forall \, \mathbf{N} \ right)$$

CTL :Examples

Liveness: “something good will happen”

$$\forall \Diamond p$$

All students will get their degree

$$\forall \Diamond (Student \wedge degree)$$

If you start something you will eventually finish it.

$$\forall \Box (start \rightarrow \forall \Diamond Finish)$$

CTL : Formula Equivalence

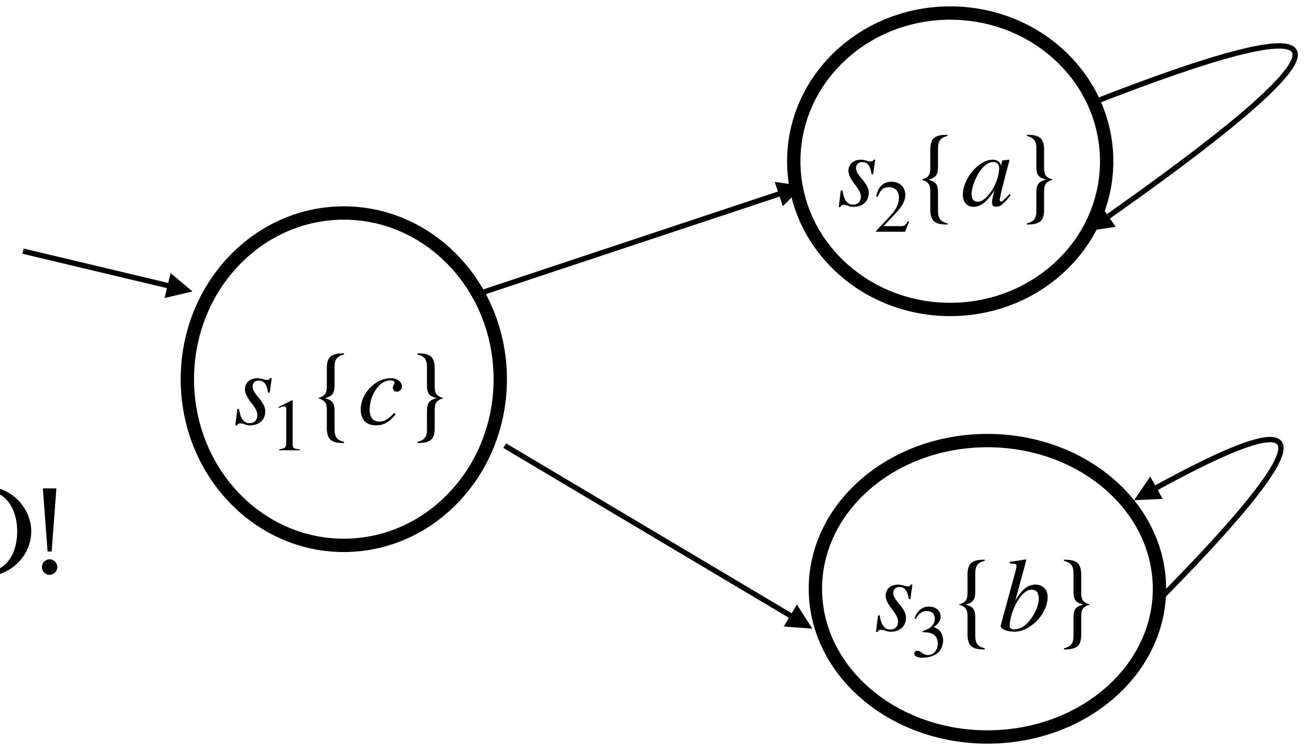
The formulae F_1, F_2 are said to be semantically equivalent if any state in any model that satisfies one also satisfies the other.

$$F_1 \equiv F_2$$

$$\exists\Diamond(a \wedge b) \equiv \exists\Diamond a \wedge \exists\Diamond b$$

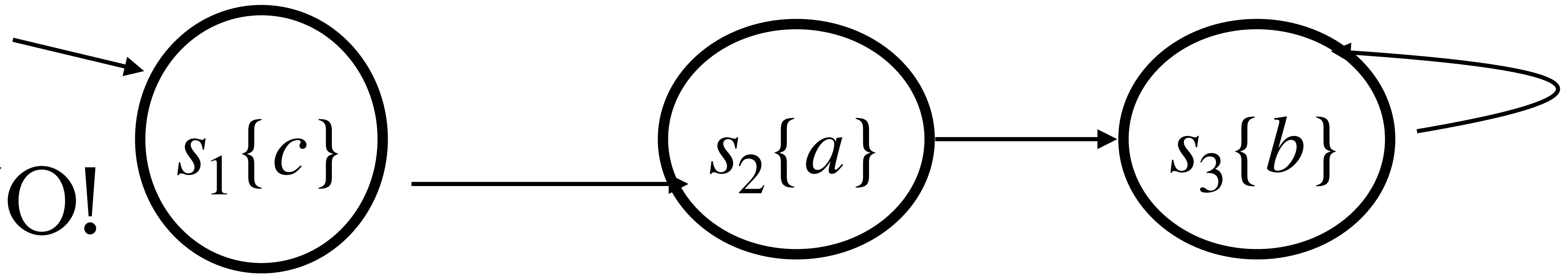
ψ

NO!



$$\forall\Diamond(a \wedge b) \equiv \forall\Diamond a \wedge \forall\Diamond b$$

NO!



CTL : Formula Equivalence

$$\forall \Box (a \wedge b) \equiv \forall \Box a \wedge \forall \Box b$$

$$< M, s_i > \models \forall \Box (a \wedge b)$$

$$\equiv \forall \pi \in \{s_o, s_1, s_2, \ldots, \} \quad \forall j \geq i, < M, s_j > \models (a \wedge b)$$

$$\equiv \forall \pi \in \{s_o, s_1, s_2, \ldots, \} \quad \forall j \geq i, (< M, s_j > \models (a) \wedge < M, s_j > \models (b))$$

$$\equiv \forall \pi \in \{s_o, s_1, s_2, \ldots, \}$$
$$\forall j \geq i, < M, s_j > \models (a) \wedge \forall \pi \in \{s_o, s_1, s_2, \ldots, \} \forall j \geq i, < M, s_j > \models (b)$$

$$\equiv < M, s_i > \models \forall \Box a \wedge \forall \Box b$$

$$\forall \Box (a \wedge b) \equiv \forall \Box a \wedge \forall \Box b$$

CTL : Formula Equivalence

$$\exists\lozenge(a \vee b) \stackrel{?}{\equiv} \exists\lozenge a \vee \exists\lozenge b$$

$$\forall\mathbf{N}\forall\square a \stackrel{?}{\equiv} \forall\square\forall\mathbf{N}a$$

$$\exists\mathbf{N}\exists\square a \stackrel{?}{\equiv} \exists\square\exists\mathbf{N}a$$

CTL : Weak Until

How to write Until in terms of equivalent weak until?

$$F_1 \, \mathbf{U} \, F_2 \equiv (F_1 \, \mathbf{W} \, F_2) \wedge \Diamond F_2$$

$$F_1 \, \mathbf{W} \, F_2 \equiv (F_1 \, \mathbf{U} \, F_2) \vee \Box F_1$$

$$\neg(F_1 \, \mathbf{U} \, F_2) \equiv (F_1 \wedge \neg F_2) \, \mathbf{U} \, (\neg F_1 \wedge \neg F_2) \vee \Box (F_1 \wedge \neg F_2)$$

$$\equiv (F_1 \wedge \neg F_2) \, \mathbf{W} \, (\neg F_1 \wedge \neg F_2)$$

$$\neg(F_1 \, \mathbf{W} \, F_2) \equiv (F_1 \wedge \neg F_2) \, \mathbf{W} \, (\neg F_1 \wedge \neg F_2) \wedge \Diamond(\neg F_1 \wedge \neg F_2)$$

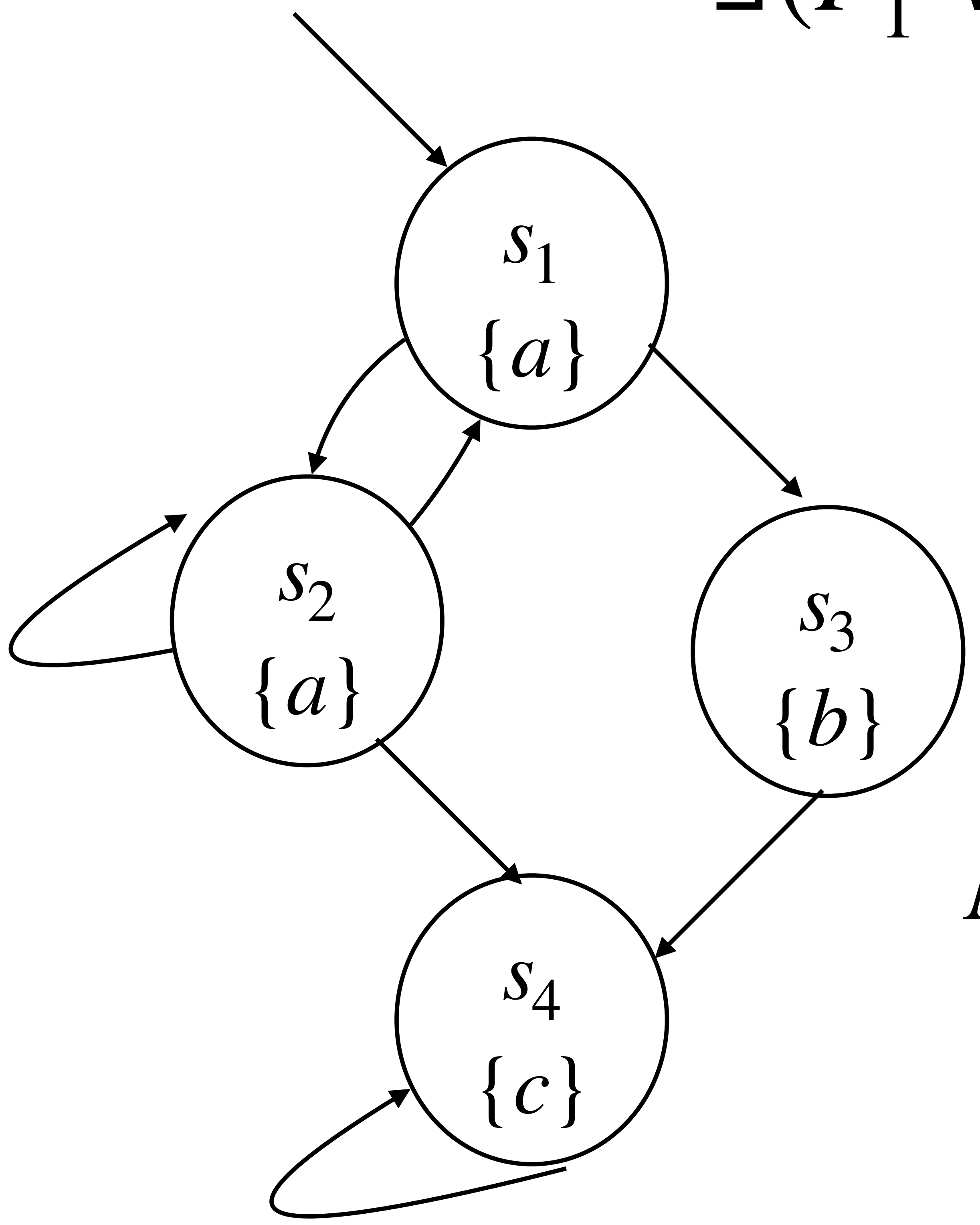
$$\equiv (F_1 \wedge \neg F_2) \, \mathbf{U} \, (\neg F_1 \wedge \neg F_2)$$

CTL : Weak Until

$$\neg(F_1\ \mathbf{W}\ F_2) \equiv (F_1 \wedge \neg F_2)\ \mathbf{U}\ (\neg F_1 \wedge \neg F_2)$$

$$\forall(F_1\ \mathbf{W}\ F_2) \equiv \neg\exists(F_1 \wedge \neg F_2)\ \mathbf{U}\ (\neg F_1 \wedge \neg F_2)$$

$$\exists(F_1\ \mathbf{W}\ F_2) \equiv \neg\forall(F_1 \wedge \neg F_2)\ \mathbf{U}\ (\neg F_1 \wedge \neg F_2)$$

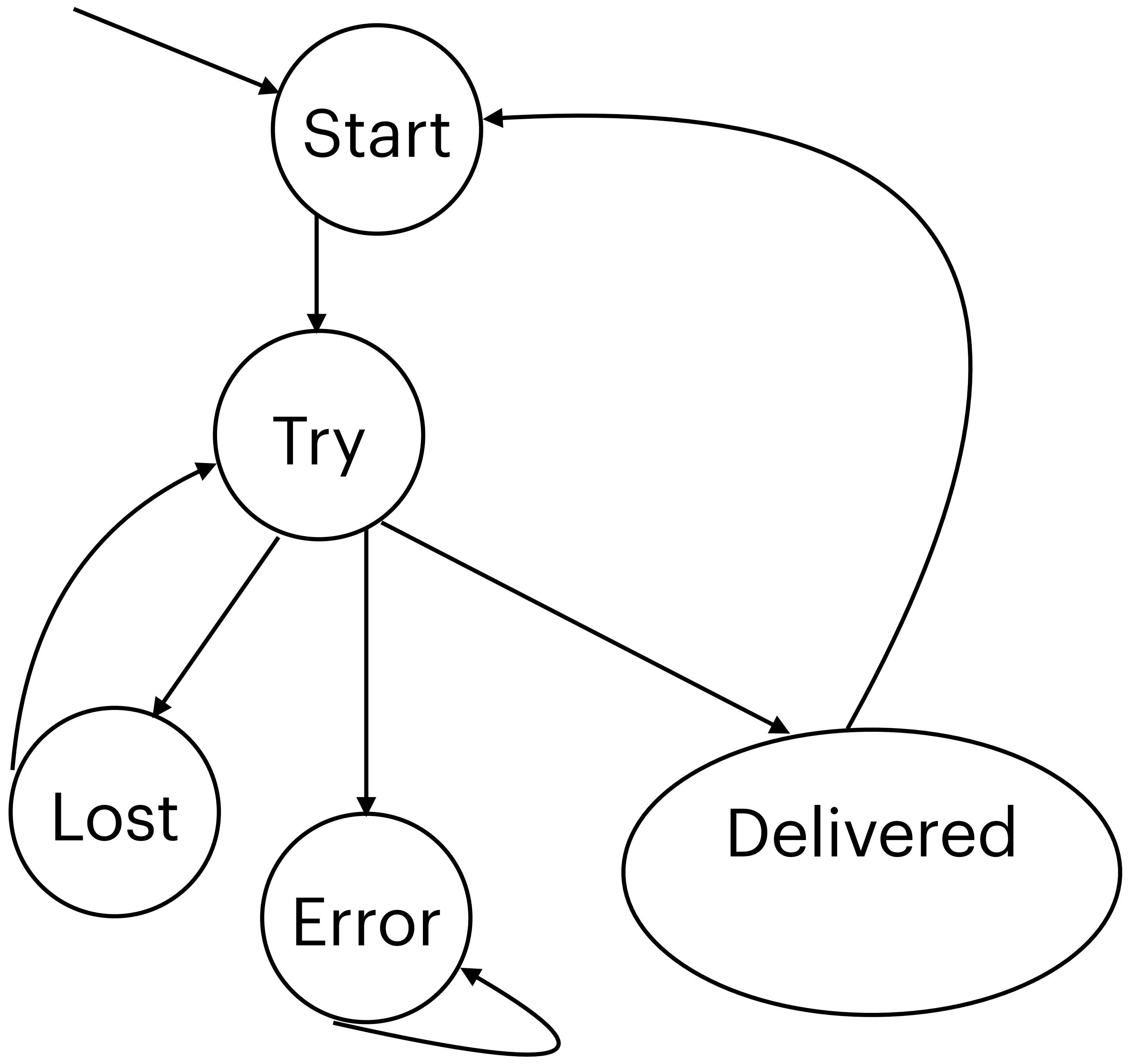


$M \overset{?}{\models} \forall\Diamond\exists(a\mathbf{W}c)$ YES

$M \overset{?}{\models} \exists(a\mathbf{W}\ \exists\Diamond b)$ YES

$M \overset{?}{\models} \forall((\exists\mathbf{N}(b \vee c))\mathbf{W}\ (a \wedge b))$ YES

CTL : Example



$M \overset{?}{\models} \forall \square \forall \lozenge start$ No!

"Infinitely often start"

$M \overset{?}{\models} \exists \lozenge \forall \square \neg start$ No!

After introducing "error" state.

$M \overset{?}{\models} \exists \lozenge \forall \square \neg start$ Yes!

$M \overset{?}{\models} \forall \mathbf{N} \exists \mathbf{N} \forall \square \neg start$ Yes!