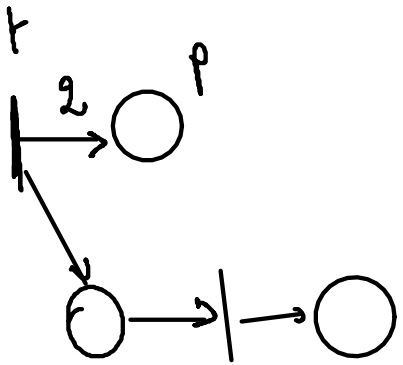


ABSTRACTION

REACHABILITY ⟶ COVERABILITY

p

[φ]

[1]

[2]

[3]

⋮

FINITE

p

[φ]

[2]

[4]

⋮

p

[φ]

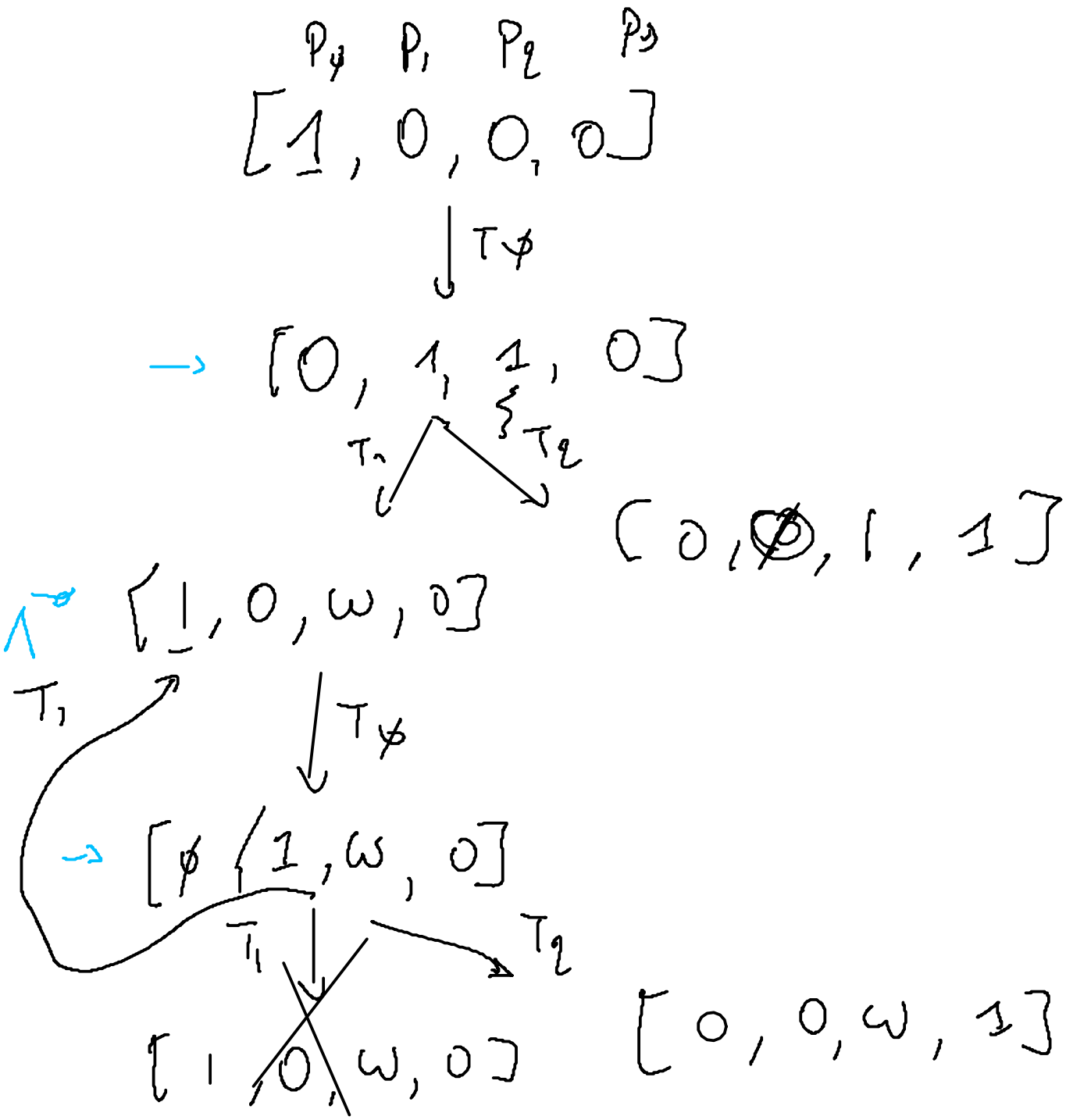
[ω] ←

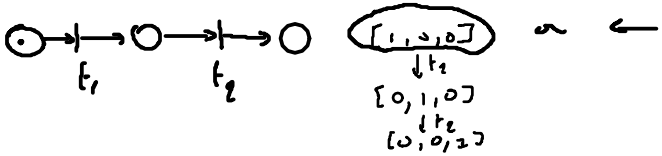
✕

REACHABILITY STATE

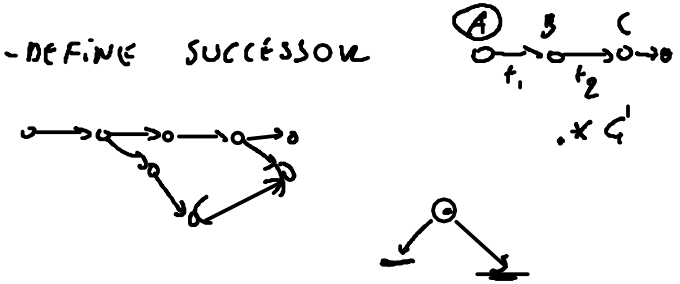
REACHABLE ([3]) ?

[3, ∅, ∗]


P_0 P_1 P_2 P_3
[1, 0, 0, 0]
T_0
[0, 1, 1, 0]
T_1
T_2
[0, ∅, 1, 1]
[1, 0, ω, 0]
T_1
T_0
[∅, {1, ω}, 0]
T_1
T_2
[1, 0, ω, 0]
[0, 0, ω, 1]



- "TEMPORAL" LOGIC — ORDERING OF EVENTS
- LINEAR LOGIC — EACH MOMENT IN "TIME" HAS A WELL-DEFINE SUCCESSOR
- BRANCHING LOGIC — MULTIPLE POSSIBLE TIME COURSES



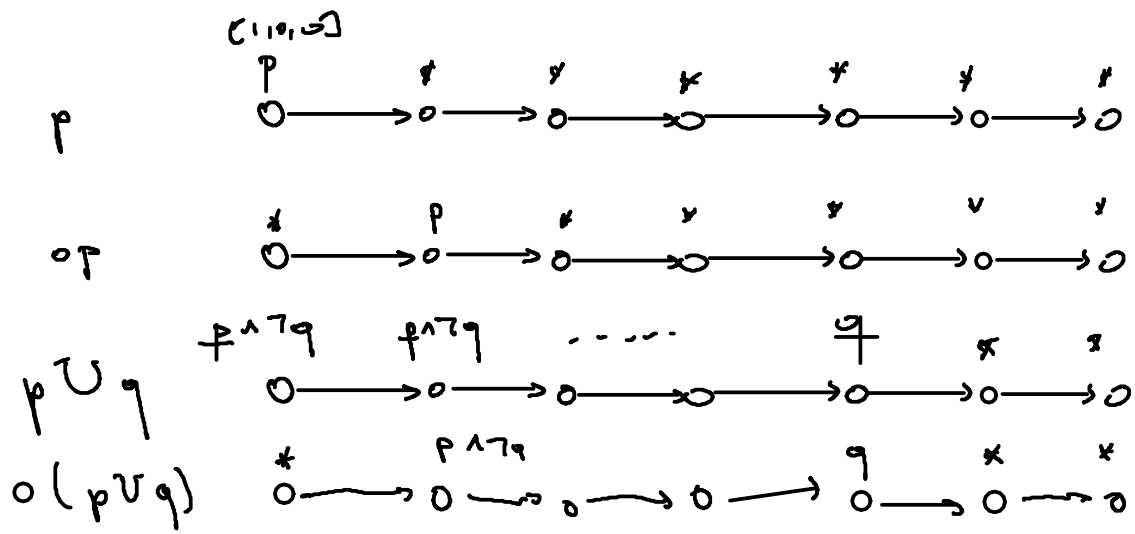
LTL : LINEAR TEMPORAL LOGIC (PNUELI 1970s)

CTL : COMPUTATION TREE LOGIC (BRANCHING TIME)

NEXT UNTIL

PROPOSITION p $\varphi ::= \text{TRUE} \mid \text{ATOMIC } p \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi_1 \mathcal{U} \varphi_2$ LTL

$\bigcirc$ X



$\bigcirc\bigcirc\bigcirc p$

SATISFY ?

PN $\Rightarrow$ LTL

REACH COVERAGE — CHECK — AUTOM.

Y WITNESS — N COUNTER-EXAMPLE

$\neg\varphi \mathcal{U} \varphi$

$\neg\varphi \wedge \neg\varphi$

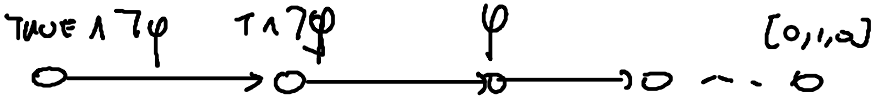
DERIVED OPERATORS

U $\varphi_1 \, U \, \varphi_2$ ¬

X $\circ \varphi$

EVENTUALLY φ F $\Diamond \varphi$:= TRUE U φ

ALWAYS / GLOBALLY φ G $\Box \varphi$:=



NEVER (EVENTUALLY (¬ φ))

F [0,1,0]

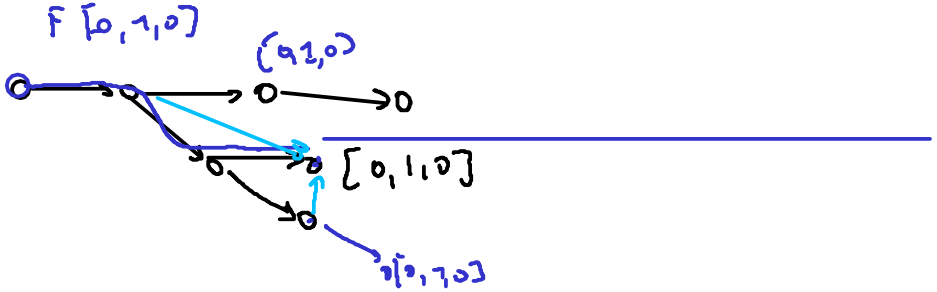
¬ ◇ (¬φ)

|

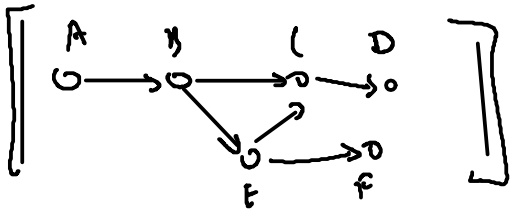
NOT

∀ PATHS A F [0,2,0]

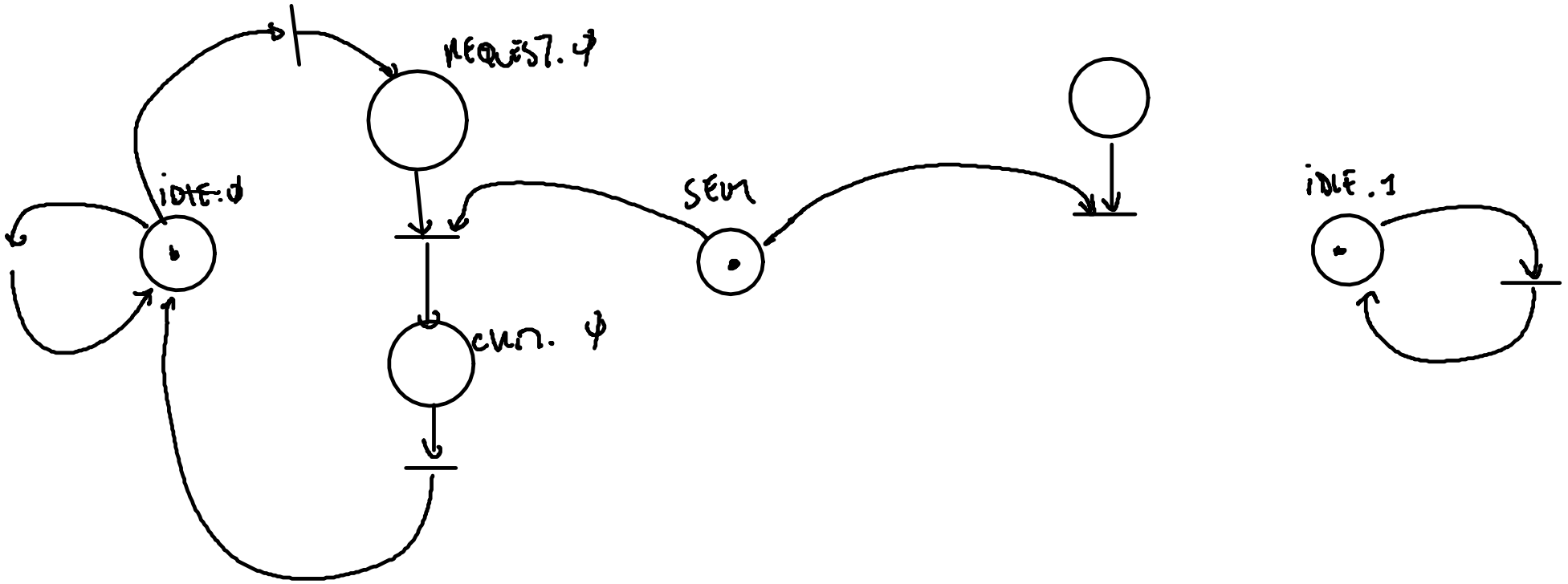
∃ A PATH E F [0,1,0]



(TLX



= { A B C D , A B E C D , A D E F }


IDLE.0
SEM
IDLE.1