Computer aided verification

Lecture 2: LTL

Def.: Kripke structure $M = \langle S, S_{\text{init}}, \rightarrow, L \rangle$

- $S_{\text{init}} \subseteq S$ nonempty set of initial states
- $\rightarrow \subseteq S \times S$ transition relation
- $L : S \rightarrow \mathcal{P}(P)$, P - propositional variables (atomic properties)

Often we assume that $\rightarrow$ is total: no deadlock!

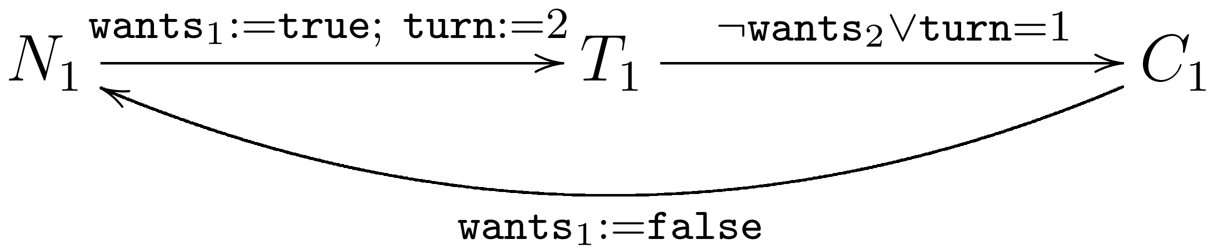
$$\forall s \in S.\ \exists s' \in S.\ s \rightarrow s'$$

Abstraction: program $\mapsto$ Kripke structure

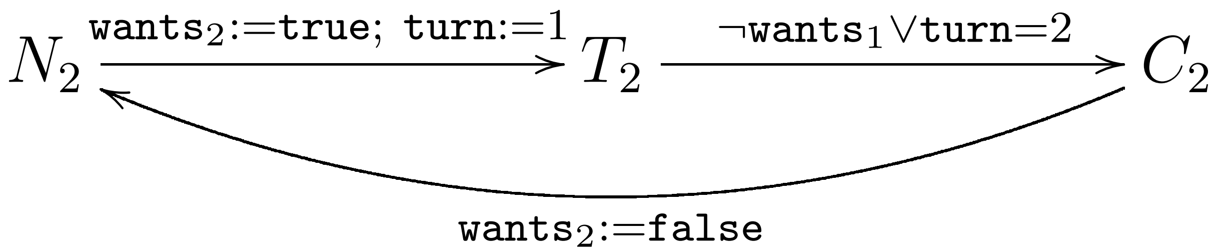
- N_i private section
- T_i attempt to enter critical section
- C_i critical section

Proc$_1$ | Proc$_2$

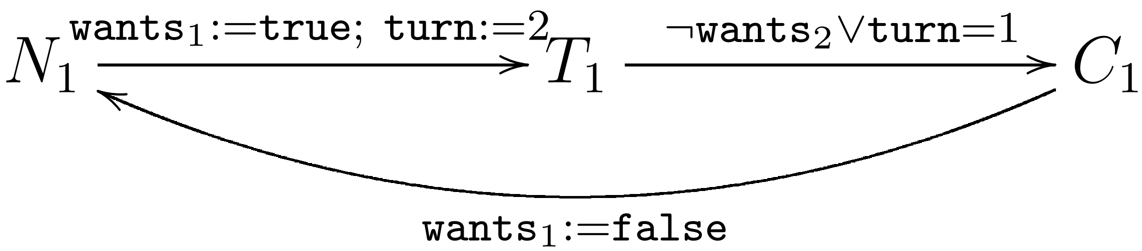
Proc$_1$:

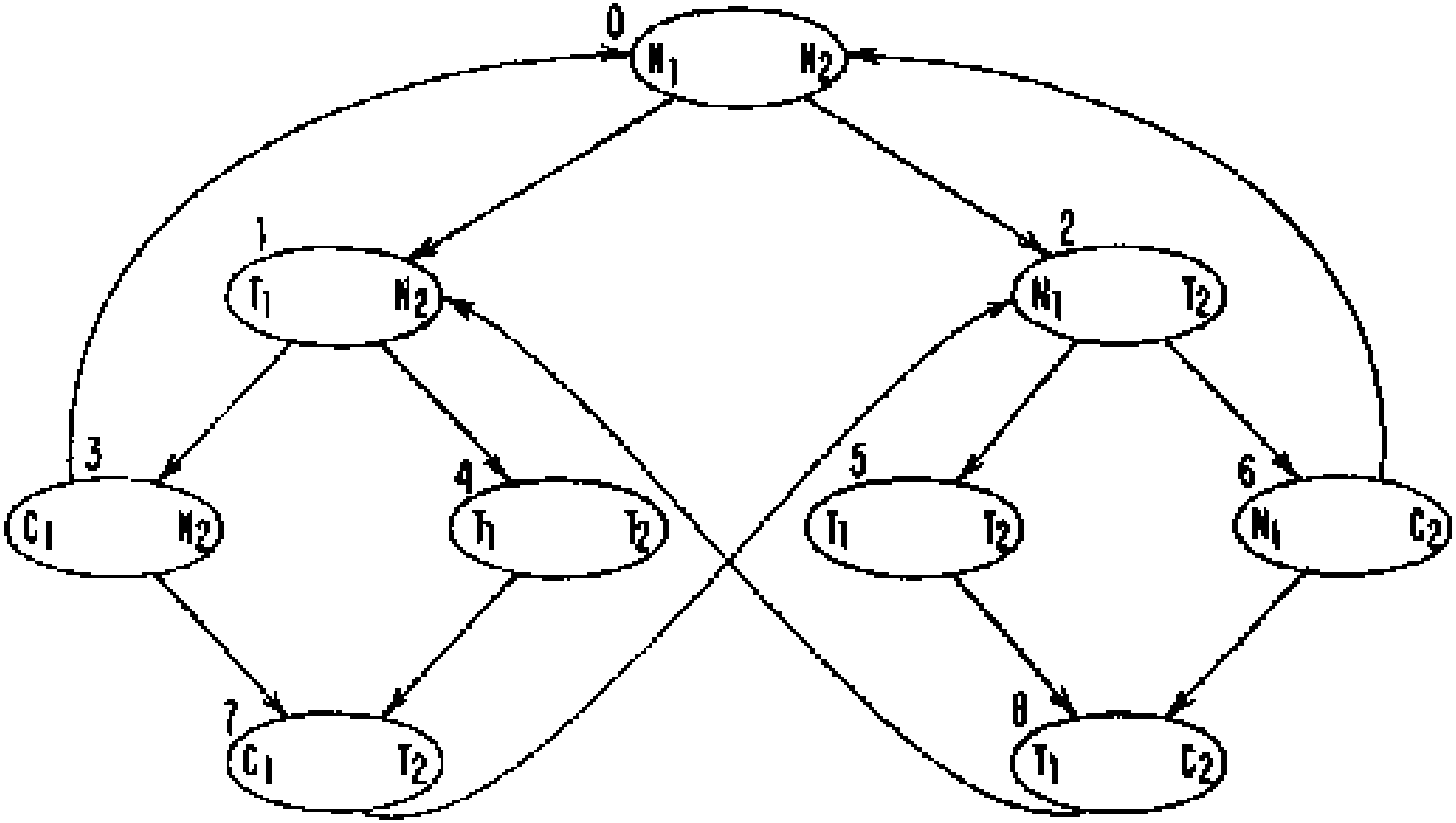


Proc$_2$:

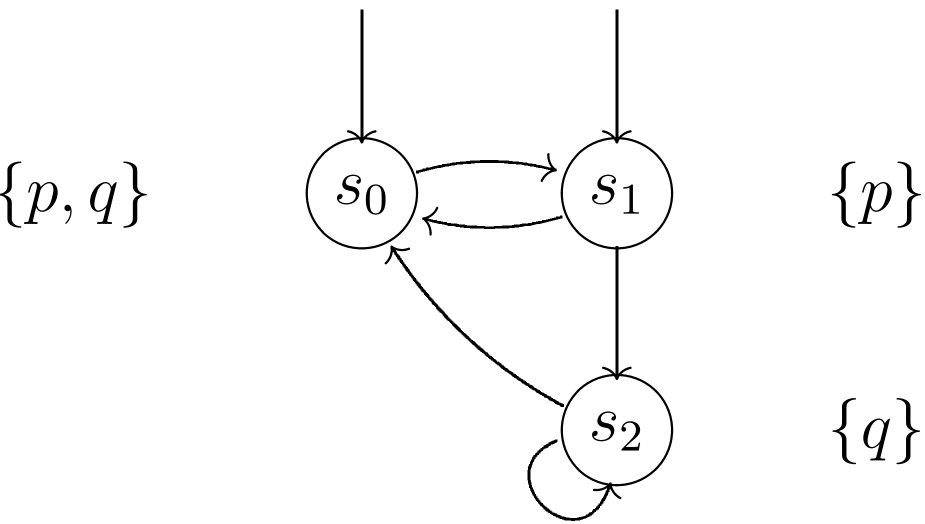


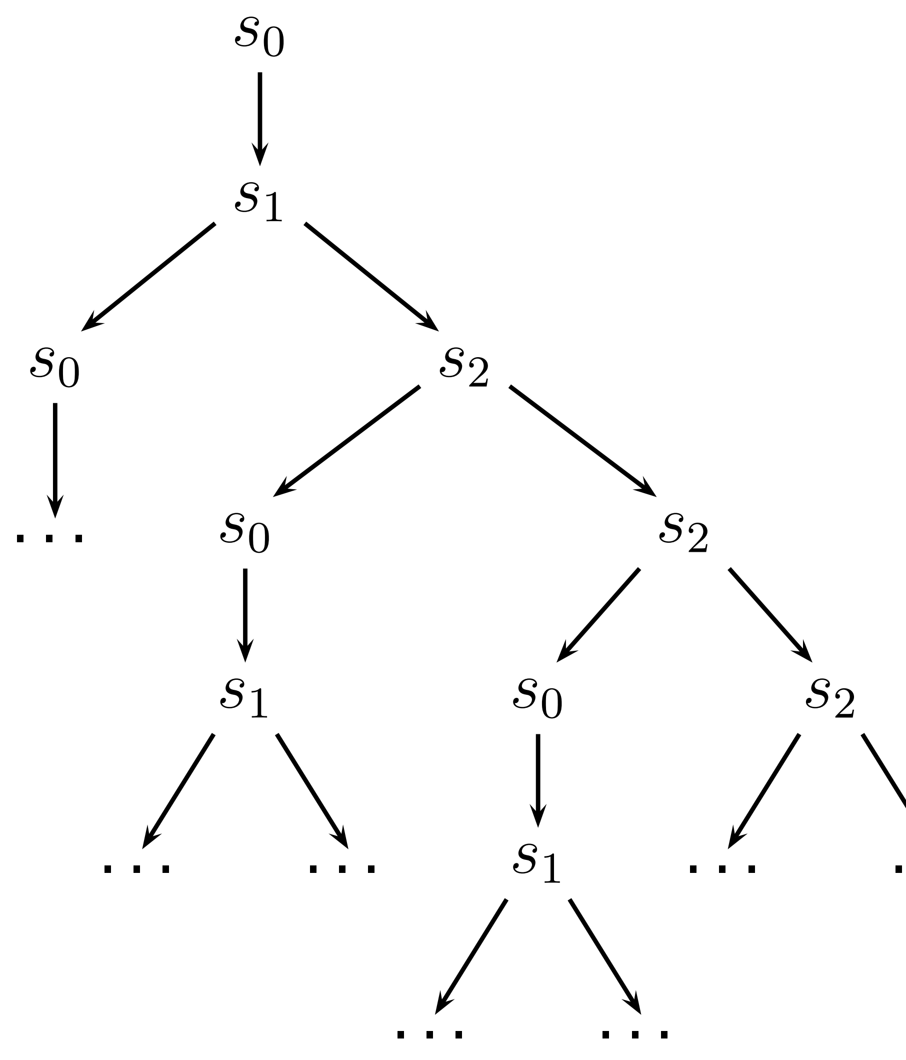
Abstraction: program $\mapsto$ Kripke structure



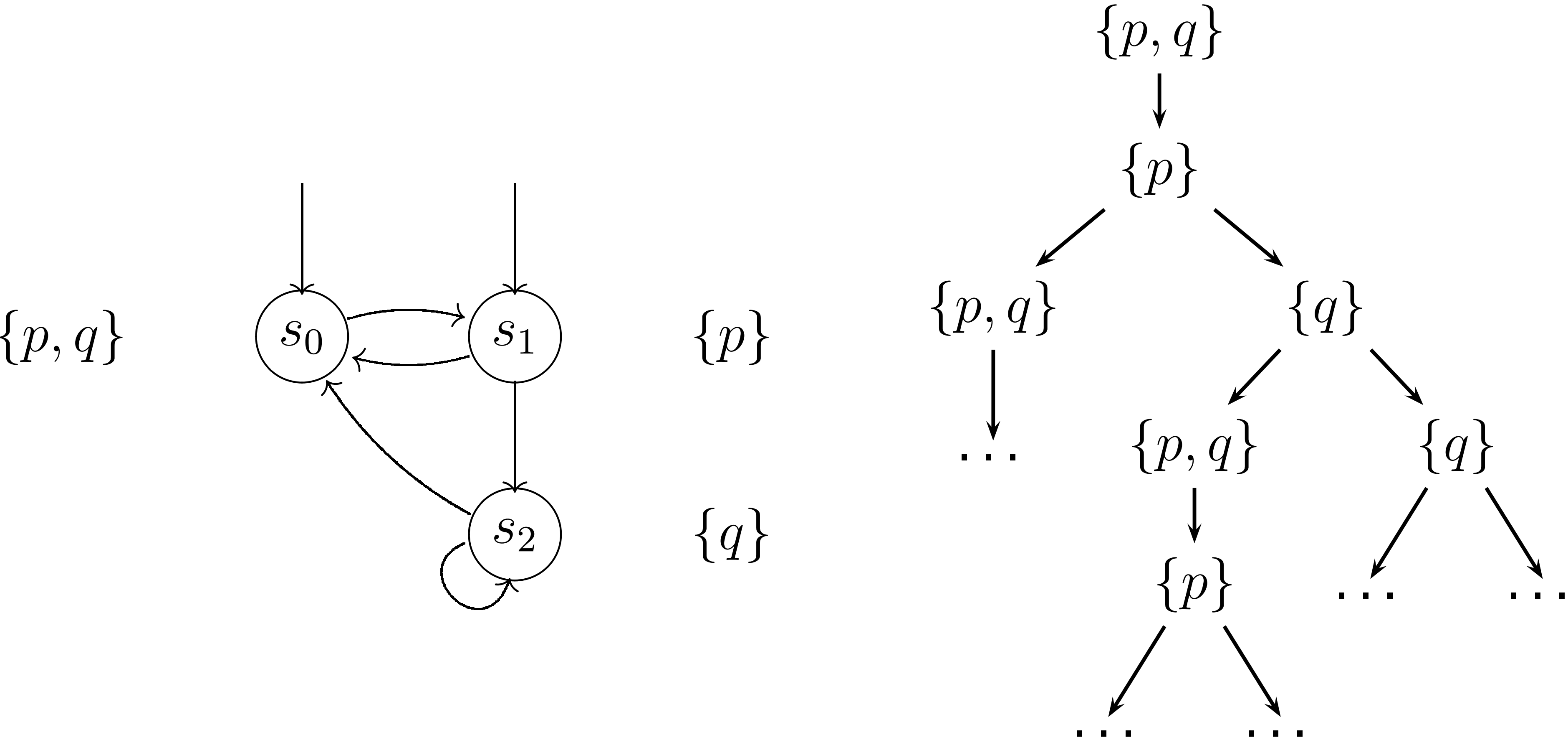


Kripke structure $\mapsto$ tree





Kripke structure $\mapsto$ tree



Def.: Path (run) is a maximal sequence

$$\Pi \;=\; s_0 \longrightarrow s_1 \longrightarrow s_2 \longrightarrow \ldots$$

Notation: $|\Pi|$ – number of states in Π

LTL says about paths. In a Kripke structure M, formula $\phi \in$ LTL is interpreted as follows:

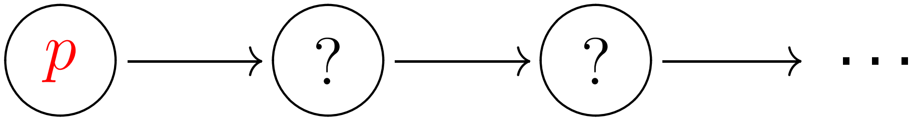
for every path such that $s_0 \in S_{\text{init}}$, ϕ holds.

Notation: $M \models \phi$, $\quad \Pi \models \phi$

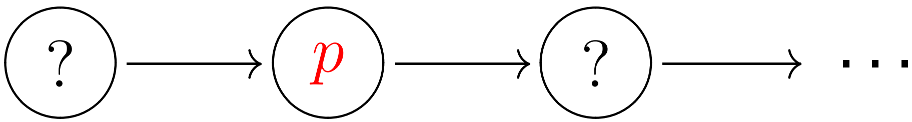
Def.: LTL (Linear Temporal Logic)

$$\phi \quad := \quad p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathsf{X}\,\phi \mid \phi_1\,\mathsf{U}\,\phi_2$$

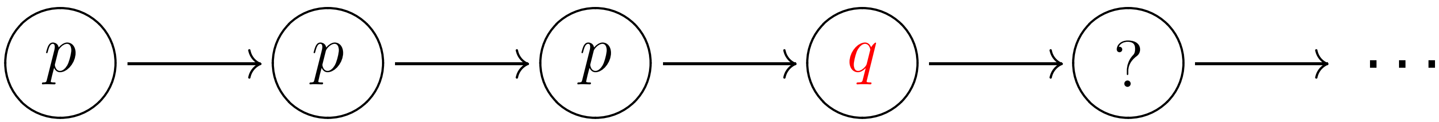
p



$\mathsf{X}\,p$



$p\,\mathsf{U}\,q$



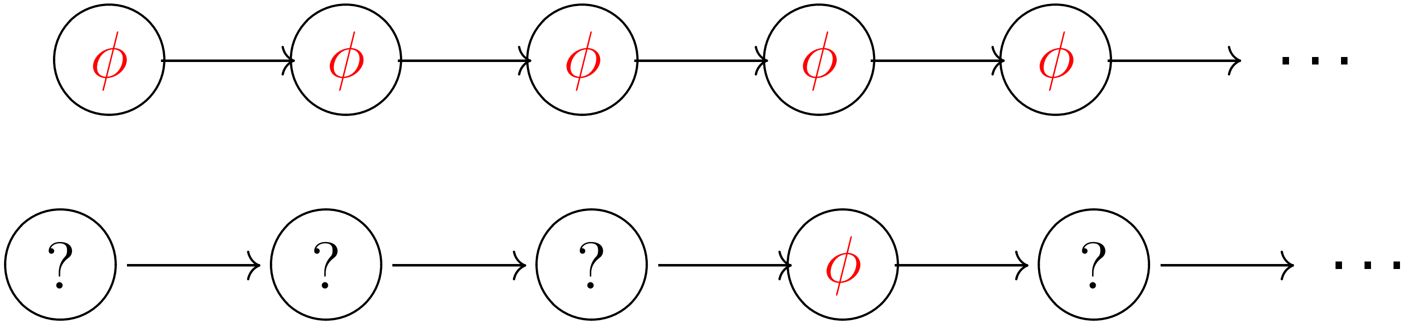
Przykład:

$$\neg\texttt{starts}\ \mathsf{U}\ \texttt{key}, \qquad \neg\texttt{starts}\ \mathsf{U}\ \neg\texttt{starts} \wedge \texttt{key}$$

Pytanie: How to write

zawsze ϕ

kiedyś ϕ

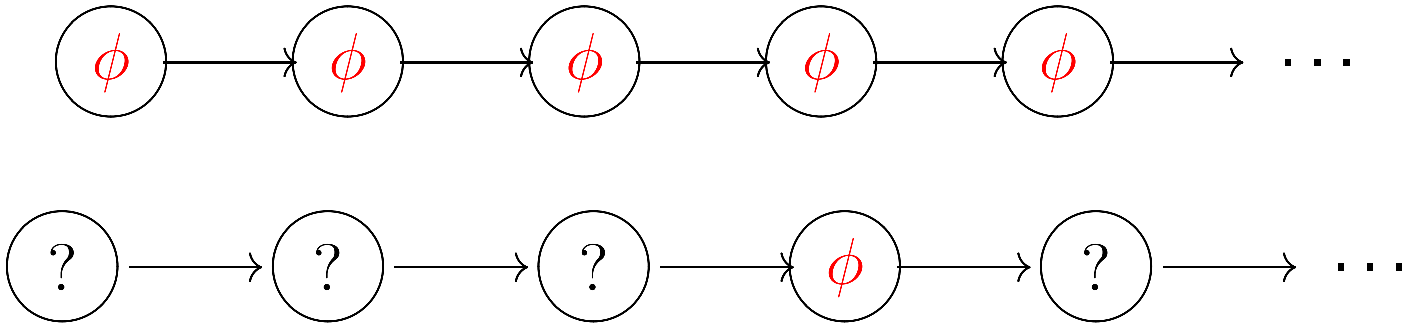


LTL - always, finally

Pytanie: How to write

zawsze ϕ

kiedyś ϕ



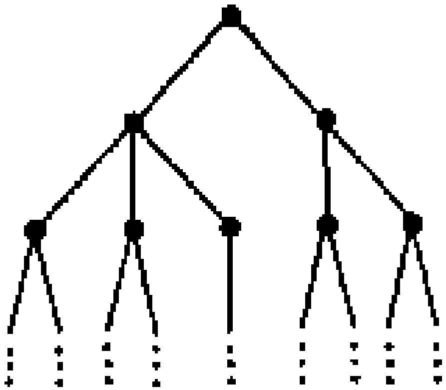
Notation:

$$\mathsf{F}\,\phi \;\equiv\; \mathtt{true}\,\mathsf{U}\,\phi$$

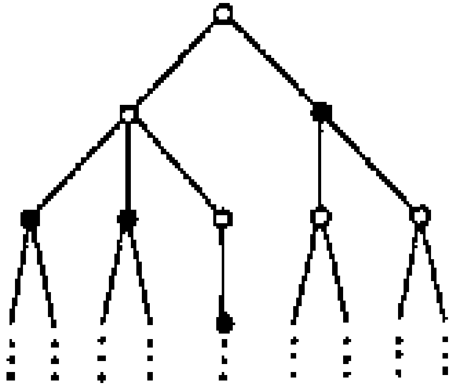
$$\mathsf{G}\,\phi \;\equiv\; \neg\,\mathsf{F}\,\neg\phi$$

$$\phi_1 \vee \phi_2 \;\equiv\; \neg(\neg\phi_1 \wedge \neg\phi_2)$$

Typical properties

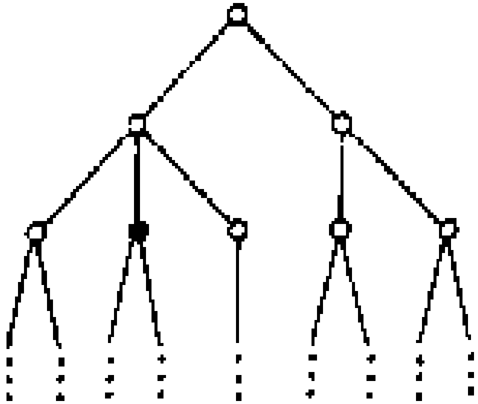


safety



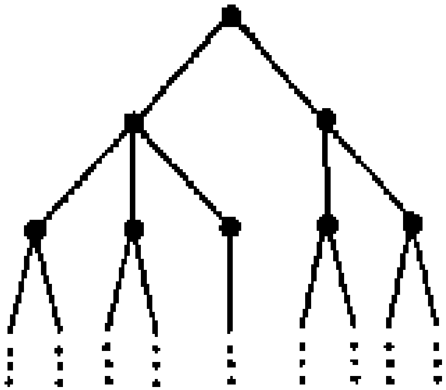
liveness

?

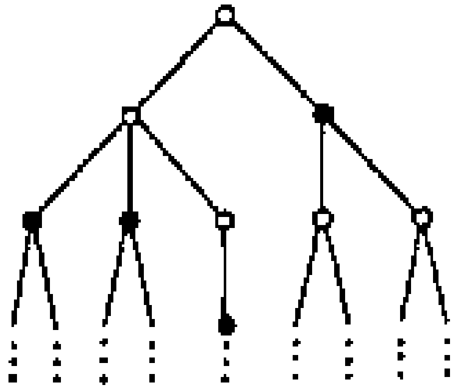


possibility

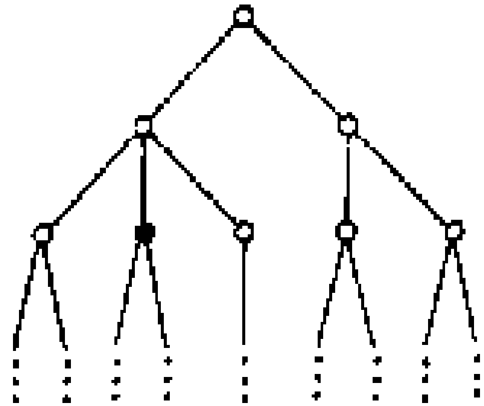
Typical properties



safety



liveness



possibility

?

$\mathsf{G}\,\phi$ $\mathsf{F}\,\phi$ $\mathsf{G}\,\neg\phi$

$\neg\,\mathsf{G}\,\neg\phi$

$\mathsf{G}\,\neg(\mathtt{cr}_1 \wedge \mathtt{cr}_2)$ $\mathsf{F}\,\mathtt{granted}$ $\mathsf{G}\,\neg\mathtt{occ}$

LTL – semantics

Semantics: $\Pi \;=\; s_0 \longrightarrow s_1 \longrightarrow s_2 \longrightarrow \ldots$

$\Pi \models p \;\text{ iff }\; p \in L(s_0)$

$\Pi \models \neg\phi \;\text{ iff }\; \ldots$

$\Pi \models \phi_1 \wedge \phi_2 \;\text{ iff }\; \ldots$

$\Pi \models \mathsf{X}\,\phi \;\text{ iff }\; \Pi^1 \models \phi$, where $\Pi^i \;=\; s_i \longrightarrow s_{i+1} \longrightarrow s_{i+2} \longrightarrow \ldots$

$\Pi \models \phi_1 \,\mathsf{U}\, \phi_2 \;\text{ iff }\; \exists i < |\Pi|.\; \Pi^i \models \phi_2 \;\wedge\; \forall j < i.\; \Pi^j \models \phi_1$

Example properties

- infinitely often ϕ ?
- almost always ϕ ?
- „weak" U : ϕ_1 W ϕ_2 (ϕ_2 not necessarily) ?
- if `req` then `granted` in future ?

Example properties

- infinitely often ϕ — $\mathsf{G}\,\mathsf{F}\,\phi$
- almost always ϕ — $\mathsf{F}\,\mathsf{G}\,\phi$
- „weak” $\phi_1 \,\mathsf{U}\, \phi_2$: ϕ_2 not necessarily — $\mathsf{G}\,\phi_1 \vee \phi_1 \,\mathsf{U}\, \phi_2$
- if `req` then `granted` in future

$$\mathsf{G}\,(\mathtt{req} \implies \mathsf{X}\,\mathsf{F}\,\mathtt{granted})$$

- fairness: if stubbornly `req` then `granted`

  „weak”: stubbornly = almost always ?

  „strong”: stubbornly = infinitely often ?

Example properties

- infinitely often ϕ — $\mathsf{G}\,\mathsf{F}\,\phi$
- almost always ϕ — $\mathsf{F}\,\mathsf{G}\,\phi$
- „weak" $\phi_1 \,\mathsf{U}\, \phi_2$: ϕ_2 not necessarily — $\mathsf{G}\,\phi_1 \vee \phi_1 \,\mathsf{U}\, \phi_2$
- if `req` then `granted` in future

$$\mathsf{G}\,(\mathtt{req} \implies \mathsf{X}\,\mathsf{F}\,\mathtt{granted})$$

- fairness: if stubbornly `req` then `granted`

  „weak": stubbornly = alm. always $\quad \mathsf{F}\,\mathsf{G}\,\mathtt{req} \implies \mathsf{F}\,\mathtt{granted}$

  „strong": stubbornly = inf. often $\quad \mathsf{G}\,\mathsf{F}\,\mathtt{req} \implies \mathsf{F}\,\mathtt{granted}$

Fairness

(if stubbornly `req` then `granted`)

Variant 1

„weak”: stubbornly = alm. always $\mathsf{F}\,\mathsf{G}\,\mathtt{req} \implies \mathsf{F}\,\mathtt{granted}$

„strong”: stubbornly = inf. often $\mathsf{G}\,\mathsf{F}\,\mathtt{req} \implies \mathsf{F}\,\mathtt{granted}$

Variant 2

„weak”:

$$\mathsf{F}\,\mathsf{G}\,\mathtt{req} \implies \mathsf{G}\,\mathsf{F}\,\mathtt{granted} = \mathsf{G}\,(\mathsf{F}\,\mathsf{G}\,\mathtt{req} \implies \mathsf{F}\,\mathtt{granted})$$

„strong”:

$$\mathsf{G}\,\mathsf{F}\,\mathtt{req} \implies \mathsf{G}\,\mathsf{F}\,\mathtt{granted} = \mathsf{G}\,(\mathsf{G}\,\mathsf{F}\,\mathtt{req} \implies \mathsf{F}\,\mathtt{granted})$$

De Morgane laws

$$\phi_1 \vee \phi_2 \equiv \neg(\neg\phi_1 \wedge \neg\phi_2)$$

$$? \equiv \neg \mathsf{X} \neg\phi$$

$$\mathsf{G}\,\phi \equiv \neg \mathsf{F} \neg\phi$$

$$\phi_1 \vee \phi_2 \equiv \neg(\neg\phi_1 \wedge \neg\phi_2)$$

$$\mathsf{X}\,\phi \equiv \neg\,\mathsf{X}\,\neg\phi$$

$$\mathsf{G}\,\phi \equiv \neg\,\mathsf{F}\,\neg\phi$$

$$? \equiv \neg(\neg\phi\,\mathsf{U}\,\neg\psi)$$

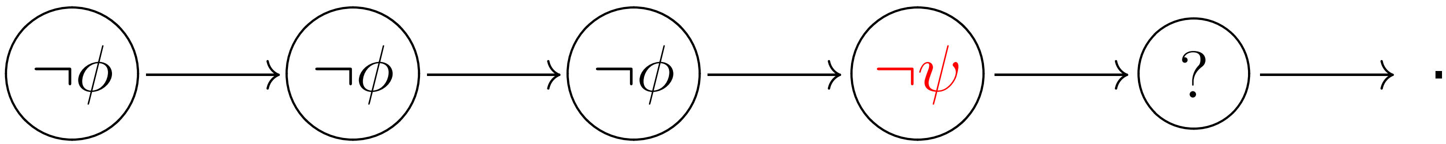
De Morgane laws

$\phi_1 \vee \phi_2 \;\equiv\; \neg(\neg\phi_1 \wedge \neg\phi_2)$ $\qquad$ $\mathsf{X}\,\phi \;\equiv\; \neg\,\mathsf{X}\,\neg\phi$

$\mathsf{G}\,\phi \;\equiv\; \neg\,\mathsf{F}\,\neg\phi$

$\phi\,\mathsf{R}\,\psi \;\equiv\; \neg(\neg\phi\,\mathsf{U}\,\neg\psi)$

$\neg\phi\,\mathsf{U}\,\neg\psi$



$\Pi \models \phi\,\mathsf{R}\,\psi$ iff ?

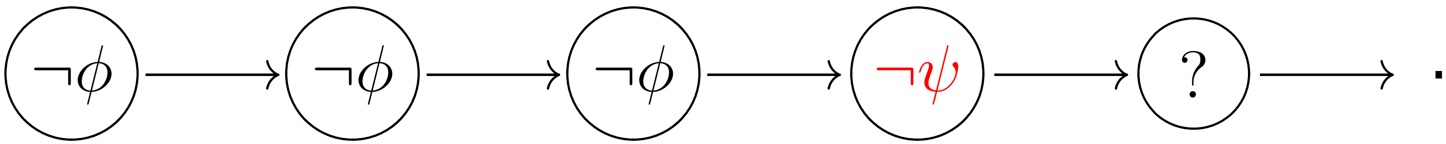
De Morgane laws

$$\phi_1 \vee \phi_2 \equiv \neg(\neg\phi_1 \wedge \neg\phi_2) \qquad \mathsf{X}\,\phi \equiv \neg\,\mathsf{X}\,\neg\phi$$

$$\mathsf{G}\,\phi \equiv \neg\,\mathsf{F}\,\neg\phi$$

$$\phi\,\mathsf{R}\,\psi \equiv \neg(\neg\phi\,\mathsf{U}\,\neg\psi)$$

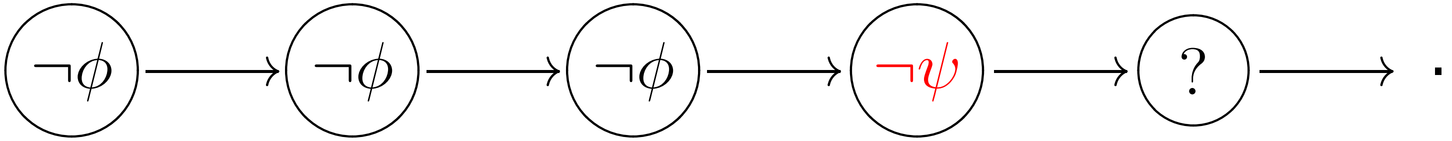
$\neg\phi\,\mathsf{U}\,\neg\psi$



$$\Pi \models \phi\,\mathsf{R}\,\psi \text{ iff } \forall i < |\Pi|.\ (\forall j < i.\ \Pi^j \models \neg\phi) \implies \Pi^i \models \psi$$

U versus R

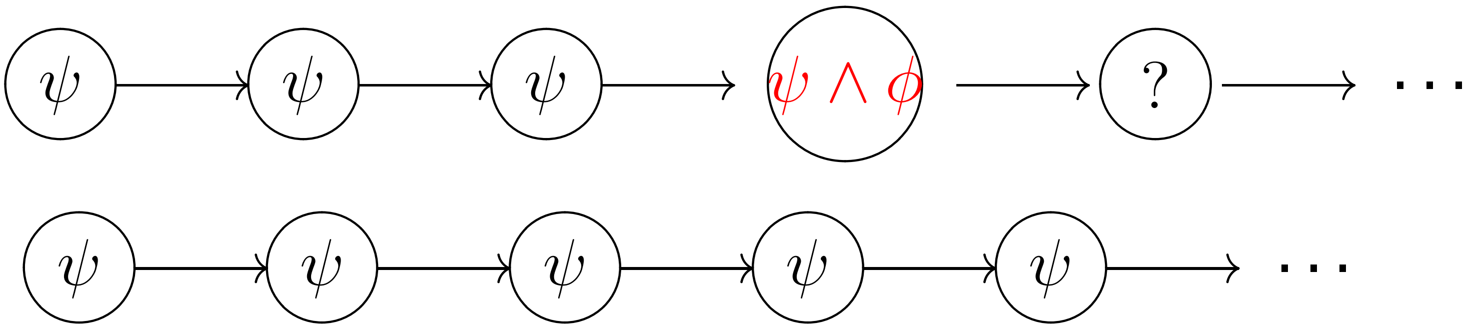
$\neg\phi\,\mathsf{U}\,\neg\psi$



$\phi\,\mathsf{R}\,\psi \;\equiv\; \neg(\neg\phi\,\mathsf{U}\,\neg\psi)$

$\Pi \vDash \phi\,\mathsf{R}\,\psi$ iff $\forall i < |\Pi|.\ (\forall j < i.\ \Pi^j \vDash \neg\phi) \implies \Pi^i \vDash \psi$

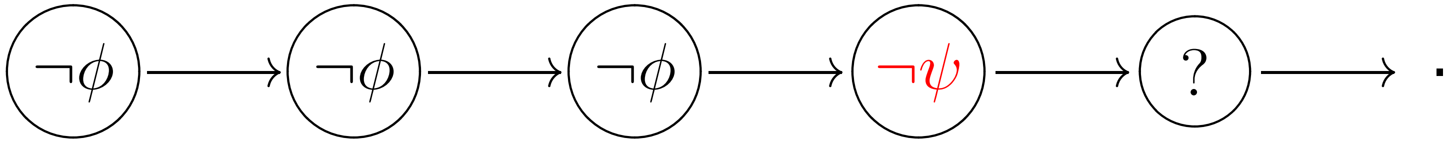
$\phi\,\mathsf{R}\,\psi$



$\phi\,\mathsf{R}\,\psi \;\equiv\; \neg(\neg\phi\,\mathsf{U}\,\neg\psi) \;\equiv\; \psi\,\mathsf{U}\,(\psi \wedge \phi) \vee \mathsf{G}\,\psi \;\equiv\; \psi\,\mathsf{W}\,(\psi \wedge \phi)$

U versus R

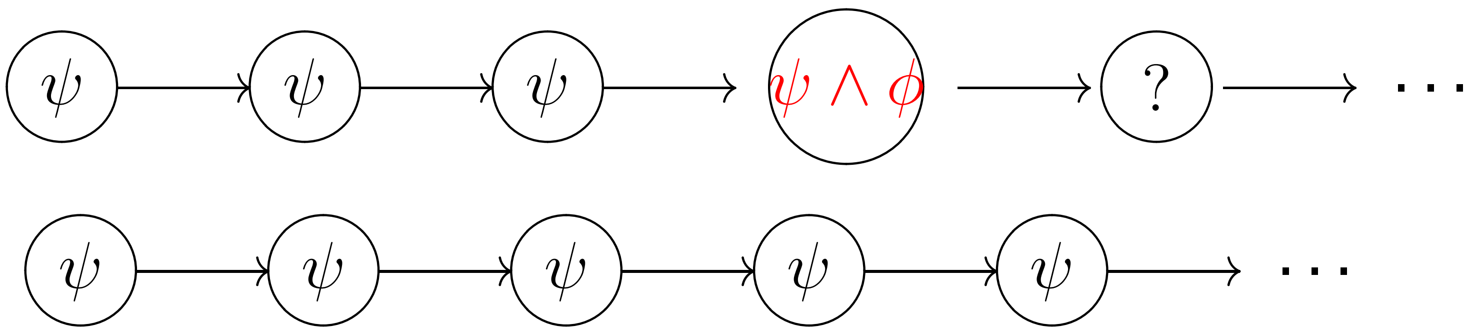
$\neg\phi \, \mathsf{U} \, \neg\psi$



$$\phi \, \mathsf{R} \, \psi \;\equiv\; \neg(\neg\phi \, \mathsf{U} \, \neg\psi)$$

$$\Pi \models \phi \, \mathsf{R} \, \psi \;\text{ iff }\; \forall i < |\Pi|.\ (\forall j < i.\ \Pi^j \models \neg\phi) \implies \Pi^i \models \psi$$

$\phi \, \mathsf{R} \, \psi$



$$\phi \, \mathsf{R} \, \psi \;\equiv\; \neg(\neg\phi \, \mathsf{U} \, \neg\psi) \;\equiv\; \psi \, \mathsf{U} \, (\psi \wedge \phi) \vee \mathsf{G} \, \psi \;\equiv\; \psi \, \mathsf{W} \, (\psi \wedge \phi)$$

– U i R as fixed points . . .

Pushing negation down

$$\neg(\phi_1 \wedge \phi_2) \;\equiv\; \neg\phi_1 \vee \neg\phi_2$$

$$\neg\,\mathsf{F}\,\phi \;\equiv\; \mathsf{G}\,\neg\phi$$

$$\neg\,\mathsf{G}\,\phi \;\equiv\; \mathsf{F}\,\neg\phi$$

$$\neg\,\mathsf{X}\,\phi \;\equiv\; \mathsf{X}\,\neg\phi$$

Pushing negation down

$\neg(\phi_1 \wedge \phi_2) \equiv \neg\phi_1 \vee \neg\phi_2$

$\neg\,\mathsf{F}\,\phi \equiv \mathsf{G}\,\neg\phi$

$\neg\,\mathsf{G}\,\phi \equiv \mathsf{F}\,\neg\phi$

$\neg\,\mathsf{X}\,\phi \equiv \mathsf{X}\,\neg\phi$

$\neg(\phi\,\mathsf{U}\,\psi) \equiv (\phi \wedge \neg\psi)\,\mathsf{W}\,(\neg\phi \wedge \neg\psi)$ why not in this way?

$\neg(\phi\,\mathsf{U}\,\psi) \equiv \neg\phi\,\mathsf{R}\,\neg\psi$

Write a formula . . .

(1) if b then some a was ?

(1') . . . strictly beforehand . . . ?

(2) every b is proceeded by a that appears after last b,

if any before ?

(3) alternating blocks of a i b („relay") ?

Write a formula . . .

(1) if b then some a was $$\mathsf{F}\, b \implies (\neg b\, \mathsf{U}\, a)$$

$$\equiv \neg b\, \mathsf{W}\, a \equiv Pr(a, b)$$

(1') . . . strictly beforehand . . . $$\mathsf{F}\, b \implies (\neg b\, \mathsf{U}\, (a \wedge \neg b))$$

$$\equiv \neg b\, \mathsf{W}\, (a \wedge \neg b) \equiv a\, \mathsf{R}\, \neg b \equiv SPr(a, b)$$

(2) every b is proceeded by a that appears after last b,

if any before $$Pr(a, b) \wedge \mathsf{G}\, (b \implies \mathsf{X}\, Pr(a, b))$$

(3) alternating blocks a i b („relay”)

$$\mathsf{G}\, (\, (a \implies a\, \mathsf{W}\, (\neg a \wedge b)) \wedge (b \implies \ldots)\,)$$

What is inexpressible?

(1) on every path a state appears such that

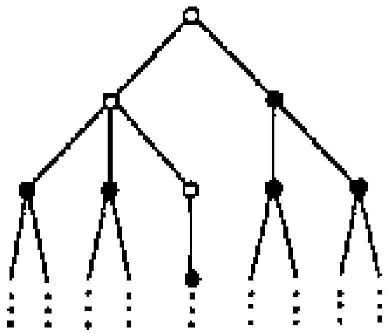
in every successor state ?

(on every path) a holds

(1') on some path . . . ?

(2) on every path a state appears such that

in every following state a holds ?



(pictures. . .)

What is inexpressible?

(1) on every path a state appears such that

in every successor — F X a ?

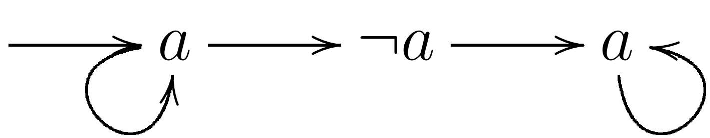
(on every path) a holds

(1') on some path . . . — ?

(2) on every path a state appears such that

in every following state a holds — F G a ?

too much!



$\models$ F G a

What is inexpressible? (cont.)

(3) even(a): on every even position a ?

(3') oddeven(a): on every even position a

and on every odd position $\neg a$

$$\mathsf{G}\,(\,(a \implies \mathsf{X}\,\neg a)\ \wedge (\neg a \implies \mathsf{X}\,a)$$

(4) from every reachable state some initial state is

reachable ?

Expressivity

Tw.: LTL = LTL(X, U) is more expressive than LTL(X, F)

Tw.: LTL = FO($\leq$, +1)

Thm: Past temporal connectives:

$$U^{-1},\ \mathsf{F}^{-1},\ \mathsf{G}^{-1}$$

do not increase expressive power.

Thm: LTL(F, G, F^{-1}, G^{-1}) = ?

Def.: Property = subset of $\mathcal{P}(P)^\omega$

Safety properties X

negative decision always after finitely many steps

Def.: Property = subset of $\mathcal{P}(P)^\omega$

Safety properties X

negative decision always after finitely many steps

if $\pi \notin X$ then there is a prefix $\rho < \pi$ such that $\rho < \pi'$ implies $\pi' \notin X$

Liveness properties X

negative decision never after finitely many steps

for every ρ exists $\pi > \rho$ such that $\pi \in X$

Model checking — PSPACE-complete

- input: M, ϕ
- question: $M \models \phi$?

Satisfiability — PSPACE-complete

- input: ϕ
- question: $\exists M.\ M \models \phi$?

Complexity of model checking:

$$|M| \cdot 2^{\mathcal{O}(|\phi|)}$$

$2^{\mathcal{O}(|\phi|)}$ OK

$|M|$ too much!

(1) $M \mapsto \mathcal{A}_M$

(2) $\neg\phi \mapsto \mathcal{A}_{\neg\phi}$ LTL $\rightarrow$ ω-automata

(3) $L(\mathcal{A}_M \times \mathcal{A}_{\neg\phi}) = \emptyset?$

yes $\rightarrow$ $M \models \phi$

no $\rightarrow$ $\neg(M \models \phi)$, counterexample = a path in M

Algorithm

(1) $M \mapsto \mathcal{A}_M$

(2) $\neg\phi \mapsto \mathcal{A}_{\neg\phi}$

LTL $\rightarrow$ ω-automata

(3) $L(\mathcal{A}_M \times \mathcal{A}_{\neg\phi}) = \emptyset?$

yes $\rightarrow$ $M \models \phi$

no $\rightarrow$ $\neg(M \models \phi)$, counterexample = a path in M

$\phi = \mathsf{G}\,(p \implies \mathsf{X}\,\mathsf{F}\,q)$

$A_{\neg\phi} =$