

Praktyczne metody weryfikacji

Wykład 2: LTL

Def.: Struktura Kripkego $M = \langle S, S_{\text{pocz}}, \rightarrow, L \rangle$

- $S_{\text{pocz}} \subseteq S$ niepusty zbiór stanów początkowych
- $\rightarrow \subseteq S \times S$ relacja przejścia
- $L : S \rightarrow \mathcal{P}(P)$, P - zmienne zdaniowe (własności atomowe)

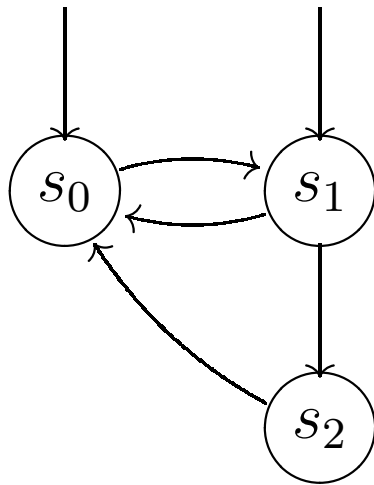
Często zakładamy, że \rightarrow jest całkowita:

brak blokady!

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

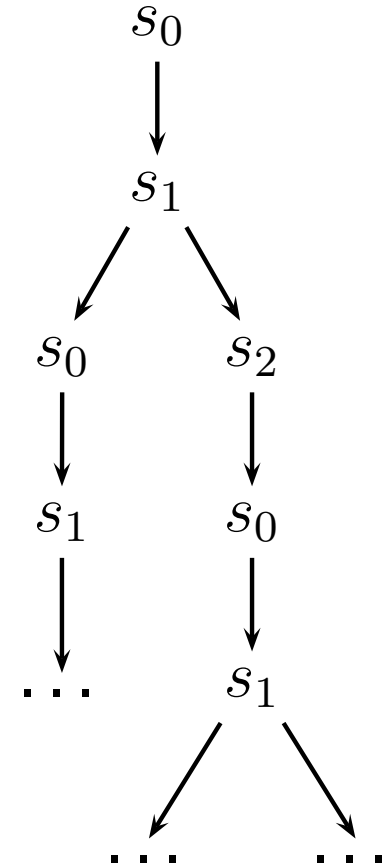
Przykład

$\{p, q\}$

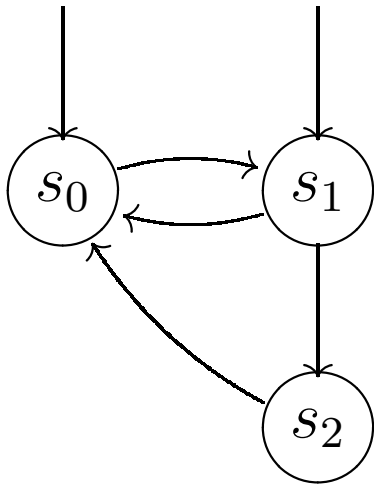


$\{p\}$

$\{q\}$

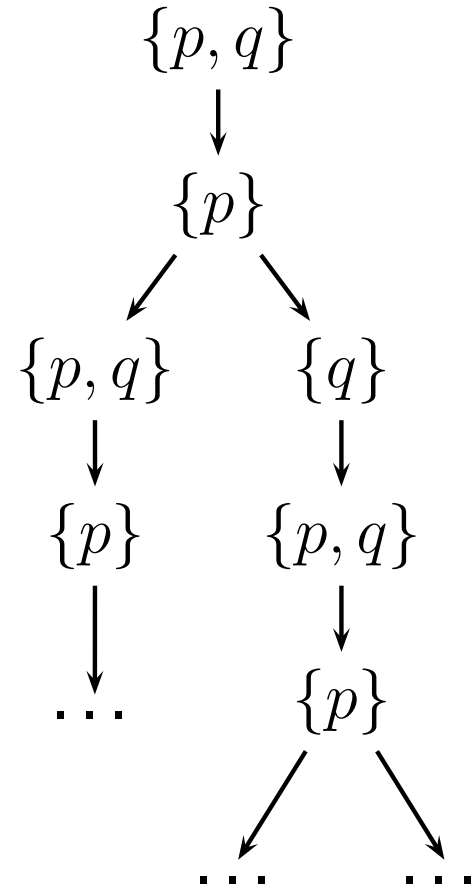


$\{p, q\}$



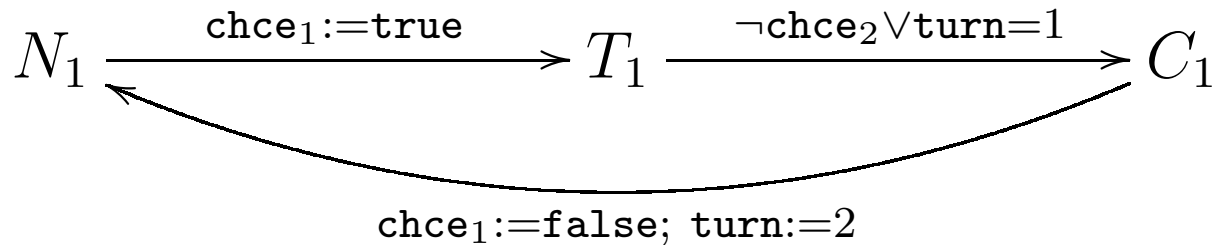
$\{p\}$

$\{q\}$

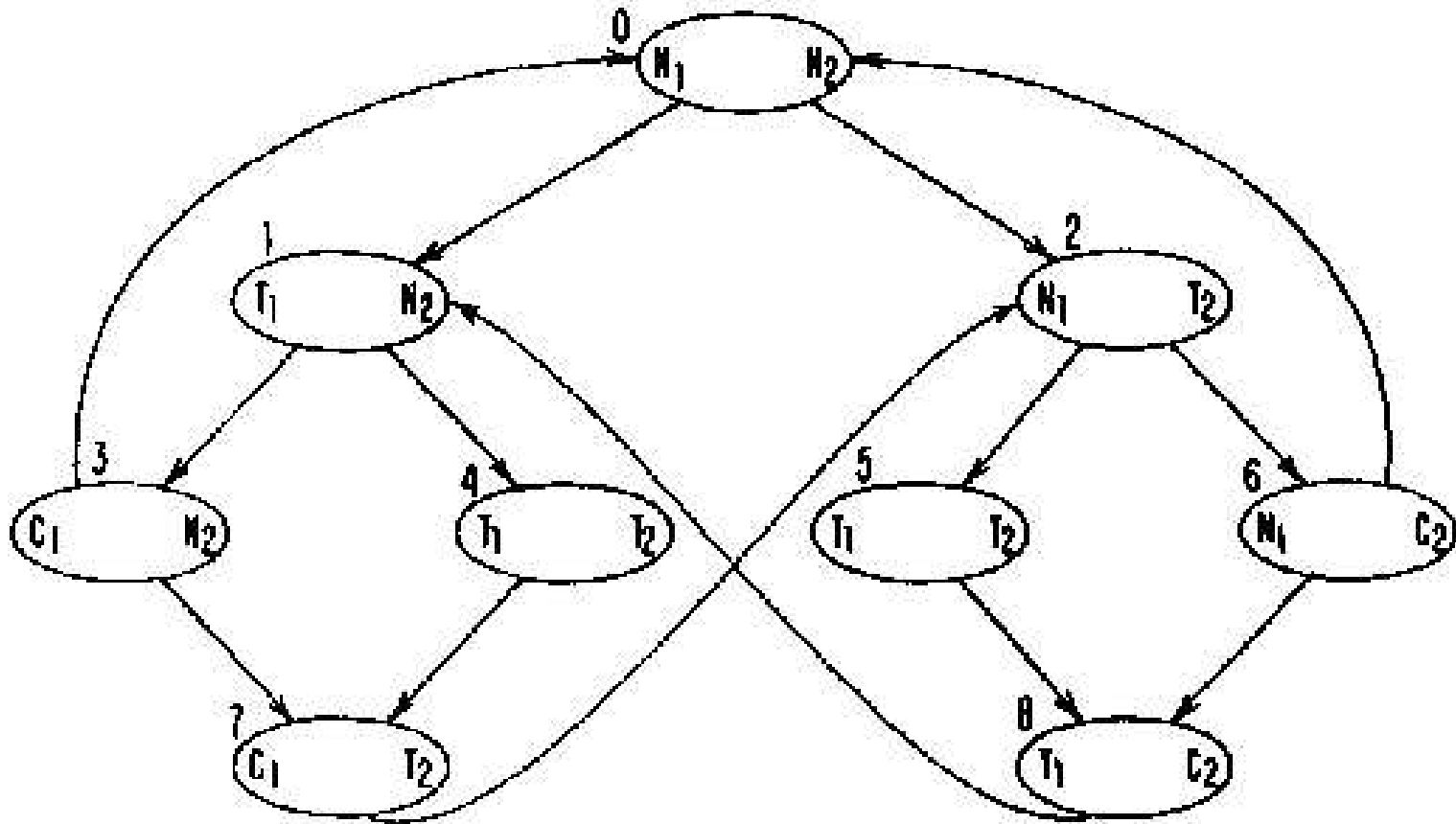
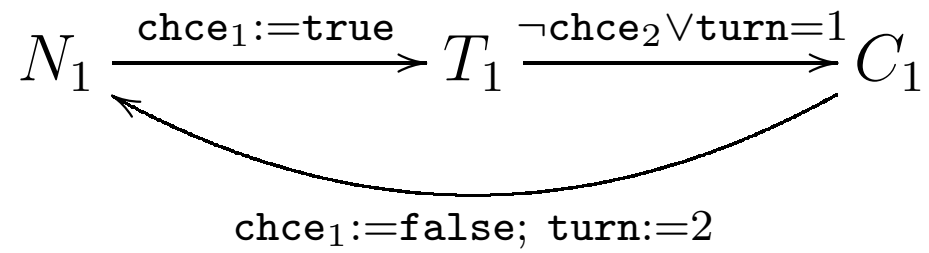


program \mapsto struktura Kripkego

- N_i własne sprawy
- T_i próbuję wejść do sekcji krytycznej
- C_i sekcja krytyczna

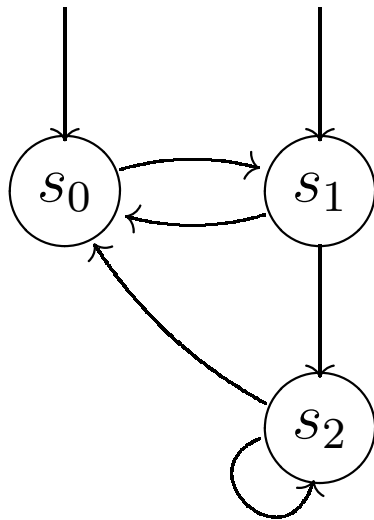


program \mapsto struktura Kripkego



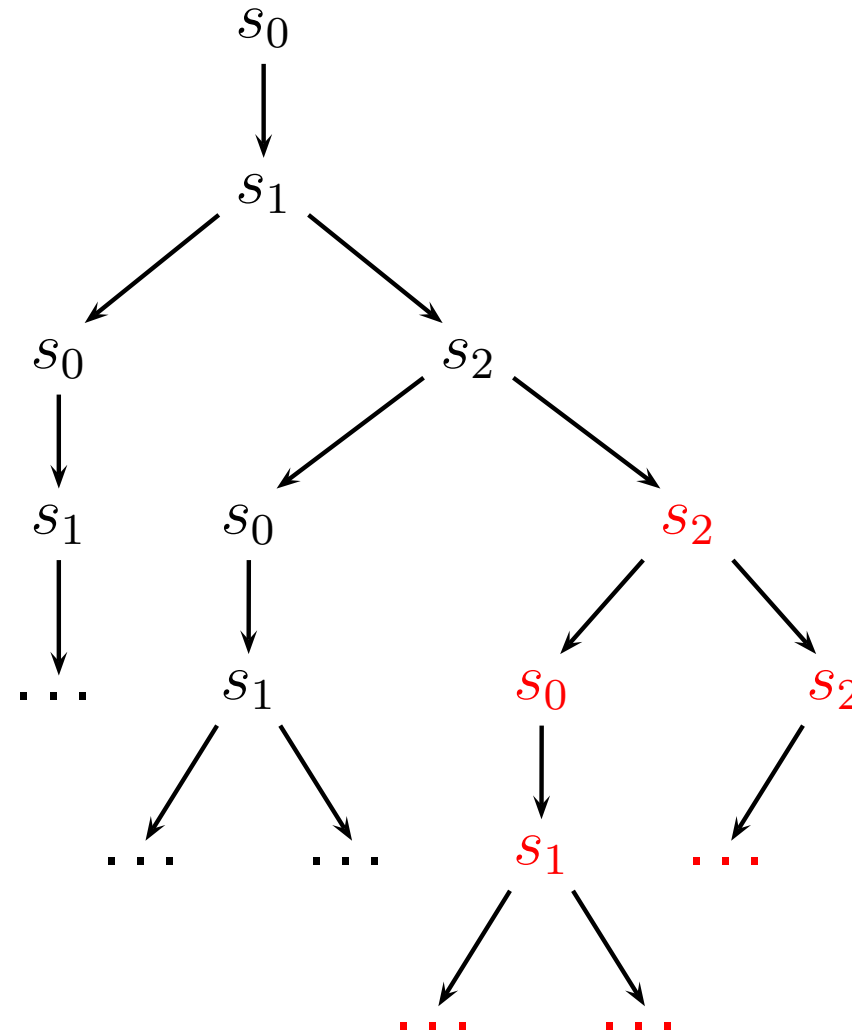
Przykład (cd)

$\{p, q\}$



$\{p\}$

$\{q\}$



Def.: Ścieżka (**przebieg**) to maksymalny ciąg

$$\Pi = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \dots$$

Ozn.: $|\Pi|$ – liczba stanów w Π

LTL wyraża własności ścieżek. Na strukturze Kripkego M ,
formułę $\phi \in \text{LTL}$ interpretujemy następująco:

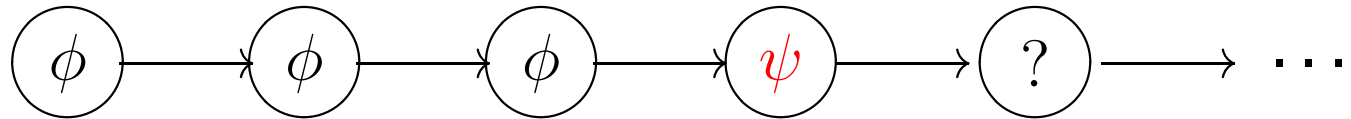
dla każdej ścieżki takiej, że $s_0 \in S_{\text{pocz}}$, zachodzi ϕ .

Ozn.: $M \models \phi$, $\Pi \models \phi$

Def.: LTL (Linear Temporal Logic)

$$\phi ::= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid X\phi \mid \phi_1 U \phi_2$$

$\phi U \psi$

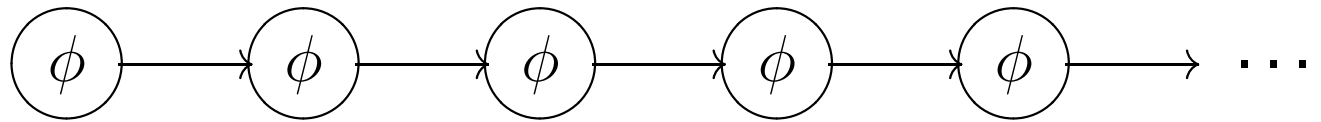


Przykład ad:

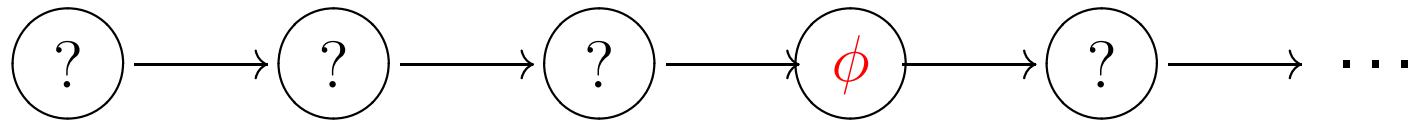
\neg starts U key, \neg starts U \neg starts \wedge key

Pytanie: Jak zapisać

zawsze ϕ

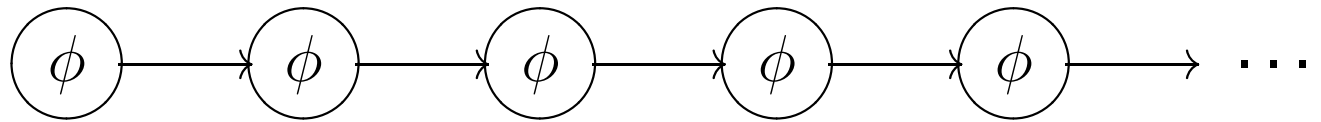


kiedyś ϕ

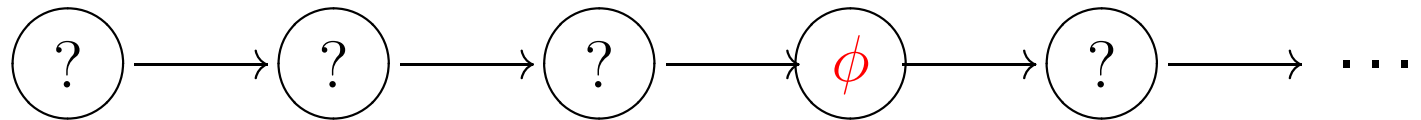


Pytanie: Jak zapisać

zawsze ϕ



kiedyś ϕ

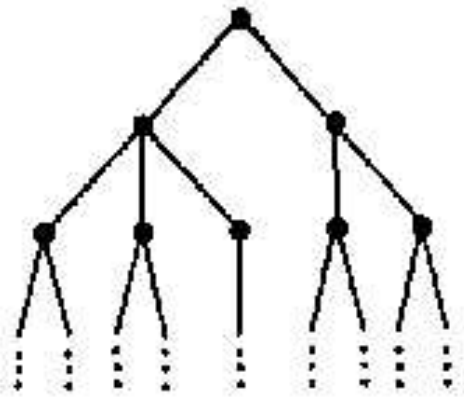


Notacja:

$$F\phi \equiv \text{true}U\phi$$

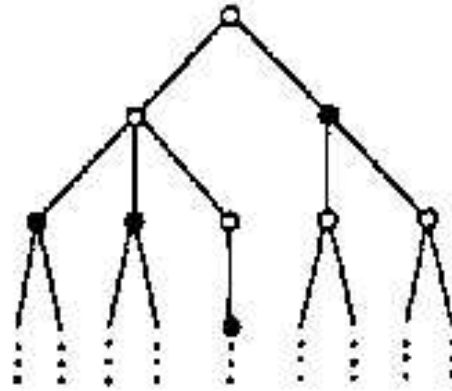
$$G\phi \equiv \neg F\neg\phi$$

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



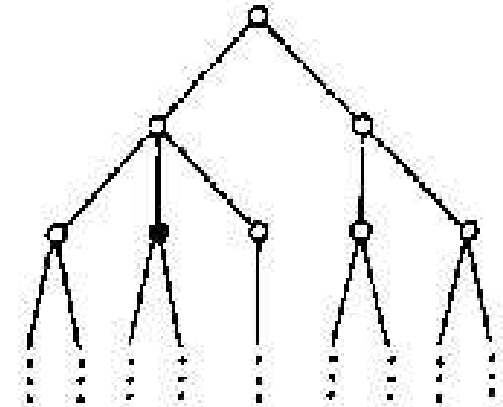
bezpieczeństwo

?



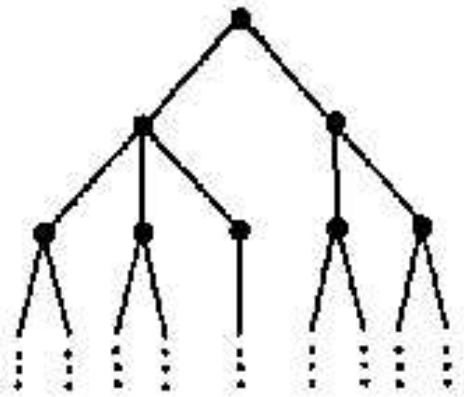
żywotność

?



możliwość

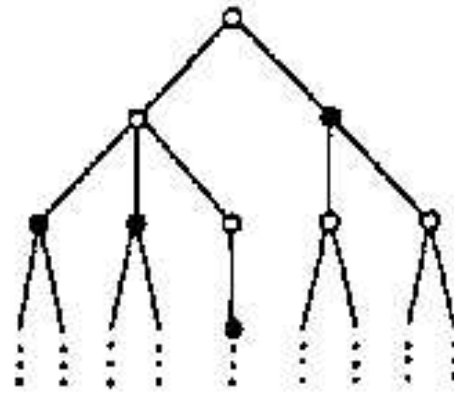
?



bezpieczeństwo

$$G\phi$$

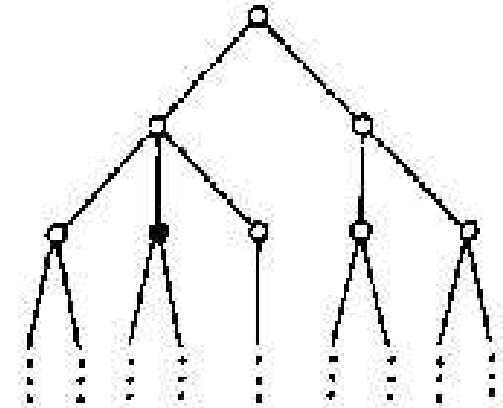
$$G\neg(cr_1 \wedge cr_2)$$



żywotność

$$F\phi$$

$$F\text{granted}$$



możliwość

$$G\neg\phi$$

$$\neg G\neg\phi$$

$$G\neg\text{occ}$$

Semantyka:

$$\Pi = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \dots$$

$$\Pi \models p \text{ wtw gdy } p \in L(s_0)$$

$$\Pi \models \neg\phi \text{ wtw gdy } \dots$$

$$\Pi \models \phi_1 \wedge \phi_2 \text{ wtw gdy } \dots$$

$$\Pi \models X\phi \text{ wtw gdy } \Pi^1 \models \phi, \text{ gdzie } \Pi^i = s_i \rightarrow s_{i+1} \rightarrow s_{i+2} \rightarrow \dots$$

$$\Pi \models \phi_1 U \phi_2 \text{ wtw gdy } \exists i < |\Pi|. \Pi^i \models \phi_2 \wedge \forall j < i. \Pi^j \models \phi_1$$

przykładowe własności

- nieskończenie wiele razy ϕ ?
- prawie zawsze ϕ ?
- „słaby” U: $\phi_1 W \phi_2$ (ϕ_2 niekoniecznie) ?
- sprawiedliwość: jeśli uparcie req to granted ?

przykładowe własności

- nieskończenie wiele razy ϕ $GF\phi$
- prawie zawsze ϕ $FG\phi$
- „słaby” $\phi_1 U \phi_2 : \phi_2$ nieobowiązkowo $G\phi_1 \vee \phi_1 U \phi_2$
- sprawiedliwość: jeśli uparcie req to granted
 - „słaba”: uparcie = prawie zawsze ?
 - „silna”: uparcie = nieskończenie wiele ?

przykładowe własności

- nieskończenie wiele razy ϕ $GF\phi$
- prawie zawsze ϕ $FG\phi$
- „słaby” $\phi_1 U \phi_2 : \phi_2$ nieobowiązkowo $G\phi_1 \vee \phi_1 U \phi_2$
- sprawiedliwość: jeśli uparcie req to granted
- „słaba”: **uparcie = pr. zawsze** $FGreq \implies Fgranted$
- „silna”: **uparcie = niesk. wiele** $GFreq \implies Fgranted$

sprawiedliwość

(jeśli uparcie req to granted)

Wariant 1

„słaba”: uparcie = pr. zawsze

$$FGreq \implies Fgranted$$

„silna”: uparcie = niesk. wiele

$$GFreq \implies Fgranted$$

Wariant 2

„słaba”: $FGreq \implies GFgranted = G(FGreq \implies Fgranted)$

„silna”: $GFreq \implies GFgranted = G(GFreq \implies Fgranted)$

Prawa de Morgane'a:

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

$$G\phi \equiv \neg F\neg\phi$$

$$? \equiv \neg(\neg\phi U \neg\psi)$$

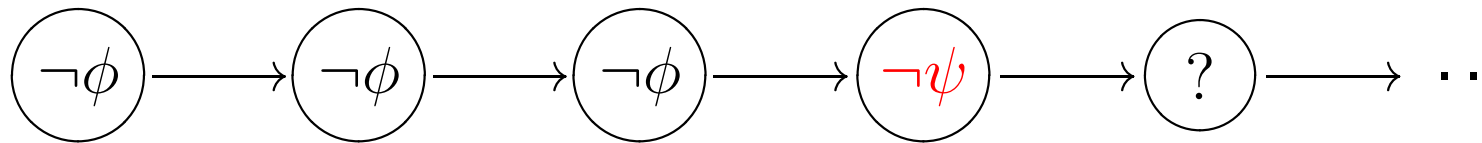
Prawa de Morgane'a:

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

$$G\phi \equiv \neg F\neg\phi$$

$$\phi R\psi \equiv \neg(\neg\phi U\neg\psi)$$

$\neg\phi U\neg\psi$



$\Pi \models \phi R\psi$ wtw gdy ?

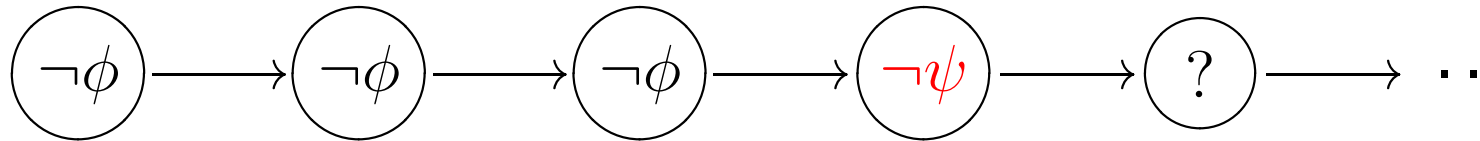
Prawa de Morgane'a:

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

$$G\phi \equiv \neg F\neg\phi$$

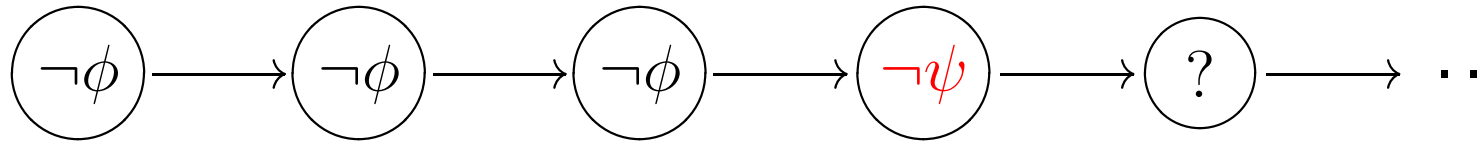
$$\phi R\psi \equiv \neg(\neg\phi U\neg\psi)$$

$\neg\phi U\neg\psi$



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

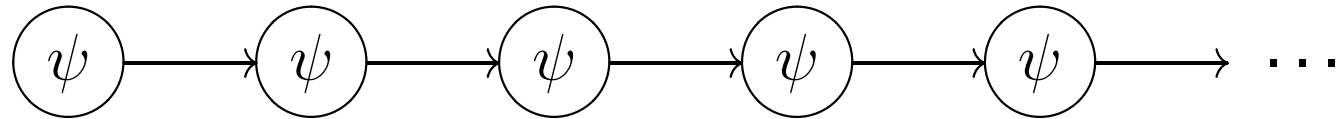
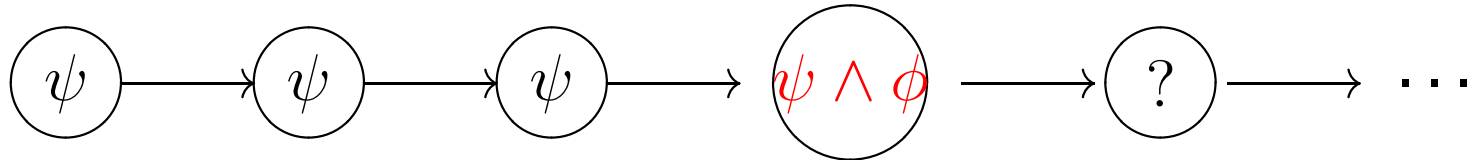
$\neg\phi U \neg\psi$



$\phi R \psi \equiv \neg(\neg\phi U \neg\psi)$

$\Pi \models \phi R \psi$ wtw gdy $\forall i < |\Pi|. (\forall j < i. \Pi^j \models \neg\phi) \implies \Pi^i \models \psi$

$\phi R \psi$



$\phi R \psi \equiv \neg(\neg\phi U \neg\psi) \equiv \psi U (\psi \wedge \phi) \vee G\psi \equiv \psi W (\psi \wedge \phi)$

(1) jeśli b to wcześniej było a ?

(1') ... ściśle wcześniej ... ?

(2) każde b jest poprzedzane przez a , ale po poprzednim b ,

jeśli takie było ?

(3) naprzemienne bloki a i b („sztafeta”) ?

(1) jeśli b to wcześniej było a

$$Fb \implies (\neg b U a)$$

$$\equiv \neg b W a \equiv Pr(a, b)$$

(1') ... ściśle wcześniej ...

$$Fb \implies (\neg b U (a \wedge \neg b))$$

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

(2) każde b jest poprzedzane przez a , ale po poprzednim b ,

jeśli takie było

$$Pr(a, b) \wedge G(b \implies XPr(a, b))$$

(3) naprzemienne bloki a i b („sztafeta”)

$$G((a \implies aW(\neg a \wedge b)) \wedge (b \implies \dots))$$

czego się nie da wyrazić?

(1) na każdej ścieżce osiągniemy stan taki, że
w każdym bezpośrednio następnym stanie
(na dowolnej ścieżce) zachodzi a

$F X a ?$

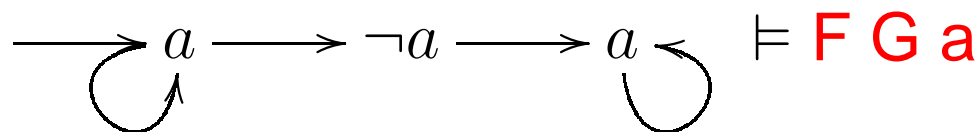
(1') możemy osiągnąć stan taki, że ...

?

(2) na każdej ścieżce osiągniemy stan taki, że
w każdym następnym stanie zachodzi a

$F G a ?$

za dużo!



czego się nie da wyrazić? (cd)

(3) even(a): na każdej parzystej pozycji jest a ?

(3') oddeven(a): na każdej parzystej pozycji jest a

a na każdej nieparzystej jest $\neg a$

$$G((a \implies X\neg a) \wedge (\neg a \implies Xa))$$

(4) z każdego stanu osiągalnego można wrócić do stanu

pocz.

Tw.: LTL = LTL(X, U) jest bardziej ekspresywny niż LTL(X, F)

Tw.: LTL = FO

Tw.: Przeszłe spójniki logiczne:

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

nie zmieniają siły wyrazu.

Tw.: LTL(F, G, F⁻¹, G⁻¹) = ?

Weryfikacja modelowa

PSPACE-zupełny

- dane: M, ϕ
- pytanie: $M \models \phi?$

Spełnialność

PSPACE-zupełny

- dane: ϕ
- pytanie: $\exists M. M \models \phi?$

$$\Phi = Q_1x_1Q_2x_2 \dots Q_nx_n \cdot \bigwedge_{i=1}^m \bigvee_{j=1}^{k_i} l_{i,j}$$

$$l_{i,j} = x_{r(i,j)} \text{ lub } l_{i,j} = \neg x_{r(i,j)}$$

Lem.: Φ prawdziwa $\iff \exists V \subseteq \{0, 1\}^{\{x_1, \dots, x_n\}}$ taki, że

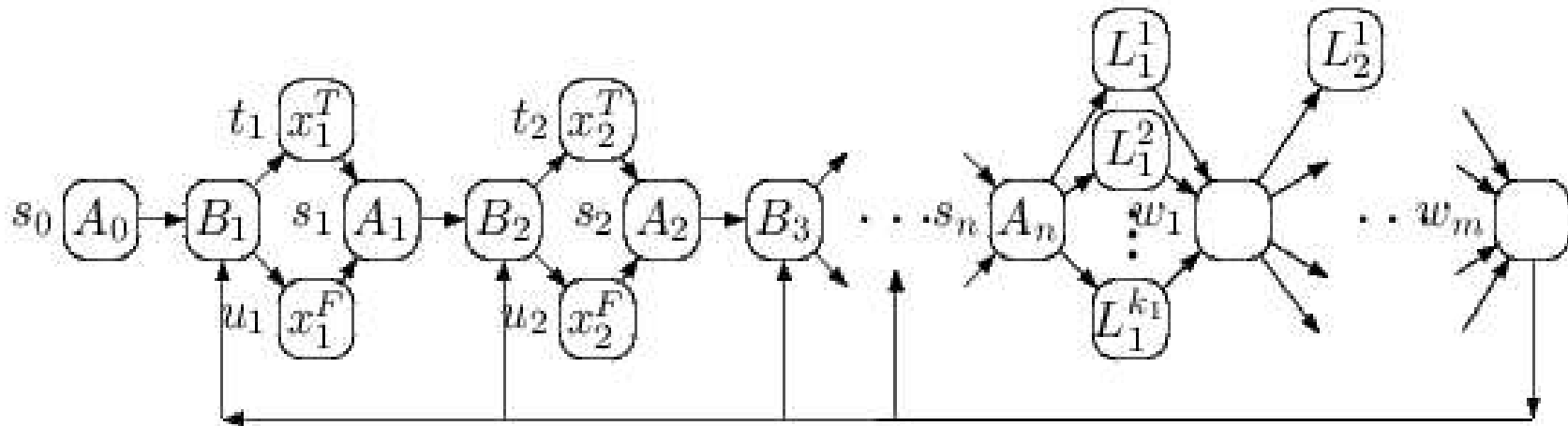
(0) $V \neq \emptyset$

(1) $\forall v \in V. v \models \Phi$

(2) $\forall v \in V. \forall i \leq n. Q_i = \text{“}\forall\text{”} \implies$

$$\exists v' \in V. v'(x_i) \neq v(x_i) \wedge \forall j < i. v(x_j) = v'(x_j)$$

$$\Phi = Q_1 x_1 Q_2 x_2 \dots Q_n x_n \cdot \bigwedge_{i=1}^m \bigvee_{j=1}^{k_i} l_{i,j}$$



Φ prawdziwa $\iff \exists$ ścieżka $\Pi. \Pi \models \phi \wedge \psi$

	$n - 1, k < \omega$	Model checking	Satisfiability
$L(\dots)$	$L_n^0(\dots)$	L	L
	$L_\omega^0(\dots)$	L [Lyn77]	NP-complete [Coo71]
$L(F)$	$L(F)$	NP-complete [SC85]	NP-complete [ON80]
	$L_\omega^1(F)$	NP-complete	NP-complete
	$L_2^\omega(F)$	NP-complete	NP-complete
	$L_1^\omega(F)$	in P, NL-hard	P
	$L_n^{k+1}(F)$	NL-complete	L
$L(U^?)$	$L(U^?)$	PSPACE-complete [SC85]	PSPACE-complete [SC85, HR83]
	$L_\omega^2(U^?)$	PSPACE-complete	PSPACE-complete
	$L_\omega^1(U^?)$	NP-complete	NP-complete
	$L_2^\omega(U^?)$	PSPACE-complete	PSPACE-complete
	$L_1^\omega(U^?)$	in P, NL-hard	P
	$L_n^{1+k}(U^?)$	NL-complete	L
$L(X)$	$L(X)$	NP-complete	NP-complete
	$L_\omega^k(X)$	L	NP-complete
	$L_1^\omega(X)$	NP-complete	NP-complete
	$L_n^k(X)$	L	L
$L(F, X)$	$L(F, X)$	PSPACE-complete [SC85]	PSPACE-complete [SC85, HR83]
	$L_\omega^{2+k}(F, X)$	NP-complete	PSPACE-complete [Har85, Spa93]
	$L_\omega^1(F, X)$	NP-complete	NP-complete
	$L_1^\omega(F, X)$	PSPACE-complete	PSPACE-complete
	$L_n^{1+k}(F, X)$	NL-complete	L
$L(U^?, X)$	$L(U^?, X)$	PSPACE-complete [SC85]	PSPACE-complete [SC85, HR83]
	$L_\omega^2(U^?, X)$	PSPACE-complete	PSPACE-complete [Har85, Spa93]
	$L_\omega^1(U^?, X)$	NP-complete	NP-complete
	$L_1^\omega(U^?, X)$	PSPACE-complete	PSPACE-complete
	$L_n^{1+k}(U^?, X)$	NL-complete	L

Złoty obszar weryfikacji modelowej:

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

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

$|M|$ za duży!

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

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

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

$$\text{tak} \rightarrow M \models \phi$$

$$\text{nie} \rightarrow \neg(M \models \phi), \text{ kontrprzykład} = \text{ścieżka w } M$$

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

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

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

tak $\rightarrow M \models \phi$

nie $\rightarrow \neg(M \models \phi)$, **kontrprzykład = ścieżka w M**

$$\phi = G(p \implies XFq)$$

