Praktyczne metody weryfikacji

Wykład 2: LTL

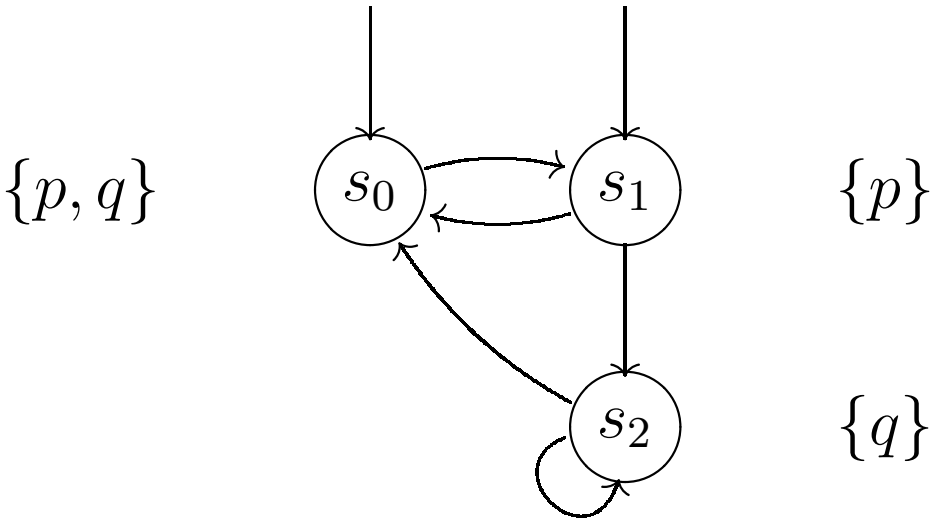
Def.: Struktura Kripkego $M = \langle S, S_{\text{pocz}}, \rightarrow, L \rangle$

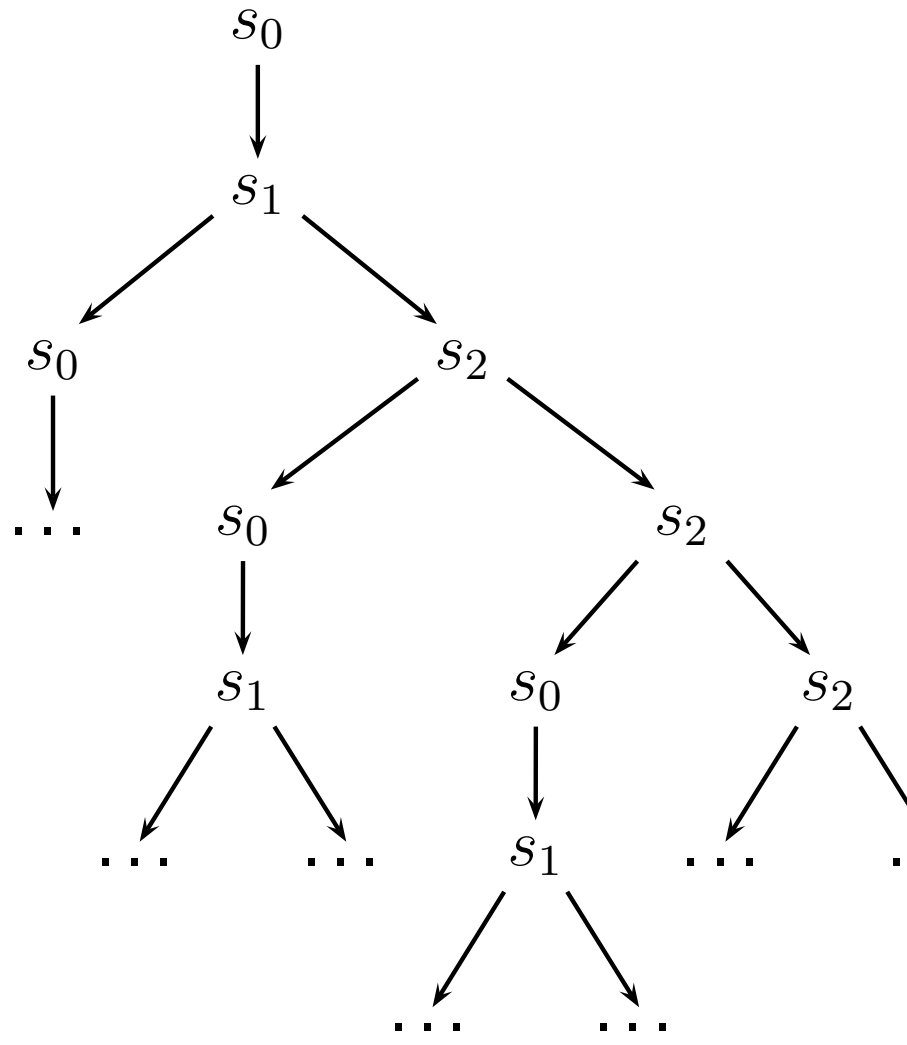
- $S_{\text{pocz}} \subseteq S$ niepusty zbiór stanów początkowych
- $\rightarrow \subseteq S \times S$ relacja przejścia
- $L : S \rightarrow \mathcal{P}(P)$, P - zmienne zdaniowe (własności atomowe)

Często zakładamy, że $\rightarrow$ jest całkowita: brak blokady!

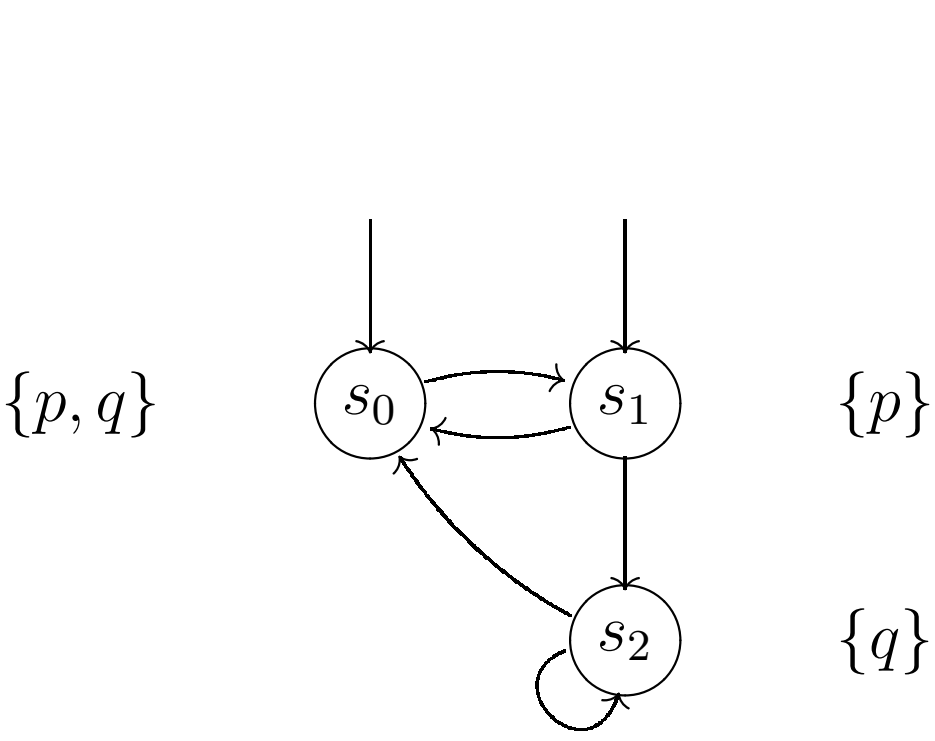
$$\forall s \in S.\ \exists s' \in S.\ s \rightarrow s'$$

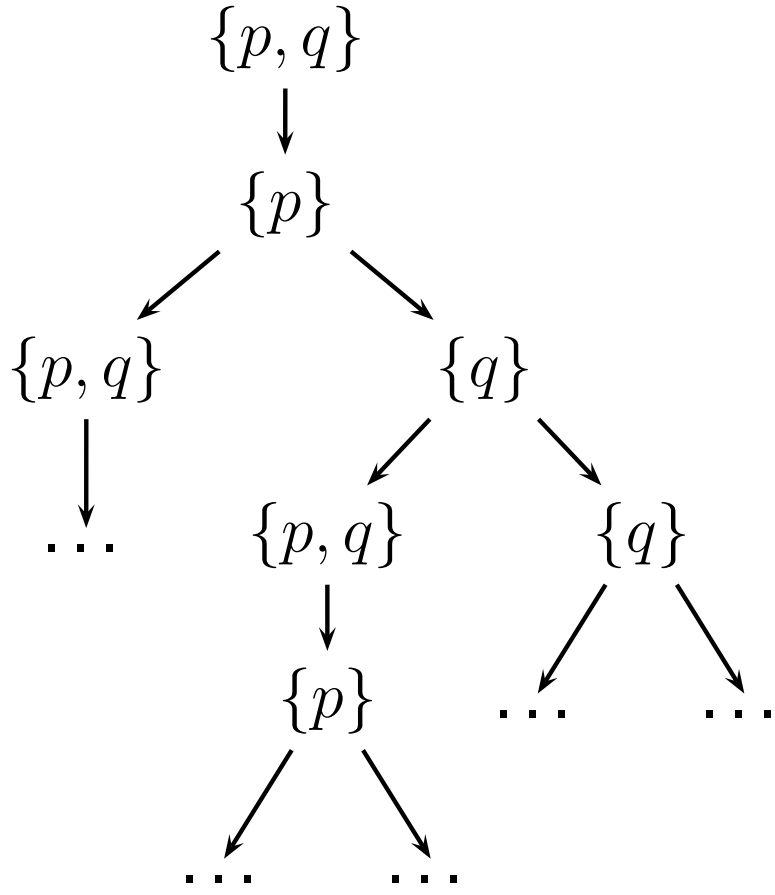
Przykład





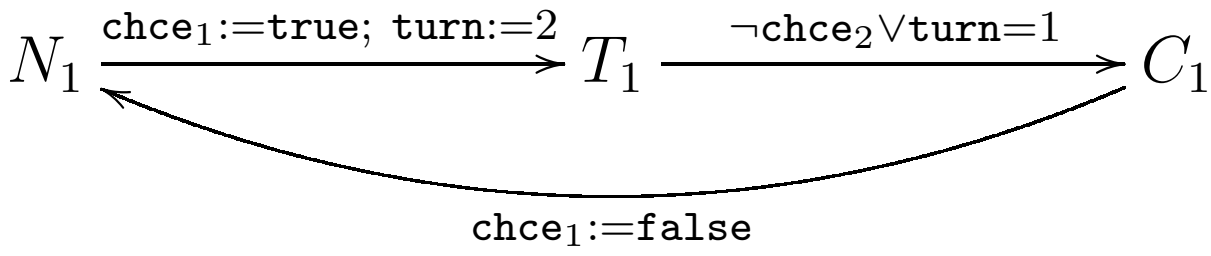
Przykład



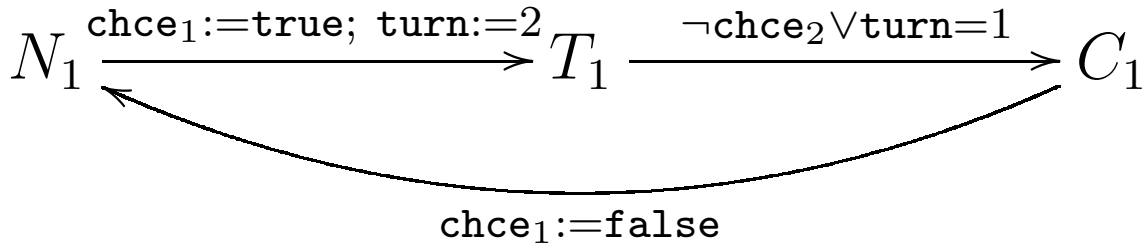


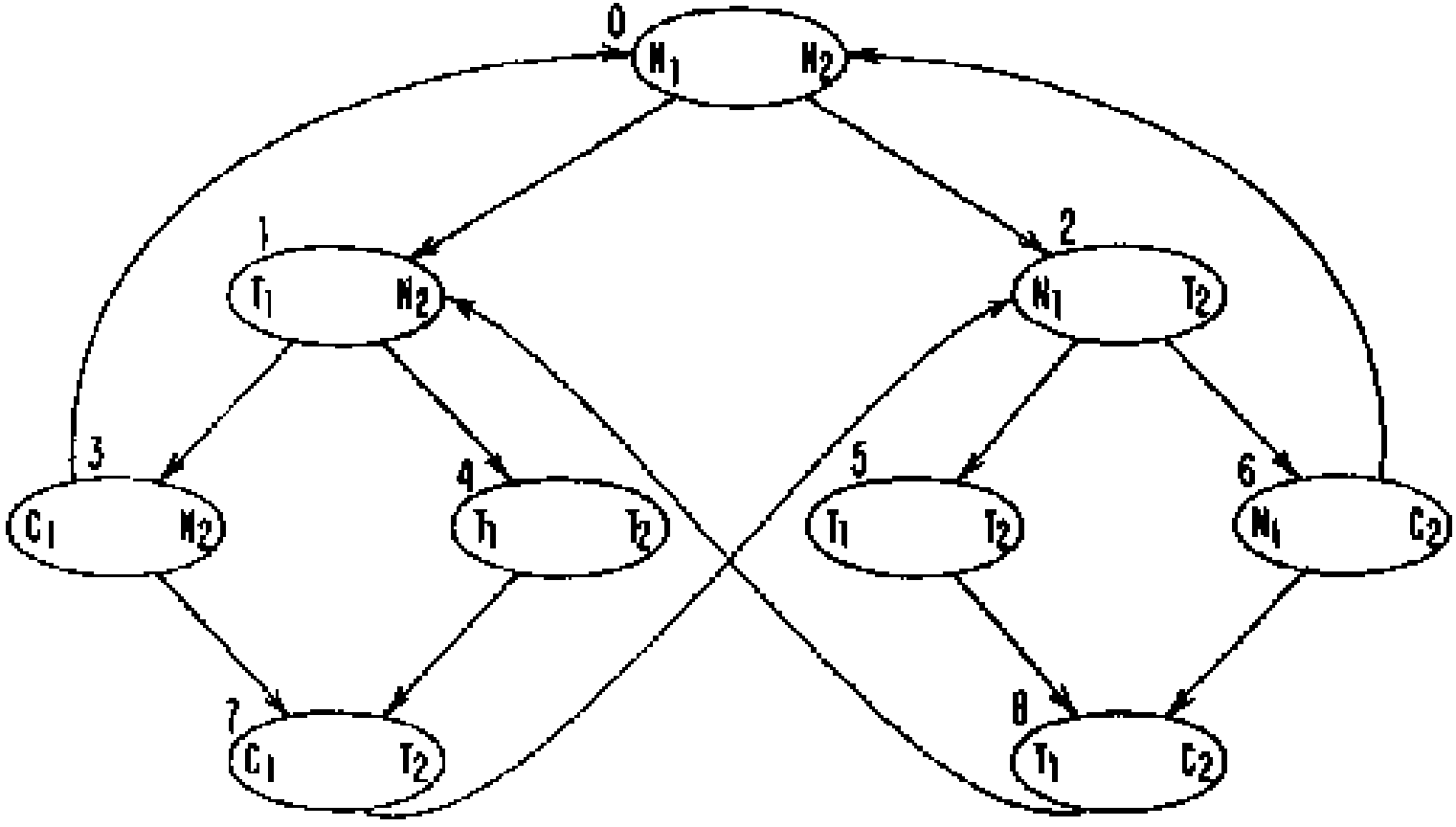
program $\mapsto$ struktura Kripkego

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



program $\mapsto$ struktura Kripkego





Def.: Ścieżka (przebieg) to maksymalny ciąg

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

Ozn.: $|\Pi|$ – liczba stanów w Π

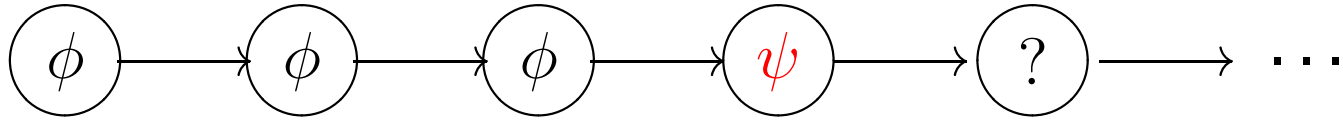
LTL wyraża własności ścieżek. Na strukturze Kripkego M, formułe $\phi \in$ LTL interpretujemy następująco:
dla każdej ścieżki takiej, że $s_0 \in S_{\text{pocz}}$, zachodzi ϕ.

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

Def.: LTL (Linear Temporal Logic)

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

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

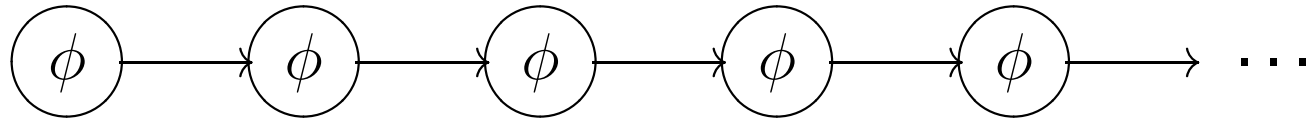


Przykład:

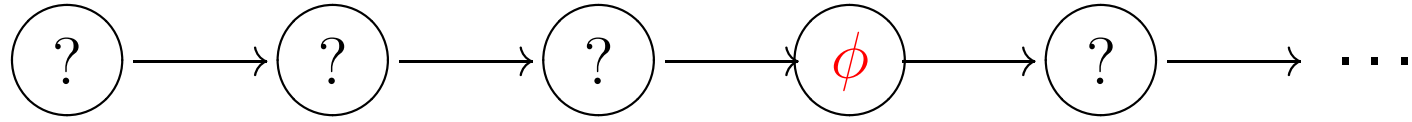
$$\neg\texttt{starts}\ \mathsf{U}\ \texttt{key}, \qquad \neg\texttt{starts}\ \mathsf{U}\ \neg\texttt{starts} \wedge \texttt{key}$$

Pytanie: Jak zapisać

zawsze ϕ

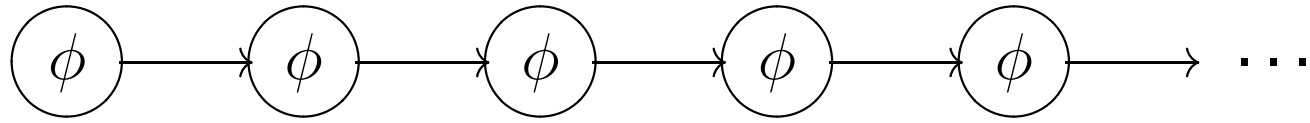


kiedyś ϕ

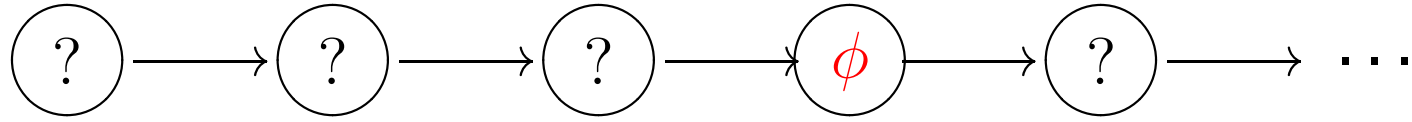


Pytanie: Jak zapisać

zawsze ϕ



kiedyś ϕ



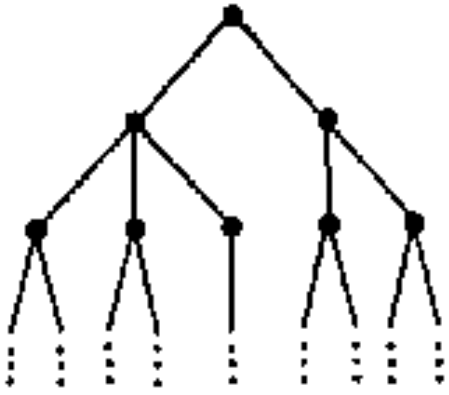
Notacja:

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

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

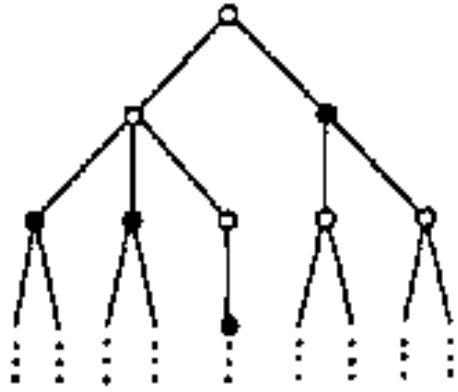
$$\phi_1 \vee \phi_2 \;\equiv\; \neg(\neg\phi_1 \wedge \neg\phi_2)$$

typowe własności



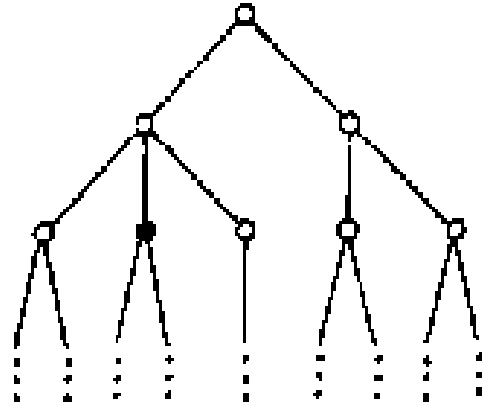
bezpieczeństwo

?



żywotność

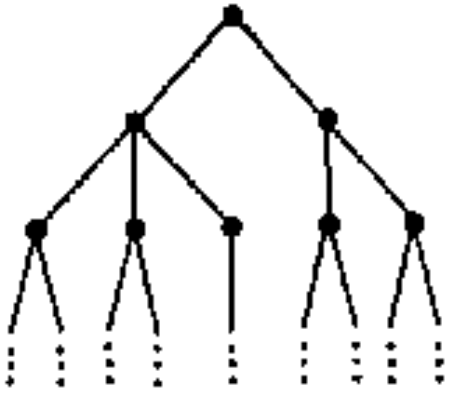
?



możliwość

?

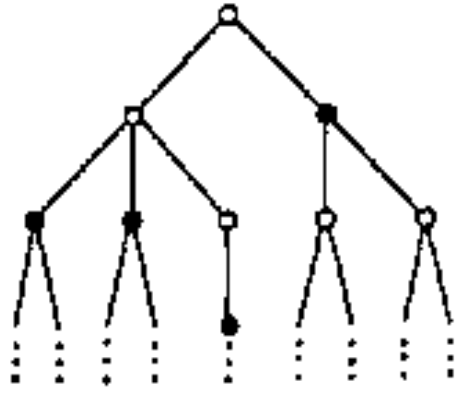
typowe własności



bezpieczeństwo

$\mathsf{G}\,\phi$

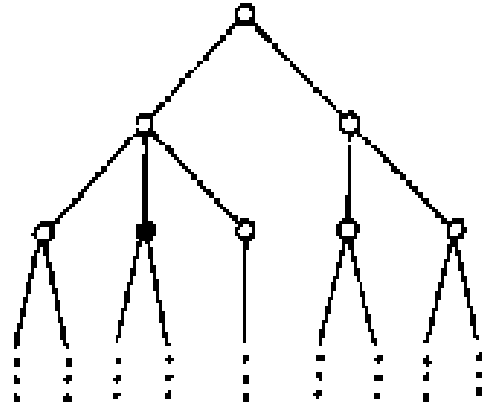
$\mathsf{G}\,\neg(\mathtt{cr}_1 \wedge \mathtt{cr}_2)$



żywotność

$\mathsf{F}\,\phi$

$\mathsf{F}\,\mathtt{granted}$



możliwość

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

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

$\mathsf{G}\,\neg\mathtt{occ}$

Semantyka: $\Pi = s_0 \to s_1 \to s_2 \to \ldots$

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

$\Pi \models \neg\phi$ wtw gdy $\ldots$

$\Pi \models \phi_1 \wedge \phi_2$ wtw gdy $\ldots$

$\Pi \models \mathsf{X}\,\phi$ wtw gdy $\Pi^1 \models \phi$, gdzie $\Pi^i = s_i \to s_{i+1} \to s_{i+2} \to \ldots$

$\Pi \models \phi_1 \,\mathsf{U}\, \phi_2$ 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 : ϕ_1 W ϕ_2 (ϕ_2 niekoniecznie) ?
- jeśli `req` to w przyszłości `granted` ?
- sprawiedliwość: jeśli uparcie `req` to `granted` ?

przykładowe własności

- nieskończenie wiele razy ϕ $\quad \mathsf{G}\,\mathsf{F}\,\phi$
- prawie zawsze ϕ $\quad \mathsf{F}\,\mathsf{G}\,\phi$
- „słaby” $\phi_1\,\mathsf{U}\,\phi_2$: ϕ_2 nieobowiązkowo $\quad \mathsf{G}\,\phi_1 \vee \phi_1\,\mathsf{U}\,\phi_2$
- jeśli `req` to w przyszłości `granted`

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

- sprawiedliwość: jeśli uparcie `req` to `granted`

  „słaba”: uparcie = prawie zawsze ?

  „silna”: uparcie = nieskończenie wiele ?

przykładowe własności

- nieskończenie wiele razy ϕ $\quad \mathsf{G}\,\mathsf{F}\,\phi$
- prawie zawsze ϕ $\quad \mathsf{F}\,\mathsf{G}\,\phi$
- „słaby” $\phi_1\,\mathsf{U}\,\phi_2$: ϕ_2 nieobowiązkowo $\quad \mathsf{G}\,\phi_1 \vee \phi_1\,\mathsf{U}\,\phi_2$
- jeśli `req` to w przyszłości `granted`

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

- sprawiedliwość: jeśli uparcie `req` to `granted`

„słaba”: uparcie = pr. zawsze $\quad \mathsf{F}\,\mathsf{G}\,\texttt{req} \implies \mathsf{F}\,\texttt{granted}$

„silna”: uparcie = niesk. wiele $\quad \mathsf{G}\,\mathsf{F}\,\texttt{req} \implies \mathsf{F}\,\texttt{granted}$

sprawiedliwość

(jeśli uparcie `req` to `granted`)

Wariant 1

„słaba”: uparcie = pr. zawsze $\quad \mathsf{F}\,\mathsf{G}\,\texttt{req} \implies \mathsf{F}\,\texttt{granted}$

„silna”: uparcie = niesk. wiele $\quad \mathsf{G}\,\mathsf{F}\,\texttt{req} \implies \mathsf{F}\,\texttt{granted}$

Wariant 2

„słaba”: $\mathsf{F}\,\mathsf{G}\,\texttt{req} \implies \mathsf{G}\,\mathsf{F}\,\texttt{granted} = \mathsf{G}\,(FG\texttt{req} \implies \mathsf{F}\,\texttt{granted})$

„silna”: $\mathsf{G}\,\mathsf{F}\,\texttt{req} \implies \mathsf{G}\,\mathsf{F}\,\texttt{granted} = \mathsf{G}\,(GF\texttt{req} \implies \mathsf{F}\,\texttt{granted})$

Prawa de Morgane'a

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

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

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

Prawa de Morgane'a

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

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

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

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

Prawa de Morgane'a

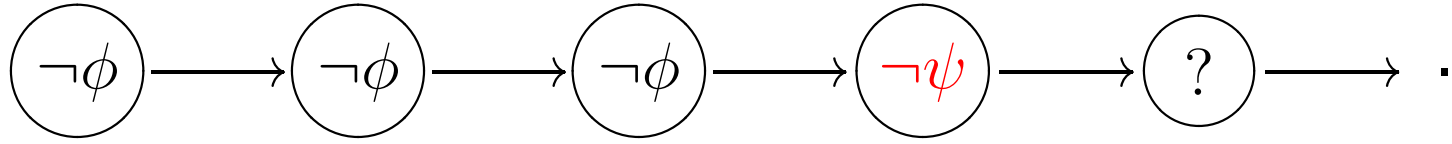
$\phi_1 \vee \phi_2 \equiv \neg(\neg\phi_1 \wedge \neg\phi_2)$

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

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

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

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



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

Prawa de Morgane'a

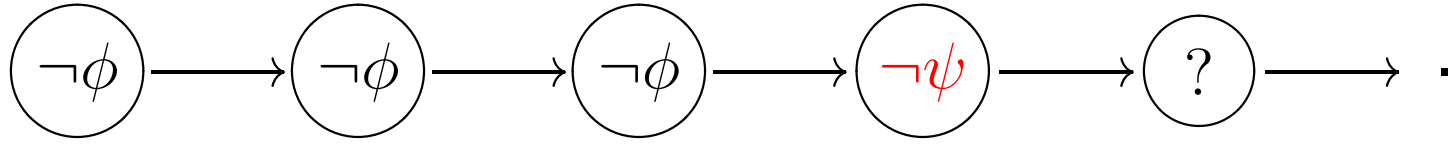
$$\phi_1 \vee \phi_2 \equiv \neg(\neg\phi_1 \wedge \neg\phi_2)$$

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

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

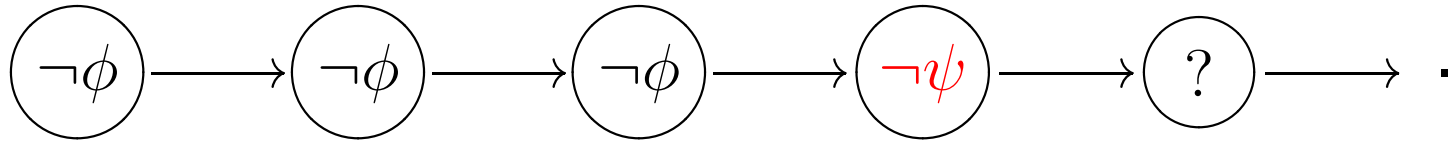
$$\phi\,\mathsf{R}\,\psi \equiv \neg(\neg\phi\,\mathsf{U}\,\neg\psi)$$

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



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

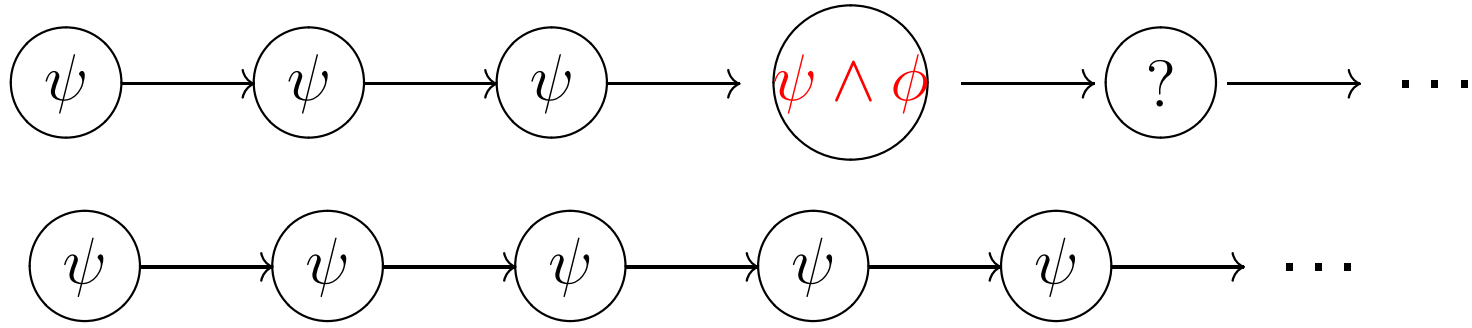
$\neg\phi \,\mathsf{U}\, \neg\psi$



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

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

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



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

Spychanie negacji

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

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

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

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

Spychanie negacji

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

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

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

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

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

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

napisz formułę . . .

(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") ?

napisz formułę

(1) jeśli b to wcześniej było a $\quad \mathsf{F}\, b \implies (\neg b\, \mathsf{U}\, a)$

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

(1') . . . ściśle wcześniej . . . $\quad \mathsf{F}\, b \implies (\neg b\, \mathsf{U}\, (a \wedge \neg b))$

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

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

jeśli takie było $\quad Pr(a, b) \wedge \mathsf{G}\, (b \implies \mathsf{X}\, Pr(a, b))$

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

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

czego się nie da wyrazić?

(1) na każdej ścieżce osiągniemy stan taki, że

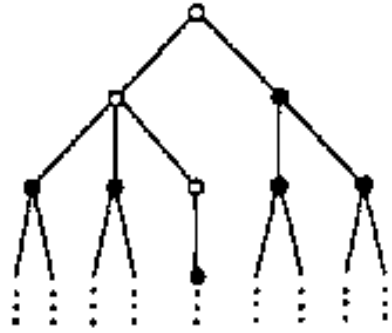
w każdym bezpośrednio następnym stanie ?

(na dowolnej ścieżce) zachodzi a

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

(2) na każdej ścieżce osiągniemy stan taki, że

w każdym następnym stanie zachodzi a ?



czego się nie da wyrazić?

(1) na każdej ścieżce osiągniemy stan taki, że

w każdym bezpośrednio następnym stanie F X a ?

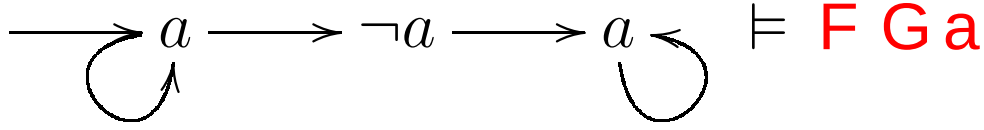
(na dowolnej ścieżce) zachodzi a

(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 $\neg a$

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

(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:

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

nie zmieniają siły wyrazu.

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

Def.: Własność = podzbiór $\mathcal{P}(P)^\omega$

Własność bezpieczeństwa X

decyzja negatywna zawsze po skończonej liczbie kroków

Własność żywotności X

decyzja negatywna nigdy po skończonej liczbie kroków

Def.: Własność = podzbiór $\mathcal{P}(P)^\omega$

Własność bezpieczeństwa X

decyzja negatywna zawsze po skończonej liczbie kroków

jeśli $\pi \notin X$ to istnieje prefiks $\rho < \pi$ t. że jeśli $\rho < \pi'$ to $\pi' \notin X$

Własność żywotności X

decyzja negatywna nigdy po skończonej liczbie kroków

dla każdego ρ istnieje $\pi > \rho$ t. że $\pi \in X$

Weryfikacja modelowa

PSPACE-zupełny

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

Spełnialność

PSPACE-zupełny

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

Redukcja: QBF $\mapsto$ MC

$$\Phi = Q_i x_1 Q_2 x_2 \ldots Q_n x_n .\ \wedge_{i=1}^{m}\ \vee_{j=1}^{k_i}\ l_{i,j}$$

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

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

(0) $V \neq \emptyset$

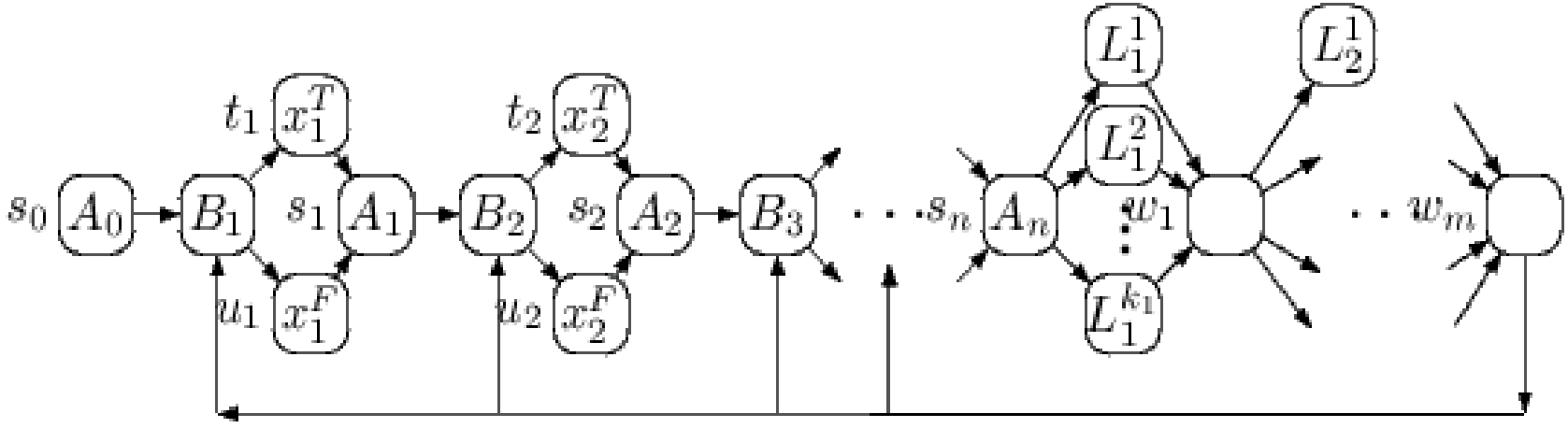
(1) $\forall v \in V.\quad v \vDash\ \wedge_{i=1}^{m}\ \vee_{j=1}^{k_i}\ l_{i,j}$

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

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

Redukcja: QBF $\mapsto$ MC

$$\Phi = Q_i x_1 Q_2 x_2 \ldots Q_n x_n . \wedge_{i=1}^{m} \vee_{j=1}^{k_i} l_{i,j}$$



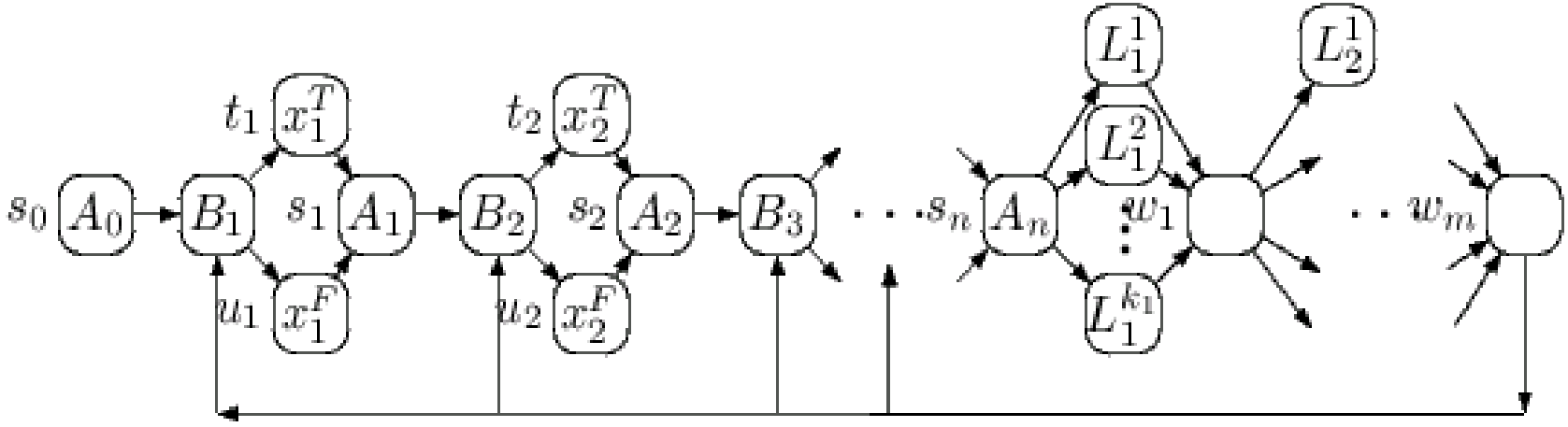
[Demri, Schnoebelen 2002]

$$\psi_{i,j} \equiv \begin{cases} \mathsf{G}\,(x_k^F \implies \mathsf{G}\,\neg L_i^j \vee \neg L_i^j \,\mathsf{U}\, B_k) & \text{gdy } l_{i,j} = x_k \\ \mathsf{G}\,(x_k^T \implies \mathsf{G}\,\neg L_i^j \vee \neg L_i^j \,\mathsf{U}\, B_k) & \text{gdy } l_{i,j} = \neg x_k \end{cases}$$

$$(1) \qquad \psi \equiv \wedge_{i=1}^{m} \wedge_{j=1}^{k_i} \psi_{i,j}$$

Redukcja: QBF $\mapsto$ MC

$$\Phi = Q_i x_1 Q_2 x_2 \ldots Q_n x_n . \wedge_{i=1}^{m} \vee_{j=1}^{k_i} l_{i,j}$$



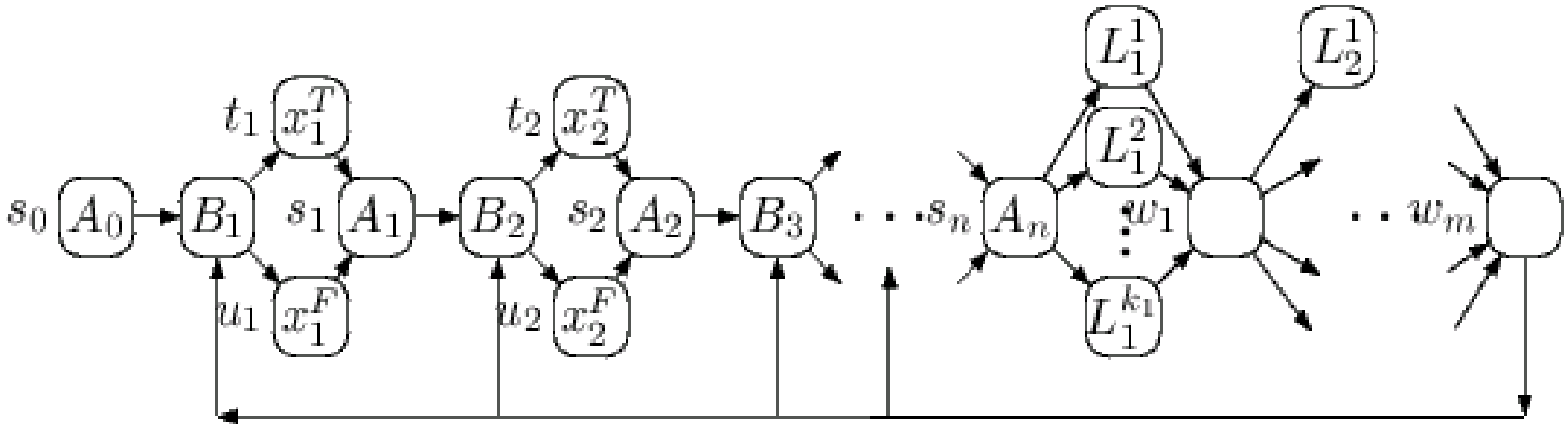
[Demri, Schnoebelen 2002]

$$\phi_i \equiv \mathsf{G}\,(A_{i-1} \implies (\neg B_{i-1}\,\mathsf{U}\,x_i^T) \wedge (\neg B_{i-1}\,\mathsf{U}\,x_i^F))$$

$$(2) \qquad \phi \equiv \wedge\{\phi_i | Q_i = \text{“}\forall''\}$$

Redukcja: QBF $\mapsto$ MC

$$\Phi = Q_i x_1 Q_2 x_2 \ldots Q_n x_n .\ \wedge_{i=1}^{m} \ \vee_{j=1}^{k_i} \ l_{i,j}$$



[Demri, Schnoebelen 2002]

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

	$n-1, k < \omega$	Model checking	Satisfiability
$\mathrm{L}(\ldots)$	$\mathrm{L}_n^0(\ldots)$	L	L
	$\mathrm{L}_\omega^0(\ldots)$	L [Lyn77]	NP-complete [Coo71]
$\mathrm{L}(\mathsf{F})$	$\mathrm{L}(\mathsf{F})$	NP-complete [SC85]	NP-complete [ON80]
	$\mathrm{L}_\omega^1(\mathsf{F})$	NP-complete	NP-complete
	$\mathrm{L}_2^\omega(\mathsf{F})$	NP-complete	NP-complete
	$\mathrm{L}_1^\omega(\mathsf{F})$	in P, NL-hard	P
	$\mathrm{L}_n^{k+1}(\mathsf{F})$	NL-complete	L
$\mathrm{L}(\mathsf{U}^?)$	$\mathrm{L}(\mathsf{U}^?)$	PSPACE-complete [SC85]	PSPACE-complete [SC85, HR83]
	$\mathrm{L}_\omega^2(\mathsf{U}^?)$	PSPACE-complete	PSPACE-complete
	$\mathrm{L}_\omega^1(\mathsf{U}^?)$	NP-complete	NP-complete
	$\mathrm{L}_2^\omega(\mathsf{U}^?)$	PSPACE-complete	PSPACE-complete
	$\mathrm{L}_1^\omega(\mathsf{U}^?)$	in P, NL-hard	P
	$\mathrm{L}_n^{1+k}(\mathsf{U}^?)$	NL-complete	L
$\mathrm{L}(\mathsf{X})$	$\mathrm{L}(\mathsf{X})$	NP-complete	NP-complete
	$\mathrm{L}_\omega^k(\mathsf{X})$	L	NP-complete
	$\mathrm{L}_1^\omega(\mathsf{X})$	NP-complete	NP-complete
	$\mathrm{L}_n^k(\mathsf{X})$	L	L
$\mathrm{L}(\mathsf{F},\mathsf{X})$	$\mathrm{L}(\mathsf{F},\mathsf{X})$	PSPACE-complete [SC85]	PSPACE-complete [SC85, HR83]
	$\mathrm{L}_\omega^{2+k}(\mathsf{F},\mathsf{X})$	NP-complete	PSPACE-complete [Har85, Spa93]
	$\mathrm{L}_\omega^1(\mathsf{F},\mathsf{X})$	NP-complete	NP-complete
	$\mathrm{L}_1^\omega(\mathsf{F},\mathsf{X})$	PSPACE-complete	PSPACE-complete
	$\mathrm{L}_n^{1+k}(\mathsf{F},\mathsf{X})$	NL-complete	L
$\mathrm{L}(\mathsf{U}^?,\mathsf{X})$	$\mathrm{L}(\mathsf{U}^?,\mathsf{X})$	PSPACE-complete [SC85]	PSPACE-complete [SC85, HR83]
	$\mathrm{L}_\omega^2(\mathsf{U}^?,\mathsf{X})$	PSPACE-complete	PSPACE-complete [Har85, Spa93]
	$\mathrm{L}_\omega^1(\mathsf{U}^?,\mathsf{X})$	NP-complete	NP-complete
	$\mathrm{L}_1^\omega(\mathsf{U}^?,\mathsf{X})$	PSPACE-complete	PSPACE-complete
	$\mathrm{L}_n^{1+k}(\mathsf{U}^?,\mathsf{X})$	NL-complete	L

[Demri, Schnoebelen 2002]

Złożoność weryfikacji modelowej:

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

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

$|M|$ za dużo!

Algorytm

(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 $\rightarrow$ $M \vDash \phi$

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

Algorytm

(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 $\rightarrow$ $M \vDash \phi$

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

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

$A_{\neg\phi} =$