

Praktyczne metody weryfikacji

Wykład 4: Weryfikacja modelowa dla LTL

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

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

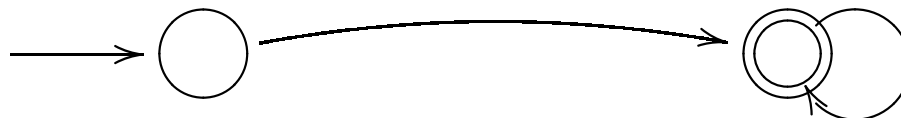
(a nie $\phi \mapsto \mathcal{A}_\phi \mapsto \bar{\mathcal{A}}_\phi$)

(iii) $L_\omega(\mathcal{A}_M) \cap L_\omega(\mathcal{A}_{\neg\phi}) = \emptyset$? (a nie $L_\omega(\mathcal{A}_M) \subseteq L_\omega(\mathcal{A}_\phi)$)

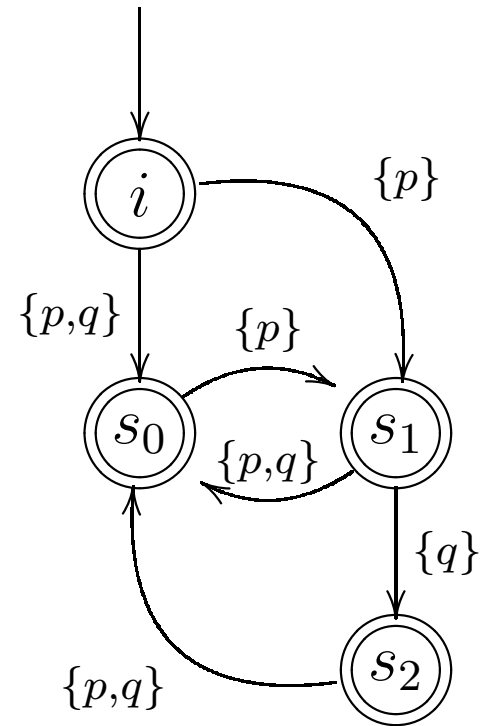
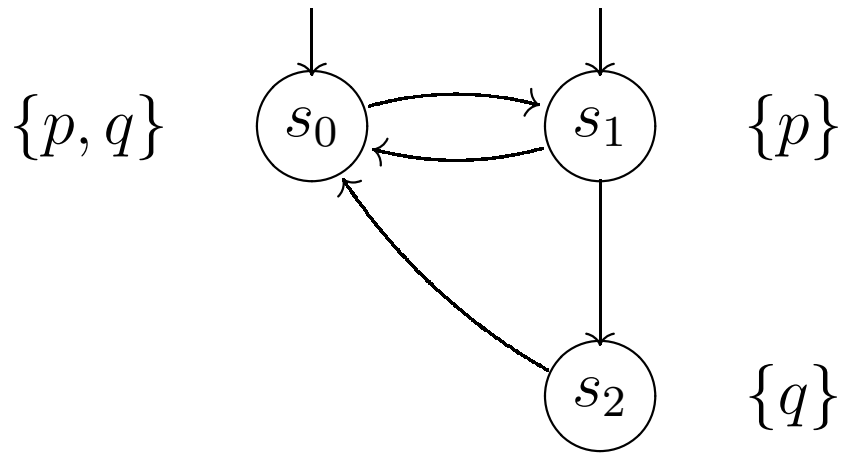
$L_\omega(\mathcal{A}_M \times \mathcal{A}_{\neg\phi}) = \emptyset$?

tak $\rightarrow M \models \phi$

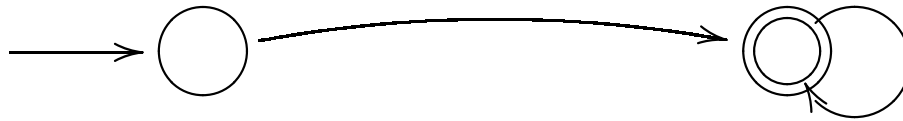
nie $\rightarrow \neg(M \models \phi)$, **kontrprzykład = ścieżka w M**

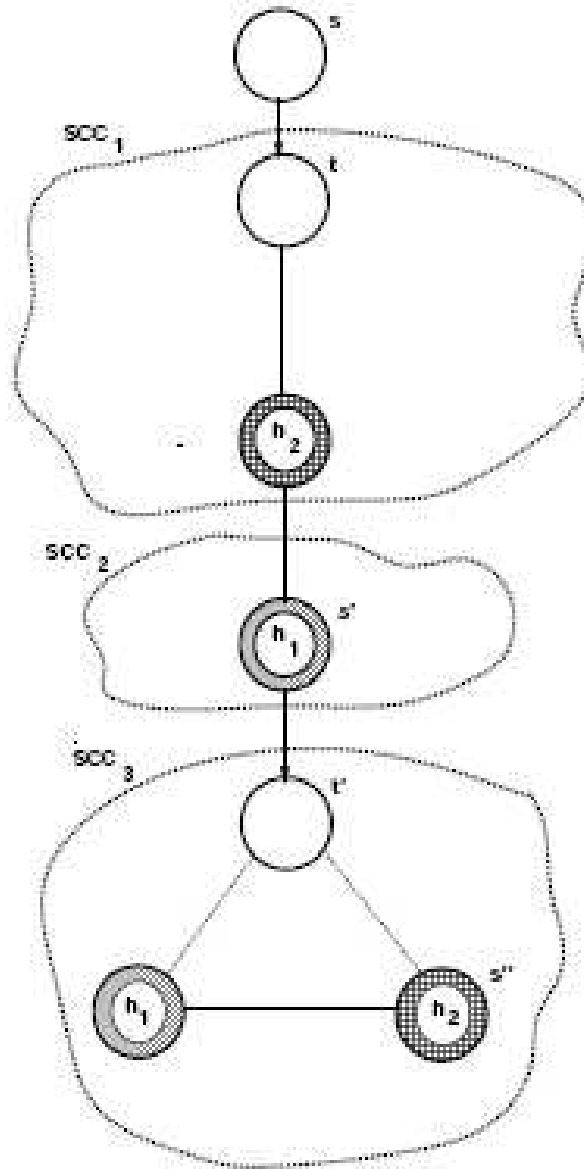


$$(i) \quad M \mapsto \mathcal{A}_M$$



(iii) $L_\omega(\mathcal{A}) \neq \emptyset?$





[Clarke, Grumberg, Peled 2000]

(1) Weryfikacja w locie

for each successor t of s do ...

...

```

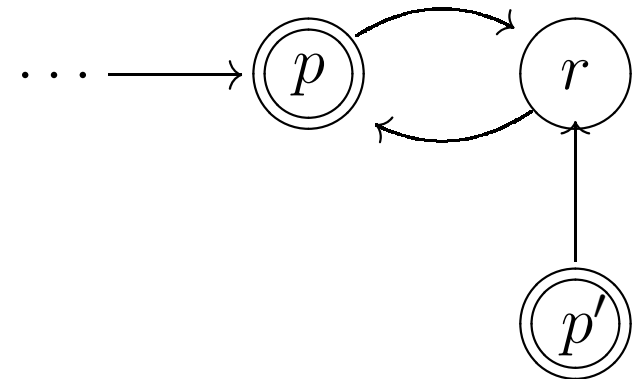
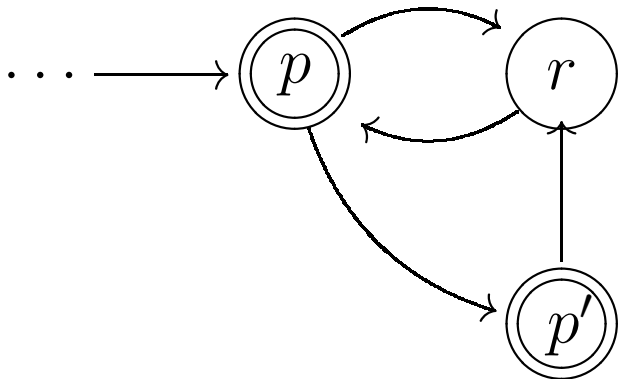
proc dfs(s)
  if error(s) then report error fi
  add {s,0} to Statespace
  for each successor t of s do
    if {t,0} not in Statespace then dfs(t) fi
  od
  if accepting(s) then seed:=s; ndfs(s) fi
end
proc ndfs(s) /* the nested search */
  add {s,1} to Statespace
  for each successor t of s do
    if {t,1} not in Statespace then ndfs(t) fi
    else if t==seed then report cycle fi
  od
end

```


Założmy, że jest stan akceptujący p , który ma cykl niewykryty w $\text{ndfs}(p)$. Niech p – pierwszy taki stan.

Niech r – pierwszy stan odwiedzony w $\text{ndfs}(p)$ t.ż. r jest na cyklu zawierającym p i $\{r, 1\}$ in Statespace.

Niech p' – stan akceptujący t.ż. r osiągnięto w $\text{ndfs}(p')$.

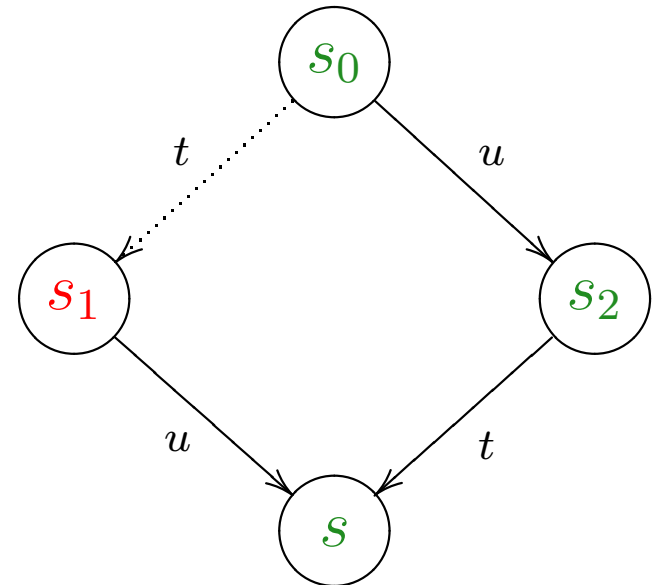


(1) Weryfikacja w locie

for each successor t of s do ...

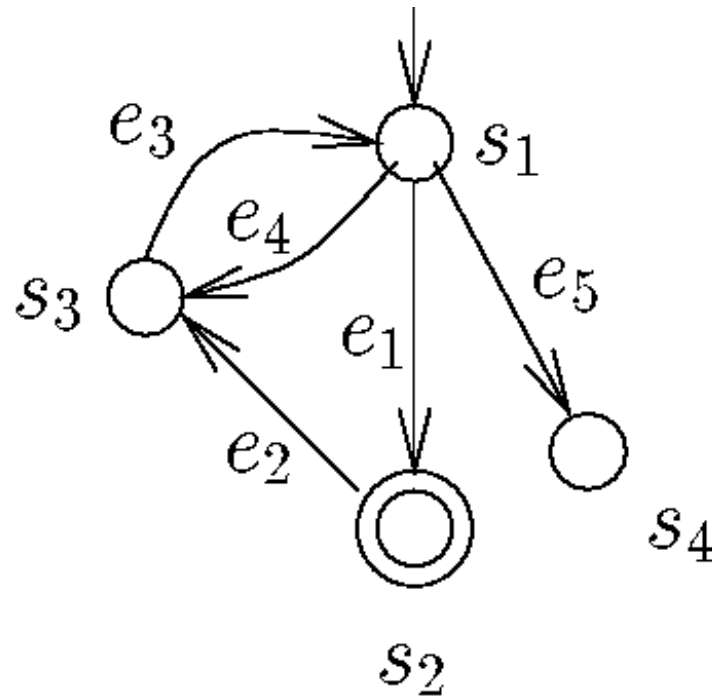
(2) Redukcje częściowo-porzędkowe

for each (**selected**) successor t of s do ...



for each (**selected**) successor t of s do ...

(**selected**) – zależy od dotychczasowej ścieżki !



[Holzmann, Peled, Yannakakis 1996]

```
proc dfs(s)
  if error(s) then report error fi
  add {s,0} to Statespace
  add s to Stack
  for each (selected) successor t of s do
    if {t,0} not in Statespace then dfs(t) fi
  od
  if accepting(s) then ndfs(s) fi
  delete s from Stack
end
proc ndfs(s) /* the nested search */
  add {s,1} to Statespace
  for each (selected) successor t of s do
    if {t,1} not in Statespace then ndfs(t) fi
    else if t in Stack then report cycle fi
  od
end
```

[Holzmann,Peled,Yannakakis 1996]

np-cycles: FG \rightarrow progress

```
proc dfs(s)
  if error(s) then report error fi
  add {s,0} to Statespace
  for each successor t of s do
    if {t,0} not in Statespace then dfs(t) fi
  od
  ndfs(s) /* different */
end
proc ndfs(s) /* the nested search */
  if s is Progress State then return fi /* new */
  add {s,1} to Statespace
  add s to Stack /* new */
  for each successor t of s do
    if {t,1} not in Statespace then ndfs(t) fi
    else if t is in Stack then report cycle fi /* different */
  od
  delete s from Stack /* new */
end
```

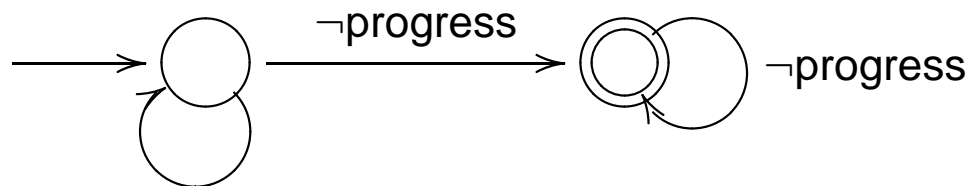
[Holzmann, Peled, Yannakakis 1996]

```

never { /* non-progress:  $\diamond \square \neg progress$  */
  do
    :: skip
    :: !progress - > break
  od;
accept: do
  :: !progress
od
}

```

[Holzmann, Peled, Yannakakis 1996]



(co-Büchi \mapsto Büchi)

$$(ii) \quad \phi \mapsto \mathcal{A}_\phi$$

- **SPIN:** $\phi \mapsto \text{GBA} \mapsto \text{BA}$
- **LTL2BA:** $\phi \mapsto \text{ABA} \mapsto \text{GBA}' \mapsto \text{BA}$

- Weryfikacja w locie

LTL⁺ :

$$\phi := p \mid \neg p \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid X\phi \mid \phi_1 \mathbf{U} \phi_2 \mid \phi_1 \mathbf{R} \phi_2 \mid \\ \text{true} \mid \text{false}$$

Def.: $X \subseteq \text{CL}(\phi)$, $\text{jutro}(X) = \{X\alpha \mid X\alpha \in X\}$

Intuicja: $\phi \equiv \text{dziś}(\phi) \wedge \text{jutro}(\phi)$

$$\phi \mathbf{U} \psi \equiv \psi \vee (\phi \wedge X(\phi \mathbf{U} \psi))$$

$$\phi \mathbf{R} \psi \equiv \psi \wedge (\phi \vee X(\phi \mathbf{R} \psi))$$

$$\alpha \mapsto \text{dnf}(\alpha) \subseteq \mathcal{P}(P \cup \bar{P} \cup \text{jutro}(\text{CL}(\alpha)))$$

$$\text{dnf}(\alpha) = \{\{\alpha\}\}, \text{ gdy } \alpha = p, \neg p, \mathbf{X} \beta$$

$$\text{dnf}(\alpha \vee \beta) = \text{dnf}(\alpha) \cup \text{dnf}(\beta)$$

$$\text{dnf}(\alpha \wedge \beta) = \{X \cup Y \mid X \in \text{dnf}(\alpha), Y \in \text{dnf}(\beta), \text{ niesprzeczne}\}$$

$$\text{dnf}(\alpha \mathbf{U} \beta) = \text{dnf}(\beta \vee (\alpha \wedge \mathbf{X}(\alpha \mathbf{U} \beta)))$$

$$\text{dnf}(\alpha \mathbf{R} \beta) = \text{dnf}(\beta \wedge (\alpha \vee \mathbf{X}(\alpha \mathbf{R} \beta)))$$

$$\text{dnf}(\text{true}) = \{\emptyset\}$$

$$\text{dnf}(\text{false}) = \emptyset$$

$$\wedge \emptyset \equiv \text{true}$$

$$\vee \emptyset \equiv \text{false}$$

$$\alpha \equiv \bigvee_{X \in \text{dnf}(\alpha)} (\bigwedge X)$$

GBA $\mathcal{A}_\phi = \langle \Sigma, S, S_{\text{pocz}}, \sigma, F \rangle$:

– $S = \mathcal{P}(P \cup \bar{P} \cup \text{jutro}(\mathbf{CL}(\phi)))$

– $S_{\text{pocz}} = \text{dnf}(\phi)$

– $X \xrightarrow{A} Y$ wtw. gdy

– $X \cap P \subseteq A$

– $\{p \mid \neg p \in X\} \cap A = \emptyset$

– $Y \in \text{dnf}(\wedge \{\alpha \mid X\alpha \in X\})$

– $F = ?$

niesprzeczność

X i A dziś

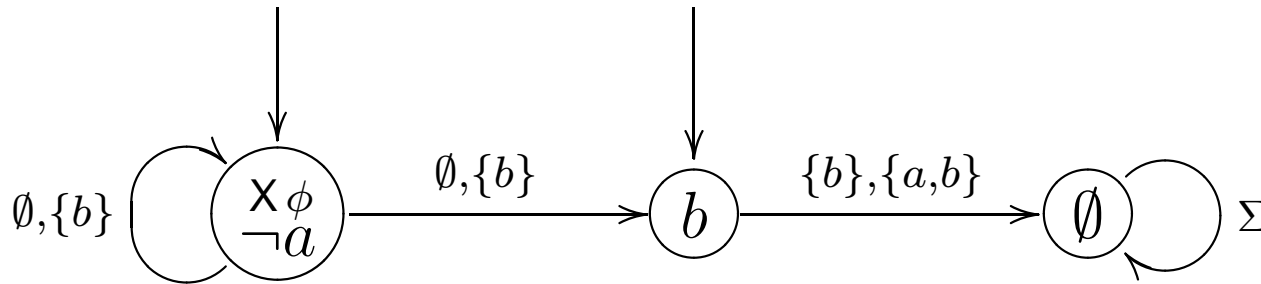
możliwe jutro

$\phi \mapsto$ GBA (przykład 1)

$$\phi = \neg a \mathbf{U} b$$

$$S = \mathcal{P}(a, \neg a, b, \neg b, \mathbf{X}(\neg a \mathbf{U} b))$$

$$\Sigma = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$



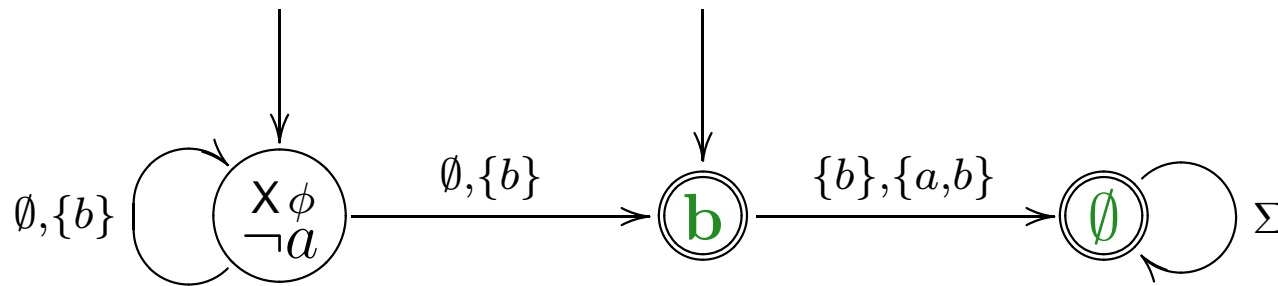
$F = ?$

$\phi \mapsto$ GBA (przykład 1)

$$\phi = \neg a \mathbf{U} b$$

$$S = \mathcal{P}(a, \neg a, b, \neg b, \mathbf{X}(\neg a \mathbf{U} b))$$

$$\Sigma = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$



$$F = \{\{\emptyset, \{b\}\}\}$$

$$- F_i = \{A \mid \alpha_i \mathbf{U} \beta_i \notin A \vee \beta_i \in A\}, \quad i = 1, \dots, n$$

$$\{\alpha_i \mathbf{U} \beta_i \mid i = 1, \dots, n\} \subseteq \mathbf{CL}(\phi)$$

$$- F_i = \{X \in S \mid \alpha_i \mathbf{U} \beta_i \notin \mathbf{cons}(X) \vee \beta_i \in \mathbf{cons}(X)\}$$

$$X \subseteq \mathbf{cons}(X)$$

$$\alpha \vee \beta \in \mathbf{cons}(X) \quad \text{jeśli} \quad \alpha \in \mathbf{cons}(X) \text{ lub } \beta \in \mathbf{cons}(X)$$

$$\alpha \wedge \beta \in \mathbf{cons}(X) \quad \text{jeśli} \quad \alpha \in \mathbf{cons}(X) \text{ i } \beta \in \mathbf{cons}(X)$$

$$\alpha \mathbf{U} \beta \in \mathbf{cons}(X) \quad \text{jeśli} \quad \beta \in \mathbf{cons}(X) \text{ lub } \alpha, X(\alpha \mathbf{U} \beta) \in \mathbf{cons}(X)$$

$$\alpha \mathbf{R} \beta \in \mathbf{cons}(X) \quad \text{jeśli} \quad \alpha, \beta \in \mathbf{cons}(X) \text{ lub } \beta, X(\alpha \mathbf{R} \beta) \in \mathbf{cons}(X)$$

$$\theta = \neg \mathbf{G} (q \implies \mathbf{F} r) \equiv \mathbf{F} (q \wedge \mathbf{G} \neg r)$$

$$\text{dnf}(\mathbf{F} \alpha) = \text{dnf}(\alpha) \cup \{ \mathbf{X} \mathbf{F} \alpha \}$$

$$\mathbf{F} \alpha \equiv \text{true} \cup \alpha$$

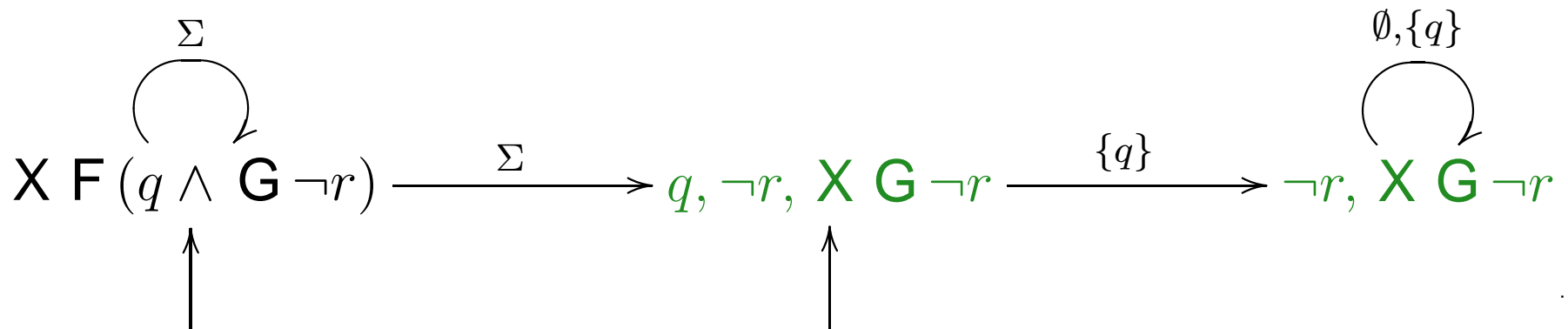
$$\text{dnf}(\mathbf{G} \alpha) = \text{dnf}(\alpha \wedge \mathbf{X} \mathbf{G} \alpha)$$

$$\mathbf{G} \alpha \equiv \text{false} \mathbf{R} \alpha$$

$$S = \mathcal{P}(q, \neg q, r, \neg r, \mathbf{X}(\mathbf{F}(q \wedge \mathbf{G} \neg r)), \mathbf{X} \mathbf{G} \neg r)$$

F = ?

$$\text{dnf}(\mathbf{F}(q \wedge \mathbf{G} \neg r)) = \mathbf{X} \mathbf{F}(q \wedge \mathbf{G} \neg r) \vee (q \wedge \neg r \wedge \mathbf{X} \mathbf{G} \neg r)$$



$$\theta = \neg(\mathbf{G F} p \implies \mathbf{G}(q \implies \mathbf{F} r)) \equiv \mathbf{G F} p \wedge \mathbf{F}(q \wedge \mathbf{G} \neg r)$$

$$\text{dnf}(\mathbf{F}(q \wedge \mathbf{G} \neg r)) = \mathbf{X F}(q \wedge \mathbf{G} \neg r) \vee (q \wedge \neg r \wedge \mathbf{X G} \neg r)$$

$$\begin{aligned} \text{dnf}(\mathbf{G F} p) &= \text{dnf}((p \vee \mathbf{X F} p) \wedge \mathbf{X G F} p) = \\ & \quad (p \wedge \mathbf{X G F} p) \vee (\mathbf{X F} p \wedge \mathbf{X G F} p) \end{aligned}$$

$$\text{dnf}(\mathbf{G F} p \wedge \mathbf{F}(q \wedge \mathbf{G} \neg r)) = \dots \vee \dots \vee \dots \vee \dots$$

$$\mathbf{X F}(q \wedge \mathbf{G} \neg r), p, \mathbf{X G F} p \qquad q, \neg r, \mathbf{X G} \neg r, p, \mathbf{X G F} p$$

$$\mathbf{X F}(q \wedge \mathbf{G} \neg r), \mathbf{X F} p, \mathbf{X G F} p \qquad q, \neg r, \mathbf{X G} \neg r, \mathbf{X F} p, \mathbf{X G F} p$$

$\phi \mapsto$ GBA (przykład 2)

$$\theta_n = \neg((\mathbf{G F} p_1 \wedge \dots \wedge \mathbf{G F} p_n) \implies \mathbf{G}(q \implies \mathbf{F} r)) \equiv$$
$$\mathbf{G F} p_1 \wedge \dots \wedge \mathbf{G F} p_n \wedge \mathbf{F}(q \wedge \mathbf{G} \neg r)$$

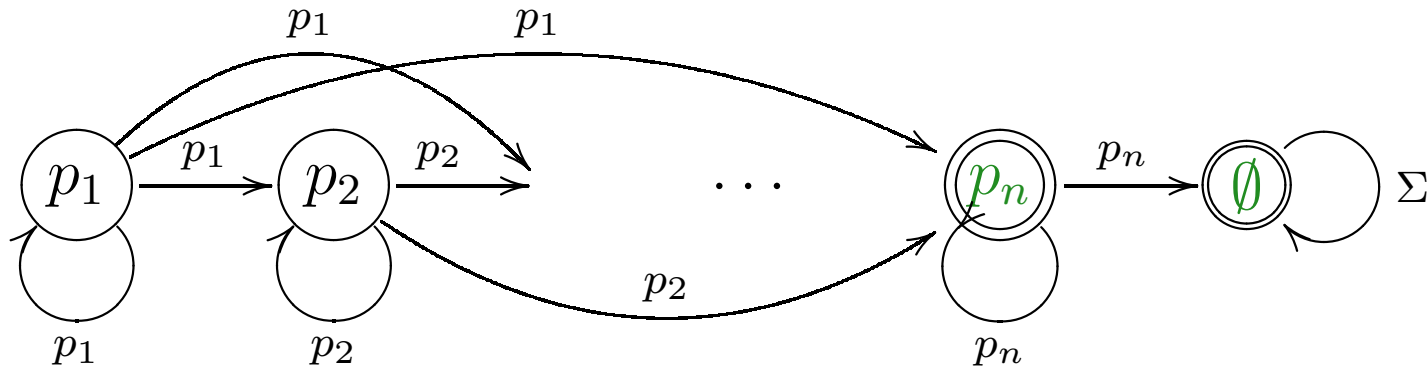


$$\theta_n = \neg((G F p_1 \wedge \dots \wedge G F p_n) \implies G(q \implies F r))$$

	Spin		Wring		EQLTL	LTL2BA-		LTL2BA	
	time	space	time	space	time	time	space	time	space
θ_1	0.18	460	0.56	4,100	16	0.01	9	0.01	9
θ_2	4.6	4,200	2.6	4,100	16	0.01	19	0.01	11
θ_3	170	52,000	16	4,200	18	0.01	86	0.01	19
θ_4	9,600	970,000	110	4,700	25	0.07	336	0.06	38
θ_5			1,000	6,500	135	0.70	1,600	0.37	48
θ_6			8,400	13,000	N/A	12	8,300	4.0	88
θ_7			72,000 [†]	43,000 [†]		220	44,000	32	175
θ_8						4,200	260,000	360	250
θ_9						97,000	1,600,000	3,000	490
θ_{10}								36,000	970

[Gastin, Oddoux 2001]

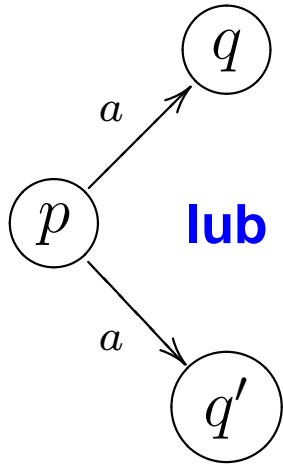
$$\phi_n = p_1 \mathbf{U} (p_2 \mathbf{U} (\dots \mathbf{U} p_n) \dots)$$



$$\theta_n = \neg(p_1 \mathbf{U} (p_2 \mathbf{U} (\dots \mathbf{U} p_n) \dots))$$

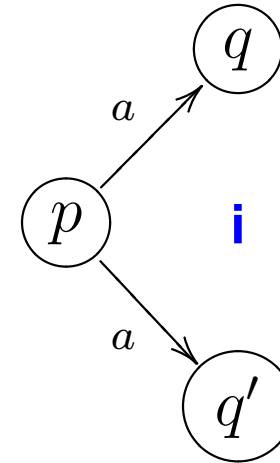


Alternacja (ABA)



$$\sigma(p, a) = q \vee q'$$

$$(p, a, q), (p, a, q') \in \sigma$$



$$\sigma(p, a) = q \wedge q'$$

—

Np.: $\sigma(p, a) = p_1 \vee p_2 \wedge p_3$ (DNF)

Pytanie: **bieg = ?**

ABA $\mathcal{A}_\phi = \langle \Sigma, S, S_{\text{pocz}}, \sigma, F \rangle$:

- $S =$ modalne podformuły ϕ $(\mathbf{X}\alpha, \alpha \mathbf{U} \beta, \alpha \mathbf{R} \beta, p)$
- $S_{\text{pocz}} =$ normalny dnf(ϕ)
- $\sigma : S \times \Sigma \rightarrow \text{Bool}^+(S)$

$\sigma(p, A) =$ true, o ile $p \in A$, wpp. false

$\sigma(\neg p, A) =$ true, o ile $p \notin A$, wpp. false

$\sigma(\mathbf{X}\alpha, A) = \alpha$ **!!!**

$\sigma(\alpha \mathbf{U} \beta, A) = \sigma(\beta, A) \vee (\sigma(\alpha, A) \wedge \alpha \mathbf{U} \beta)$

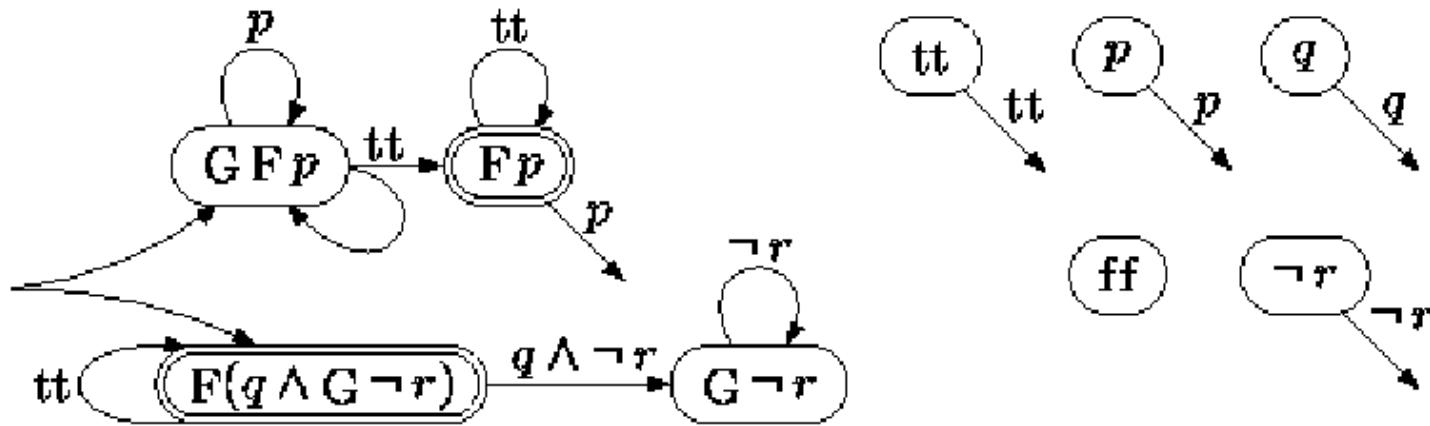
$\sigma(\alpha \mathbf{R} \beta, A) = \sigma(\beta, A) \wedge (\sigma(\alpha, A) \vee \alpha \mathbf{R} \beta)$

$\sigma(\mathbf{F}\alpha, A) = \sigma(\alpha, A) \vee \mathbf{F}\alpha$

$\sigma(\mathbf{G}\alpha, A) = \sigma(\alpha, A) \wedge \mathbf{G}\alpha$

$\phi \mapsto$ ABA (przykład)

$$\phi = \neg(\mathbf{G F} p \implies \mathbf{G}(q \implies \mathbf{F} r)) \equiv \mathbf{G F} p \wedge \mathbf{F}(q \wedge \mathbf{G} \neg r)$$



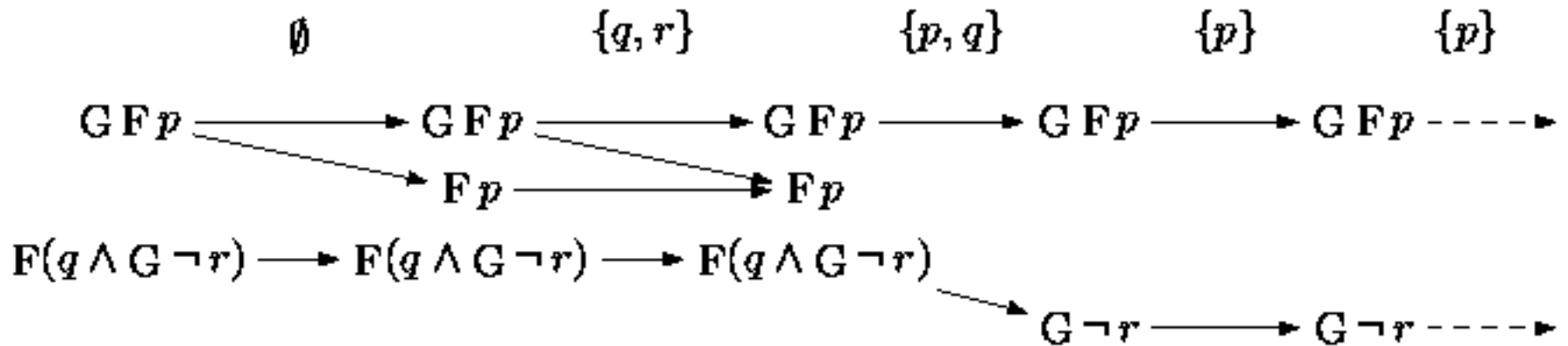
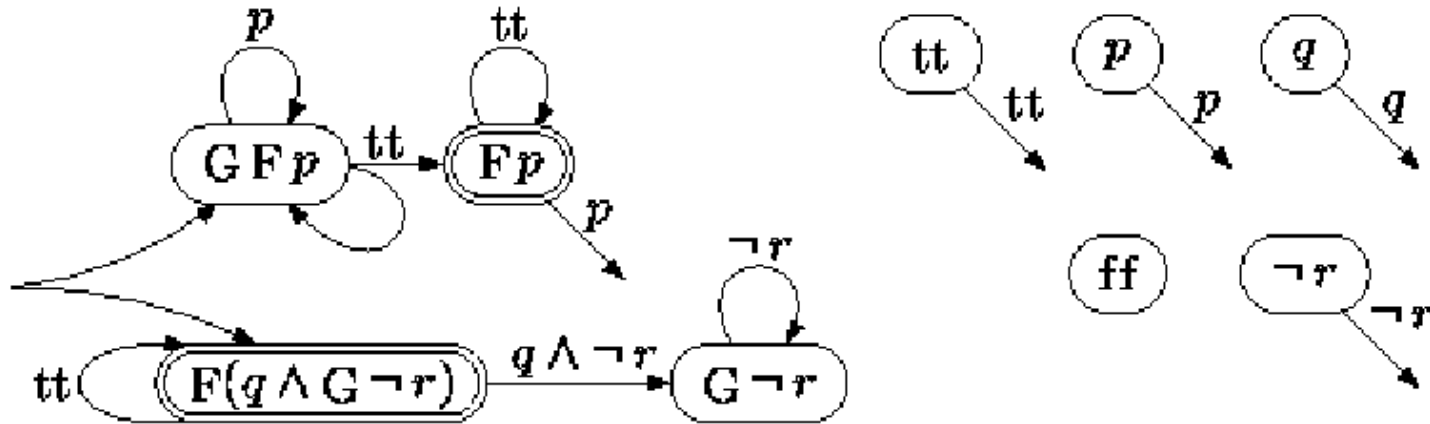
[Gastin, Oddoux 2001]

$$\text{dnf}(\mathbf{F}(q \wedge \mathbf{G} \neg r)) = \mathbf{X F}(q \wedge \mathbf{G} \neg r) \vee (q \wedge \neg r \wedge \mathbf{X G} \neg r)$$

$$\text{dnf}(\mathbf{G F} p) = (p \wedge \mathbf{X G F} p) \vee (\mathbf{X F} p \wedge \mathbf{X G F} p)$$

$\phi \mapsto$ ABA (przykład)

$$\phi = \neg(\mathbf{G F} p \implies \mathbf{G}(q \implies \mathbf{F} r)) \equiv \mathbf{G F} p \wedge \mathbf{F}(q \wedge \mathbf{G} \neg r)$$

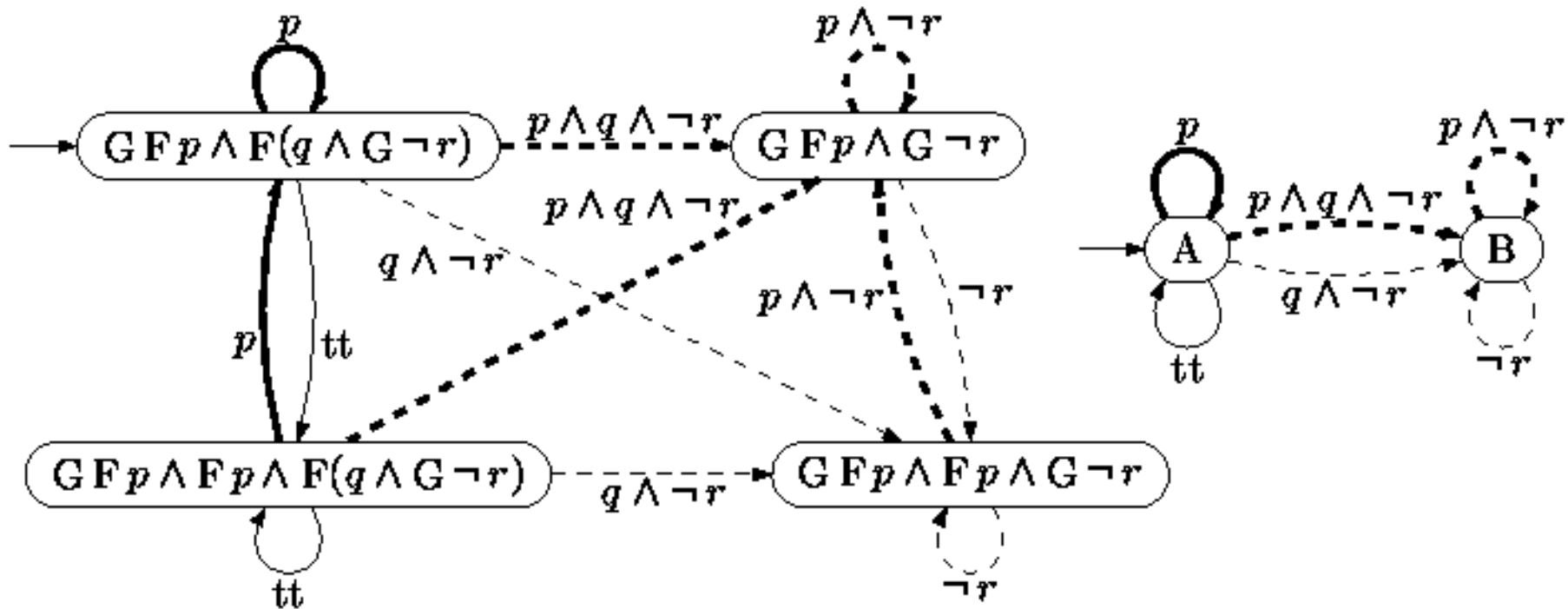
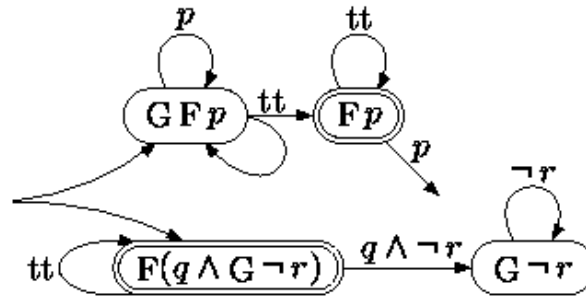


[Gastin, Oddoux 2001]

ABA $\mathcal{A}_\phi = \langle \Sigma, S, S_{\text{pocz}}, \sigma, F \rangle$:

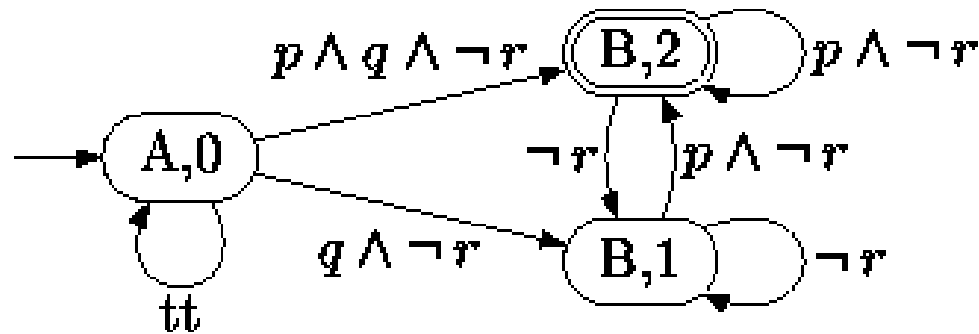
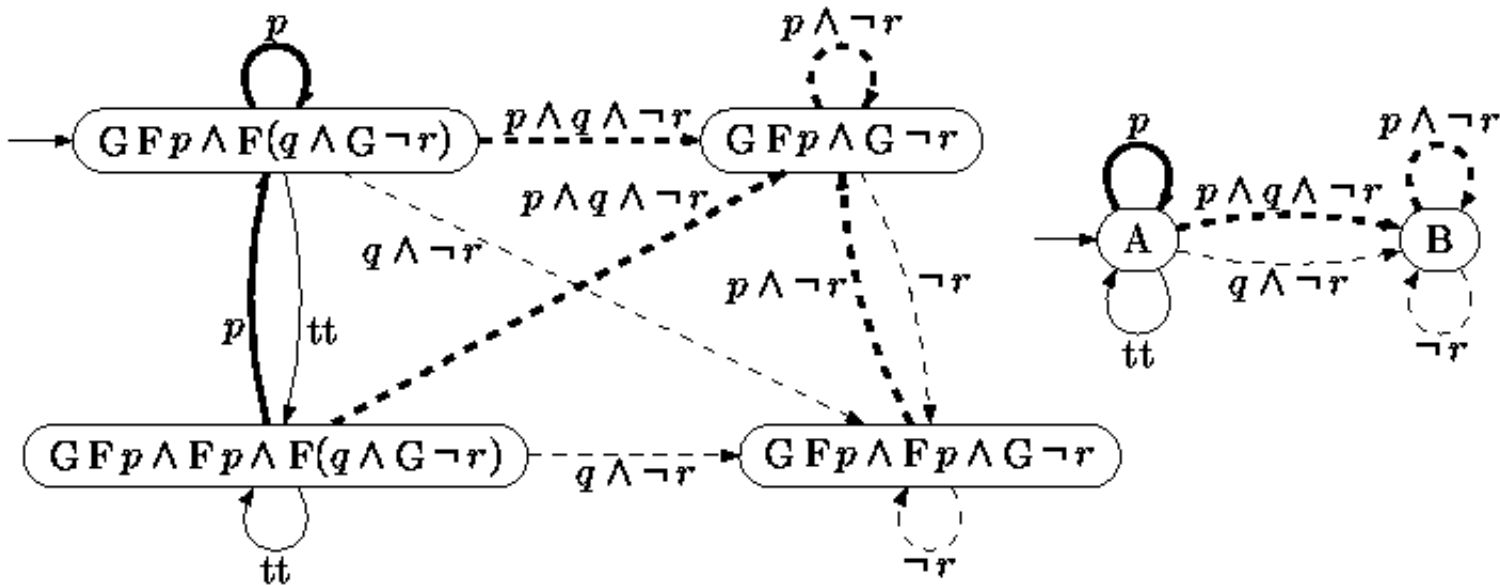
- $S =$ modalne podformuły ϕ ($X\alpha, \alpha U \beta, \alpha R \beta$)
- $S_{\text{pocz}} = \text{dnf}(\phi)$
- $\sigma : S \times \Sigma \rightarrow \mathbf{Bool}^+(S)$
- \dots
- $F = \{\alpha R \beta\}$

ABA \mapsto GBA'



[Gastin, Oddoux 2001]

GBA' \mapsto BA



[Gastin, Oddoux 2001]