Praktyczne metody weryfikacji

Wykład 4: Weryfikacja modelowa dla LTL

Algorytm

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

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

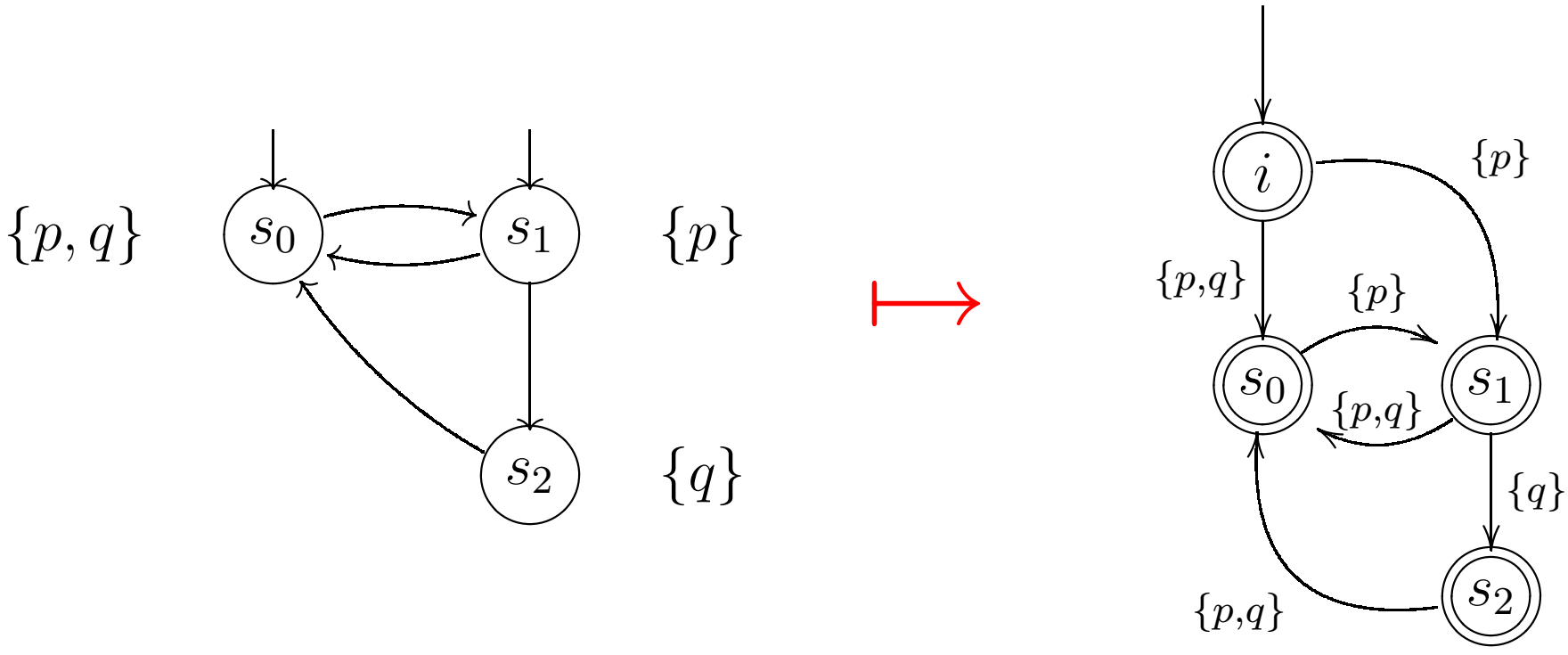
(iii) $L_\omega(\mathcal{A}_M) \cap L_\omega(\mathcal{A}_{\neg\phi}) = \emptyset\,?$ (a nie $L_\omega(\mathcal{A}_M) \subseteq L_\omega(\mathcal{A}_\phi)$)

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

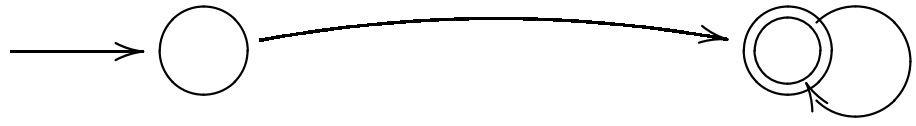
tak $\rightarrow$ $M \vDash \phi$

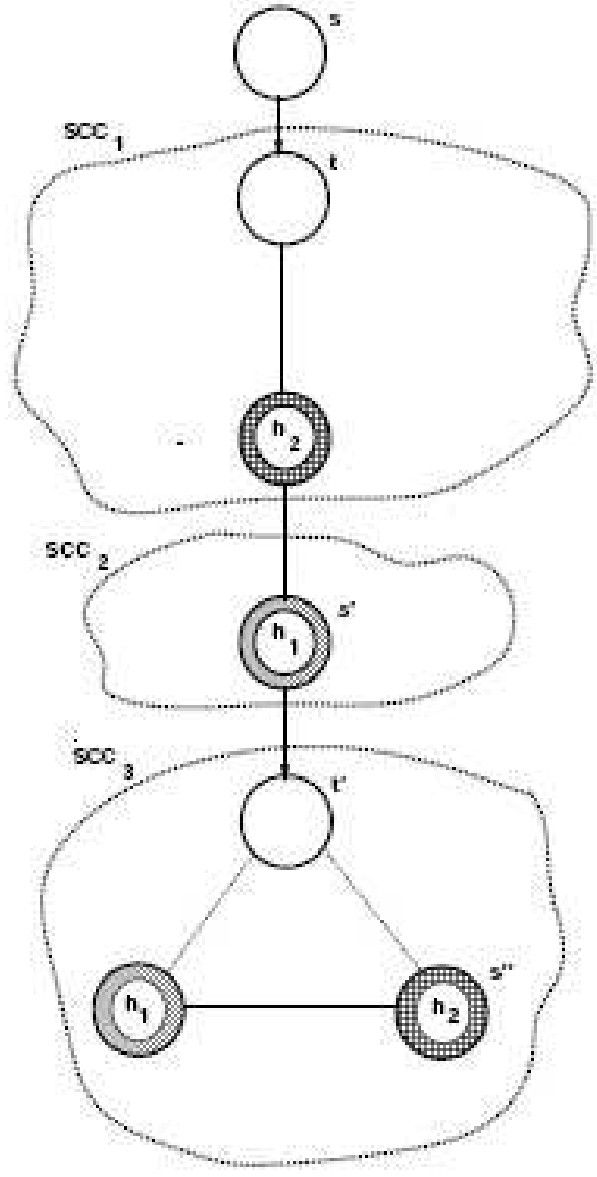
nie $\rightarrow$ $\neg(M \vDash \phi)$, kontrprzykład = ścieżka w M

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


{p, q}
s0
s1
{p}
s2
{q}
i
{p}
{p,q}
{p}
s0
s1
{p,q}
{q}
s2
{p,q}

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




s
SCC 1
t
h 2
SCC 2
h 1
s'
SCC 3
t'
h 1
h 2
s''

Ograniczenia

(1) Weryfi kcja w locie

for each successsor t of s do . . .

. . .

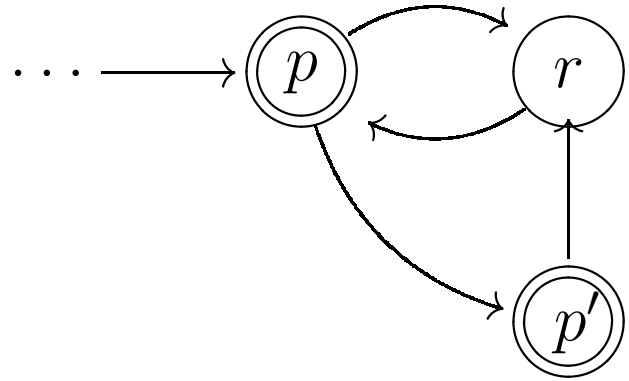
```
proc dfs(s)
    if error(s) then report error fi
    add {s,0} to Statespace
    for each successor t of s do
      if {t,0} not in Statespace then dfs(t) fi
    od
    if accepting(s) then seed:=s; ndfs(s) fi
end
proc ndfs(s) /* the nested search */
    add {s,1} to Statespace
    for each successor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

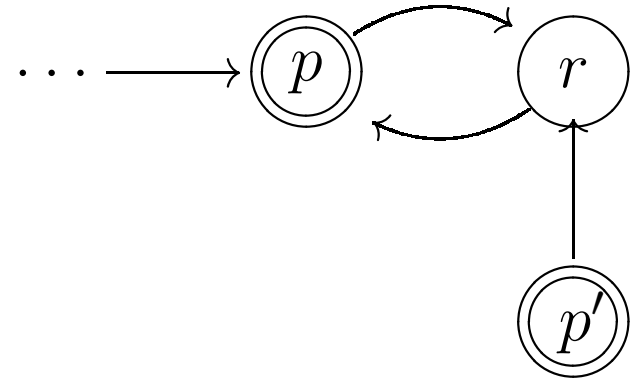
Dowód

Załóżmy, że jest stan akceptujący `p`, który ma cykl niewykryty w `ndfs(p)`. Niech `p` – pierwszy taki stan.

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

Niech `p'` – stan akceptujący t.że `r` osiągnięto w `ndfs(p')`.





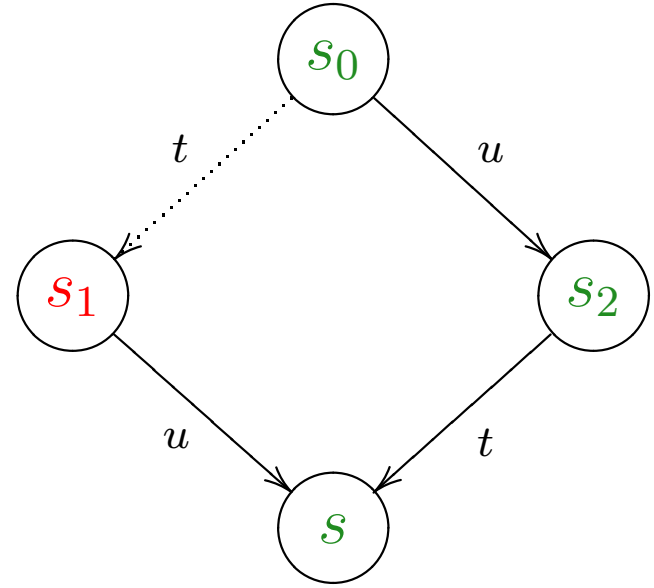
Ograniczenia (cd)

(1) Weryfi kcja w locie

for each successsor t of s do . . .

(2) Redukcje częściowo-porządkowe

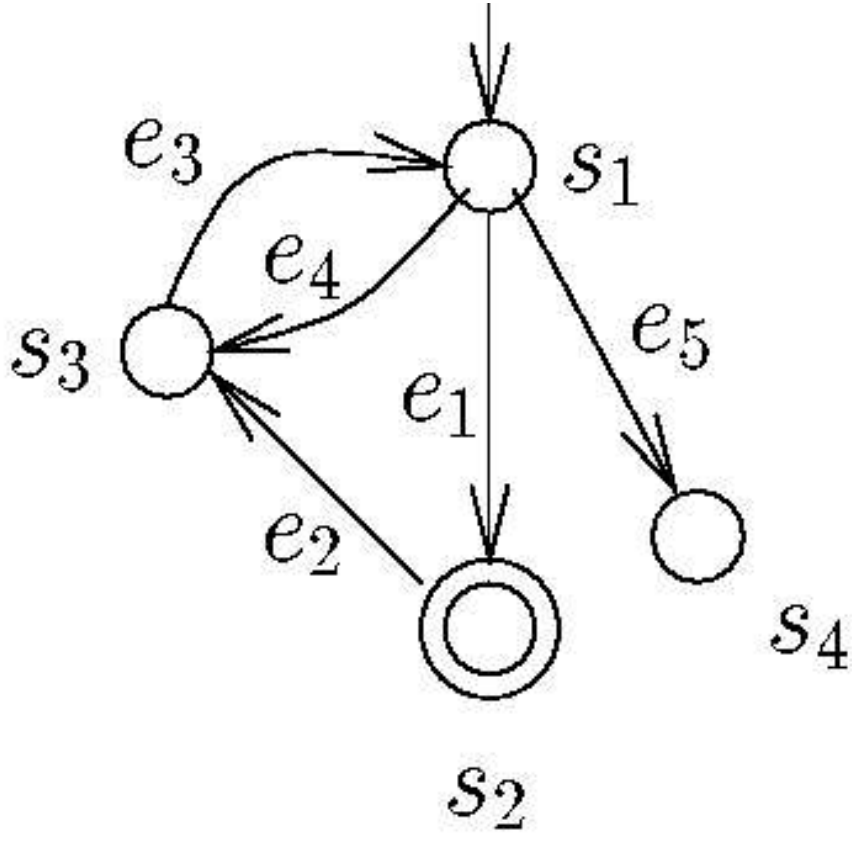
for each (selected) successsor t of s do . . .



Kontrprzykład

for each (selected) successsor t of s do . . .

(selected) – zależy od dotychczasowej ścieżki !



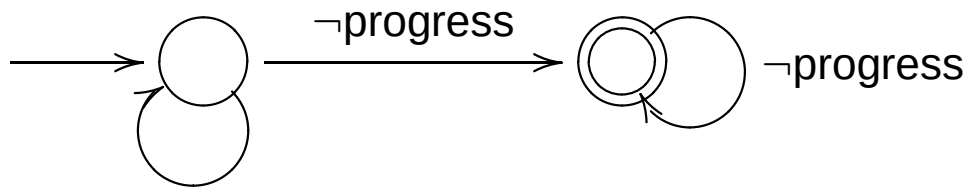
rozwiązanie

```
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
```

np-cycles: FG ¬ 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
```

```
never { /* non-progress: ◇□¬progress */
    do
    :: skip
    :: !progress -> break
    od;
accept: do
    :: !progress
    od
}
```



(co-Büchi $\mapsto$ Büchi)

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

– **SPIN:** $\phi \mapsto$ GBA $\mapsto$ BA

– **LTL2BA:** $\phi \mapsto$ ABA $\mapsto$ GBA' $\mapsto$ BA

– Weryfi kacja w locie

LTL$^+$:

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

$$\texttt{true} \mid \texttt{false}$$

Def.: $X \subseteq \mathsf{CL}(\phi)$, $\mathsf{next}(X) = \{\mathsf{X}\,\alpha \mid \mathsf{X}\,\alpha \in X\}$ „jutro(X)”

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

$$\phi \,\mathsf{U}\, \psi \;\equiv\; \psi \;\vee\; (\phi \wedge \mathsf{X}\,(\phi \,\mathsf{U}\, \psi))$$

$$\phi \,\mathsf{R}\, \psi \;\equiv\; \psi \;\wedge\; (\phi \vee \mathsf{X}\,(\phi \,\mathsf{R}\, \psi))$$

$$\alpha \mapsto \mathsf{dnf}(\alpha) \subseteq \mathcal{P}(P \cup \bar{P} \cup \mathsf{next}(\mathsf{CL}(\alpha)))$$

$$\begin{aligned}
\mathsf{dnf}(\alpha) &= \{\{\alpha\}\}, \quad \text{gdy} \quad \alpha = p, \neg p, \mathsf{X}\,\beta \\
\mathsf{dnf}(\alpha \vee \beta) &= \mathsf{dnf}(\alpha) \cup \mathsf{dnf}(\beta) \\
\mathsf{dnf}(\alpha \wedge \beta) &= \{X \cup Y \mid X \in \mathsf{dnf}(\alpha),\ Y \in \mathsf{dnf}(\beta),\ \text{niesprzeczne} \\
\mathsf{dnf}(\alpha\,\mathsf{U}\,\beta) &= \mathsf{dnf}(\beta \vee (\alpha \wedge \mathsf{X}\,(\alpha\,\mathsf{U}\,\beta))) \\
\mathsf{dnf}(\alpha\,\mathsf{R}\,\beta) &= \mathsf{dnf}(\beta \wedge (\alpha \vee \mathsf{X}\,(\alpha\,\mathsf{R}\,\beta)))
\end{aligned}$$

$$\begin{aligned}
\mathsf{dnf}(\texttt{true}) &= \{\emptyset\} \qquad \wedge\emptyset \equiv \texttt{tru} \\
\mathsf{dnf}(\texttt{false}) &= \emptyset \qquad \vee\emptyset \equiv \texttt{fals}
\end{aligned}$$

$$\alpha \equiv \vee_{X \in \mathsf{dnf}(\alpha)} \left(\wedge X \right)$$

$\phi \mapsto$ GBA (3)

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

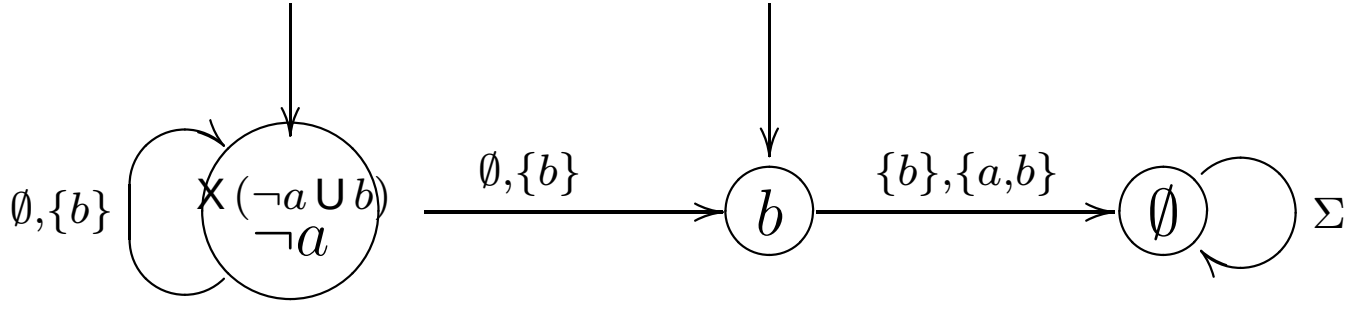
- $S = \mathcal{P}(P \cup \bar{P} \cup \mathsf{next}(\mathsf{CL}(\phi)))$
- $S_{\mathsf{pocz}} = \mathsf{dnf}(\phi)$
- $X \xrightarrow{A} Y$ wtw. gdy
  - $X \cap P \subseteq A$ niesprzeczność
  - $\{p \mid \neg p \in X\} \cap A = \emptyset$ X i A dziś
  - $Y \in \mathsf{dnf}(\wedge \{\alpha \mid \mathsf{X}\,\alpha \in X\})$ możliwe jutro
- $F =?$

$\phi \mapsto$ GBA (przykład 1)

$\phi = \neg a \,\mathsf{U}\, b$

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

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



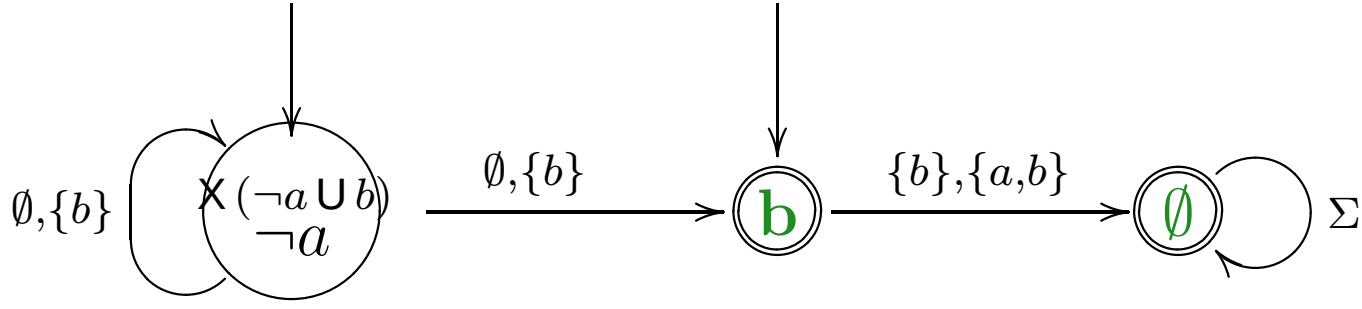
$F = ?$

$\phi \mapsto$ GBA (przykład 1)

$\phi = \neg a \,\mathsf{U}\, b$

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

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



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

– $F_i = \{A \mid \alpha_i U \beta_i \notin A \vee \beta_i \in A\}, \quad i = 1, \ldots, n$

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

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

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

$\alpha \vee \beta \in \mathsf{cons}(X)$ jeśli $\alpha \in \mathsf{cons}(X)$ lub $\beta \in \mathsf{cons}(X)$

$\alpha \wedge \beta \in \mathsf{cons}(X)$ jeśli $\alpha \in \mathsf{cons}(X)$ i $\beta \in \mathsf{cons}(X)$

$\alpha \,\mathsf{U}\, \beta \in \mathsf{cons}(X)$ jeśli $\beta \in \mathsf{cons}(X)$ lub α, $\mathsf{X}\,(\alpha \,\mathsf{U}\, \beta) \in \mathsf{cons}(X)$

$\alpha \,\mathsf{R}\, \beta \in \mathsf{cons}(X)$ jeśli $\alpha, \beta \in \mathsf{cons}(X)$ lub β, $\mathsf{X}\,(\alpha \,\mathsf{R}\, \beta) \in \mathsf{cons}(X$

$\phi \mapsto$ GBA (przykład 2)

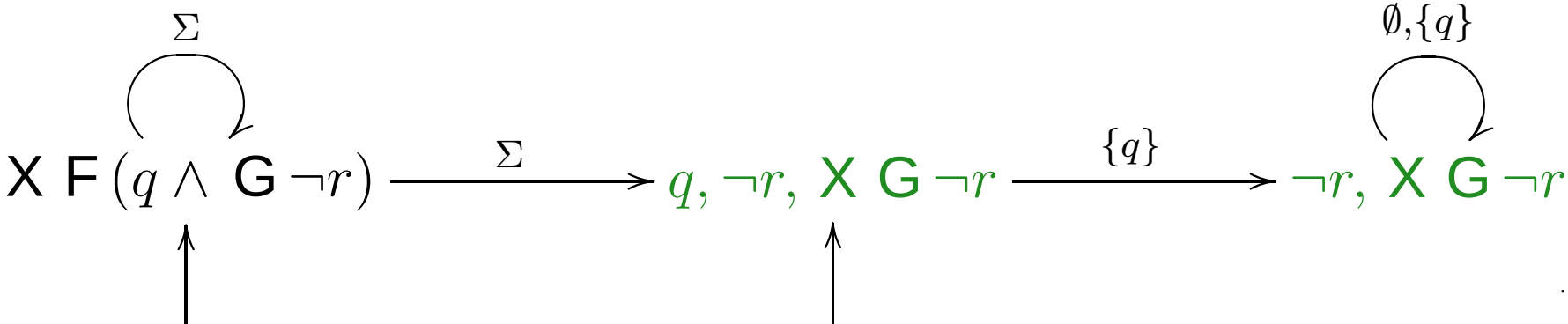
$$\theta = \neg \mathsf{G}\,(q \implies \mathsf{F}\,r) \equiv \mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)$$

$$\mathrm{dnf}(\mathsf{F}\,\alpha) = \mathrm{dnf}(\alpha) \cup \{\mathsf{X}\,\mathsf{F}\,\alpha\} \qquad \mathsf{F}\,\alpha \equiv \mathtt{true}\,\mathsf{U}\,\alpha$$

$$\mathrm{dnf}(\mathsf{G}\,\alpha) = \mathrm{dnf}(\alpha \wedge \mathsf{X}\,\mathsf{G}\,\alpha) \qquad \mathsf{G}\,\alpha \equiv \mathtt{false}\,\mathsf{R}\,\alpha$$

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

$$\mathrm{dnf}(\mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)) = \mathsf{X}\,\mathsf{F}\,(q \wedge \mathsf{G}\,\neg r) \vee (q \wedge \neg r \wedge \mathsf{X}\,\mathsf{G}\,\neg r)$$



$\phi \mapsto$ GBA (przykład 2)

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

$$\mathrm{dnf}(\mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)) = \mathsf{X}\,\mathsf{F}\,(q \wedge \mathsf{G}\,\neg r) \vee (q \wedge \neg r \wedge \mathsf{X}\,\mathsf{G}\,\neg r)$$

$$\mathrm{dnf}(\mathsf{G}\,\mathsf{F}\,p) = \mathrm{dnf}((p \vee \mathsf{X}\,\mathsf{F}\,p) \wedge \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p) = (p \wedge \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p) \vee (\mathsf{X}\,\mathsf{F}\,p \wedge \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p)$$

$$\mathrm{dnf}(\mathsf{G}\,\mathsf{F}\,p \wedge \mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)) = \ldots \vee \ldots \vee \ldots \vee \ldots$$

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

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

$\phi \mapsto$ GBA (przykład 2)

$$\theta_n = \neg((\mathsf{G}\,\mathsf{F}\,p_1 \wedge \ldots \wedge \mathsf{G}\,\mathsf{F}\,p_n) \Longrightarrow \mathsf{G}\,(q \Longrightarrow \mathsf{F}\,r)) \equiv$$

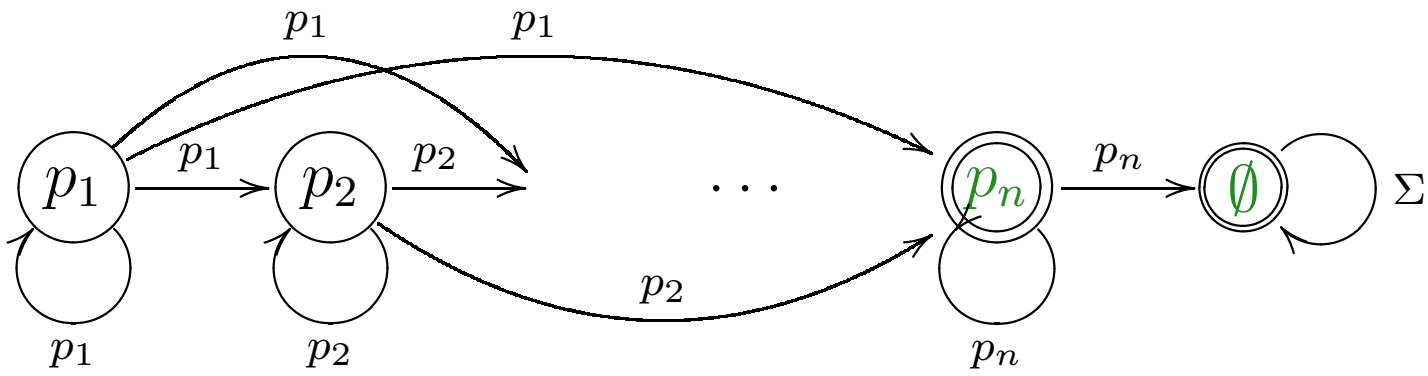
$$\mathsf{G}\,\mathsf{F}\,p_1 \wedge \ldots \wedge \mathsf{G}\,\mathsf{F}\,p_n \wedge \mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)$$

$$\theta_n \;=\; \neg((\,\mathsf{G}\,\mathsf{F}\,p_1 \;\wedge\; \ldots \;\wedge\; \mathsf{G}\,\mathsf{F}\,p_n) \;\Longrightarrow\; \mathsf{G}\,(q \;\Longrightarrow\; \mathsf{F}\,r))$$

	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

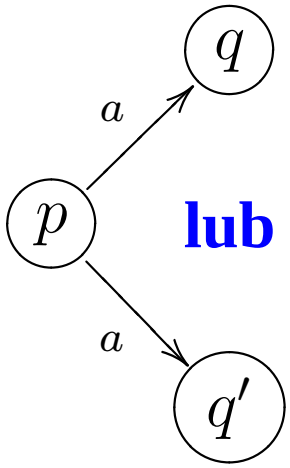
$\phi \mapsto$ GBA (przykład 2)

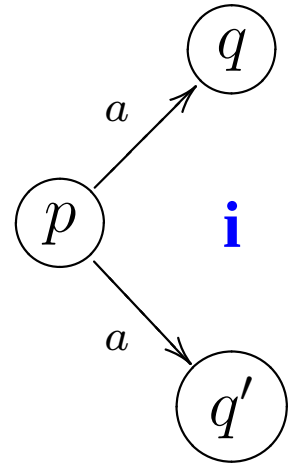
$$\phi_n \;=\; p_1 \,\mathsf{U}\, (p_2 \,\mathsf{U}\, (\ldots \,\mathsf{U}\, p_n) \ldots)$$



$$\theta_n \;=\; \neg\big(p_1 \,\mathsf{U}\, (p_2 \,\mathsf{U}\, (\ldots \,\mathsf{U}\, p_n) \ldots)\big)$$

Alternacja (ABA)





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

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

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

—

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 $\qquad$ ($\mathsf{X}\,\alpha$, $\alpha\,\mathsf{U}\,\beta$, $\alpha\,\mathsf{R}\,\beta$)
- $S_{\text{pocz}} = \text{dnf}(\phi)$
- $\sigma : S \times \Sigma \to \text{Bool}^+(S)$

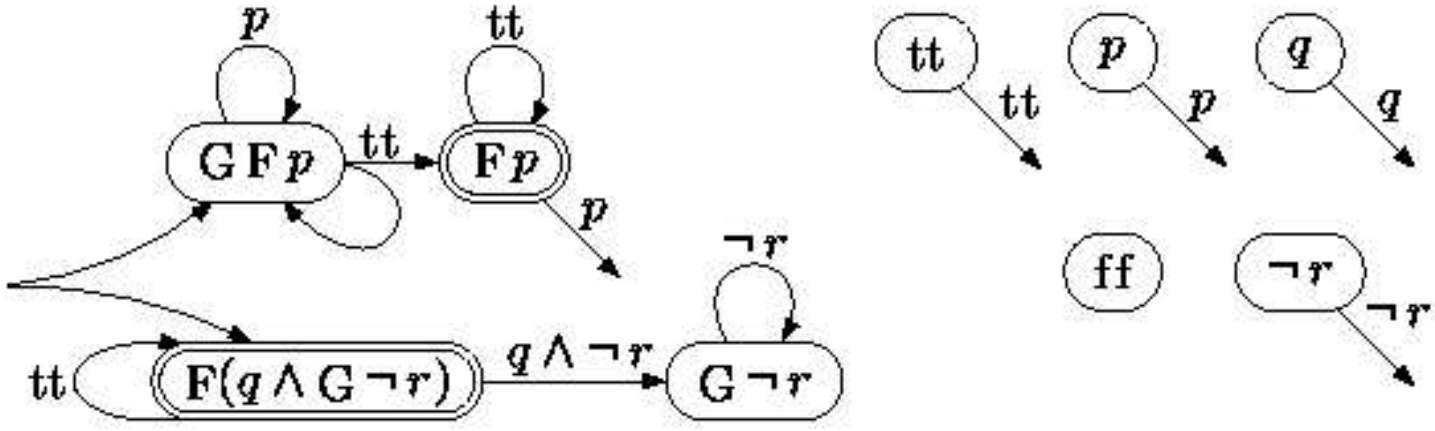
$$
\begin{array}{lcl}
\sigma(p, A) & = & \texttt{true}, \text{ o ile } p \in A, \text{ wpp. } \texttt{false} \\
\sigma(\neg p, A) & = & \texttt{true}, \text{ o ile } p \notin A, \text{ wpp. } \texttt{false} \\
\sigma(\mathsf{X}\,\alpha, A) & = & \alpha \qquad \text{!!!} \\
\sigma(\alpha\,\mathsf{U}\,\beta, A) & = & \sigma(\beta, A) \ \vee \ (\sigma(\alpha, A) \ \wedge \ \alpha\,\mathsf{U}\,\beta) \\
\sigma(\alpha\,\mathsf{R}\,\beta, A) & = & \sigma(\beta, A) \ \wedge \ (\sigma(\alpha, A) \ \vee \ \alpha\,\mathsf{R}\,\beta)
\end{array}
$$

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

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

$\phi \mapsto$ ABA (przykład)

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

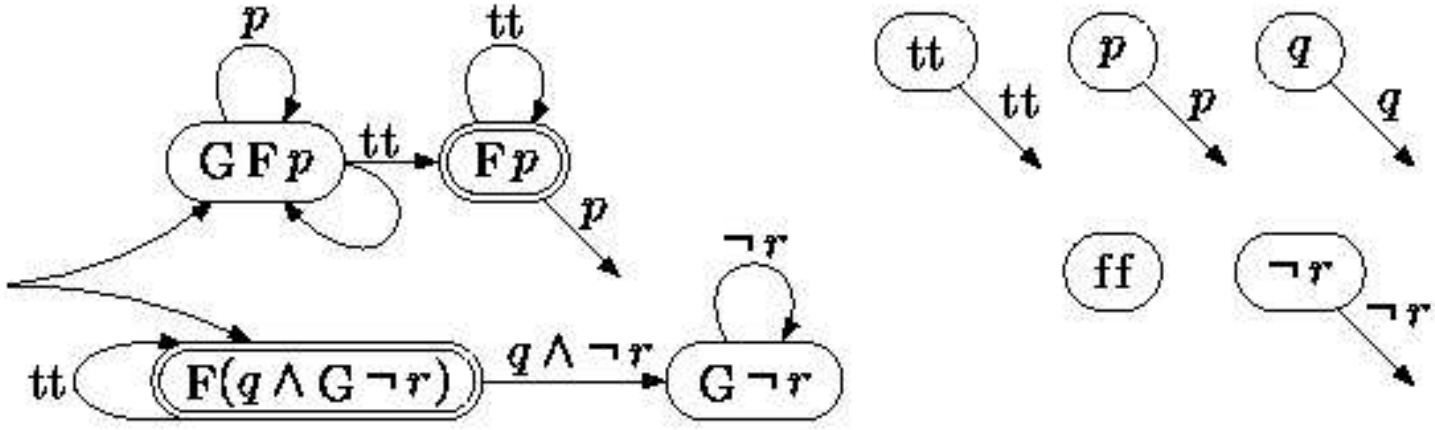


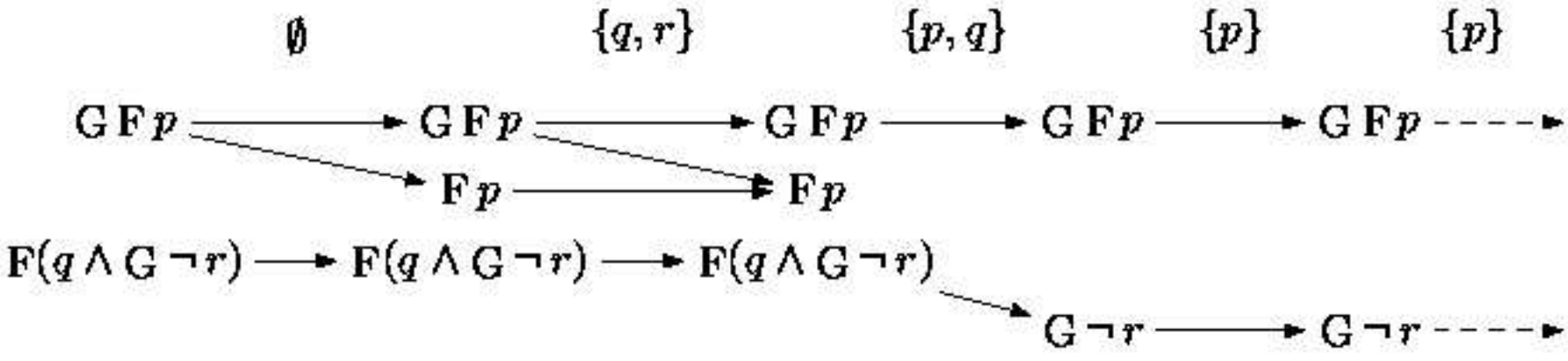
$$\mathsf{dnf}(\mathsf{F}\,(q \wedge \mathsf{G}\,\neg r)) = \mathsf{X}\,\mathsf{F}\,(q \wedge \mathsf{G}\,\neg r) \vee (q \wedge \neg r \wedge \mathsf{X}\,\mathsf{G}\,\neg r)$$

$$\mathsf{dnf}(\mathsf{G}\,\mathsf{F}\,p) = (p \wedge \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p) \vee (\mathsf{X}\,\mathsf{F}\,p \wedge \mathsf{X}\,\mathsf{G}\,\mathsf{F}\,p)$$

$\phi \mapsto$ ABA (przykład)

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





$\phi \mapsto$ ABA (2)

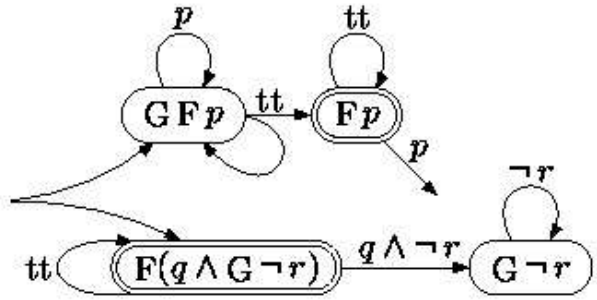
ABA $\mathcal{A}_\phi = \langle \Sigma, S, S_{\mathsf{pocz}}, \sigma, F \rangle$:

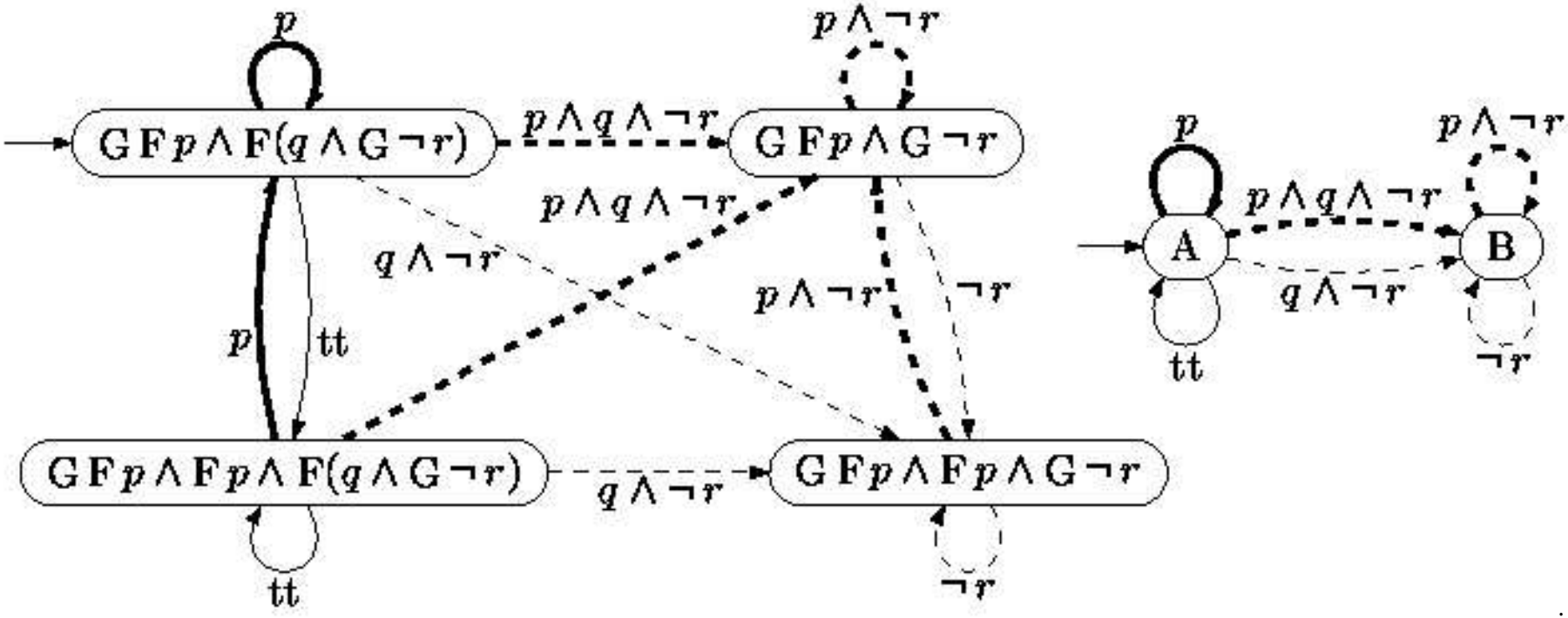
- $S =$ modalne podformuły ϕ $\qquad$ ($\mathsf{X}\,\alpha$, $\alpha\,\mathsf{U}\,\beta$, $\alpha\,\mathsf{R}\,\beta$)
- $S_{\mathsf{pocz}} = \mathsf{dnf}(\phi)$
- $\sigma : S \times \Sigma \to \mathsf{Bool}^+(S)$

  ...

- $F = \{\alpha\,\mathsf{R}\,\beta\}$

ABA $\mapsto$ GBA'





GBA' $\mapsto$ BA