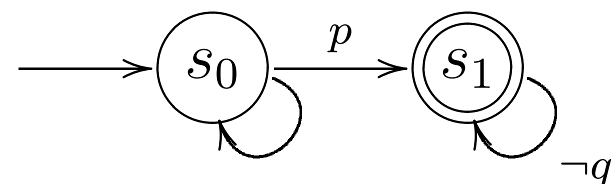
Praktyczne metody weryfikacji

Wykład 3: ω-automaty

Po co nam ω-automaty?

Przykład:

$$\phi = \neg G(p \implies XFq) \quad \mapsto \quad A_\phi \quad =$$



LTL $\subseteq$ ω-automaty

Def.: ω-automat $\mathcal{A} = \langle \Sigma, S, S_{\text{pocz}}, \sigma, F \rangle$

- $S_{\text{pocz}} \subseteq S$ niepusty zbiór stanów początkowych
- $\sigma \subseteq S \times \Sigma \times S$ relacja przejścia
- $F \subseteq S$ niepusty zbiór stanów akceptujących

(automat **Büchiego**)

$\mathcal{A}$ jest deterministyczny gdy $|S_{\text{pocz}}| = 1$ i $\forall s, a.\ |\sigma(s,a)| \leq 1$.

ω-słowa: $w = a_0\ a_1\ a_2\ \ldots$

Def.: Dla $w = a_0\ a_1\ a_2\ \ldots$, bieg automatu $\mathcal{A}$ to
$r = s_0\ s_1\ s_2\ \ldots$ taki, że $\forall i.\ (s_i, a_i, s_{i+1}) \in \sigma$.

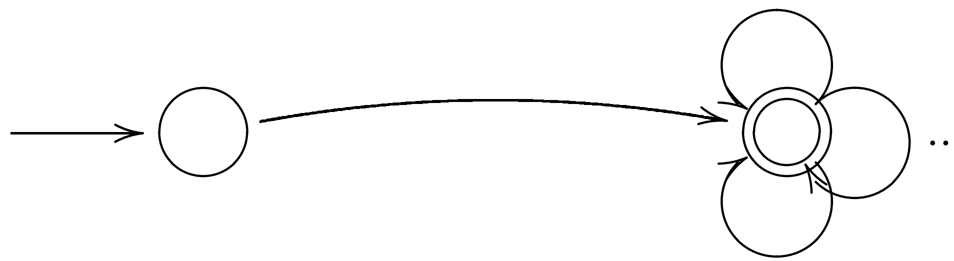
Niech $\inf(r) = \{s \in S : s = s_i$ dla nieskończenie wielu $i\}$.

$\boxed{\text{Bieg jest akceptujący gdy } \inf(r) \cap F \neq \emptyset.}$

$w \in L_\omega(\mathcal{A}) \iff \mathcal{A}$ ma bieg akceptujący dla w.

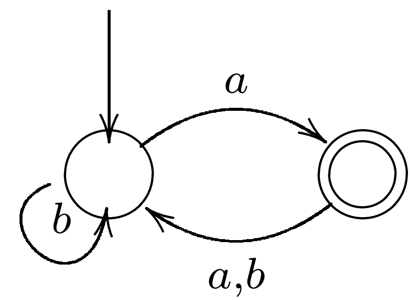
Def.: Język $L \subseteq \Sigma^\omega$ jest ω-regularny gdy $L = L_\omega(\mathcal{A})$
dla pewnego $\mathcal{A}$.

Bieg akceptujący wygląda tak:

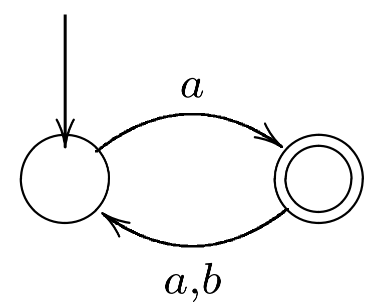


Przykłady: $\Sigma = \{a, b\}$

nieskończenie wiele a $(b^* \ a)^\omega$



even(a) $(a \ (a+b))^\omega$



Wniosek: $LTL \subsetneq \omega$-automaty

Ćwiczenie:

– nieskończenie wiele a i b

– między każdymi dwoma a
parzysta liczba b

Ćwiczenie:

– nieskończenie wiele a i b

$$b^* \ (aa^* \ bb(bb)^*)^\omega$$

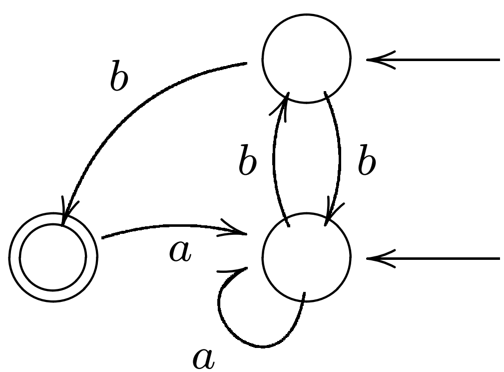
– między każdymi dwoma a parzysta liczba b

Ćwiczenie:

– nieskończenie wiele a i b

$$b^* \ (aa^* \ bb(bb)^*)^\omega$$

– między każdymi dwoma a
parzysta liczba b



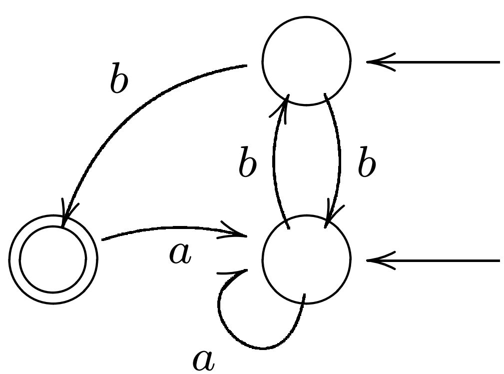
a deterministyczny ?

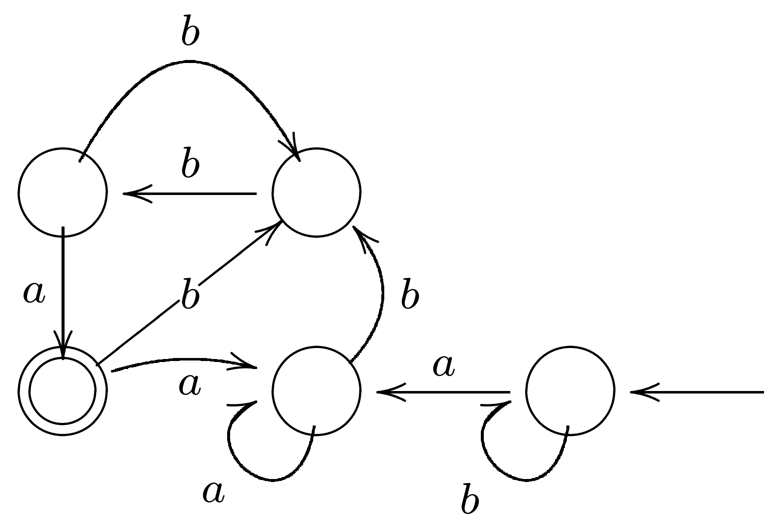
Ćwiczenie:

– nieskończenie wiele a i b

$$b^* \ (aa^* \ bb(bb)^*)^\omega$$

– między każdymi dwoma a
parzysta liczba b





Ćwiczenie: $\Sigma = \{a, b\}$

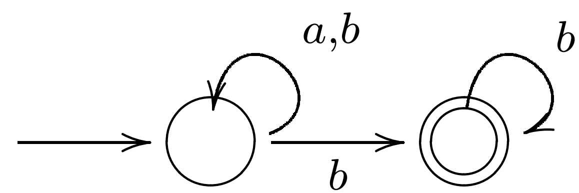
skończenie wiele a

Ćwiczenie: $\Sigma = \{a, b\}$

skończenie wiele a $(b + a)^* b^\omega$

Ćwiczenie: $\Sigma = \{a, b\}$

skończenie wiele a $(b + a)^* b^\omega$



a deterministyczny ?

Tw: Języki ω-regularne są zamknięte na $\cup$, $\cap$ i uzupełnienie.

$\vee$, $\wedge$ i $\neg$

$$\mathcal{A}_1, \mathcal{A}_2 \ \mapsto \ \mathcal{A}$$

(1) $L_\omega(\mathcal{A}) \ = \ L_\omega(\mathcal{A}_1) \ \cup \ L_\omega(\mathcal{A}_2)$

(2) $L_\omega(\mathcal{A}) \ = \ L_\omega(\mathcal{A}_1) \ \cap \ L_\omega(\mathcal{A}_2)$

$$\mathcal{A} \ \mapsto \ \bar{\mathcal{A}}$$

(3) $L_\omega(\bar{\mathcal{A}}) \ = \ \Sigma^\omega \ \setminus \ L_\omega(\mathcal{A})$

(2) $\mathcal{A}_1, \mathcal{A}_2 \;\mapsto\; \mathcal{A}$ $\qquad L_\omega(\mathcal{A}) \;=\; L_\omega(\mathcal{A}_1) \;\cap\; L_\omega(\mathcal{A}_2)$

?

(2) $\mathcal{A}_1, \mathcal{A}_2 \;\mapsto\; \mathcal{A}$ $\qquad L_\omega(\mathcal{A}) \;=\; L_\omega(\mathcal{A}_1) \;\cap\; L_\omega(\mathcal{A}_2)$

$$S \;=\; S_1 \times S_2$$

$$S_{\text{pocz}} \;=\; S_{1,\text{pocz}} \times S_{2,\text{pocz}} \times \{1\}$$

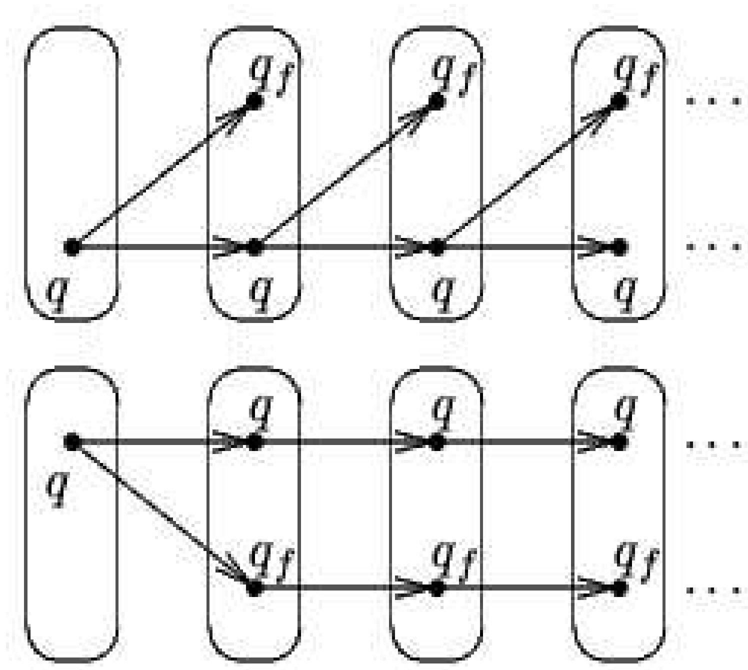
$$F \;=\; F_1 \times S_2 \times \{1\}$$

$$((s,t,i),a,(s',t',j)) \in \sigma \iff (s,a,s') \in \sigma_1,\ (t,a,t') \in \sigma_2,$$

$$j \;=\; \begin{cases} 2 & \text{gdy } i = 1,\ s \in F_1 \\ 1 & \text{gdy } i = 2,\ t \in F_2 \\ i & \text{wpp} \end{cases}$$

(3) $\mathcal{A} \mapsto \bar{\mathcal{A}}$ $\qquad L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$

– brak determinizacji!



(3) $\mathcal{A} \mapsto \bar{\mathcal{A}}$ $\qquad$ $L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$

- brak determinizacji
- skomplikowana konstrukcja
- $|\bar{\mathcal{A}}| = 2^{\mathcal{O}(n \cdot \log n)}$, gdzie $n = |\mathcal{A}|$

Morał: Najlepiej unikać uzupełnienia

$$\begin{tikzcd}
\phi \arrow[rr, mapsto] \arrow[d, mapsto, dotted] & & \neg\phi \arrow[d, mapsto] \\
\mathcal{A}_\phi \arrow[r, mapsto, dotted] & \bar{\mathcal{A}}_\phi \equiv & \mathcal{A}_{\neg\phi}
\end{tikzcd}$$

Pytanie:

Jak wygląda uzupełnienie, gdy $\mathcal{A}$ jest deterministyczny?

$$\mathcal{A} \mapsto \bar{\mathcal{A}}$$

$$F \mapsto Q \backslash F$$

Czy $L_\omega(\bar{\mathcal{A}}) \ = \ \Sigma^\omega \ \backslash \ L_\omega(\mathcal{A})$?

Pytanie:

Jak wygląda uzupełnienie, gdy $\mathcal{A}$ jest deterministyczny?

$$\mathcal{A} \longmapsto \bar{\mathcal{A}}$$

$$F \longmapsto Q \backslash F$$

Czy $L_\omega(\bar{\mathcal{A}}) = \Sigma^\omega \setminus L_\omega(\mathcal{A})$? **NIE!**

co-Büchi: bieg $r = s_0\ s_1\ s_2\ \ldots$ jest akceptujący gdy $s_i \in F$ dla prawie wszystkich i ($\inf(r) \subseteq F$).

Brak determinizacji!

Tw:
$(a+b)^*b^\omega$ nie jest akceptowany przez automat deterministyczny

Dowód: Załóżmy, że $L_\omega(\mathcal{A}) = (a+b)^*b^\omega$, $\mathcal{A}$ deterministyczny.

$w_0 = b^\omega$. Dla pewnego k_0, $\sigma(s_0, b^{k_0}) \in F$.
$w_1 = b^{k_0}ab^\omega$. Dla pewnego k_1, $\sigma(s_0, b^{k_0}ab^{k_1}) \in F$.
...

$\exists i < j$ takie, że $\sigma(s_0, b^{k_0}ab^{k_1}\dots ab^{k_i}) \; = \; \sigma(s_0, b^{k_0}ab^{k_1}\dots ab^{k_j})$

Więc $\mathcal{A}$ akceptuje $b^{k_0}ab^{k_1}\dots ab^{k_i}(a\dots ab^{k_j})^\omega$

sprzeczność!

problem dla automatów sk.	problem dla ω-automatów	złożoność	koszt algorytmu
$L(A) \neq \emptyset$	$L_\omega(A) \neq \emptyset$	NLOGSPACE	$\mathcal{O}(n)$
$L(A) = \Sigma^*$	$L_\omega(A) = \Sigma^\omega$	PSPACE	$2^{\mathcal{O}(n \cdot \log n)}$
$L(A) \subseteq L(B)$	$L_\omega(A) \subseteq L_\omega(B)$	PSPACE	$2^{\mathcal{O}(n \cdot \log n)}$

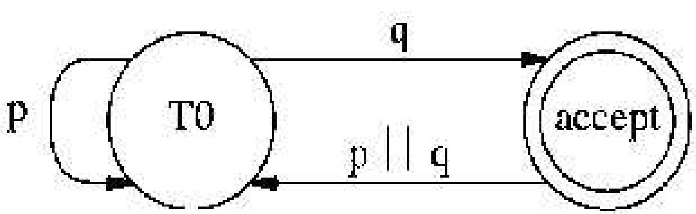
Lasso

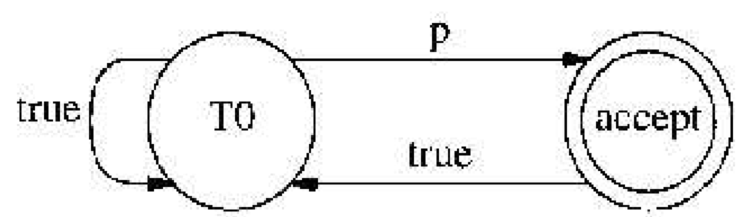
Tw: $L_\omega(A) \neq \emptyset$ wtw gdy $\mathcal{A}$ ma lasso.

SPIN – przykł ady

```
$ spin -f "[](p U q)"
never {
T0:
        if
        :: (p) -> goto T0
        :: (q) -> goto accept
        fi;
accept:
        if
        :: ((p) || (q)) -> goto T0
        fi
}
```

```
$ spin -f "[]<>p"
never {
T0:
        if
        :: (true) -> goto T0
        :: (p) -> goto accept
        fi;
accept:
        if
        :: (true) -> goto T0
        fi
}
```





Uogólnione ω-automaty Büchiego (GBA)

- $\{F_1, \ldots, F_n\}$ zamiast F
- bieg r jest akceptujący gdy $\forall i.\ \mathrm{inf}(r) \cap F_i \neq \emptyset$

Pytanie: Czy automaty uogólnione są ogólniejsze?

Uogólnione ω-automaty Büchiego (GBA)

- $\{F_1, \ldots, F_n\}$ zamiast F
- bieg r jest akceptujący gdy $\forall i.\ \inf(r) \cap F_i \neq \emptyset$

Pytanie: Czy automaty uogólnione są ogólniejsze?

$$L_\omega(\mathcal{A}_{F_1,\ldots,F_n}) \;=\; L_\omega(\mathcal{A}_F) \;\subseteq\; L_\omega(\mathcal{A}_{F_1}) \;\cap\; \ldots \;\cap\; L_\omega(\mathcal{A}_{F_n})$$

$$|\mathcal{A}_F| = \mathcal{O}(|\mathcal{A}_{F_1,\ldots,F_n}| \cdot n)$$

CL(ϕ) – najmniejszy zbiór formuł t. że

- $\phi \in$ CL(ϕ)
- $\alpha \in$ CL(ϕ) $\iff$ $\neg\alpha \in$ CL(ϕ) $\qquad \neg\neg\alpha \;\equiv\; \alpha$
- $\alpha \vee \beta \in$ CL(ϕ) $\implies$ $\alpha,\ \beta \in$ CL(ϕ)
- $X\alpha \in$ CL(ϕ) $\implies$ $\alpha \in$ CL(ϕ)
- $\alpha U \beta \in$ CL(ϕ) $\implies$ $\alpha,\ \beta,\ X(\alpha U \beta) \in$ CL(ϕ)

$$\alpha U \beta \;\equiv\; \beta \,\vee\, \alpha \wedge X(\alpha U \beta)$$

$A \subseteq$ CL(ϕ) jest atomem wtw. gdy

- $\alpha \in A \iff \neg\alpha \notin A$
- $\alpha \vee \beta \in A \iff \alpha \in A$ lub $\beta \in A$
- $\alpha U \beta \in A \iff \beta \in A$ lub $\alpha,\ X(\alpha U \beta) \in A$

$$\alpha U \beta \equiv \beta \vee \alpha \wedge X(\alpha U \beta)$$

LTL $\longrightarrow$ GBA (3)

$$\phi \;\mapsto\; \mathcal{A}_\phi \;=\; \langle \Sigma, S, S_{\textsf{pocz}}, \sigma, F \rangle$$

– $\Sigma \;=\; \mathcal{P}(P)$ załóżmy, że $P \subseteq$ CL(ϕ)

– $S \;=\;$ atomy

– $A \xrightarrow{X} B$ wtw. gdy

$$X \;=\; A \cap \Sigma \quad \text{i} \quad X\alpha \in A \;\iff\; \alpha \in B$$

– $S_{\textsf{pocz}} \;=\; \{A \in \text{atomy} \mid \phi \in A\}$

– $F \;=\; ?$

Przykład

$\phi = \neg a U b$

$\mathsf{CL}(\phi) \;=\; \{\phi,\ \neg\phi,\ X\phi,\ \neg X\phi,\ a,\ \neg a,\ b,\ \neg b\}$

$\longrightarrow \{\phi,\ b,\ \neg a,\ \neg X\phi\}$

$\{\neg\phi,\ \neg b,\ \neg X\phi,\ \neg a\}$

$\{\neg\phi,\ \neg b,\ X\phi,\ a\}$

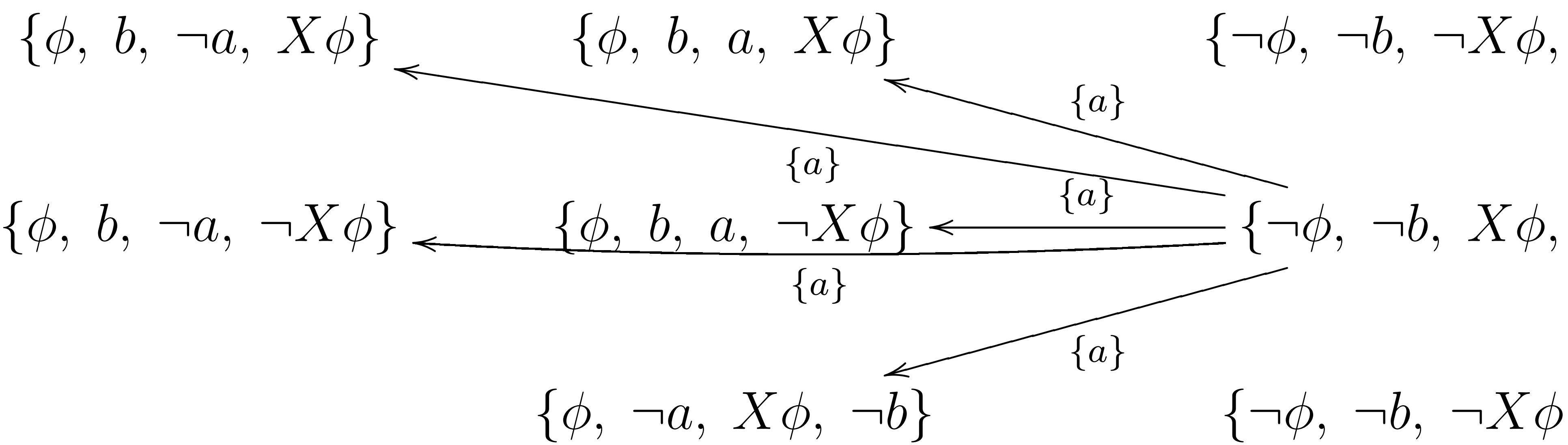
$\longrightarrow \{\phi,\ \neg a,\ X\phi,\ \neg b\}$

$\{\neg\phi,\ \neg b,\ \neg X\phi,\ a\}$

Przykład

$\phi = \neg a U b$

$$\mathsf{CL}(\phi) = \{\phi,\ \neg\phi,\ X\phi,\ \neg X\phi,\ a,\ \neg a,\ b,\ \neg b\}$$



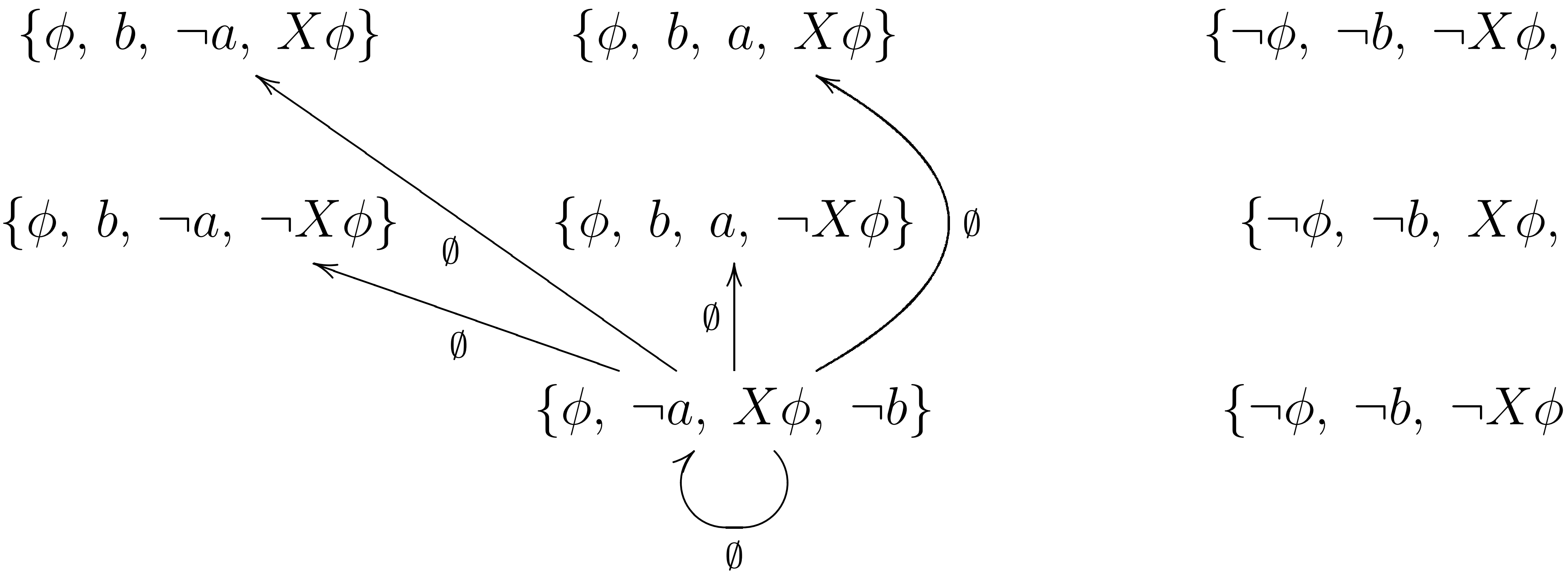
Przykł ad

$\phi = \neg a U b$

$\mathsf{CL}(\phi) \; = \; \{\phi,\ \neg\phi,\ X\phi,\ \neg X\phi,\ a,\ \neg a,\ b,\ \neg b\}$

$$
\begin{tikzcd}
\{\phi,\ b,\ \neg a,\ X\phi\} & \{\phi,\ b,\ a,\ X\phi\} & \{\neg\phi,\ \neg b,\ \neg X\phi, \\
\{\phi,\ b,\ \neg a,\ \neg X\phi\} & \{\phi,\ b,\ a,\ \neg X\phi\} \arrow[ur, "\{a{,}b\}"] \arrow[r, "\{a{,}b\}"] \arrow[dr, "\{a{,}b\}"'] & \{\neg\phi,\ \neg b,\ X\phi, \\
 & \{\phi,\ \neg a,\ X\phi,\ \neg b\} & \{\neg\phi,\ \neg b,\ \neg X\phi,
\end{tikzcd}
$$

$\phi = \neg a U b$ $\qquad$ $\mathsf{CL}(\phi) = \{\phi,\ \neg\phi,\ X\phi,\ \neg X\phi,\ a,\ \neg a,\ b,\ \neg b\}$



$F = ?$ $\qquad$ $\phi\ \phi \ldots b$ $\qquad$ $\phi\ \phi \ldots \{\phi, b\}$

$\phi = \neg aUb$ $\qquad$ $\mathsf{CL}(\phi) \; = \; \{\phi, \; \neg\phi, \; X\phi, \; \neg X\phi, \; a, \; \neg a, \; b, \; \neg b\}$

$$
\begin{tikzcd}
\{\phi, \; b, \; \neg a, \; X\phi\} & \{\phi, \; b, \; a, \; X\phi\} & \{\neg\phi, \; \neg b, \; \neg X\phi, \\
\{\phi, \; b, \; \neg a, \; \neg X\phi\} & \{\phi, \; b, \; a, \; \neg X\phi\} & \{\neg\phi, \; \neg b, \; X\phi, \\
 & \{\phi, \; \neg a, \; X\phi, \; \neg b\} \arrow[ul, "\emptyset"] \arrow[uul, "\emptyset"'] \arrow[u, "\emptyset"] \arrow[uu, bend right=60, "\emptyset"'] \arrow[loop below, "\emptyset"] & \{\neg\phi, \; \neg b, \; \neg X\phi,
\end{tikzcd}
$$

$F \; = \; \{A \; | \; \neg aUb \notin A \; \vee \; b \in A\}$ $\qquad$ $\phi \; \phi \ldots \{\phi, b\}$

LTL $\longrightarrow$ GBA (4)

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

- $\Sigma \;=\; \mathcal{P}(P)$ założmy, że $P \subseteq$ CL(ϕ)
- $S \;=\;$ atomy
- $A \xrightarrow{X} B$ wtw. gdy

  $X \;=\; A \cap \Sigma$ i $X\alpha \in A \iff \alpha \in B$

- $S_{\text{pocz}} \;=\; \{A \in \text{atomy} \mid \phi \in A\}$
- $F_i \;=\; \{A \mid \alpha_i U \beta_i \notin A \;\vee\; \beta_i \in A\}$, $\quad i = 1, \ldots, n$

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

Tw: $w \models \phi \iff w \in L_\omega(\mathcal{A}_\phi)$

Wniosek: ϕ spełnialna $\iff L_\omega(\mathcal{A}_\phi) \neq \emptyset$

Dowód tw.:

$\Longrightarrow$: niech $A_i = \{\alpha \in \mathsf{CL}(\phi) \mid w^i \models \alpha\}$

$A_0 A_1 A_2 \ldots$ jest biegiem akceptującym

$\Longleftarrow$: niech $w \in L_\omega(\mathcal{A}_\phi)$, niech $A_0 A_1 A_2 \ldots$ bieg akceptujący dla w

$$w^i \models \alpha \iff \alpha \in A_i, \quad \text{dla } i \geq 0,\ \alpha \in \mathsf{CL}(\phi)$$

(indukcja po α)

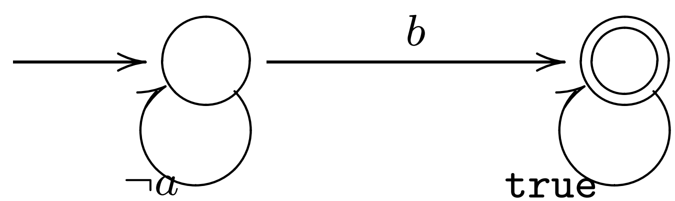
Przykł ad

$\phi = \neg a U b$

Czy automat $\mathcal{A}_\phi$ może być mniejszy?

$\phi = \neg a U b$

Czy automat $\mathcal{A}_\phi$ może być mniejszy? **TAK!**



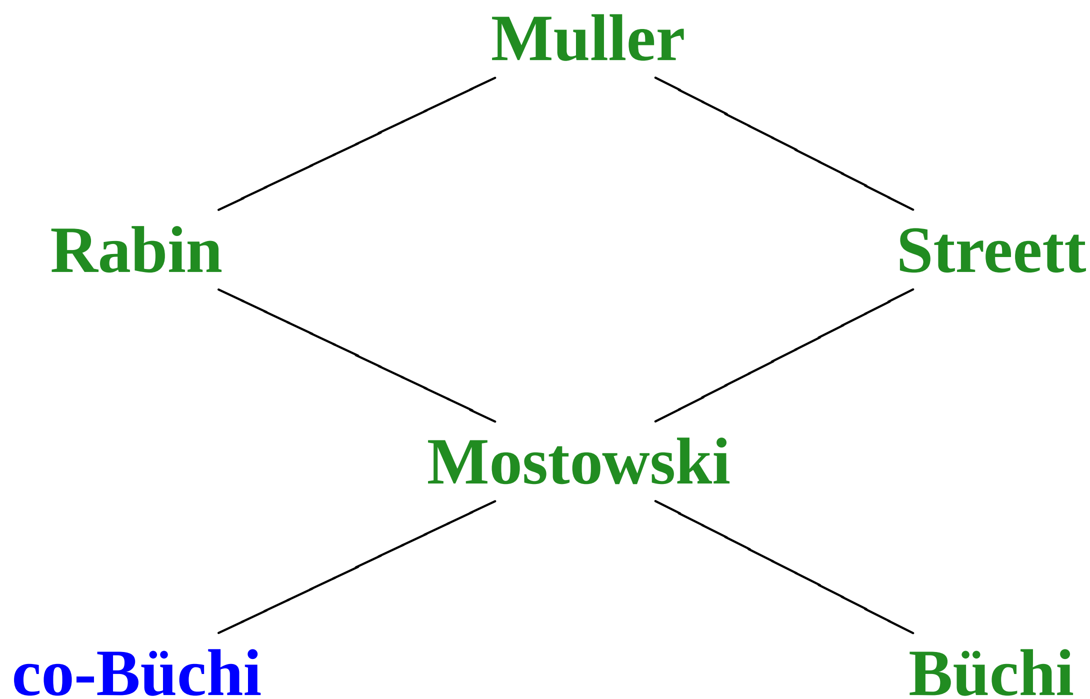
Inne warunki akceptacji

- **Büchi:** j.w.
- **co-Büchi:** j.w.
- **Muller:** $F \subseteq \mathcal{P}(Q)$

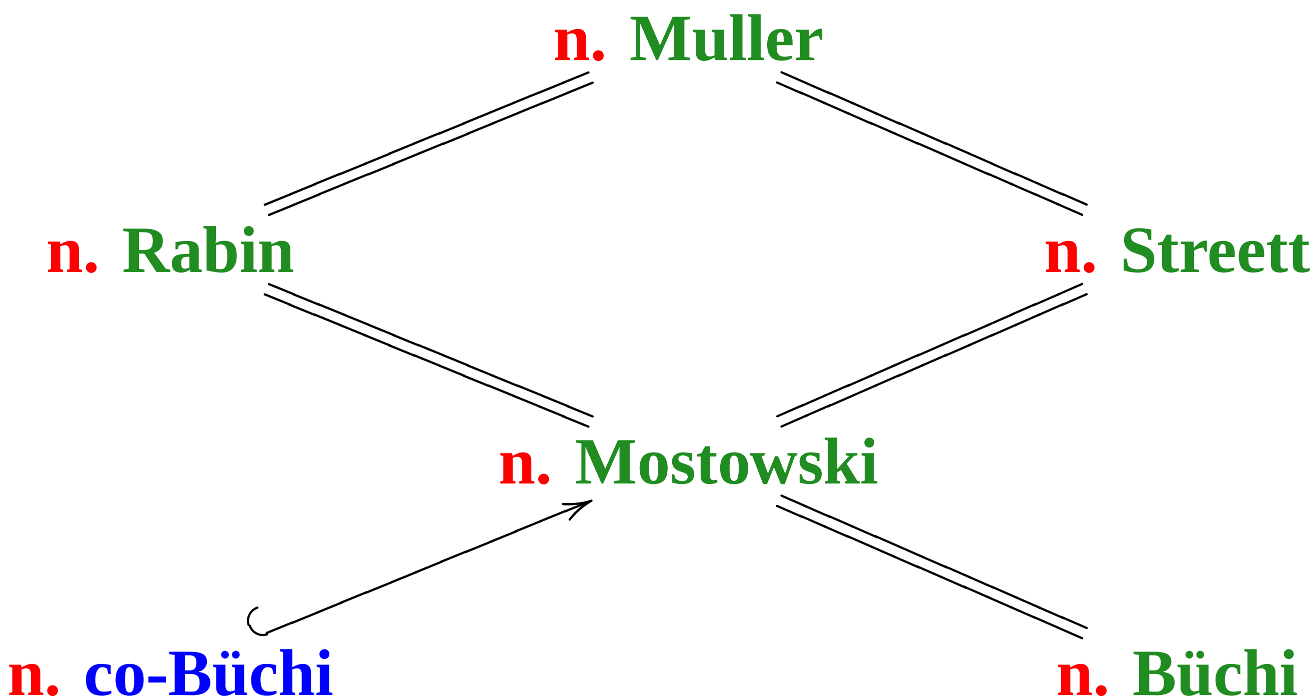
  r akceptujący $\iff \inf(r) \in F$
- **Rabin:** $F = \{(E_1, F_1), \ldots, (E_n, F_n)\} \subseteq \mathcal{P}(Q) \times \mathcal{P}(Q)$

  r akceptujący $\iff \exists i.\ \inf(r) \subseteq E_i \wedge \inf(r) \cap F_i \neq \emptyset$
- **Streett:** = co-Rabin
- **Mostowski (warunek parzystości):** ...

Inne warunki akceptacji



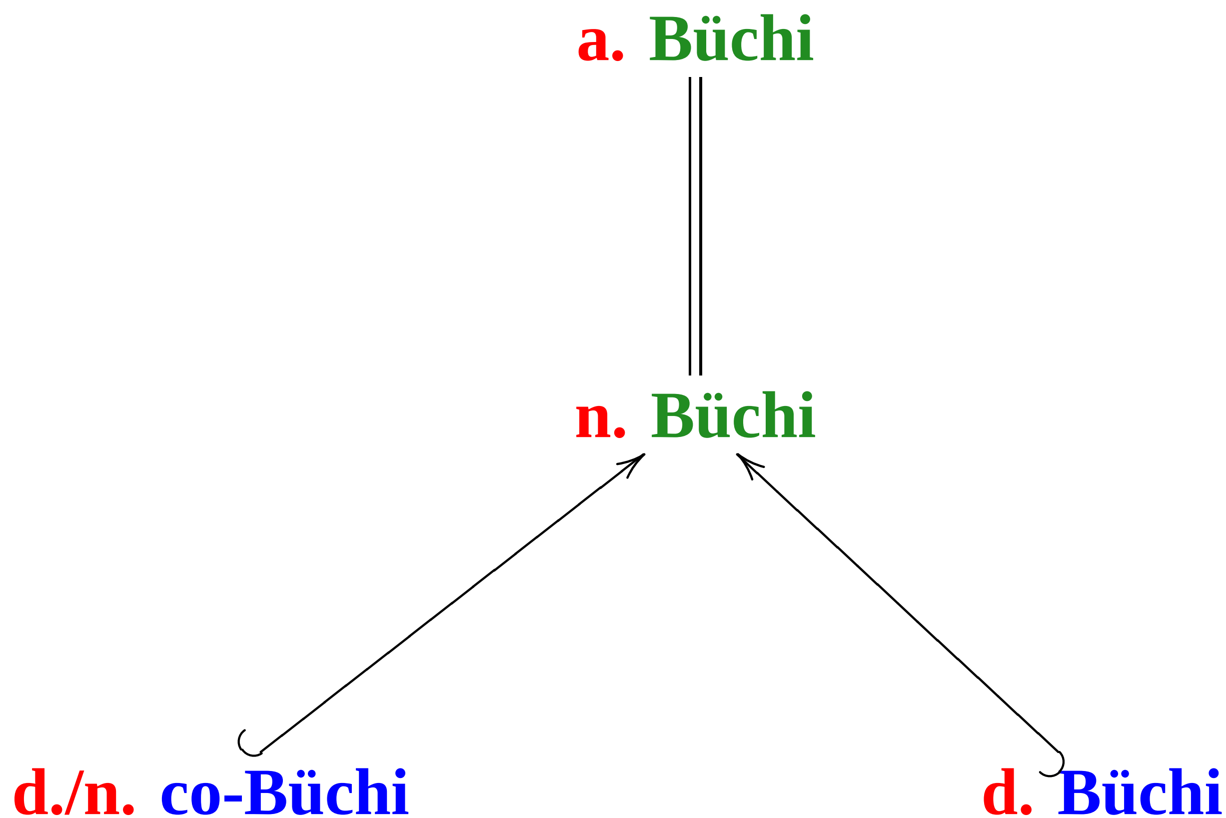
Klasy języków



$$\begin{tikzcd}
 & \textbf{d./n. Muller} \arrow[dl, equal] \arrow[dr, equal] & \\
\textbf{d./n. Rabin} \arrow[dr, equal] & & \textbf{d./n. Streett} \arrow[dl, equal] \\
 & \textbf{d./n. Mostowski} \arrow[dr, equal] & \\
\textbf{d./n. co-Büchi} \arrow[ur, hook] & & \textbf{n. Büchi} \\
 & \textbf{d. Büchi} \arrow[ur, hook] &
\end{tikzcd}$$

Języki ω-regularne: równoważne definicje

- niedeterministyczne ω-automaty
- wyrażenia ω-regularne: $\bigcup_{i=1}^{n} L_i \cdot K_i^{\omega}$
- S1S = FO + $\exists$ (drugiego rzędu)
- LTL + $\exists$, np. $\exists a.\, Fa \wedge G(a \implies (XFb \wedge XFa))$
- rachunek μ na ω-słowach
- alternujące ω-automaty
- słabe alternujące ω-automaty
- ...


a. Büchi
n. Büchi
d./n. co-Büchi
d. Büchi

LTL a ω-automaty

$$
\begin{tikzcd}
\text{LTL} \arrow[r, hook] \arrow[d, equal] & \text{LTL} + \exists \arrow[d, equal] \\
\text{liniowe alternujące } \omega\text{-automaty} \arrow[r, hook] & \text{alternujące } \omega\text{-automaty}
\end{tikzcd}
$$