

# Praktyczne metody weryfikacji

## Wykład 3: $\omega$ -automaty

# Po co nam $\omega$ -automaty?

## Przykład:



**LTL  $\subseteq$   $\omega$ -automaty**

**Def.:**  $\omega$ -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  $\forall s, a. |\sigma(s, a)| \leq 1$ .

$\omega$ -słowa:  $w = a_0 a_1 a_2 \dots$

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

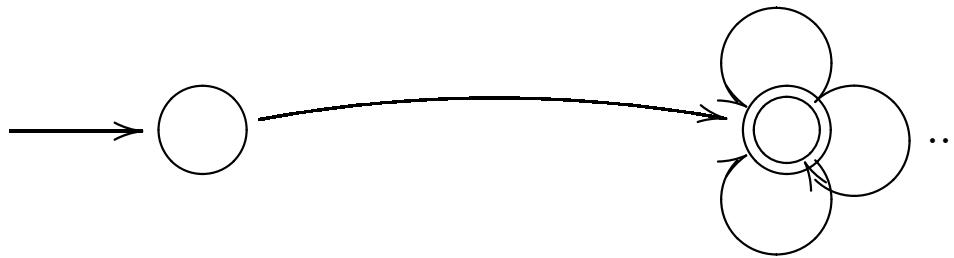
Niech  $\text{inf}(r) = \{s \in S : s = s_i \text{ dla nieskończenie wielu } i\}$ .

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

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

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

Bieg akceptujący wygląda tak:

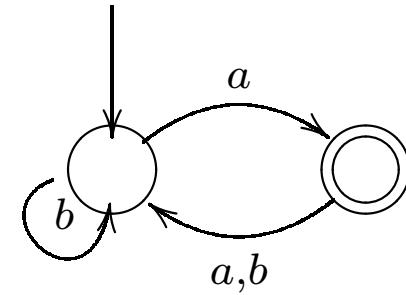


## Przykłady:

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

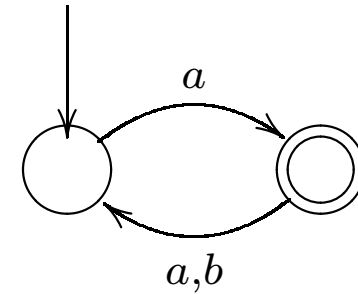
nieskończenie wiele  $a$

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



odd( $a$ )

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



**Wniosek:**  $LTL \subsetneq \omega$ -automaty

## Ćwiczenie:

- nieskończenie wiele  $a$  i  $b$
- między każdymi dwoma  $a$   
parzysta liczba  $b$

## Ćwiczenie:

- nieskończenie wiele  $a$  i  $b$
- między każdymi dwoma  $a$  parzysta liczba  $b$

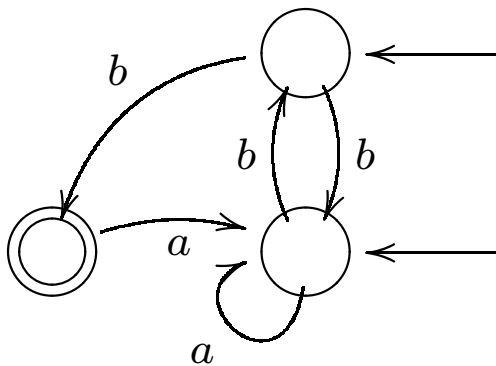
$$b^* (aa^* bb(bb)^*)^\omega$$



## Ćwiczenie:

- nieskończenie wiele  $a$  i  $b$
- między każdymi dwoma  $a$  parzysta liczba  $b$

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

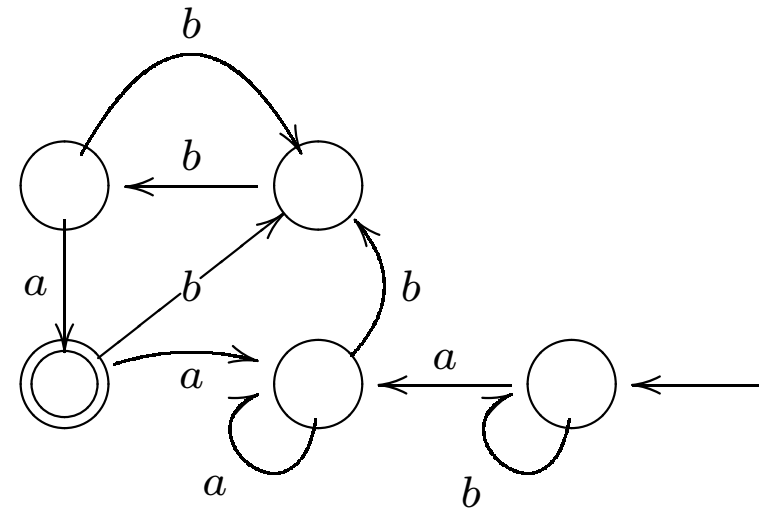
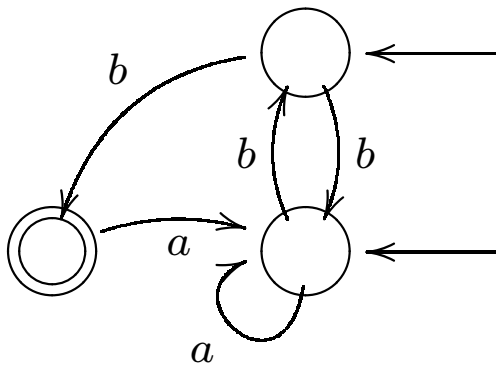


a deterministyczny ?

## Ćwiczenie:

- nieskończenie wiele  $a$  i  $b$
- między każdymi dwoma  $a$  parzysta liczba  $b$

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



**Ćwiczenie:**

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

skończenie wiele  $a$

**Ćwiczenie:**

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

skończenie wiele  $a$

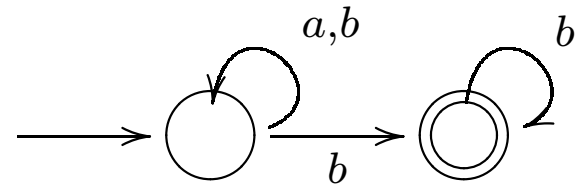
$$(b + a)^* b^\omega$$

## Ćwiczenie:

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

skończenie wiele  $a$

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



a deterministyczny ?

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

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

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

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

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

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

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

$$(2) \mathcal{A}_1, \mathcal{A}_2 \mapsto \mathcal{A}$$

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

?

$$(2) \mathcal{A}_1, \mathcal{A}_2 \mapsto \mathcal{A}$$

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

$$S = S_1 \times S_2 \times \{1, 2\}$$

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

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

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

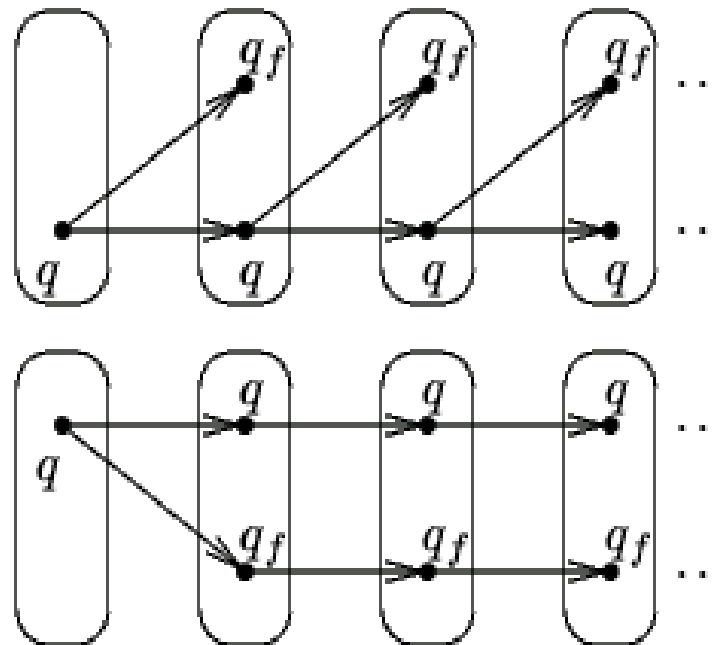
$$j = \begin{cases} 2 & \text{gdy } i = 1, s \in F_1 \\ 1 & \text{gdy } i = 2, t \in F_2 \\ i & \text{wpp} \end{cases}$$



(3)  $\mathcal{A} \mapsto \bar{\mathcal{A}}$

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

– brak determinizacji!



$$(3) \mathcal{A} \mapsto \bar{\mathcal{A}}$$

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

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

**Morał:** Najlepiej unikać uzupełnienia

$$\begin{array}{ccc} \phi & \xrightarrow{\quad} & \neg\phi \\ \vdots & & \downarrow \\ \mathcal{A}_\phi & \xrightarrow{\quad} & \bar{\mathcal{A}}_\phi \equiv \mathcal{A}_{\neg\phi} \end{array}$$

## Pytanie:

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

$$\mathcal{A} \dashrightarrow \bar{\mathcal{A}}$$

$$F \dashrightarrow Q \setminus F$$

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

## Pytanie:

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

$$\mathcal{A} \dashrightarrow \bar{\mathcal{A}}$$

$$F \dashrightarrow Q \setminus F$$

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

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

**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  $k_0$ ,  $\sigma(s_0, b^{k_0}) \in F$ .

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

...

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

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

**sprzeczność!**

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

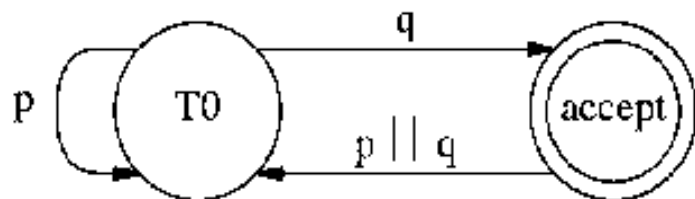
**Lasso**



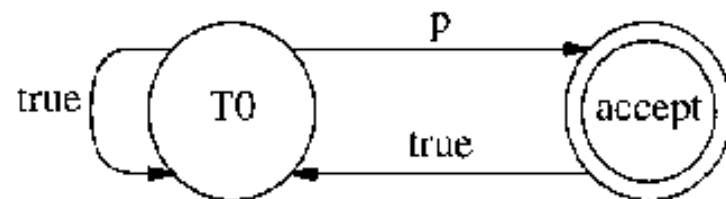
**Tw:**  $L_\omega(A) \neq \emptyset$  wtw gdy  $\mathcal{A}$  ma lasso.

# SPIN – przykłady

```
$ 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
}
```



dokumentacja SPIN'a

## Uogólnione $\omega$ -automaty Büchiego

(GBA)

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

**Pytanie:** Czy automaty uogólnione są ogólniejsze?



## Uogólnione $\omega$ -automaty Büchiego

(GBA)

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

**Pytanie:** Czy automaty uogólnione są ogólniejsze?

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

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

$\mathbf{CL}(\phi)$  – najmniejszy zbiór formuł t. że

$$- \phi \in \mathbf{CL}(\phi)$$

$$- \alpha \in \mathbf{CL}(\phi) \iff \neg\alpha \in \mathbf{CL}(\phi) \qquad \neg\neg\alpha \equiv \alpha$$

$$- \alpha \wedge \beta \in \mathbf{CL}(\phi) \implies \alpha, \beta \in \mathbf{CL}(\phi)$$

$$- X\alpha \in \mathbf{CL}(\phi) \implies \alpha \in \mathbf{CL}(\phi)$$

$$- \alpha \mathbf{U} \beta \in \mathbf{CL}(\phi) \implies \alpha, \beta, X(\alpha \mathbf{U} \beta) \in \mathbf{CL}(\phi)$$

$$\alpha \mathbf{U} \beta \equiv \beta \vee \alpha \wedge X(\alpha \mathbf{U} \beta)$$

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

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

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

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

$A \subseteq \mathbf{CL}(\phi)$  jest **atomem** wtw. gdy

$$- \alpha \in A \iff \neg\alpha \notin A$$

$$- \alpha \wedge \beta \in A \iff \alpha \in A \text{ i } \beta \in A$$

$$- \alpha \mathbf{U} \beta \in A \iff \beta \in A \text{ lub } \alpha, \mathbf{X}(\alpha \mathbf{U} \beta) \in A$$

$$\alpha \mathbf{U} \beta \equiv \beta \vee \alpha \wedge \mathbf{X}(\alpha \mathbf{U} \beta)$$

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

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

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

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

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

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

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

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

$$- \Sigma = \mathcal{P}(P)$$

załóżmy, że  $P \subseteq \text{CL}(\phi)$

$$- S = \text{atomy}$$

$$- A \xrightarrow{X} B \text{ wtw. gdy}$$

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

$$- S_{\text{pocz}} = \{A \in \text{atomy} \mid \phi \in A\}$$

$$- F = ?$$

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

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

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

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

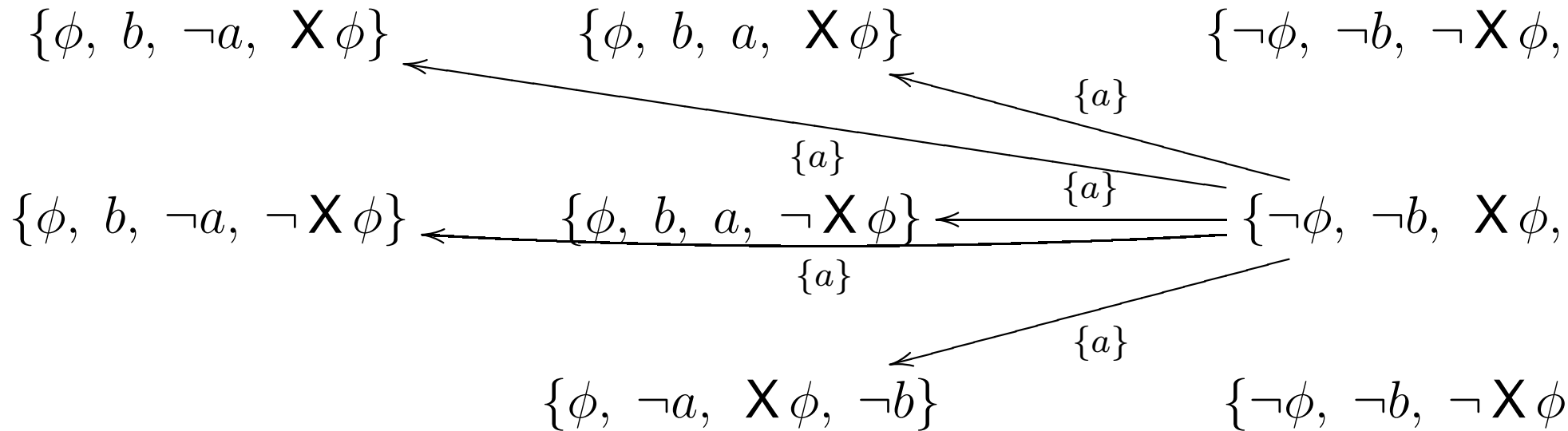
$$\{\neg\phi, \neg b, \mathbf{X}\phi, a\}$$

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

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

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

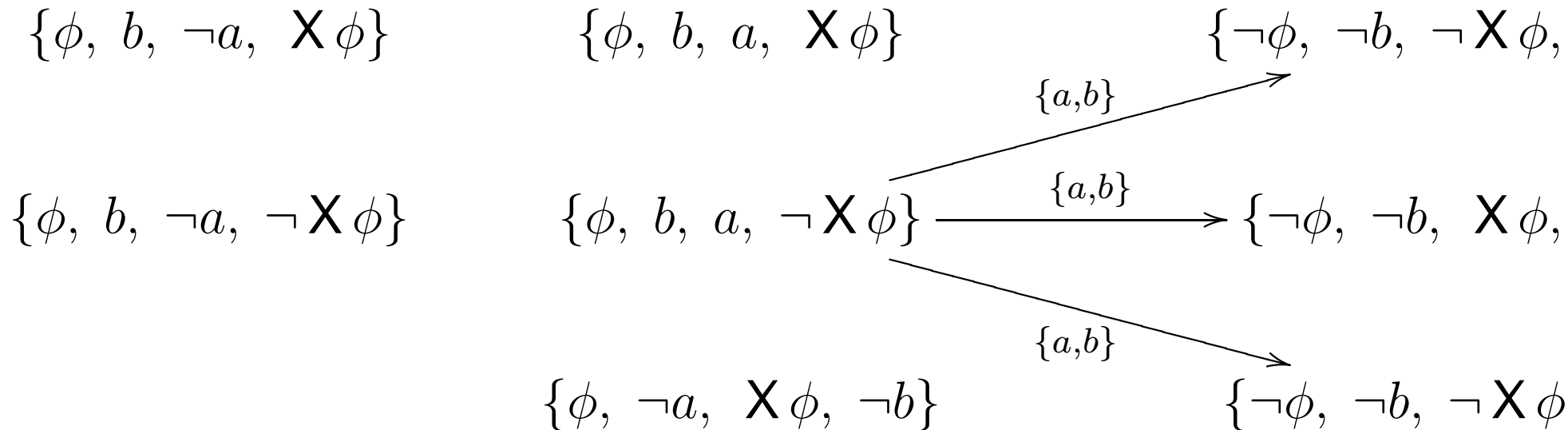
$$\mathbf{CL}(\phi) = \{\phi, \neg\phi, \mathbf{X}\phi, \neg\mathbf{X}\phi, a, \neg a, b, \neg b\}$$





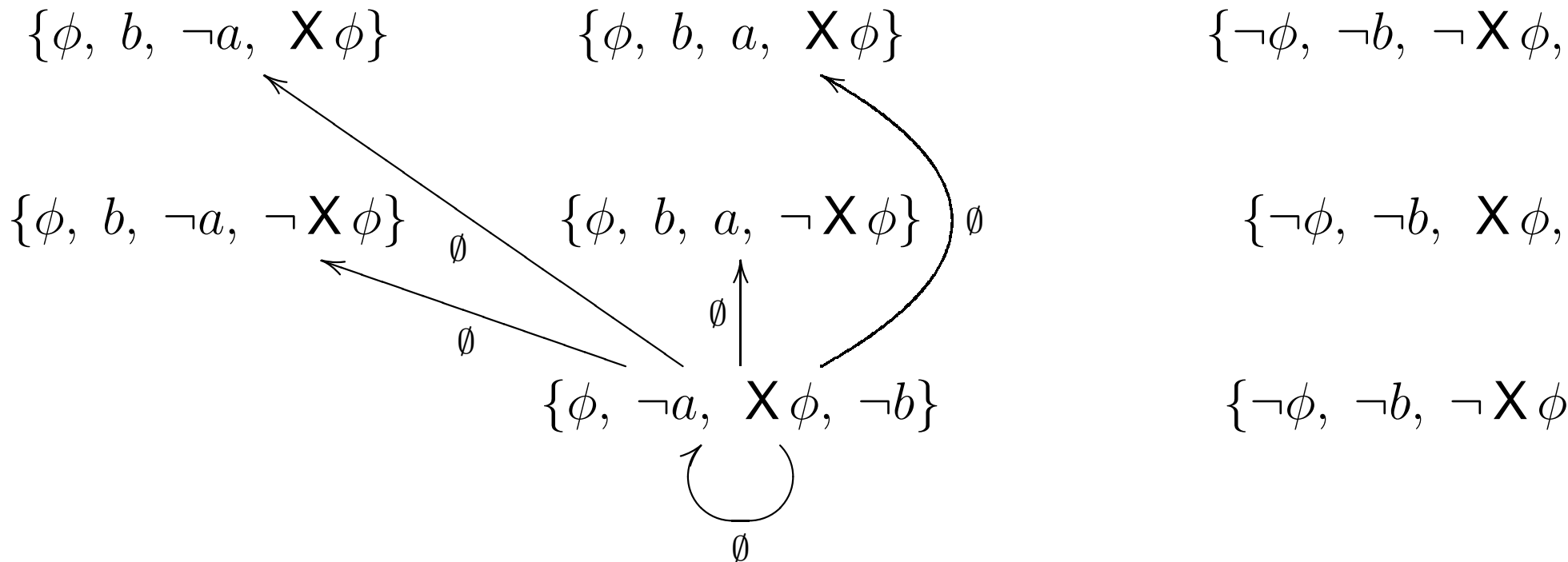
$$\phi = \neg a \mathbf{U} b$$

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



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

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



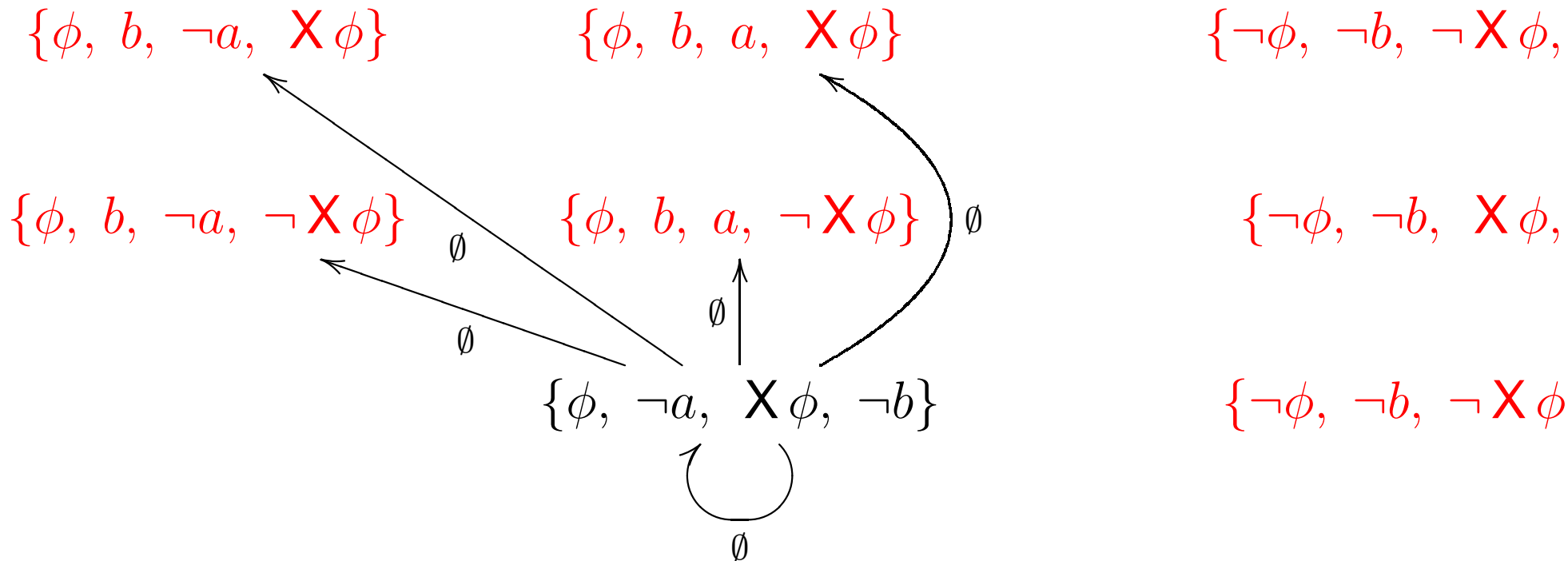
$$F = ?$$

$$\phi \phi \dots b$$

$$\phi \phi \dots \{\phi, b\}$$

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

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



$$F = \{A \mid \neg a \mathbf{U} b \notin A \vee b \in A\}$$

$$\phi \phi \dots \{\phi, b\}$$

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

$$- \Sigma = \mathcal{P}(P)$$

załóżmy, że  $P \subseteq \mathbf{CL}(\phi)$

$$- S = \text{atomy}$$

$$- A \xrightarrow{X} B \text{ wtw. gdy}$$

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

$$- S_{\text{pocz}} = \{A \in \text{atomy} \mid \phi \in A\}$$

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

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

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

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

**Dowód tw.:**

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

$A_0A_1A_2\dots$  jest biegiem akceptującym

$\impliedby$ : niech  $w \in L_\omega(\mathcal{A}_\phi)$ , niech  $A_0A_1A_2\dots$  bieg akceptujący dla  $w$

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

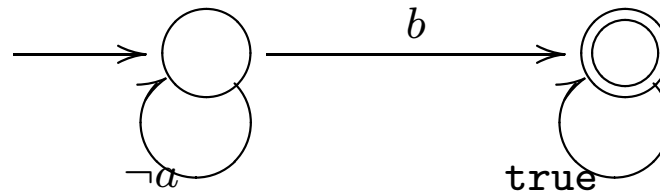
(indukcja po  $\alpha$ )

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

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

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

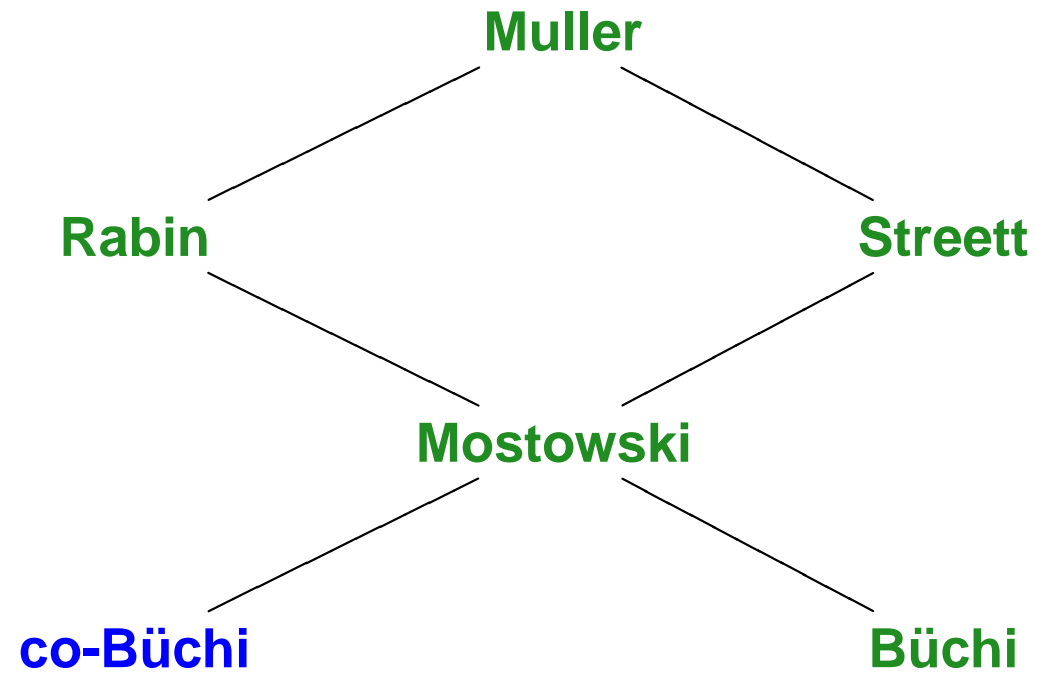
Czy automat  $\mathcal{A}_\phi$  może być mniejszy? **TAK!**

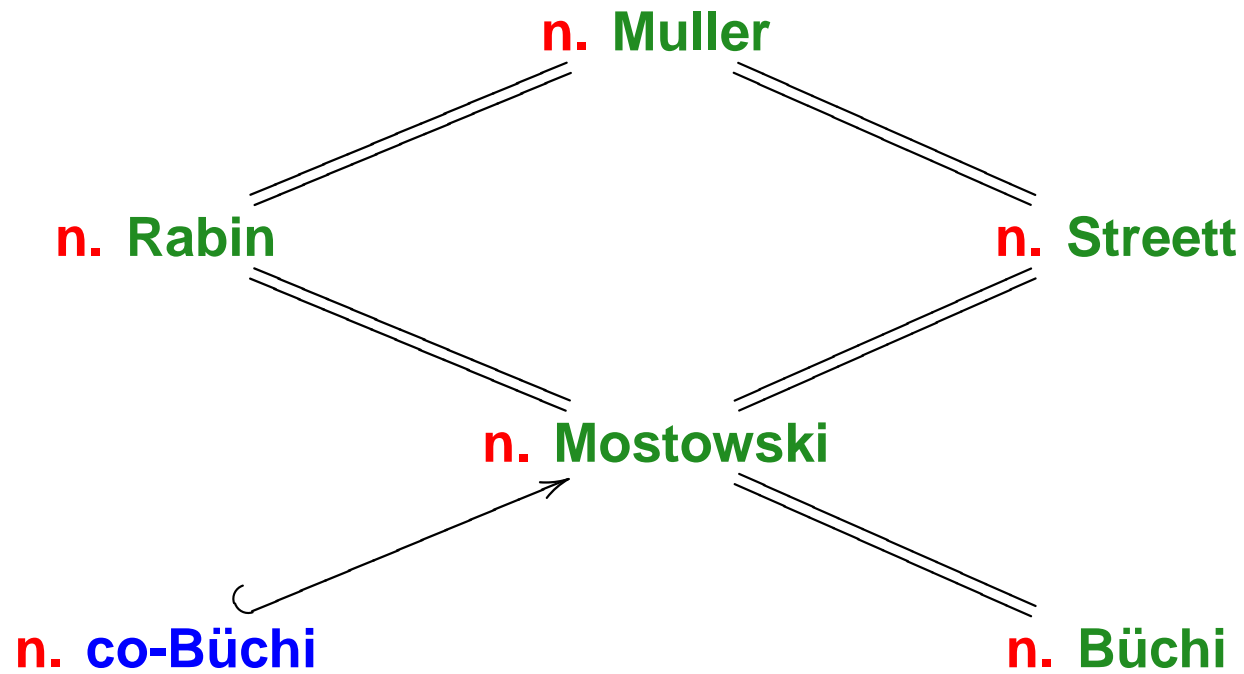


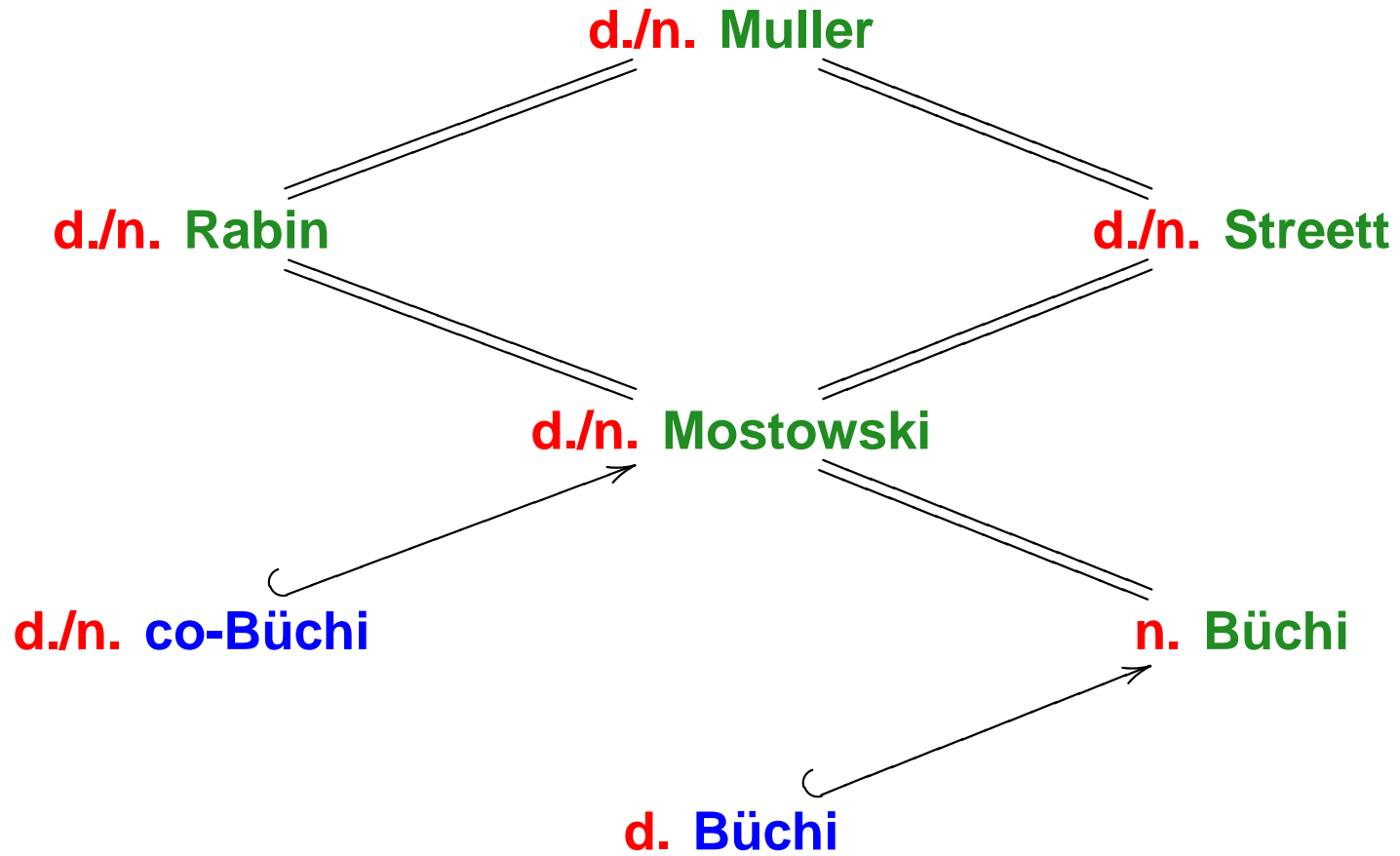
- **Büchi:** j.w.
- **co-Büchi:** j.w.
- **Muller:**  $F \subseteq \mathcal{P}(Q)$   
 $r$  akceptujący  $\iff \text{inf}(r) \in F$
- **Rabin:**  $F = \{(E_1, F_1), \dots, (E_n, F_n)\} \subseteq \mathcal{P}(Q) \times \mathcal{P}(Q)$   
 $r$  akceptujący  $\iff \exists i. \text{inf}(r) \subseteq E_i \wedge \text{inf}(r) \cap F_i \neq \emptyset$
- **Streett:** = co-Rabin
- **Mostowski (warunek parzystości):** ...



# Inne warunki akceptacji

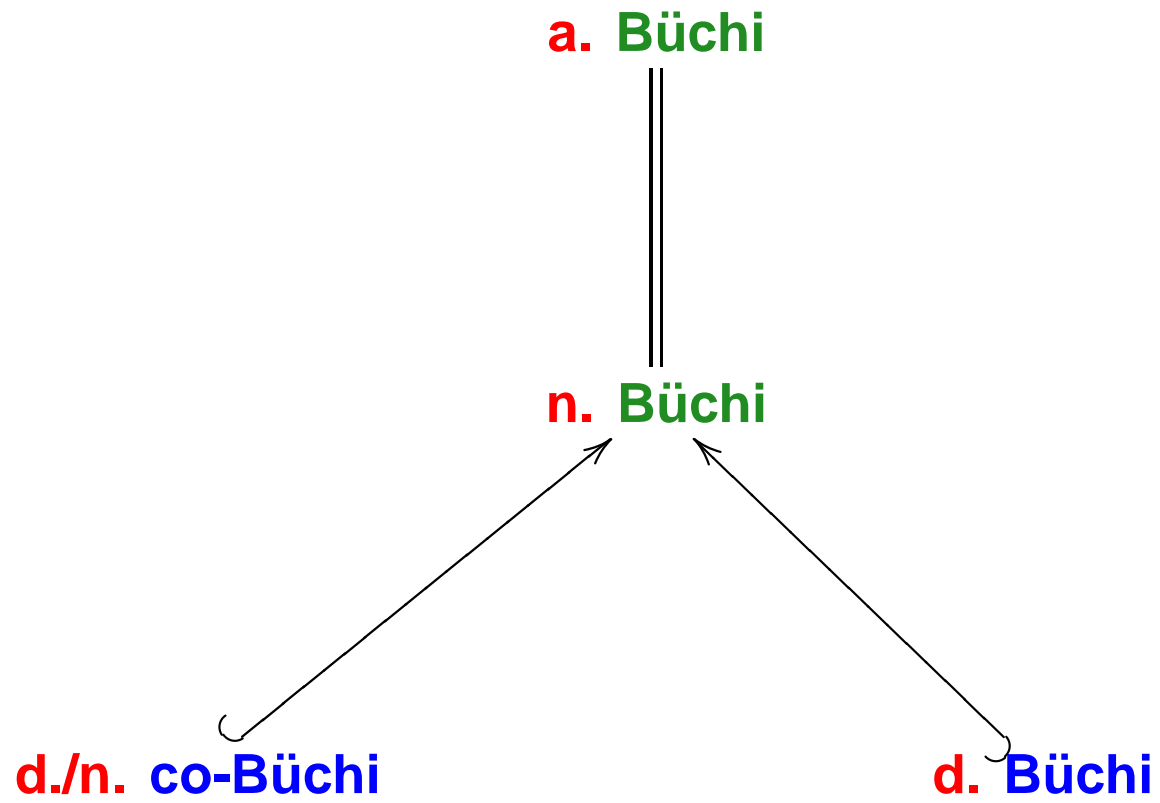




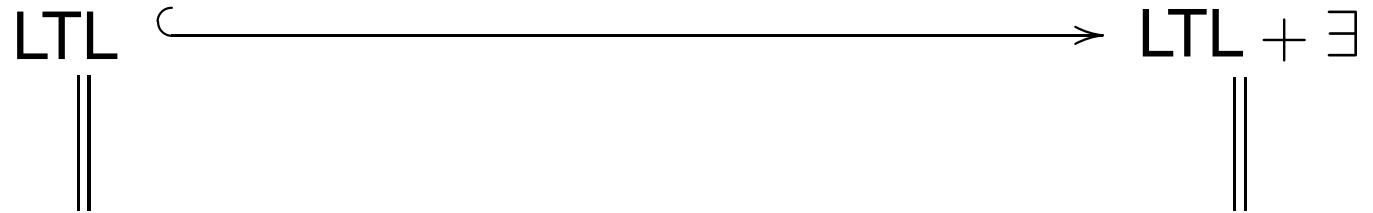


# Języki $\omega$ -regularne: równoważne definicje

- niedeterministyczne  $\omega$ -automaty
- wyrażenia  $\omega$ -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  $\mu$  na  $\omega$ -słowach
- **alternujące**  $\omega$ -automaty
- **słabe alternujące**  $\omega$ -automaty
- ...



## LTL a $\omega$ -automaty



liniowe alternujące  $\omega$ -automaty  $\hookrightarrow$  alternujące  $\omega$ -automaty