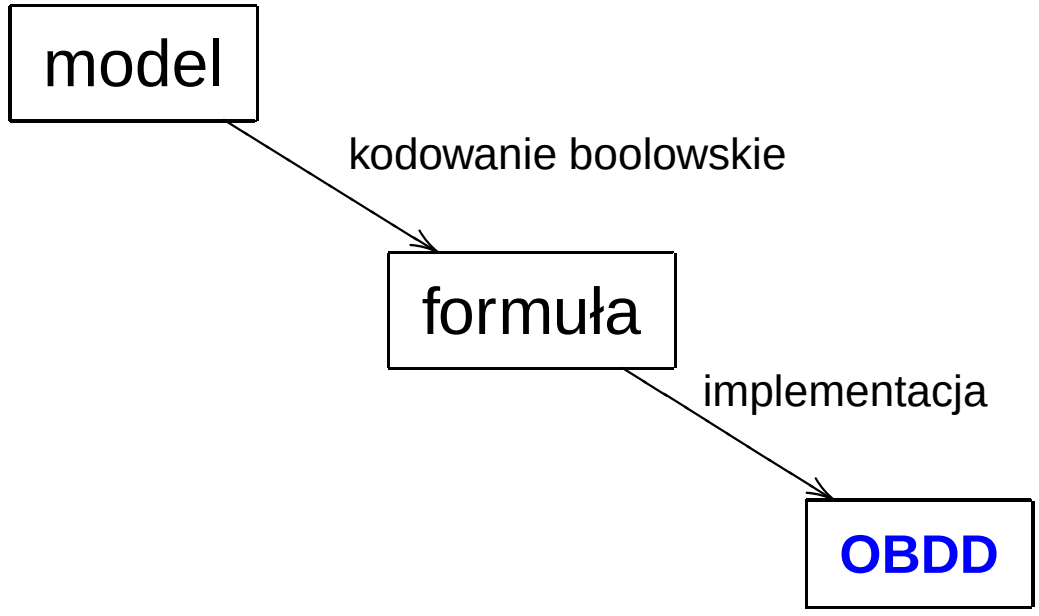
Praktyczne metody weryfikacji

Wykład 7: Weryfikacja symboliczna (I)

Symboliczna weryfikacja modelowa

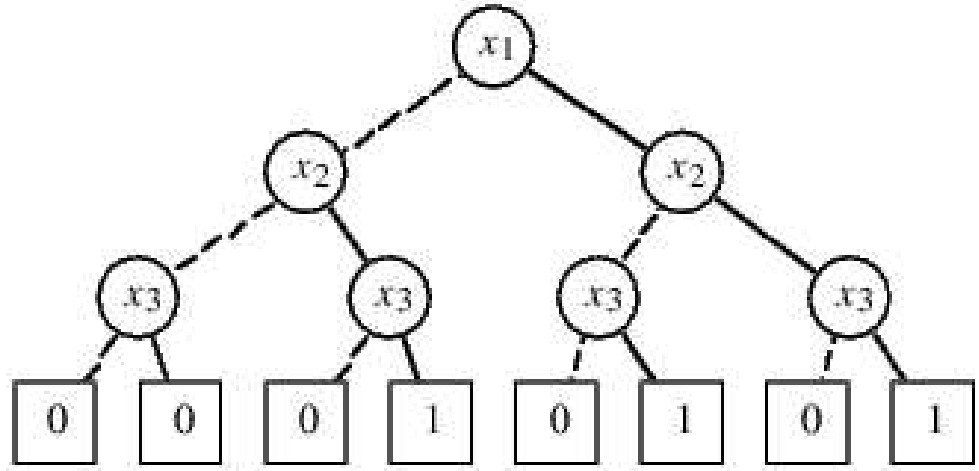


(kwantyfikowane) formuły boolowskie

I. OBDDs

OBDDs Ordered Binary Decision Diagrams

x_1	x_2	x_3	f
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1



– $f : \{0,1\}^3 \rightarrow \{0,1\}$

– ustalona kolejność zmiennych: $x_1 < x_2 < x_3$

OBDD = ukorzeniony graf acykliczny

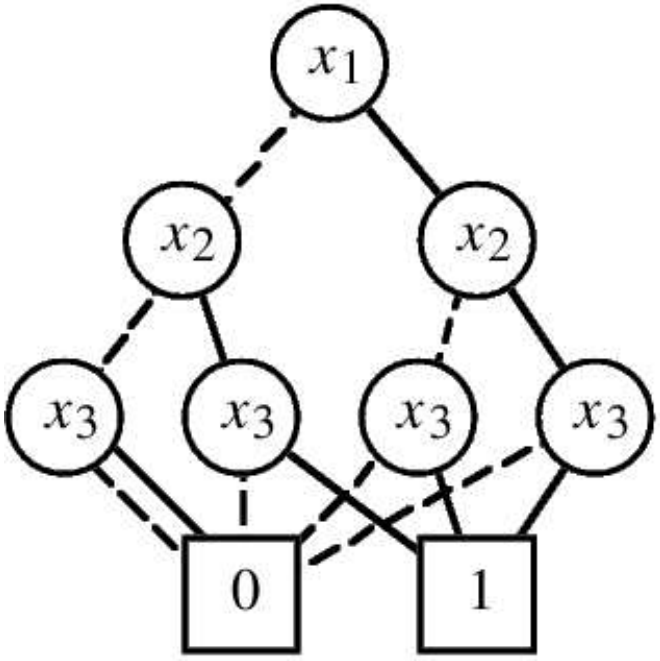
Atrybuty wierzchołka v:

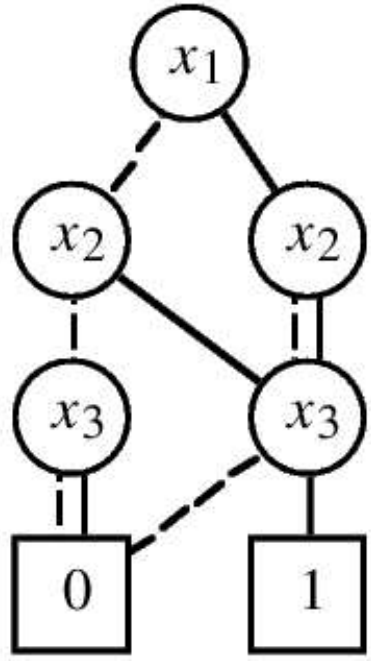
- gdy v jest końcowy (liść)
  - $\mathrm{val}(v) \in \{0, 1\}$
- gdy v nie jest końcowy
  - $\mathrm{var}(v) \in \{x_1, x_2, \ldots\}$
  - $\mathrm{lo}(v), \mathrm{hi}(v)$ – 2 wierzchołki

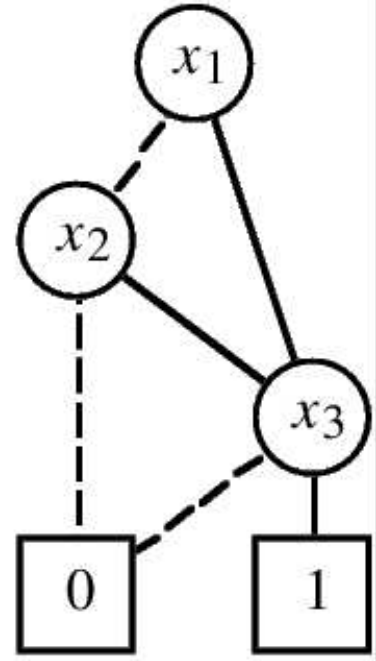
Kolejność zmiennych musi być przestrzegana na każdej ścieżce.

Upraszczanie OBDD

- usuń nadmiarowe wierzchołki końcowe
- usuń nadmiarowe wierzchołki niekońcowe
- usuń nadmiarowe testy







Postać kanoniczna dla funkcji boolowskiej f:

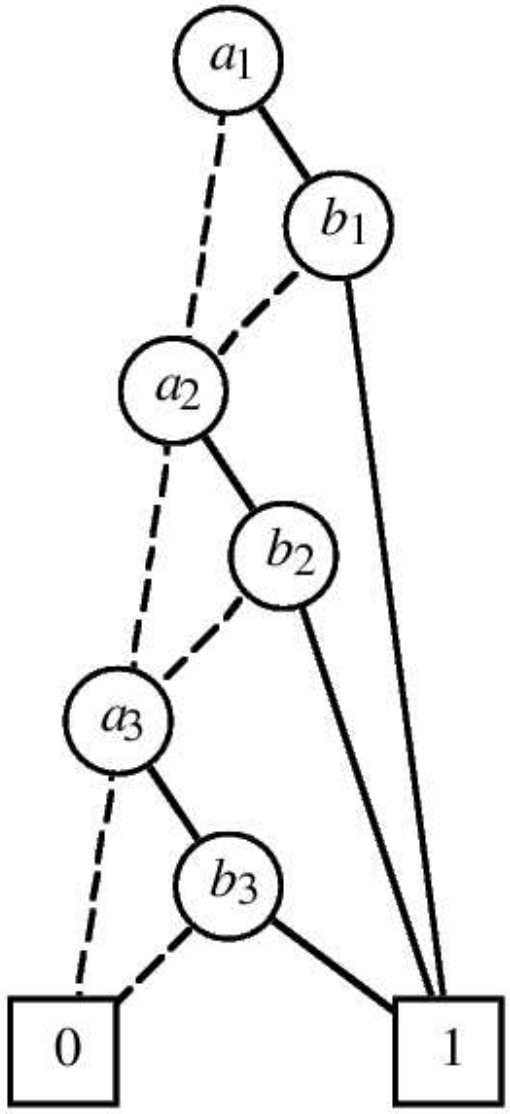
- niezależna od grafu wyjściowego
- (silnie) zależna od kolejności zmiennych

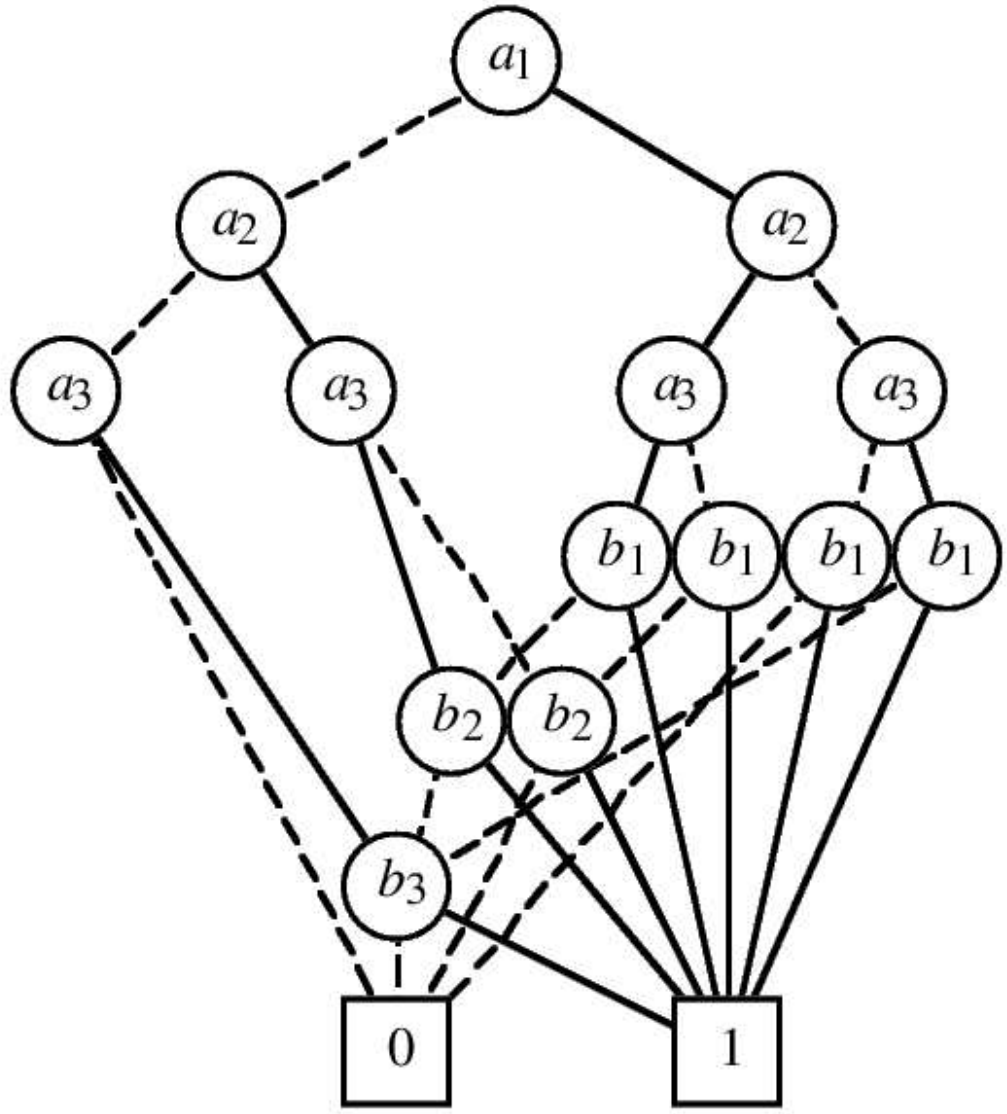
Naiwna konstrukcja OBBD dla formuły boolowskiej ϕ:

$$\phi \longmapsto \text{drzewo} \longmapsto \text{kanoniczny OBDD}$$

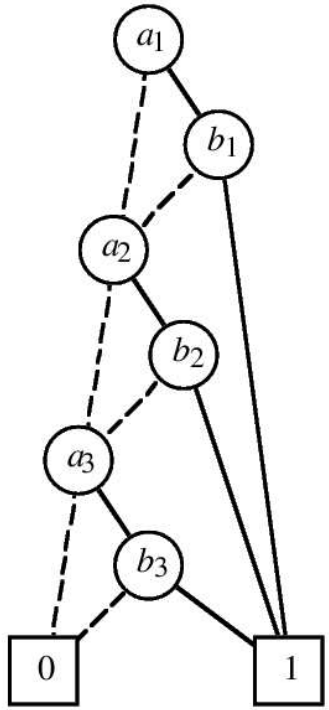
Znalezienie właściwej kolejności zmiennych jest kluczowe!

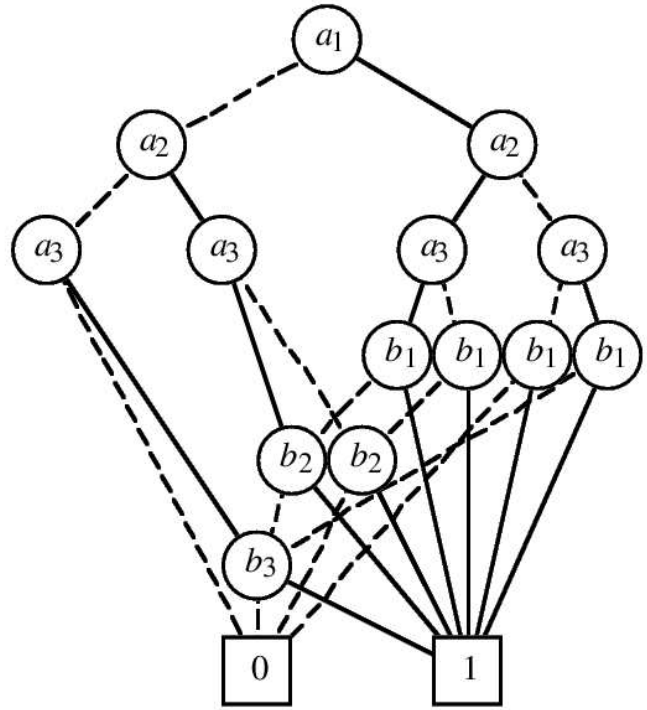
$$a_1 \wedge b_1 \ \vee \ a_2 \wedge b_2 \ \vee \ a_3 \wedge b_3$$





$$f(a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n) = a_1 \wedge b_1 \ \vee \ a_2 \wedge b_2 \ \vee \ \ldots \ \vee \ a_n \wedge b_n$$





$2 \cdot n$ $\qquad\qquad$ $2 \cdot (2^n - 1)$

Rozmiar OBDD

Heurystyka: zmienne powiązane powinny być blisko

klasa funkcji boolowskich	dolna granica	górna granica
funkcje symetryczne	$\mathcal{O}(n)$	$\mathcal{O}(n^2)$
dodawanie (dowolny bit)	$\mathcal{O}(n)$	$\mathcal{O}(2^n)$
mnożenie (środkowe bity)	$\mathcal{O}(2^n)$	$\mathcal{O}(2^n)$

Wzór Shannona

$$f \quad = \quad x \wedge f\big|_{x \leftarrow 1} \quad \vee \quad \neg x \wedge f\big|_{x \leftarrow 0}$$

$$f\big|_{x_i \leftarrow b}(x_1, \ldots, x_n) \quad = \quad f(x_1, \ldots, x_{i-1}, b, x_{i+1}, \ldots, x_n)$$

Wzór Shannona

$$f \;=\; x \wedge f\big|_{x\leftarrow 1} \;\vee\; \neg x \wedge f\big|_{x\leftarrow 0}$$

$$v \;=\; x \wedge \mathrm{hi}(v) \;\vee\; \neg x \wedge \mathrm{lo}(v)$$

$$x = \mathrm{var}(v)$$

Abstrakcyjny typ danych **funkcje boolowskie**

Operacje:

$f \vee g, \quad f \wedge g, \quad \neg f, \quad \texttt{false}, \quad \texttt{true}$ $\qquad BF \mapsto OBDD$

$f = g$

$f|_{x \leftarrow 0}, \quad f|_{x \leftarrow 1}$

$\exists x.\ f, \quad \forall x.\ f$ $\qquad QBF \mapsto OBDD$

$\ldots$

Uwaga!: operacje na **funkcjach**, nie na wartościach $\{0, 1\}$.

Implementacja operacji 1-arg.

– $f|_{x \leftarrow b}$

r – korzeń OBDD reprezentującego f, $\quad x \leq \mathrm{var}(r)$

$$\text{OBDD dla } f|_{x \leftarrow b} \quad = \quad \begin{cases} r & x < \mathrm{var}(r) \\ \mathrm{lo}(r) & x = \mathrm{var}(r),\ b = 0 \\ \mathrm{hi}(r) & x = \mathrm{var}(r),\ b = 1 \end{cases}$$

– $\exists x.\ f \quad = \quad f|_{x \leftarrow 0} \vee f|_{x \leftarrow 1}$

– $\neg f$ **?**

Implementacja operacji 2-arg.

- $\bullet : \{0,1\}^2 \to \{0,1\}$

$$f \bullet g \quad = \quad x \wedge (f|_{x \leftarrow 1} \bullet g|_{x \leftarrow 1}) \quad \vee \quad \neg x \wedge (f|_{x \leftarrow 0} \bullet g|_{x \leftarrow 0})$$

Apply(f, g, $\bullet$) (utożsammy f, g z korzeniem OBDD dla f, g)

- f, g końcowe: $\mathrm{val}(f \bullet g) = \mathrm{val}(f) \bullet \mathrm{val}(g)$
- f końcowe, g nie: $f \bullet g = op(g)$
- $\mathrm{var}(f) = \mathrm{var}(g) = x$:

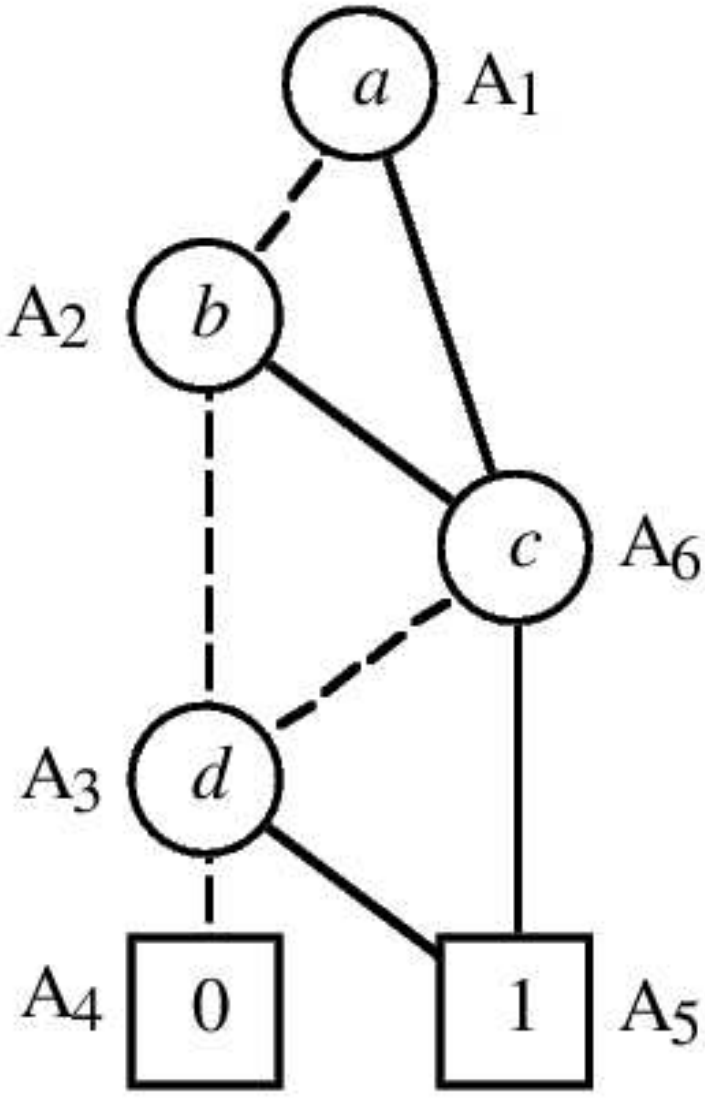
$$\mathrm{hi}(f \bullet g) = \mathrm{hi}(f) \bullet \mathrm{hi}(g) \qquad \mathrm{lo}(f \bullet g) = \mathrm{lo}(f) \bullet \mathrm{lo}(g)$$

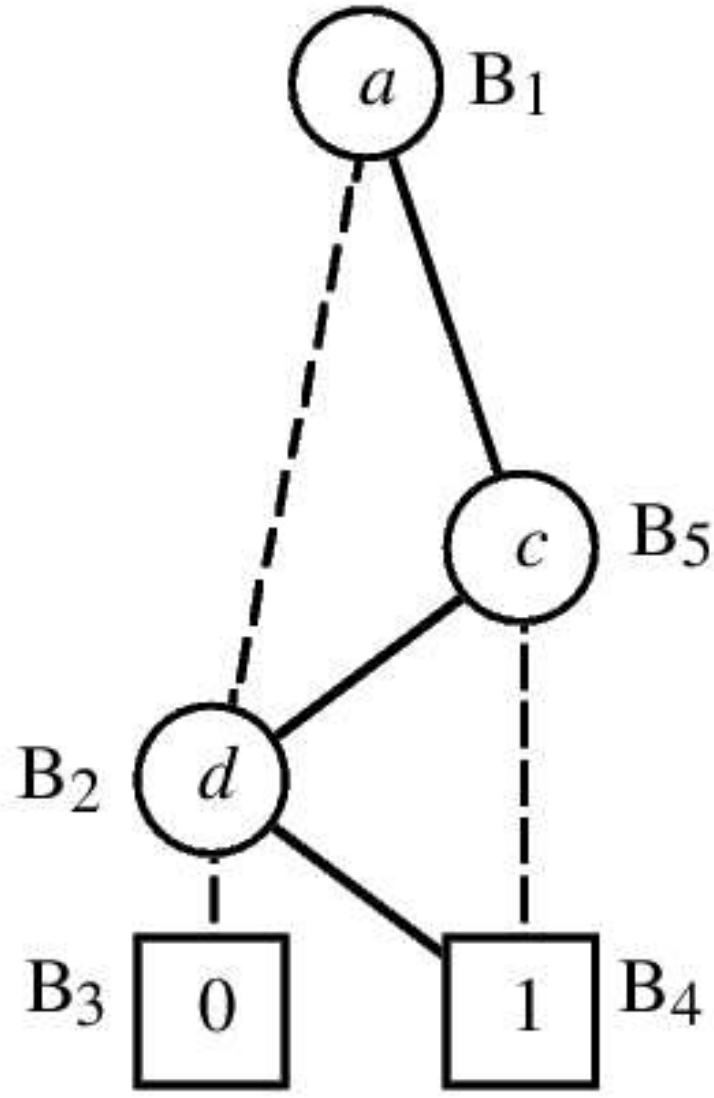
- $\mathrm{var}(f) = x < y = \mathrm{var}(g)$:

$$\mathrm{hi}(f \bullet g) = \mathrm{hi}(f) \bullet g \qquad \mathrm{lo}(f \bullet g) = \mathrm{lo}(f) \bullet g$$

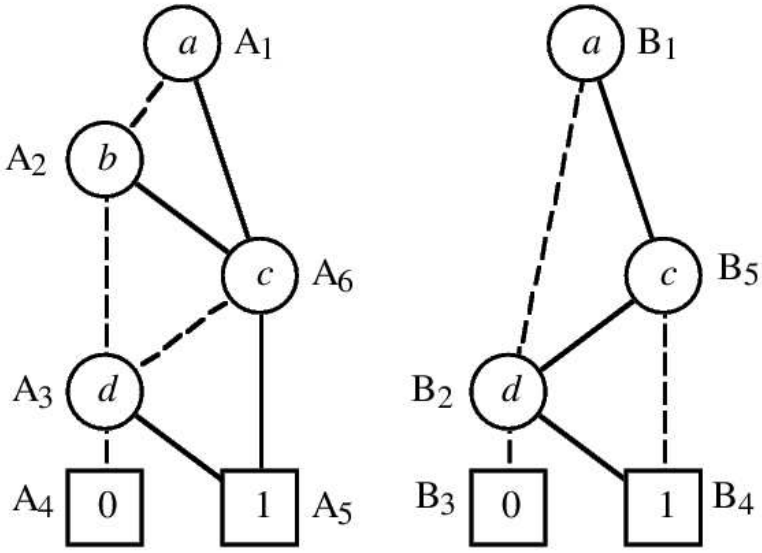
$$f \bullet g = x \wedge (f|_{x \leftarrow 1} \bullet g|_{x \leftarrow 1}) \vee \neg x \wedge (f|_{x \leftarrow 0} \bullet g|_{x \leftarrow 0})$$

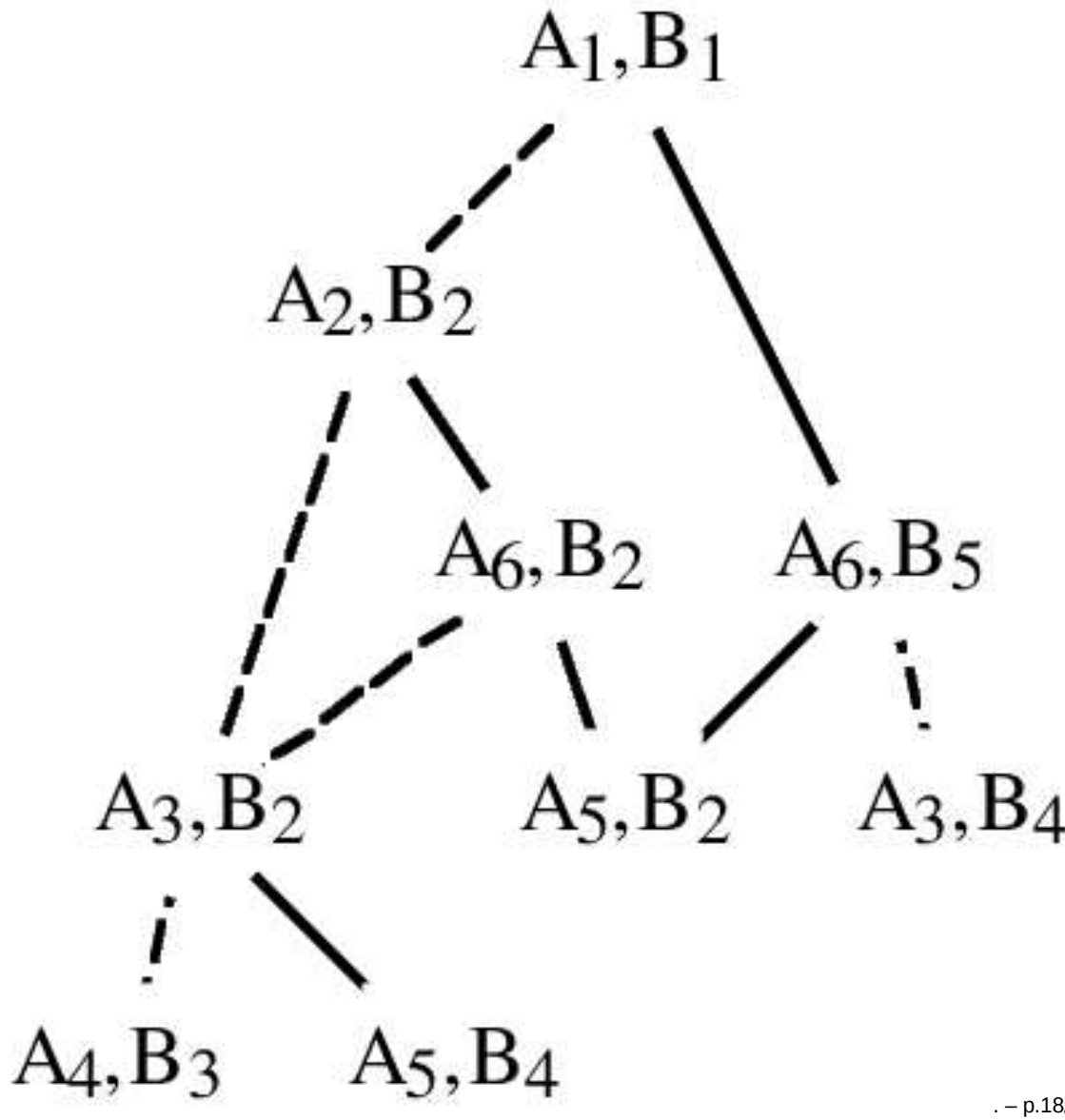
Przykład: dane wyjściowe



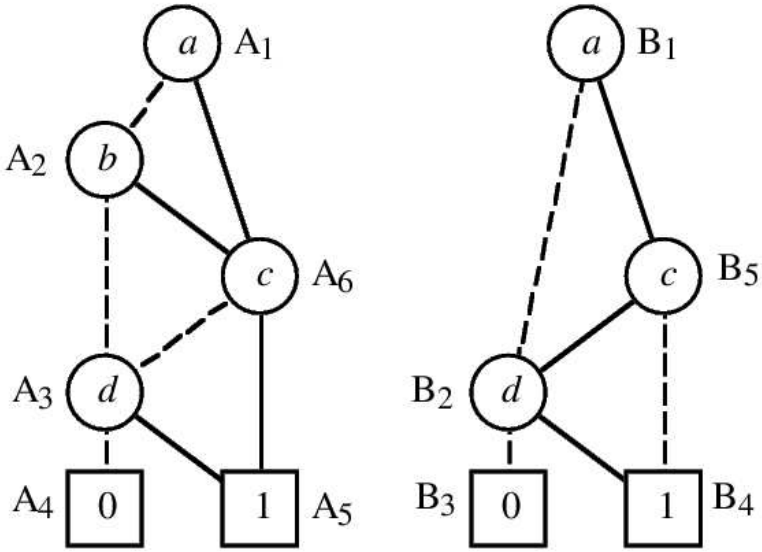


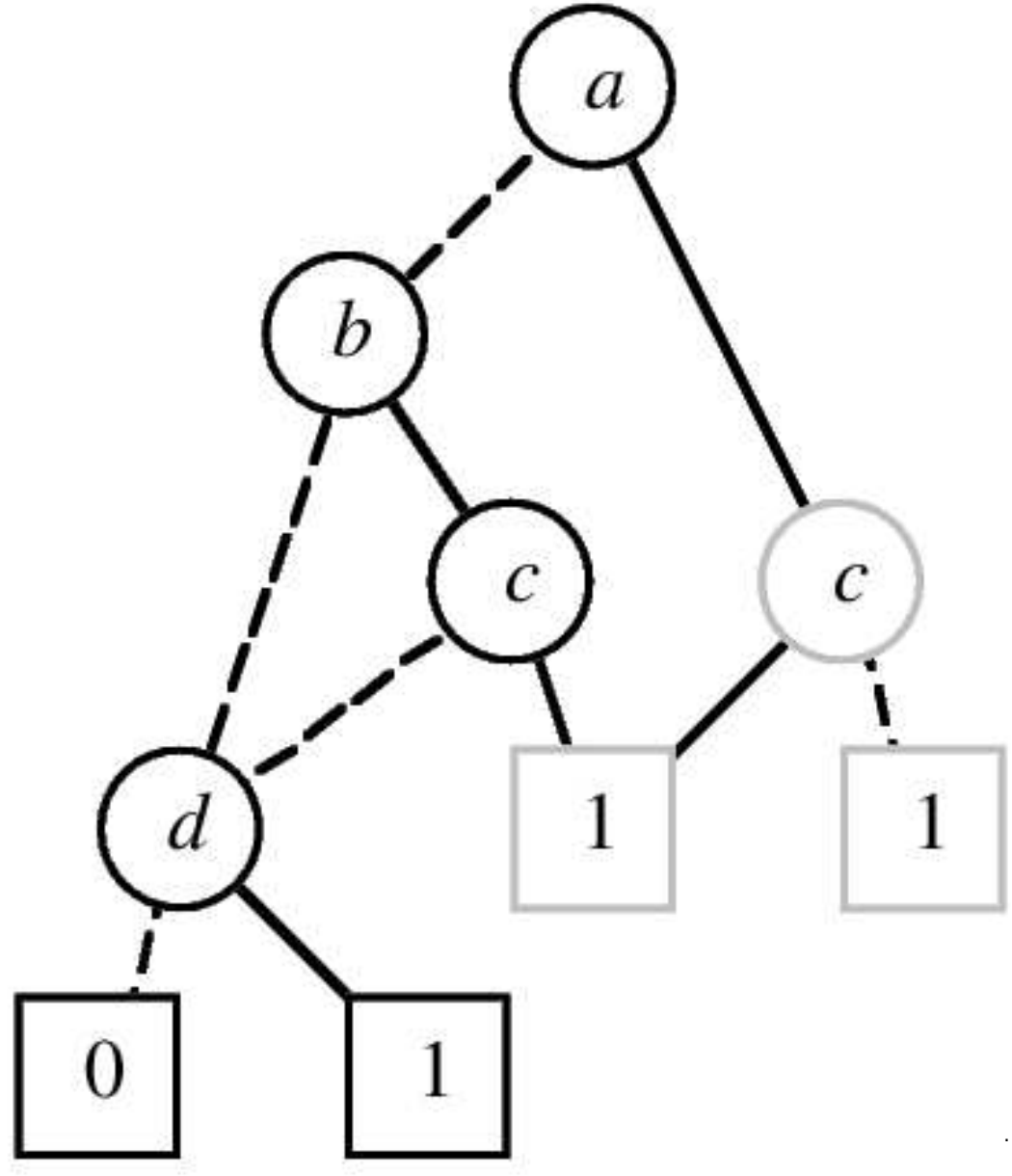
Przykład: wywołania rekurencyjne



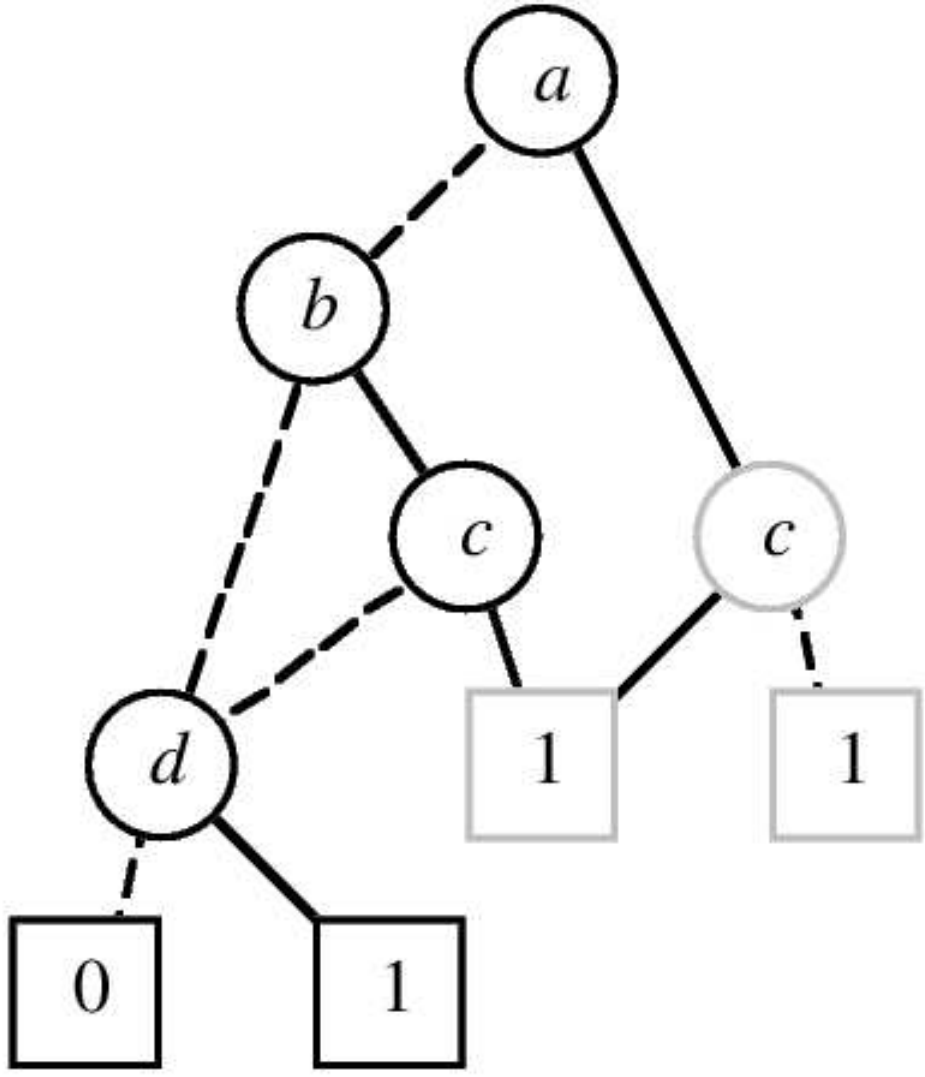


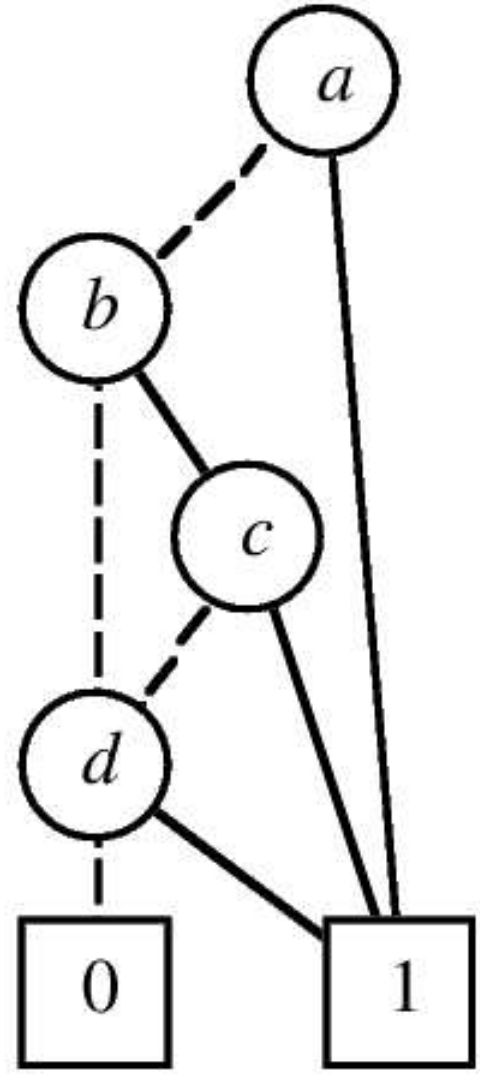
Przykład: wynik = $a \vee b \wedge c \vee d$





Przykład: wynik = $a \vee b \wedge c \vee d$





$\mathrm{Apply}(\ f,\ g,\ \bullet\ )$

- koszt czasowy: $\mathcal{O}(|f| \cdot |g|)$
- wynik w postaci kanonicznej

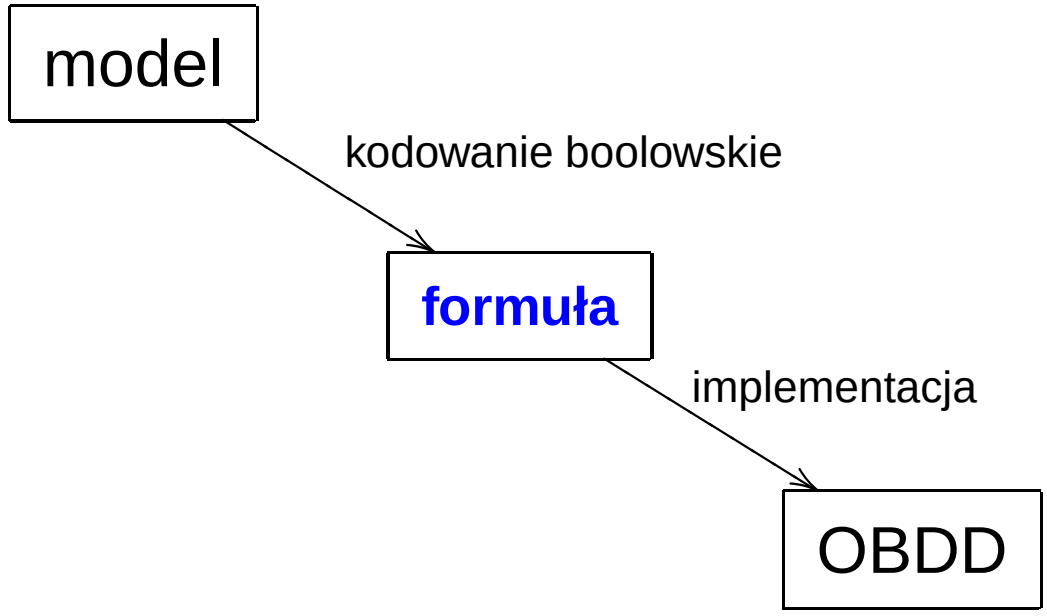
Pytanie: $f = g$ **?**

Odmiany:

- wspólny OBDD dla wszystkich funkcji
  - $=$ w czasie stałym
- krawędzie dla $\neg$

II. Kodowanie boolowskie

Kodowanie boolowskie



(kwantyfi kowane) formuły boolowskie

Opis symboliczny

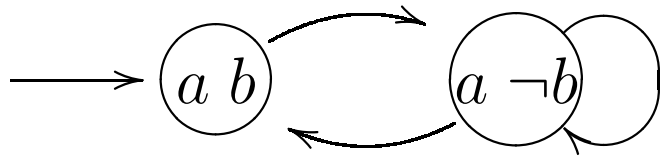
- S opisany przez m zmiennych $\{0,1\}$-owych
- bijekcja $\gamma : \{0,1\}^m \to S$
- relacja przejścia R:

$$\widehat{R}(x_1,\ldots,x_m,x'_1,\ldots,x'_m) = 1 \iff R(\gamma(x_1,\ldots,x_m),\gamma(x'_1,\ldots,x'_m))$$

- $L_p = \{s \mid p \in L(s)\} \subseteq S, \quad S_0 \subseteq S$

  $\widehat{X}(x_1,\ldots,x_m) = 1 \iff \gamma(x_1,\ldots,x_m) \in X$ dla $X \subseteq S$

Przykład



$$\widehat{R} = (a \wedge b \wedge a' \wedge \neg b') \vee (a \wedge \neg b \wedge a' \wedge \neg b') \vee (a \wedge \neg b \wedge a' \wedge b')$$

$$\widehat{S_0} = a \wedge b$$

$$\widehat{L_p} = \ldots$$

struktura Kripkego $\longmapsto$ OBDDs **ŹLE!**

opis struktury K. $\longmapsto$ OBDDs **DOBRZE!**

kompozycjonalny **opis** systemu

Procesy synchroniczne:

$$R \;=\; R_1 \;\wedge\; R_2 \wedge \;\ldots\; \wedge\; R_n$$

Procesy asynchroniczne (model przeplotowy):

$$R \;=\; R'_1 \;\vee\; R'_2 \vee \;\ldots\; \vee\; R'_n$$

$$R'_i \;=\; R_i \wedge (\textstyle\bigwedge_{j \neq i} \mathrm{Id}_j)$$

Procesy asynchroniczne (model jednoczesny):

$$R \;=\; R'_1 \;\wedge\; R'_2 \wedge \;\ldots\; \wedge\; R'_n$$

$$R'_i \;=\; R_i \vee \mathrm{Id}_i$$

Ograniczenie do stanów osiągalnych:

$$\widehat{R}(x_1, \ldots, x_m, x'_1, \ldots, x'_m) = 1$$

$$\Updownarrow$$

$$R(\gamma(x_1, \ldots, x_m), \gamma(x'_1, \ldots, x'_m)) \ \wedge$$

$$\gamma(x_1, \ldots, x_m), \gamma(x'_1, \ldots, x'_m) \text{ osiągalne}$$

III. Weryfikacja symboliczna

Punkty stałe w kracie zupełnej $\langle A, \leq \rangle$.

Niech $f : A \to A$ monotoniczna.

- najmniejszy p.s.: $\bot \leq f(\bot) \leq f^2(\bot) \leq \ldots \rightsquigarrow \mu Z.\, f(Z)$
- największy p.s.: $\top \geq f(\top) \geq f^2(\top) \geq \ldots \rightsquigarrow \nu Z.\, f(Z)$

Gdy A skończony, kres osiągamy po $\leq |A|$ krokach.

Punkty stałe w kracie zupełnej $\langle A, \leq \rangle$.

Niech $f : A \to A$ monotoniczna.

- najmniejszy p.s.: $\bot \leq f(\bot) \leq f^2(\bot) \leq \ldots \rightsquigarrow \mu Z.\, f(Z)$
- największy p.s.: $\top \geq f(\top) \geq f^2(\top) \geq \ldots \rightsquigarrow \nu Z.\, f(Z)$

Przykł ad: $A = \mathcal{P}(S)$

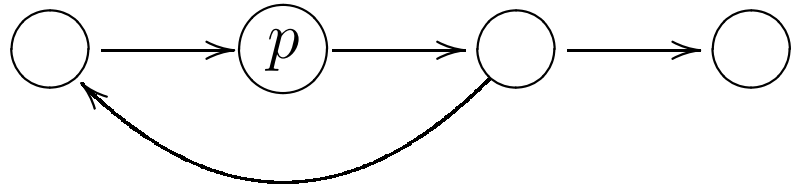
$Z \mapsto \mathsf{EX}\, Z$ $\qquad \mu Z.\, \mathsf{EX}\, Z = \bot = \emptyset \qquad$ $\nu Z.\, \mathsf{EX}\, Z =$ **?**

$Z \mapsto p \vee \mathsf{EX}\, Z$ $\qquad \mu Z.\, p \vee \mathsf{EX}\, Z =$ **?**

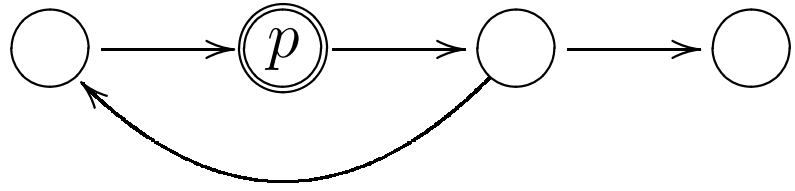
Przykład

$\mathsf{EF}\, p \;=\; \mu Z.\, p \vee \mathsf{EX}\, Z$

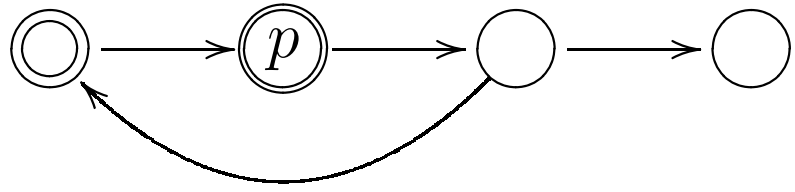
$\texttt{false}$



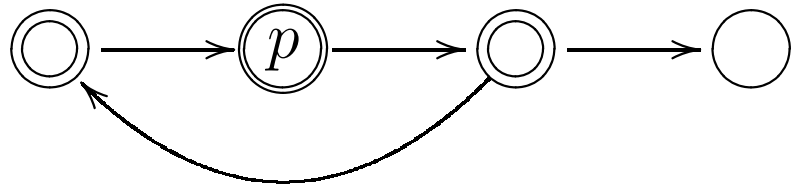
$p \vee \mathsf{EX}\, \texttt{false} \equiv p$



$p \vee \mathsf{EX}\, p$



$p \vee \mathsf{EX}\, (p \vee \mathsf{EX}\, p)$

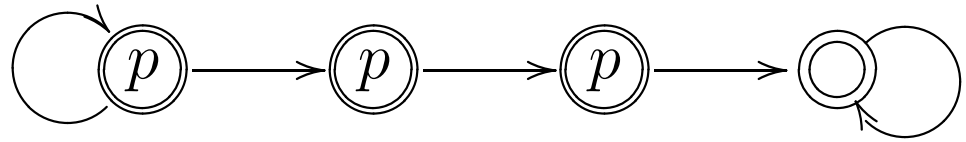


- $\mathsf{EF}\,\phi \;=\; \mu Z.\, \phi \vee \mathsf{EX}\, Z$ $\qquad Z \mapsto \phi \vee \mathsf{EX}\, Z$
- $\mathsf{AF}\,\phi \;=\; \mu Z.\, \phi \vee \mathsf{AX}\, Z$ $\qquad Z \mapsto \phi \vee \mathsf{AX}\, Z$
- $\mathsf{EG}\,\phi \;=\; \nu Z.\, \phi \wedge \mathsf{EX}\, Z$ $\qquad Z \mapsto \phi \wedge \mathsf{EX}\, Z$
- $\mathsf{AG}\,\phi \;=\; \nu Z.\, \phi \wedge \mathsf{AX}\, Z$ $\qquad Z \mapsto \phi \wedge \mathsf{AX}\, Z$
- $\mathsf{E}\,\phi\,\mathsf{U}\,\psi \;=\; \mu Z.\, \psi \vee \phi \wedge \mathsf{EX}\, Z$ $\qquad Z \mapsto \psi \vee (\phi \wedge \mathsf{EX}\, Z)$
- $\mathsf{A}\,\phi\,\mathsf{U}\,\psi \;=\; \mu Z.\, \psi \vee \phi \wedge \mathsf{AX}\, Z$ $\qquad Z \mapsto \psi \vee (\phi \wedge \mathsf{AX}\, Z)$
- ...

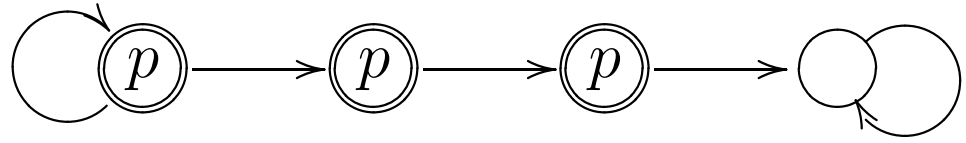
Przykład

$\mathsf{EG}\, p \;=\; \nu Z.\, \phi \wedge \mathsf{EX}\, Z$

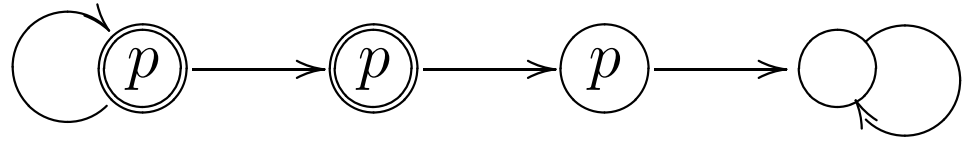
$\texttt{true}$



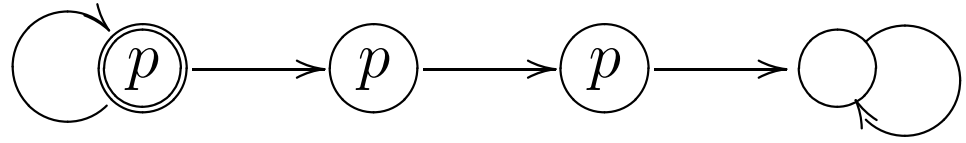
$p \wedge \mathsf{EX}\, \texttt{true} \equiv p$



$p \wedge \mathsf{EX}\, p$



$p \wedge \mathsf{EX}\, (p \wedge \mathsf{EX}\, p)$



CTL $(\neg, \wedge,$ **EX**, **E_U_**, **EG**$)$ (wystarczą te spójniki)

$$\mathrm{Check} : \mathrm{CTL} \mapsto \mathrm{OBDD}$$

$\mathrm{Check}(\phi)$ reprezentuje $\{s \mid s \vDash \phi\}$

Weryfikacja symboliczna (EX _)

$\mathrm{Check} : \mathsf{CTL} \to \mathsf{OBDD}$

$\mathrm{Check}(\phi)$ reprezentuje $\{s \mid s \vDash \phi\}$

$\mathrm{Check}(\mathsf{EX}\,\phi) \quad := \quad \exists \vec{x}'.\ \widehat{R}(\vec{x}, \vec{x}') \wedge f(\vec{x}') \qquad$ gdzie $\quad f = \mathrm{Check}(\phi)$

$\mathrm{Check}(\mathsf{EX}\,\phi) \quad := \quad \mathsf{EX}\, f$

- $\mathsf{EX}\,\phi$
- $\mathsf{EX}\, Z$
- $\mathsf{EX}\, f$

Weryfikacja symboliczna (E _ U _)

$\mathrm{Check} : \mathsf{CTL} \to \mathsf{OBDD}$

$\mathrm{Check}(\phi)$ reprezentuje $\{s \mid s \models \phi\}$

$\mathrm{Check}(\mathsf{E}\,\phi\,\mathsf{U}\,\psi) \;:=\; \mu Z.\; g \vee (f \wedge \mathsf{EX}\, Z)$ gdzie $f = \mathrm{Check}(\phi)$, $g = \mathrm{Check}(\psi)$

$$Z \mapsto g \vee (f \wedge \exists \vec{x}'.\; \widehat{R}(\vec{x}, \vec{x}') \wedge Z[\vec{x}'/\vec{x}])$$

$\mathtt{false}$

$g \vee (f \wedge \mathsf{EX}\,\mathtt{false}) \equiv g$

$g \vee (f \wedge \mathsf{EX}\,(g \vee (f \wedge \mathsf{EX}\,\mathtt{false}))) \equiv g \vee (f \wedge \mathsf{EX}\, g)$

$\ldots \equiv g \vee (f \wedge \mathsf{EX}\,(g \vee (f \wedge \mathsf{EX}\, g$

$\downarrow$

$\mu Z.\; g \vee (f \wedge \mathsf{EX}\, Z)$

Weryfikacja symboliczna (EG _)

$\mathrm{Check} : \mathsf{CTL} \to \mathsf{OBDD}$

$\mathrm{Check}(\phi)$ reprezentuje $\{s \mid s \vDash \phi\}$

$\mathrm{Check}(\mathsf{EG}\,\phi) \quad := \quad \nu Z.\ f \wedge \mathsf{EX}\, Z \qquad \text{gdzie} \quad f = \mathrm{Check}(\phi)$

$$Z \mapsto f \wedge \exists \vec{x}'.\ \widehat{R}(\vec{x}, \vec{x}') \wedge Z[\vec{x}'/\vec{x}]$$

EX ϕ	E ϕ U ψ	EG ϕ
EX Z	E Z U Z'	EG Z
EX f	E f U g	EG f