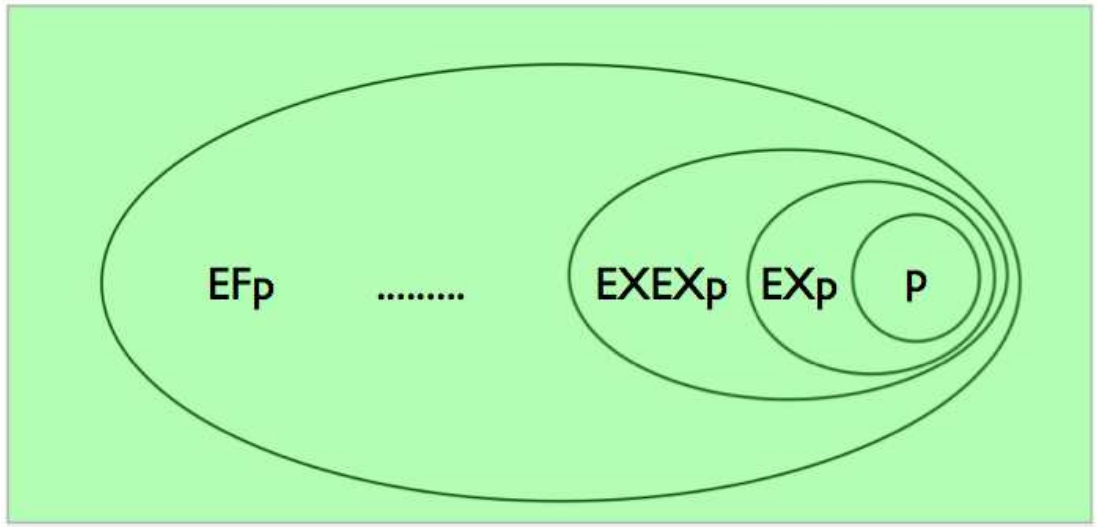
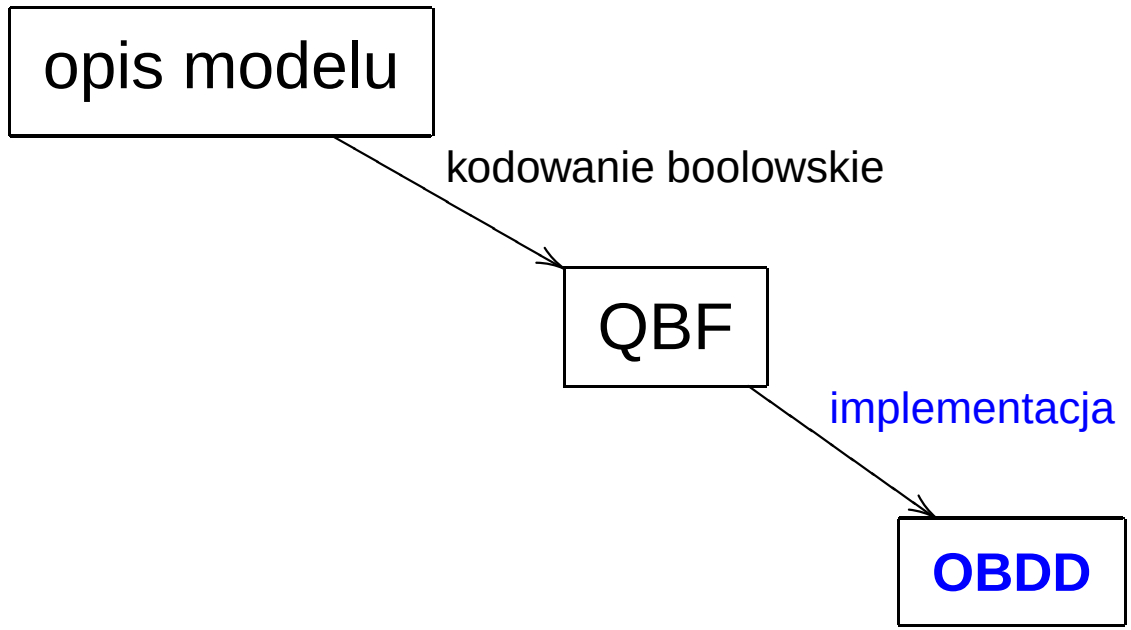
Weryfikacja wspomagana komputerowo

Wykład 6: Weryfikacja symboliczna I

Idea: EF p



Symboliczna weryfikacja modelowa

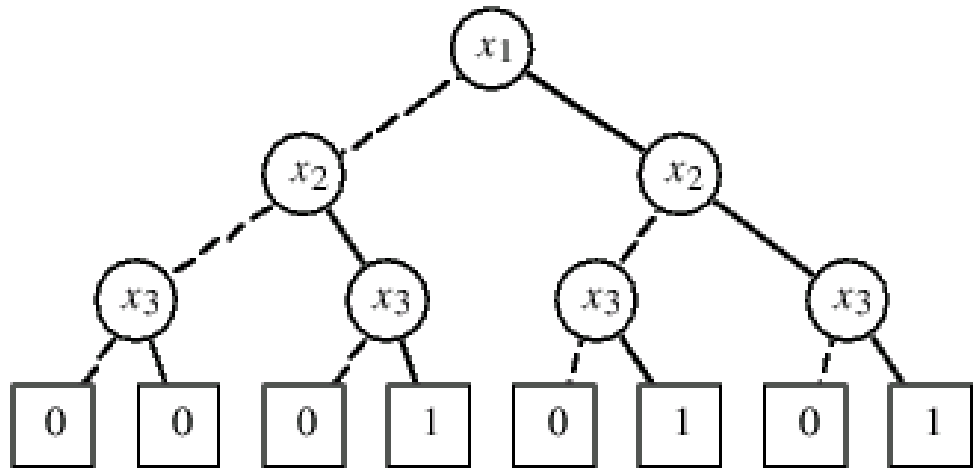


weryfikacja modelowa = operacje na OBDDs

I. OBDD

ang. *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



[Bryant 1992]

– $f : \{0,1\}^3 \rightarrow \{0,1\}$

– 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

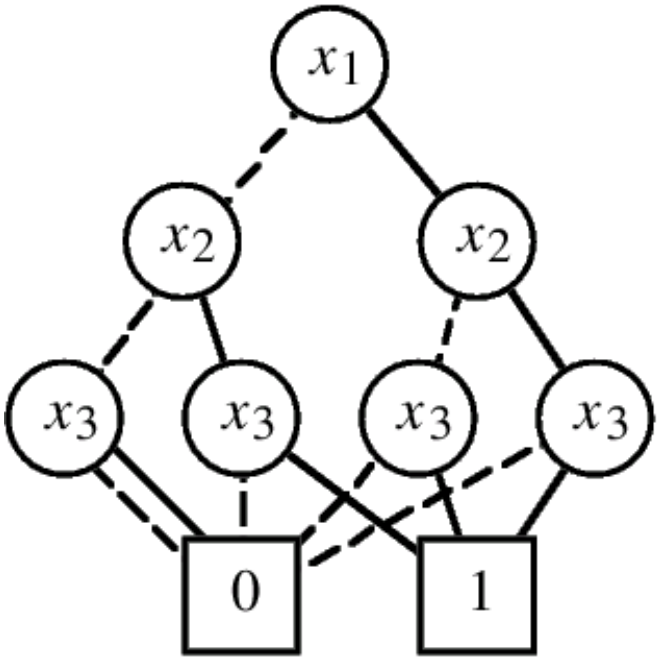
Kolejność zmiennych musi być przestrzegana na każdej ścieżce.

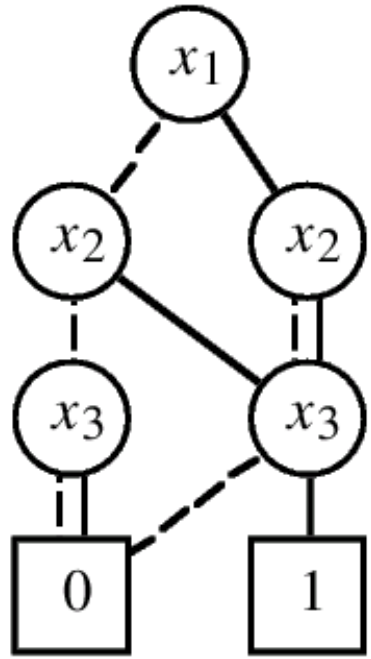
Upraszczanie OBDD

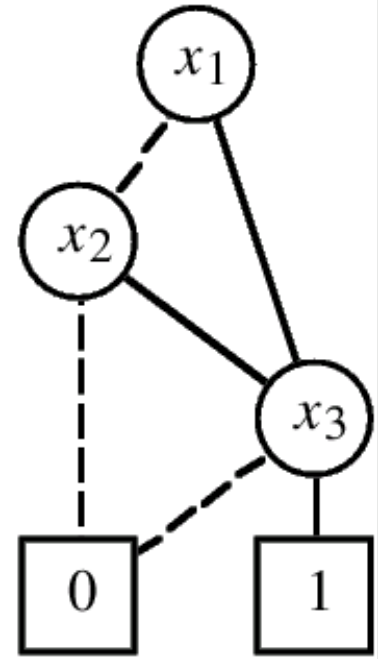
– usuń nadmiarowe wierzchołki końcowe

– usuń nadmiarowe wierzchołki niekońcowe

– usuń nadmiarowe testy







[Bryant 1992]

Postać kanoniczna dla funkcji boolowskiej:

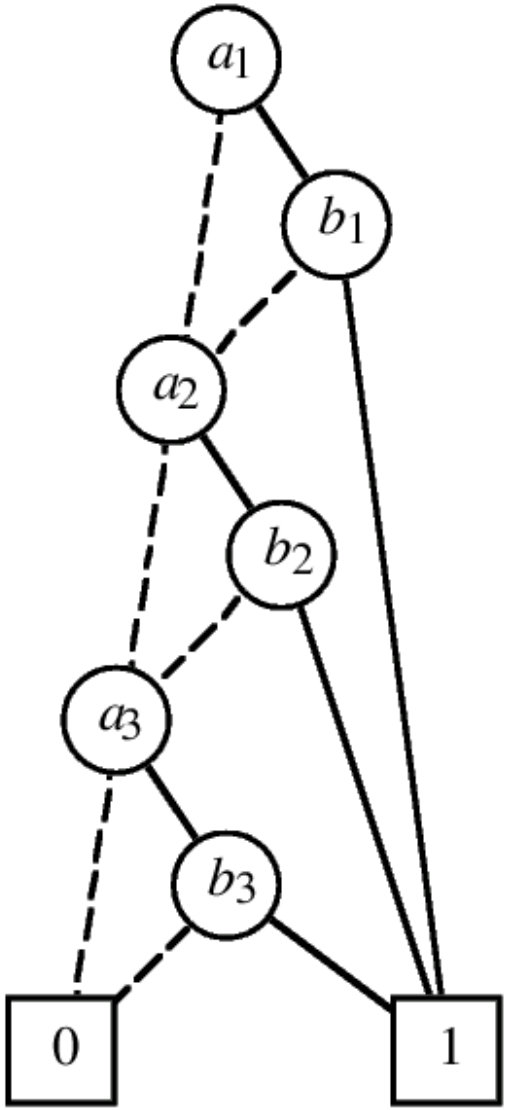
- niezależna od grafu wyjściowego
- (silnie) zależna od kolejności zmiennych

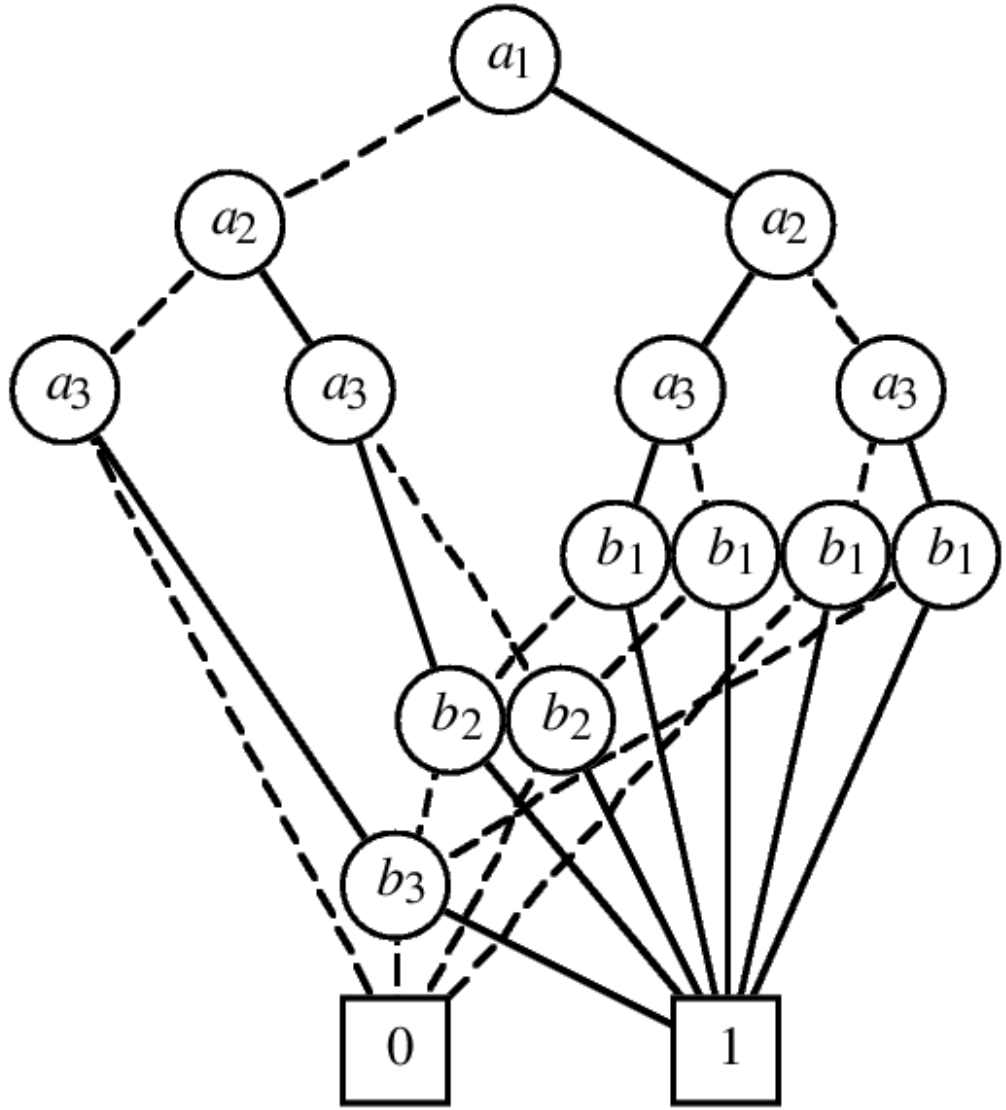
Naiwna konstrukcja OBBD dla formuły boolowskiej ϕ:

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

Znalezienie właściwej kolejności zmiennych jest kluczowe!

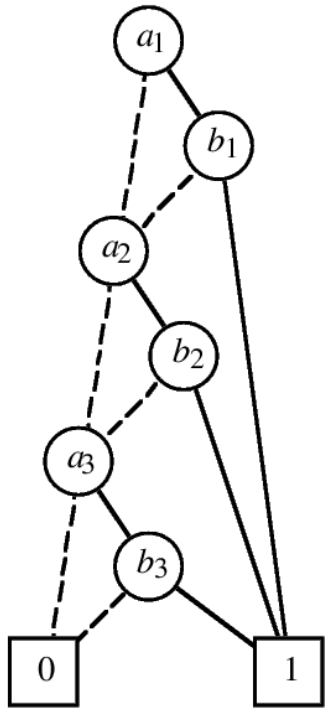
$$a_1 \wedge b_1 \ \vee \ a_2 \wedge b_2 \ \vee \ a_3 \wedge b_3$$

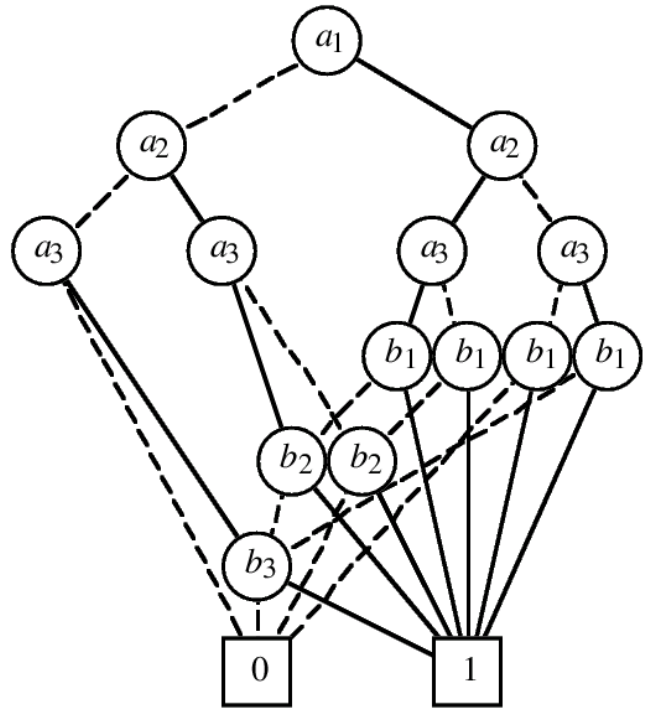




[Bryant 1992]

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





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

Rozmiar OBDD

Heurystyka: zmienne powiązane powinny być blisko

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

Wzór Shannona

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

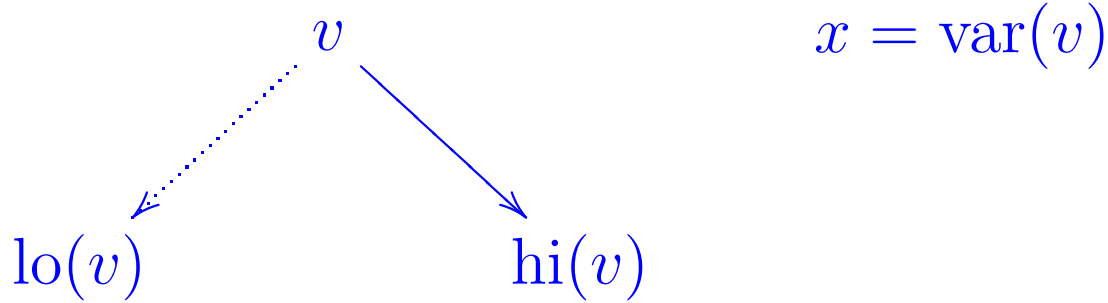
$$f\big|_{x_i \leftarrow b}(x_1, \ldots, x_n) \quad = \quad f(x_1, \ldots, x_{i-1}, b, x_{i+1}, \ldots, x_n)$$

Wzór Shannona

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

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

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



OBDD jako abstrakcyjny typ danych

kolejność zmiennych taka sama dla wszystkich OBDD

Operacje:

$f \vee g$, $f \wedge g$, $\neg f$, `false`, `true` $\qquad BF \mapsto OBDD$

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

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

$f = g$

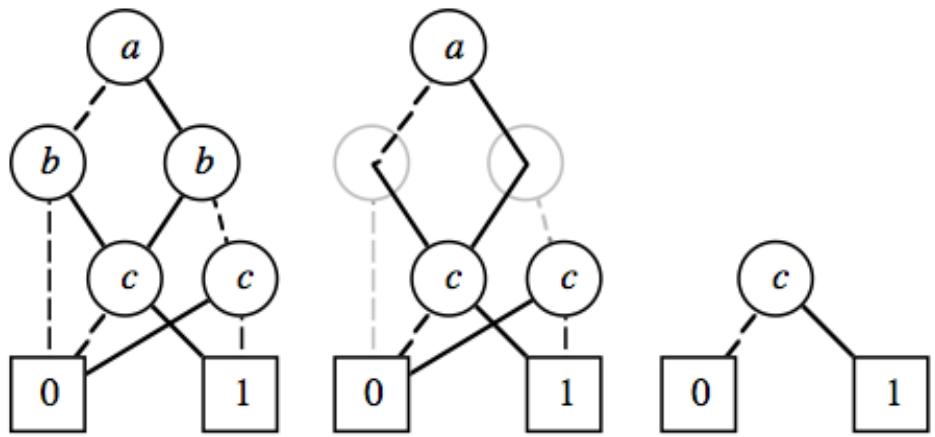
Uwaga!: operacje na **funkcjach**, nie na wartościach $\{0, 1\}$.

Implementacja operacji 1-arg.

– $f|_{x \leftarrow b}$

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

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



[Bryant 1992]

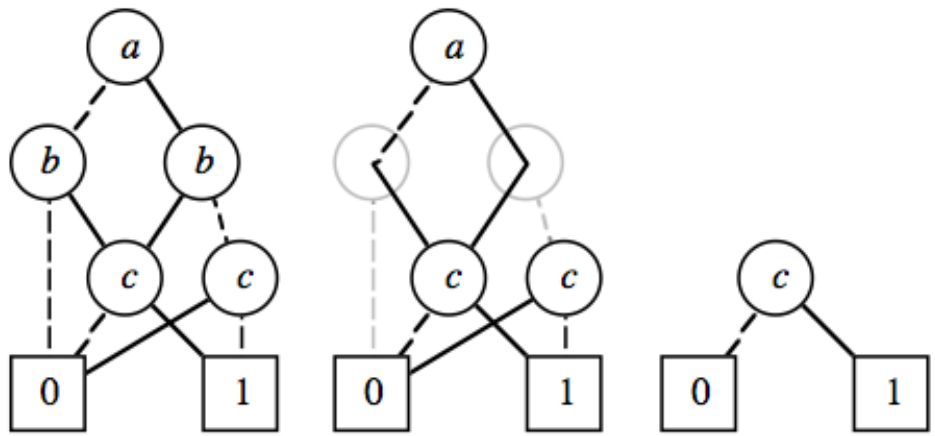
Implementacja operacji 1-arg. (cd)

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

kolejność zmiennych

pozostaje taka sama!

– $\neg f$ **?**



[Bryant 1992]

Implementacja operacji 2-arg.

kolejność zmiennych taka sama dla wszystkich OBDD

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

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

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

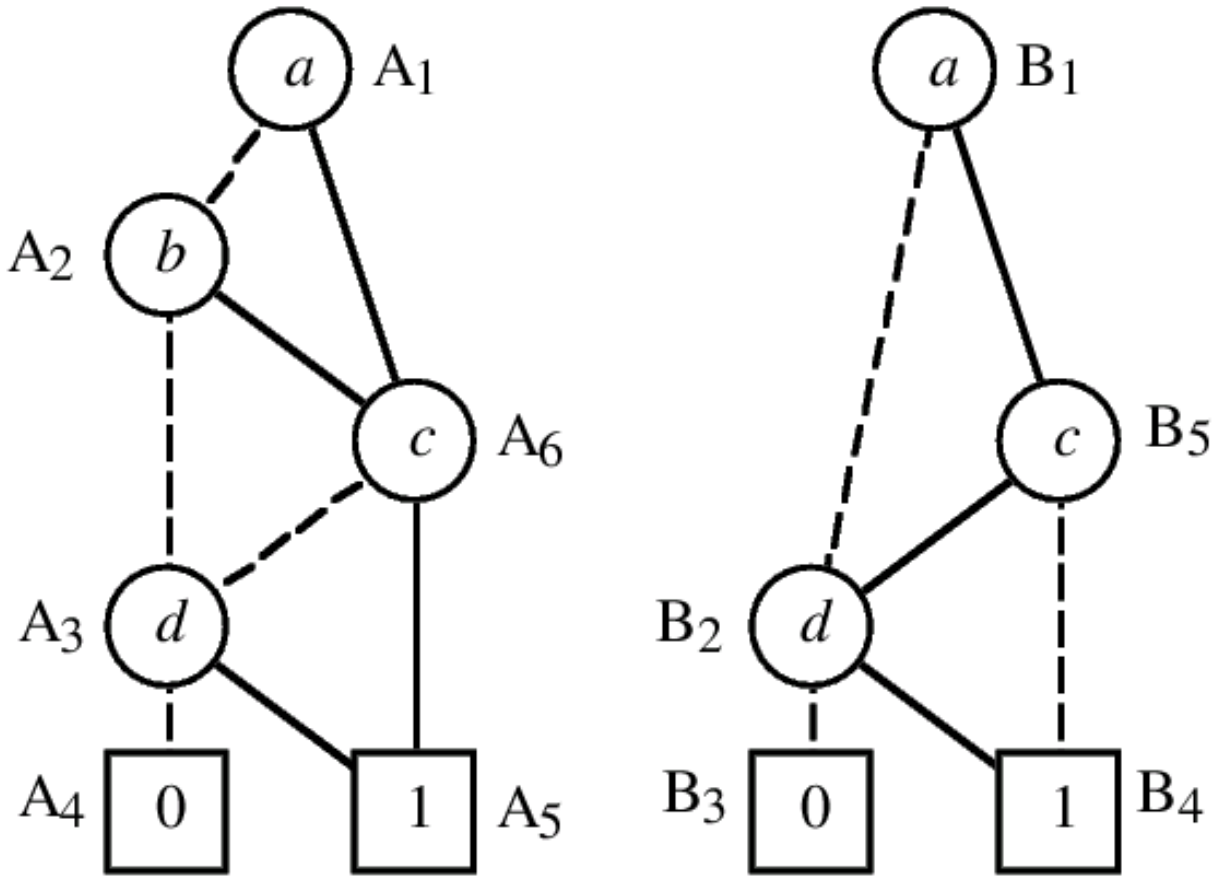
$$\mathrm{lo}(f \bullet g) = \mathrm{lo}(f) \bullet \mathrm{lo}(g) \qquad \mathrm{hi}(f \bullet g) = \mathrm{hi}(f) \bullet \mathrm{hi}(g)$$

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

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

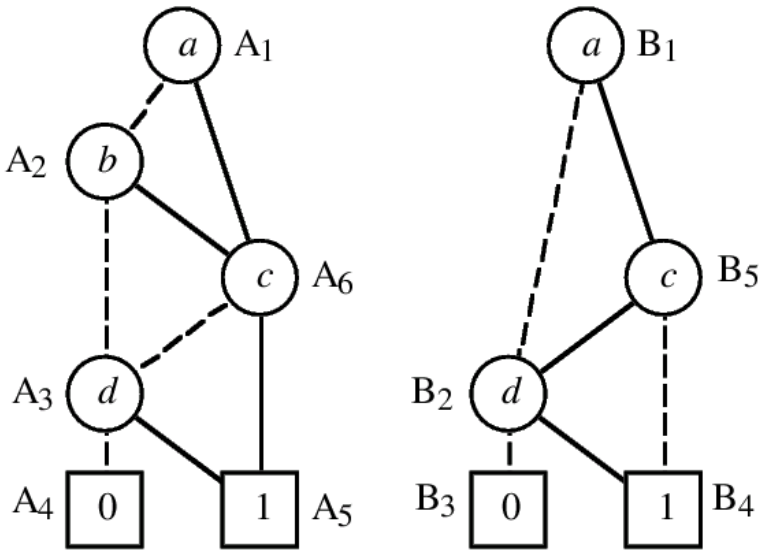
$$f \bullet g = \neg x \wedge (f \bullet g)|_{x \leftarrow 0} \quad \vee \quad x \wedge (f \bullet g)|_{x \leftarrow 1}$$
$$f \bullet g = \neg x \wedge (f|_{x \leftarrow 0} \bullet g|_{x \leftarrow 0}) \quad \vee \quad x \wedge (f|_{x \leftarrow 1} \bullet g|_{x \leftarrow 1})$$

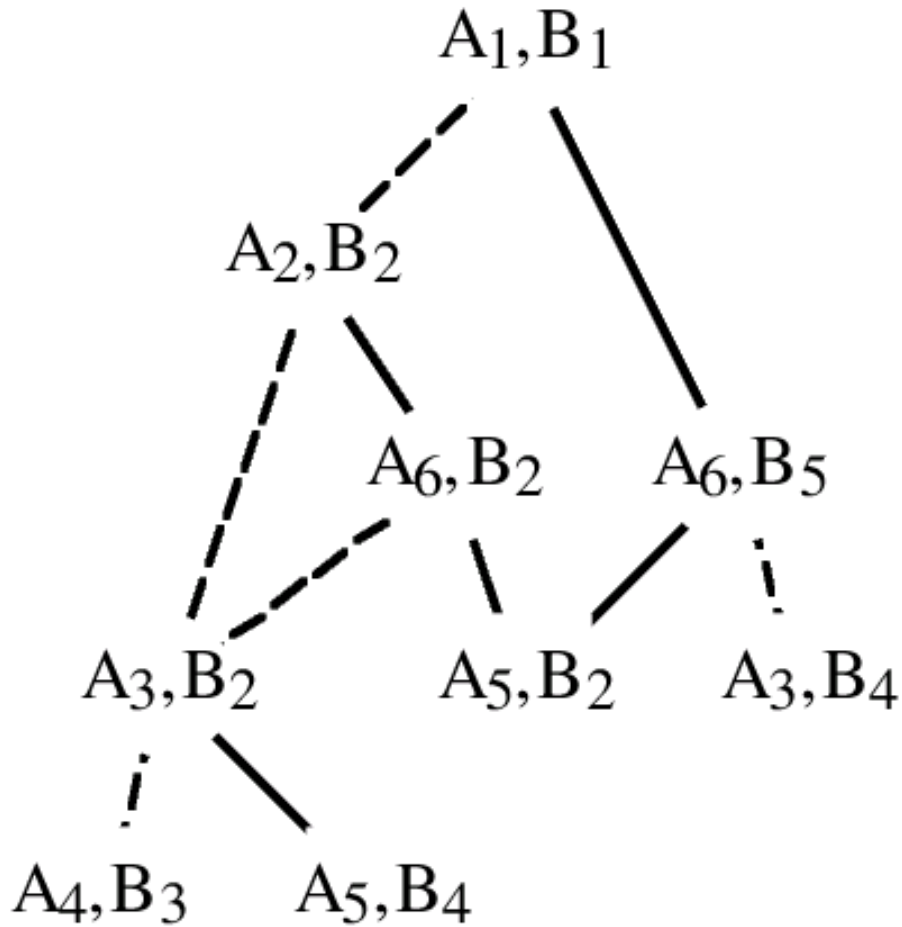
Przykład: dane wyjściowe



[Bryant 1992]

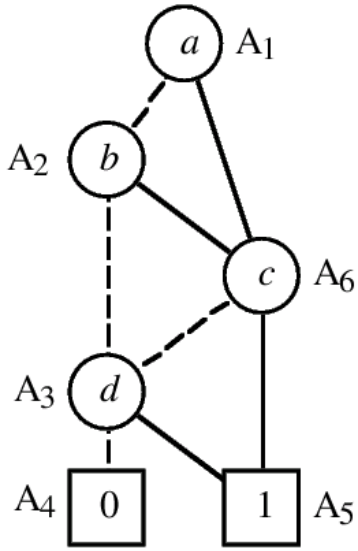
Przykład: wywołania rekurencyjne



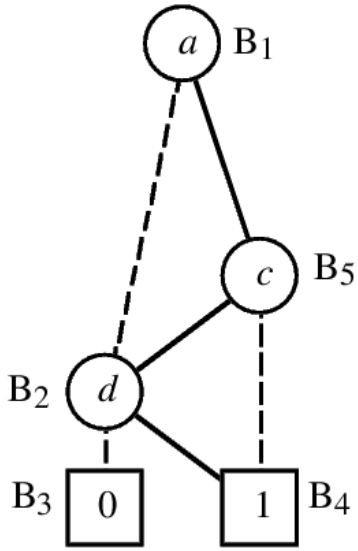


[Bryant 1992]

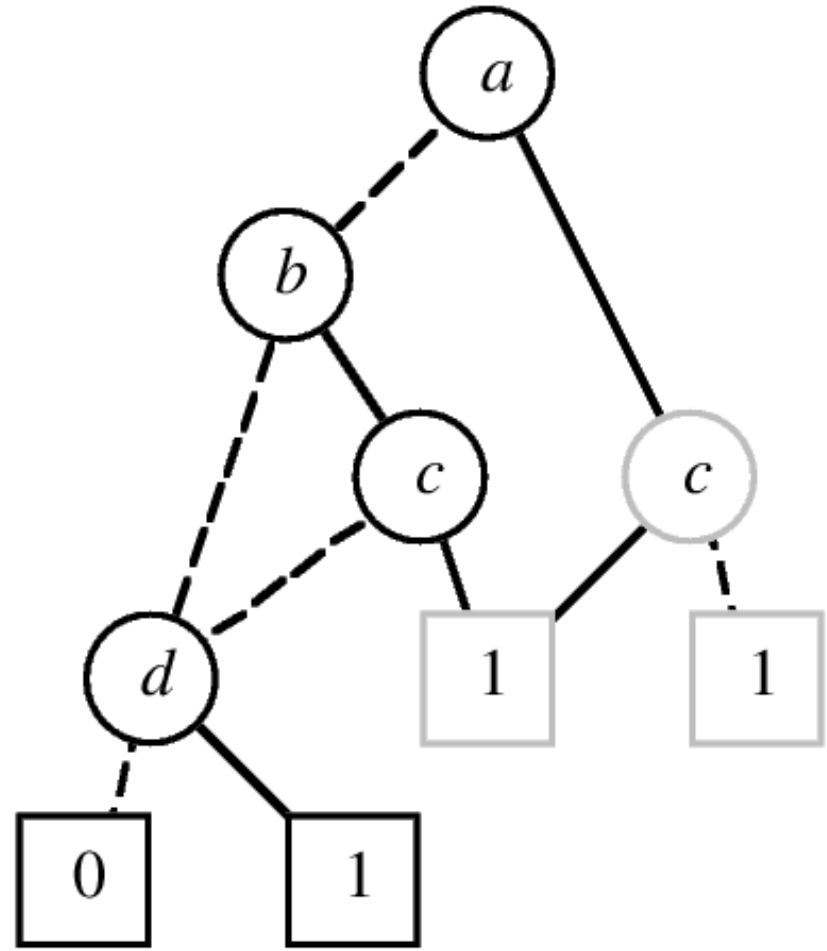
Przykład: wynik = $a \vee b \wedge c \vee d$



$(a \vee b) \wedge c \vee d$

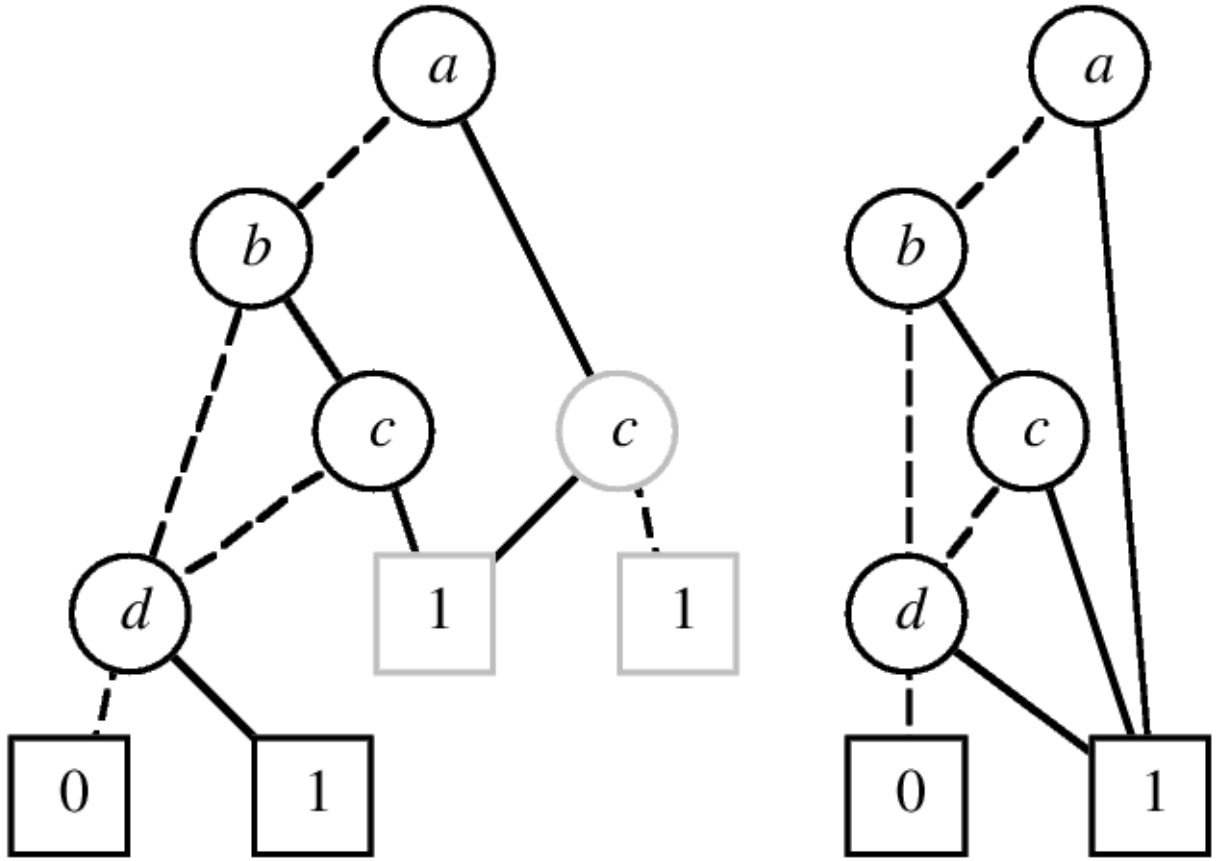


$a \wedge \neg c \vee d$



[Bryant 1992]

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



[Bryant 1992]

Implementacja operacji 2-arg.

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

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

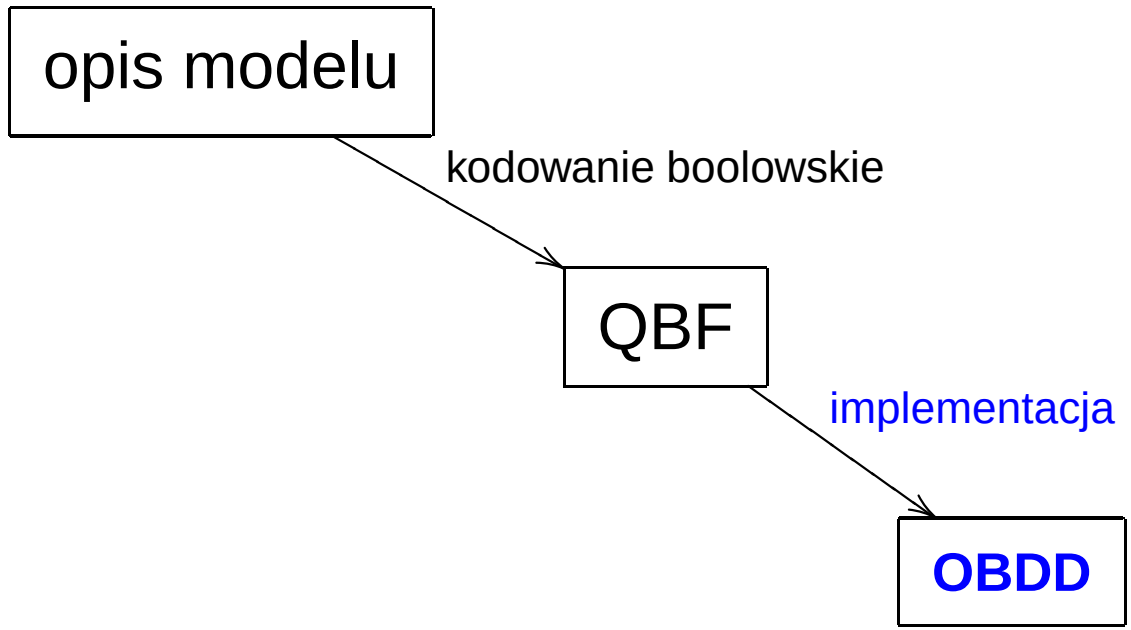
Pytanie: $f \iff g$ **?** $\qquad\qquad$ $f = g$ **?**

Odmiany

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

II. Kodowanie boolowskie

Kodowanie boolowskie



weryfikacja modelowa = operacje na OBDDs

Opis modelu

– S opisany przez m zmiennych $\{0,1\}$-owych: $S \equiv \{0,1\}^m$

– relacja przejścia $R : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$

$$R(x_1, \ldots, x_m, x'_1, \ldots, x'_m) \in \{0,1\}$$

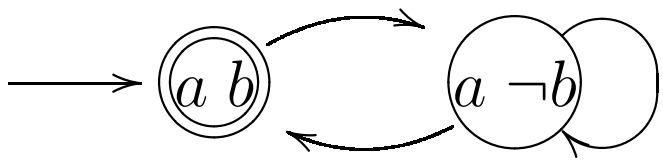
– stany początkowe $S_0 : \{0,1\}^m \to \{0,1\}$

$$S_0(x_1, \ldots, x_m) \in \{0,1\}$$

– własności atomowe $L_p = \{s \mid p \in L(s)\} : \{0,1\}^m \to \{0,1\}$

$$L_p(x_1, \ldots, x_m) \in \{0,1\}$$

Przykład

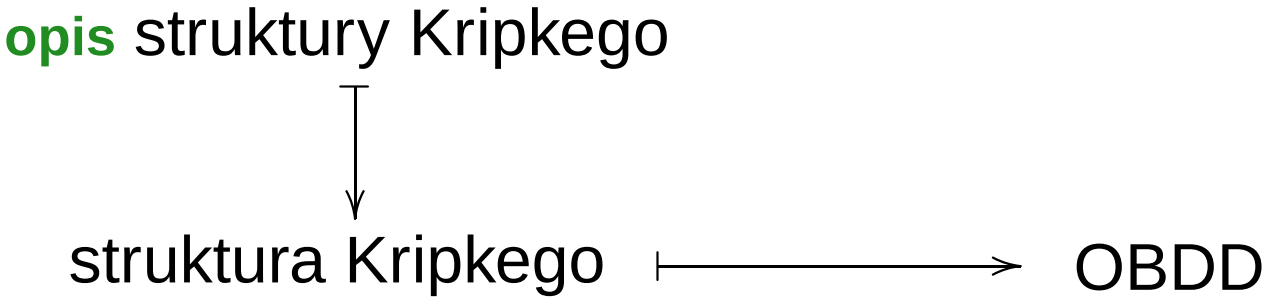


(stany osiągalne)

$$
\begin{aligned}
R &= (a \wedge b \wedge a' \wedge \neg b') \vee (a \wedge \neg b \wedge a' \wedge \neg b') \vee (a \wedge \neg b \wedge a' \wedge b') \\
S_0 &= a \wedge b \\
L_p &= b
\end{aligned}
$$

Od modelu do OBDD

ŹLE!



Od modelu do OBDD

opis struktury Kripkego

struktura Kripkego $\longmapsto$ OBDD

ŹLE!

opis struktury Kripkego $\longmapsto$ OBDD

DOBRZE!

Kompozycjonalny opis modelu

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

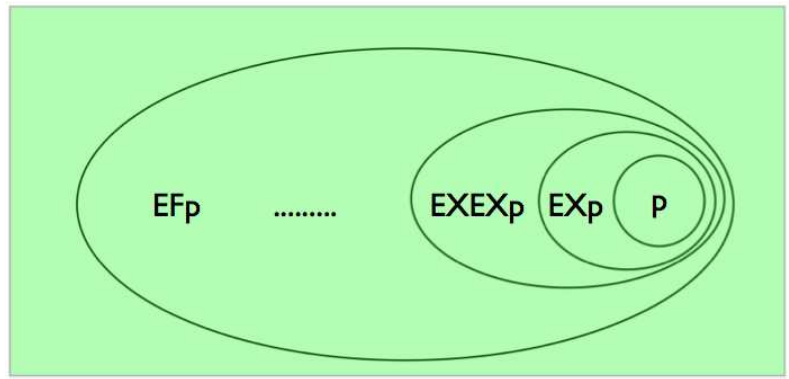
$$\widehat{R}(x_1, \ldots, x_m, x'_1, \ldots, x'_m) = 1$$

$$\Updownarrow$$

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

$(x_1, \ldots, x_m), (x'_1, \ldots, x'_m)$ osiągalne

III. Weryfikacja symboliczna



Przypomnienie

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.: $\top \geq f(\top) \geq f^2(\top) \geq \ldots \rightsquigarrow \nu Z.\, f(Z)$

Przykład: $\langle A, \leq \rangle = \langle \mathcal{P}(S), \subseteq \rangle$

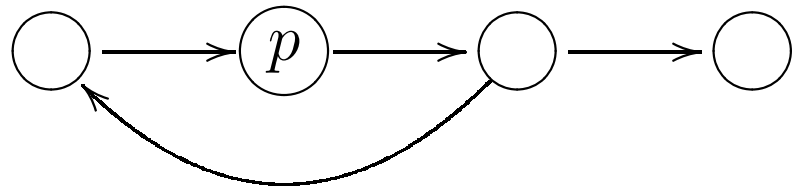
$Z \mapsto \mathsf{EX}\, Z$ $\qquad \mu Z.\, \mathsf{EX}\, Z = \bot = \emptyset \qquad \nu Z.\, \mathsf{EX}\, Z =$ **?**

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

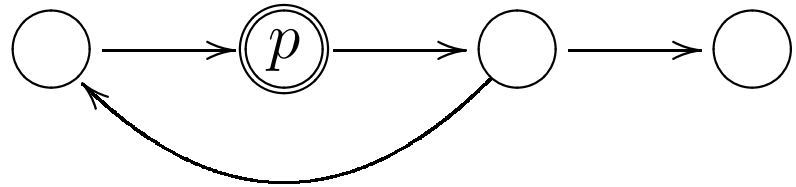
Przykład

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

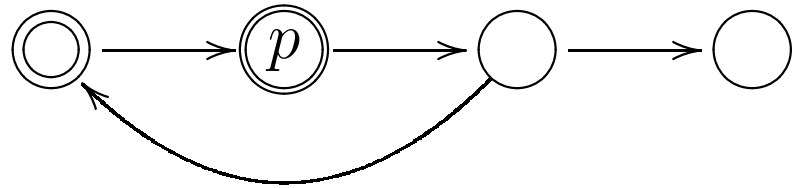
$\mathtt{false}$



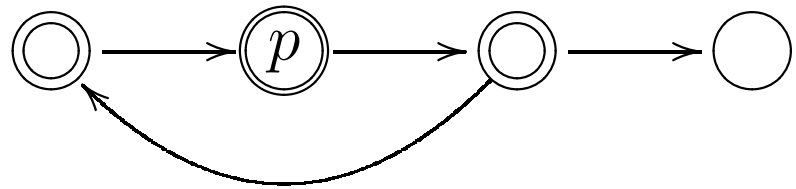
$p \vee \mathsf{EX}\, \mathtt{false} \equiv p$



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



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



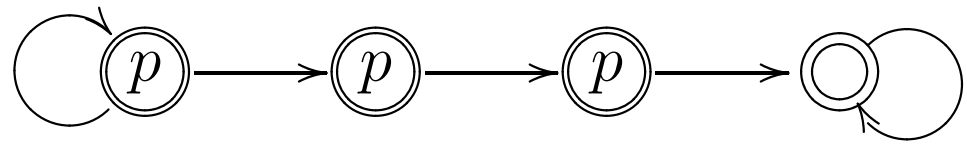
CTL stałopunktowo

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

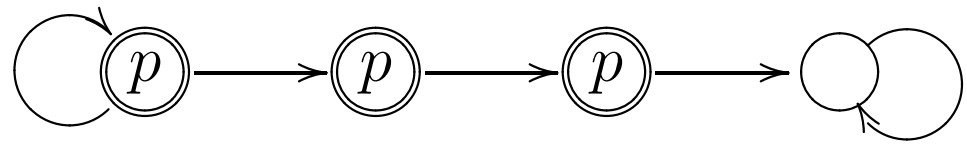
Przykład

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

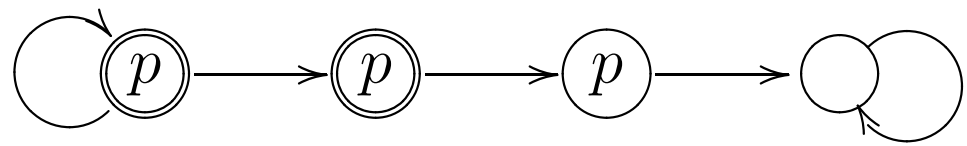
$\mathtt{true}$



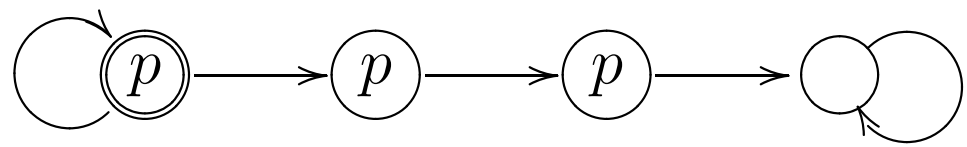
$p \wedge \mathsf{EX}\, \mathtt{true} \equiv p$



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



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



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

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

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

Przykład: $\mathrm{Check}(p)$ reprezentuje L_p

Weryfikacja symboliczna (EX _)

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

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

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

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

$\mathsf{EX}\,\phi$

$\mathsf{EX}\,Z$

$\mathsf{EX}\,f$

Kolejność zmiennych

$$\exists \vec{x}'.\ R(\vec{x}, \vec{x}') \wedge f(\vec{x}')$$

$$\vec{x} = x_1, x_2, \ldots, x_m$$

$$x_1 < x'_1 < x_2 < x'_2 < \ldots < x_m < x'_m$$

Weryfikacja symboliczna (E _ U _)

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

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

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

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

$$\begin{array}{lcl}
\texttt{false} & & \\
g \vee (f \wedge \mathsf{EX}\,\texttt{false}) & \equiv & g \\
g \vee (f \wedge \mathsf{EX}\,(g \vee (f \wedge \mathsf{EX}\,\texttt{false}))) & \equiv & g \vee (f \wedge \mathsf{EX}\, g) \\
\ldots & \equiv & g \vee (f \wedge \mathsf{EX}\,(g \vee (f \wedge \mathsf{EX}\, g)
\end{array}$$

$\downarrow$

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

Weryfikacja symboliczna (EG _)

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

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

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

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

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