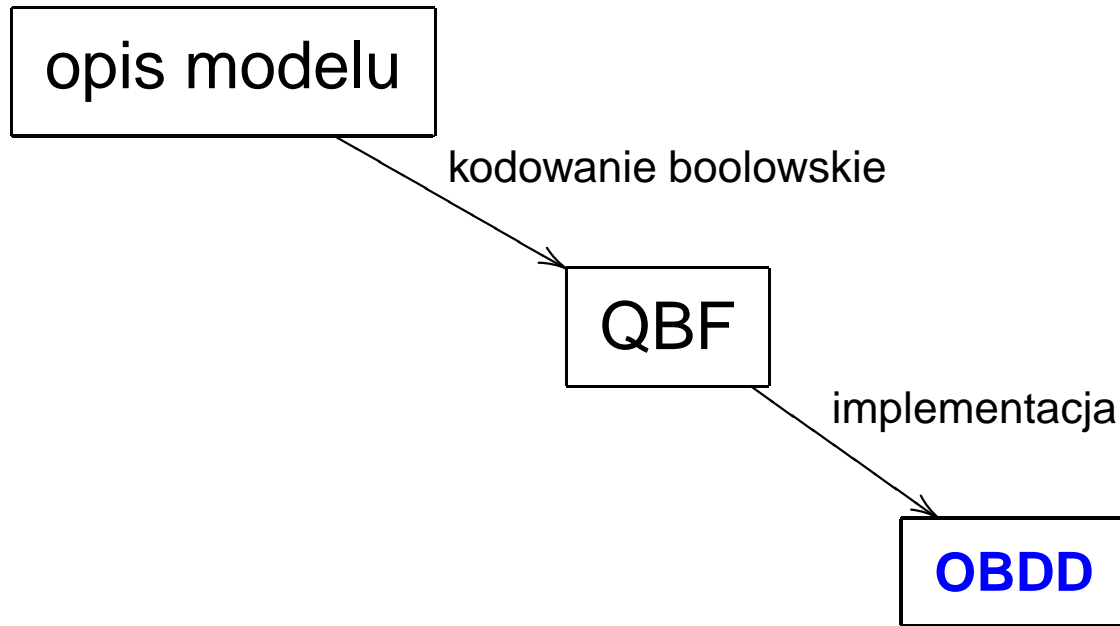


Praktyczne metody weryfikacji

Wykład 7: Weryfikacja symboliczna (I)

Symboliczna weryfikacja modelowa

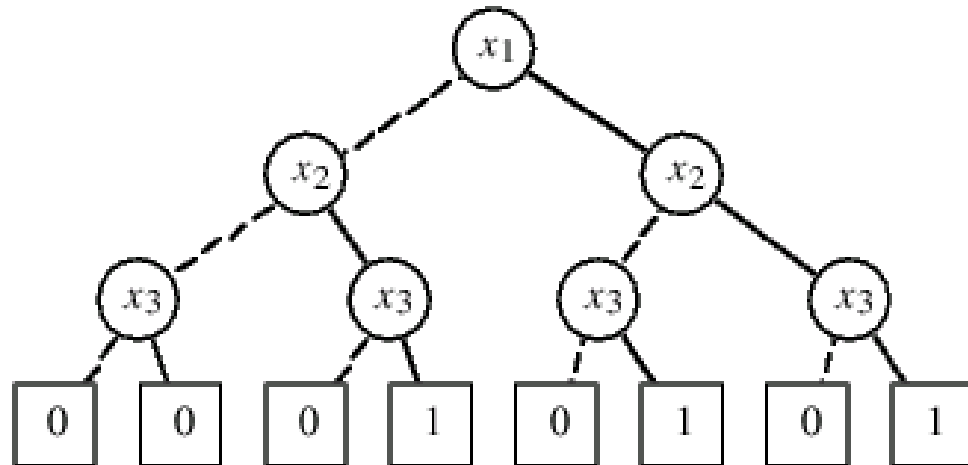


weryfikacja modelowa = operacje na OBDDs

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



[Bryant 1992]

- $f : \{0, 1\}^3 \rightarrow \{0, 1\}$
- ustalona kolejność zmiennych: $x_1 < x_2 < x_3$

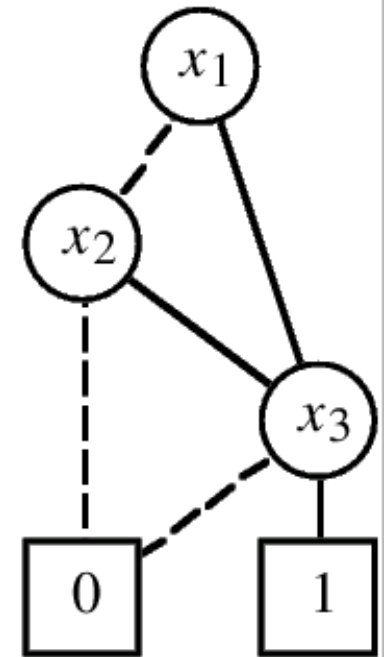
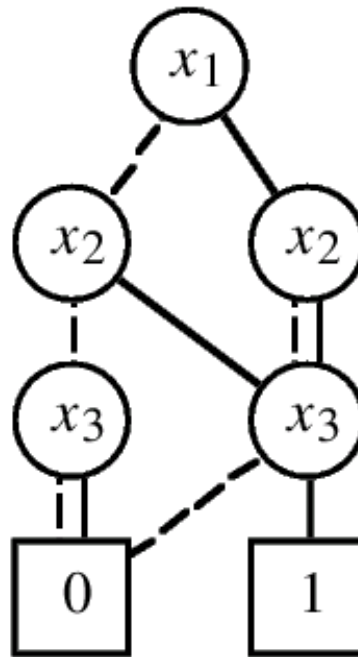
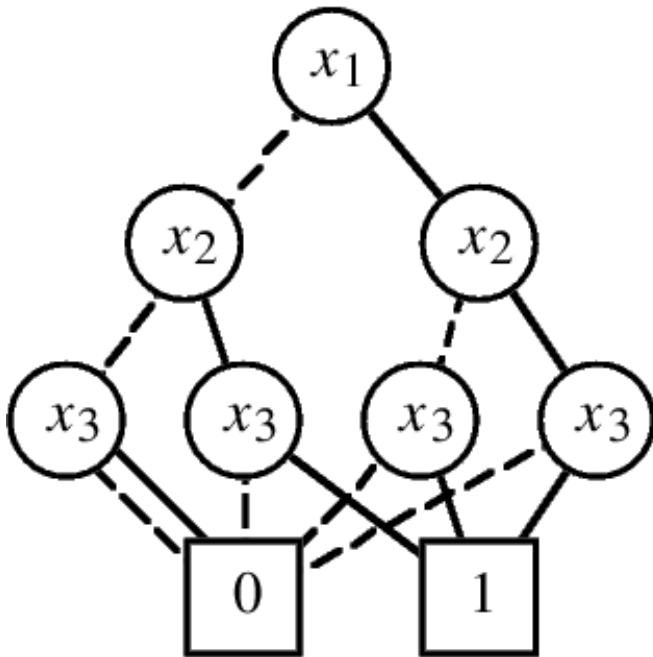
OBDD = ukorzeniony graf acykliczny

Atrybuty wierzchołka v :

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

Kolejność zmiennych musi być przestrzegana na każdej ścieżce.

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



[Bryant 1992]

Postać kanoniczna dla funkcji boolowskiej f :

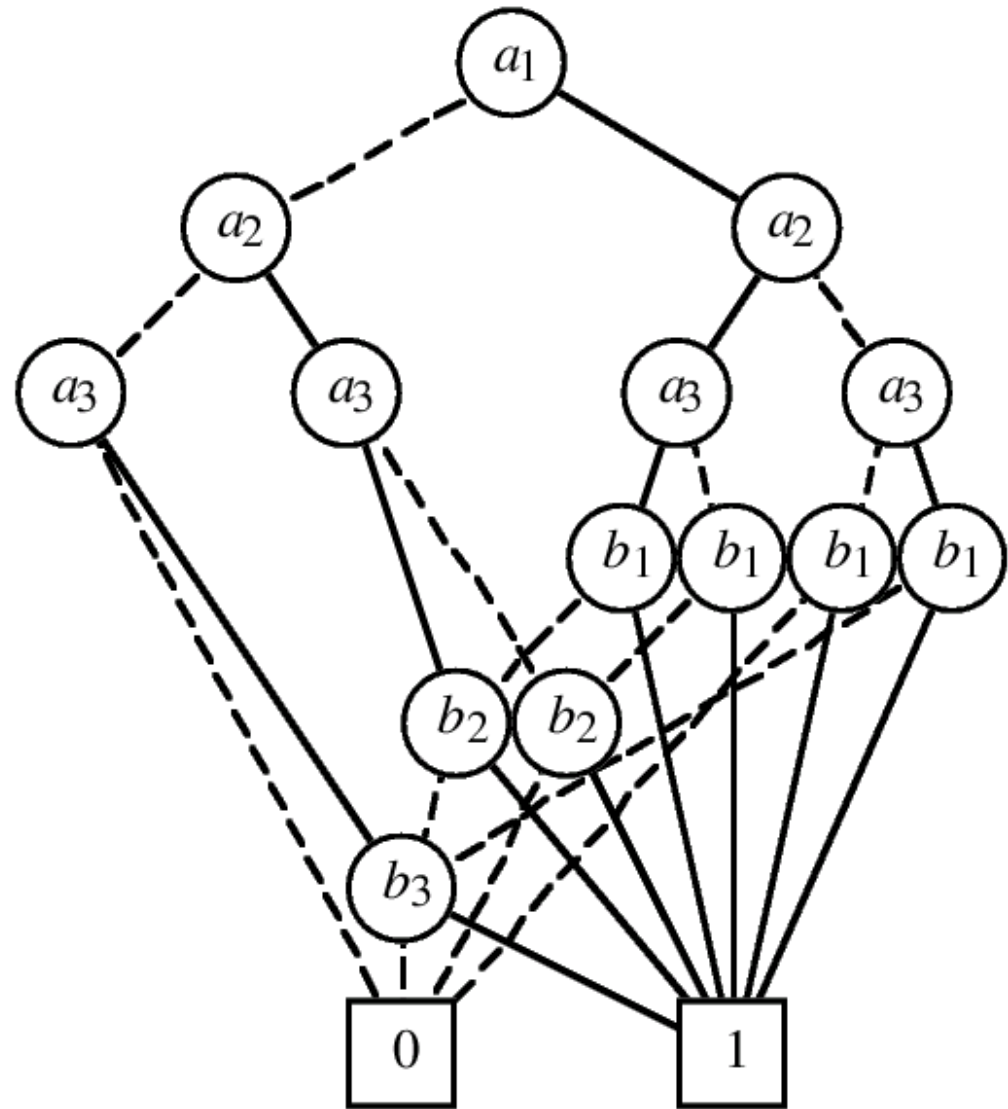
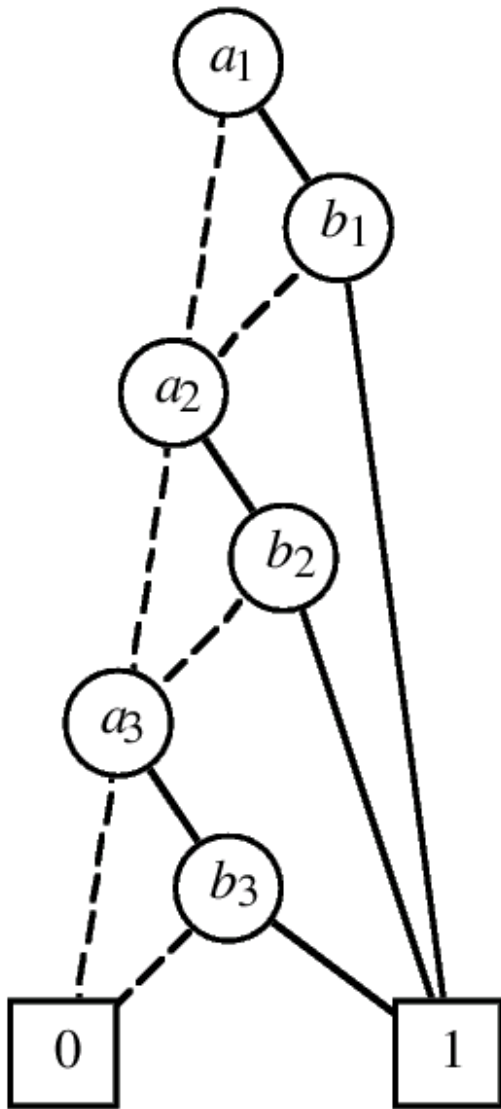
- niezależna od grafu wyjściowego
- (**silnie**) zależna od kolejności zmiennych

Naiwna konstrukcja OBDD dla formuły boolowskiej ϕ :

$\phi \longmapsto$ drzewo \longmapsto kanoniczny OBDD

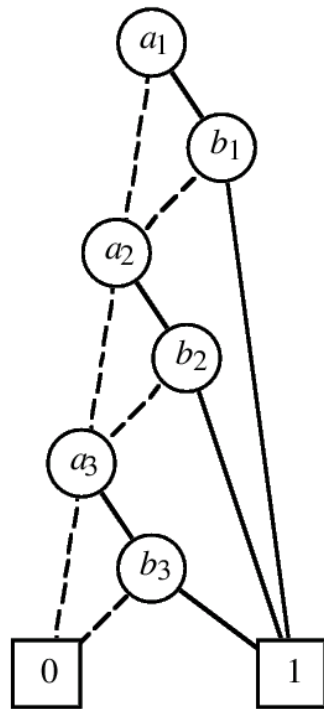
Znalezienie właściwej kolejności zmiennych jest **kluczowe!**

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

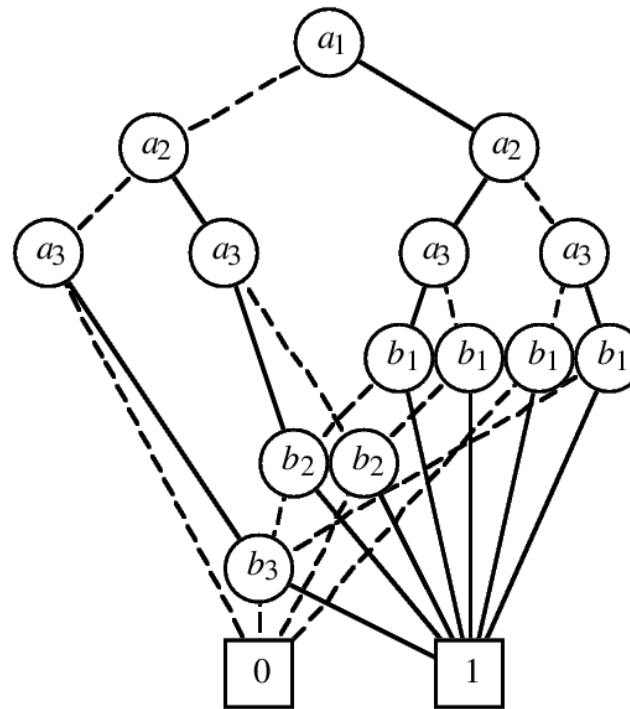


[Bryant 1992]

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



$$2 \cdot n$$



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

Heurystyka: zmienne powiązane powinny być blisko

przykład 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

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

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

Wzór Shannona

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

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

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

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

Abstrakcyjny typ danych **funkcje boolowskie**

Operacje:

$f \vee g, f \wedge g, \neg f, \text{false}, \text{true}$

$BF \mapsto OBDD$

$f = g$

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

$\exists x. f, \forall x. f$

$QBF \mapsto OBDD$

...

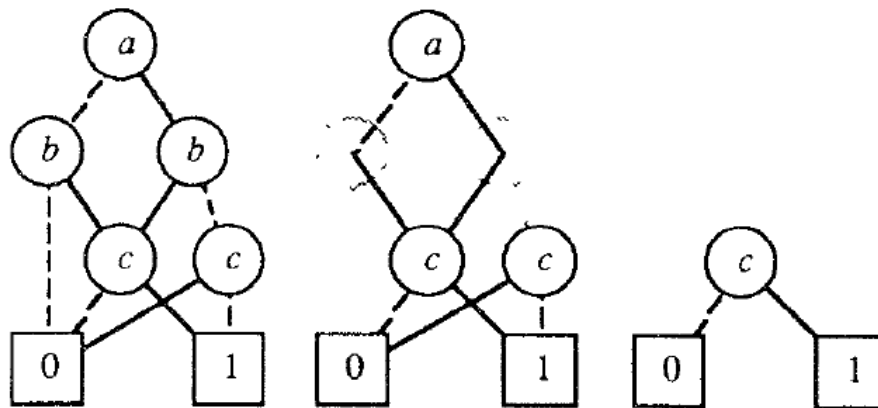
Uwaga!: operacje na **funkcjach**, nie na wartościach $\{0, 1\}$.

Implementacja operacji 1-arg.

– $f|_{x \leftarrow b}$

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

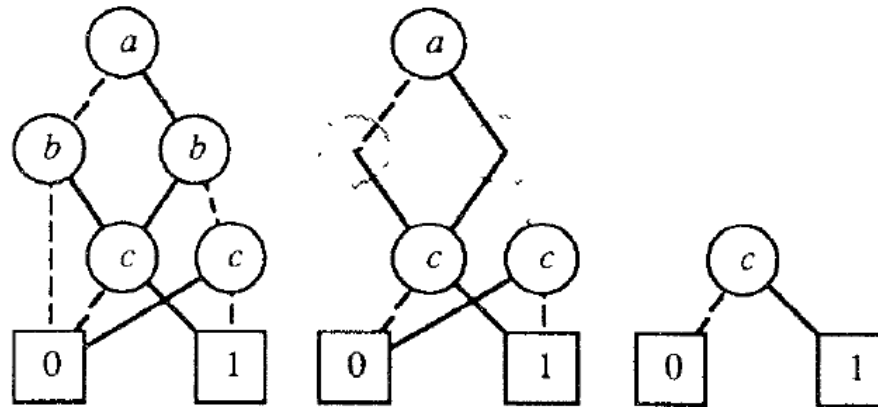
$$\text{OBDD dla } f|_{x \leftarrow b} = \begin{cases} r & x < \text{var}(r) \\ \text{lo}(r) & x = \text{var}(r), b = 0 \\ \text{hi}(r) & x = \text{var}(r), b = 1 \end{cases}$$



[Bryant 1992]

Implementacja operacji 1-arg. (cd)

- $\exists x. f = f|_{x \leftarrow 0} \vee f|_{x \leftarrow 1}$
- $\neg f$?



[Bryant 1992]

Implementacja operacji 2-arg.

• : $\{0, 1\}^2 \rightarrow \{0, 1\}$

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

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

– f, g końcowe: $\text{val}(f \bullet g) = \text{val}(f) \bullet \text{val}(g)$

– f końcowe, g nie: $f \bullet g = \text{op}(g)$

– $\text{var}(f) = \text{var}(g) = x$:

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

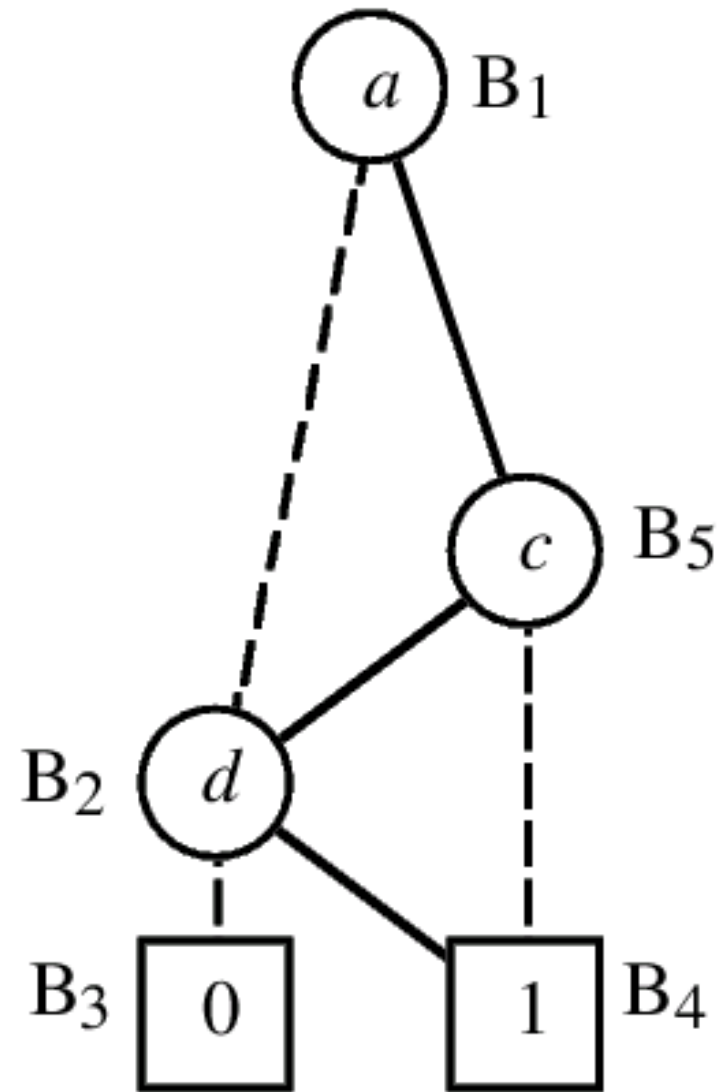
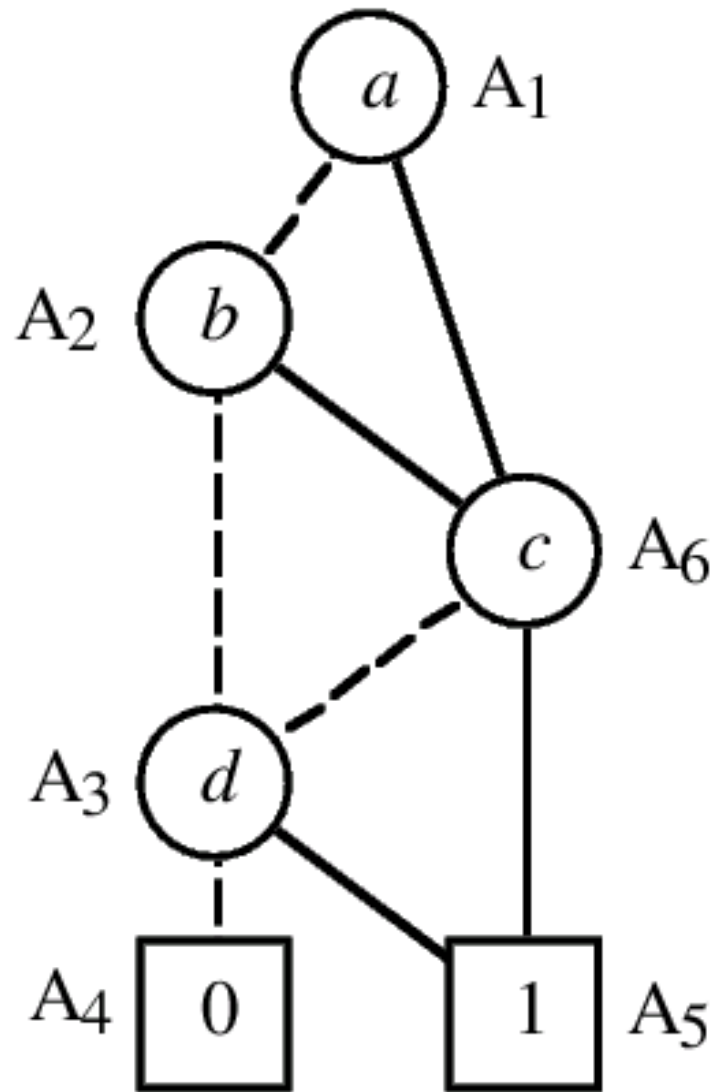
– $\text{var}(f) = x < y = \text{var}(g)$:

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

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

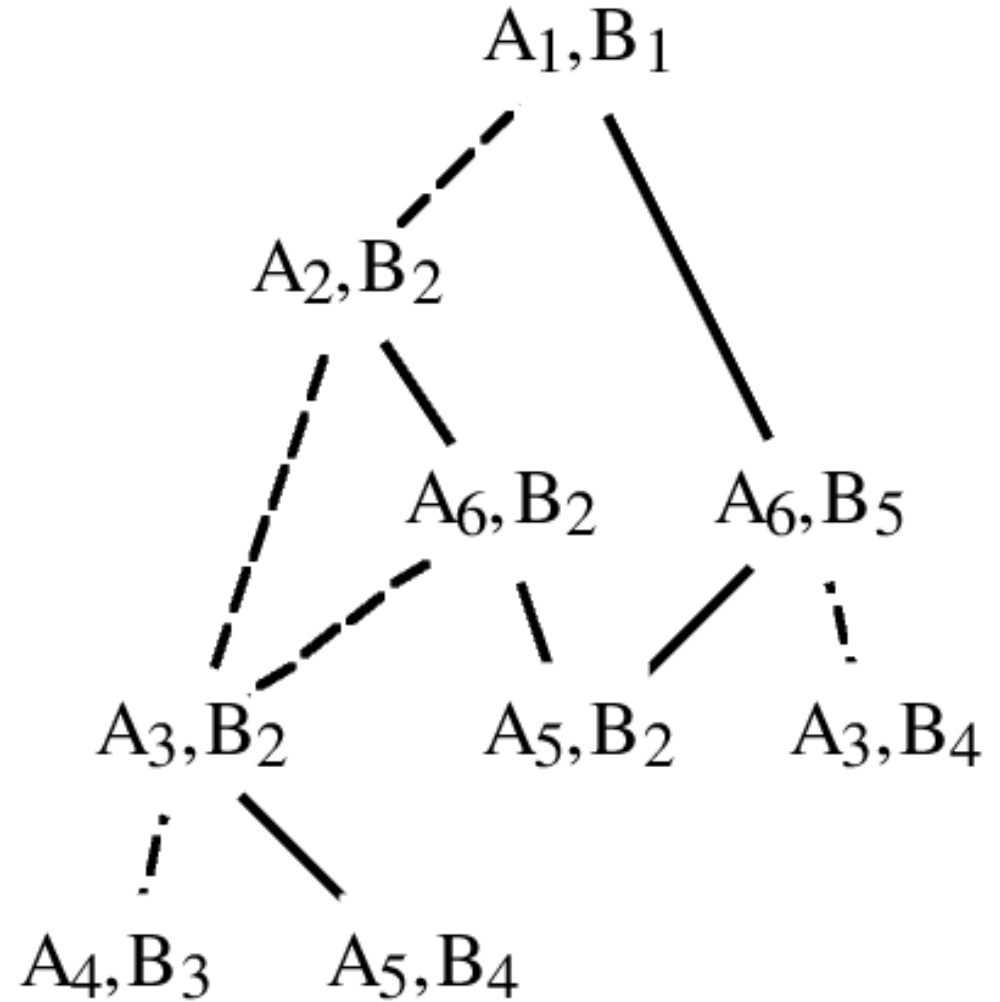
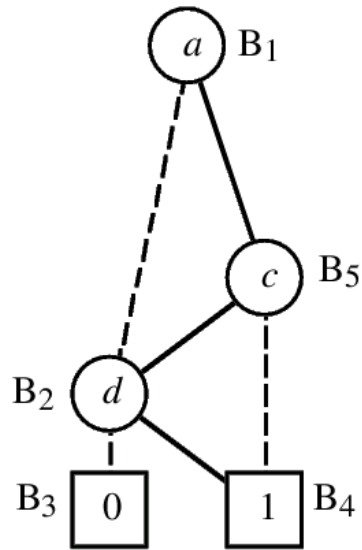
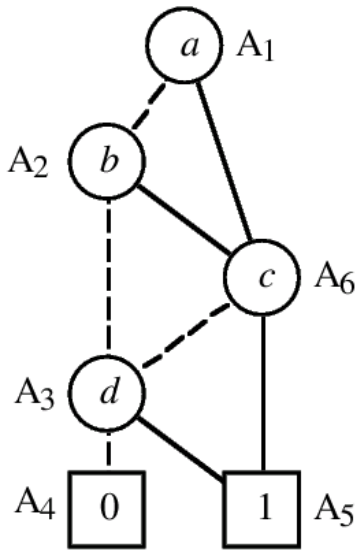
$$f \bullet g = x \wedge (f|_{x \leftarrow 1} \bullet g|_{x \leftarrow 1}) \quad \vee \quad \neg x \wedge (f|_{x \leftarrow 0} \bullet g|_{x \leftarrow 0})$$

Przykład: dane wyjściowe



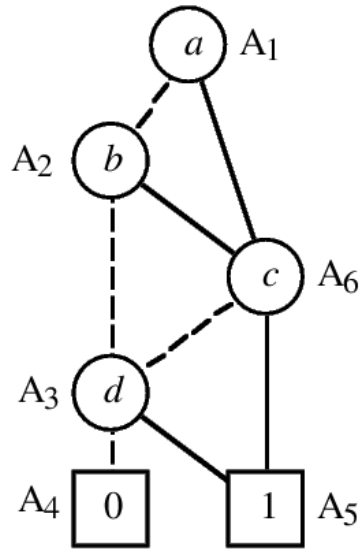
[Bryant 1992]

Przykład: wywołania rekurencyjne

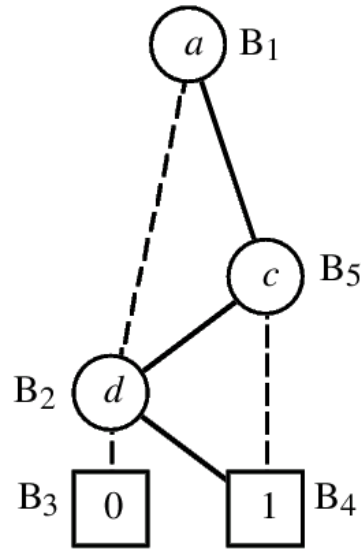


[Bryant 1992]

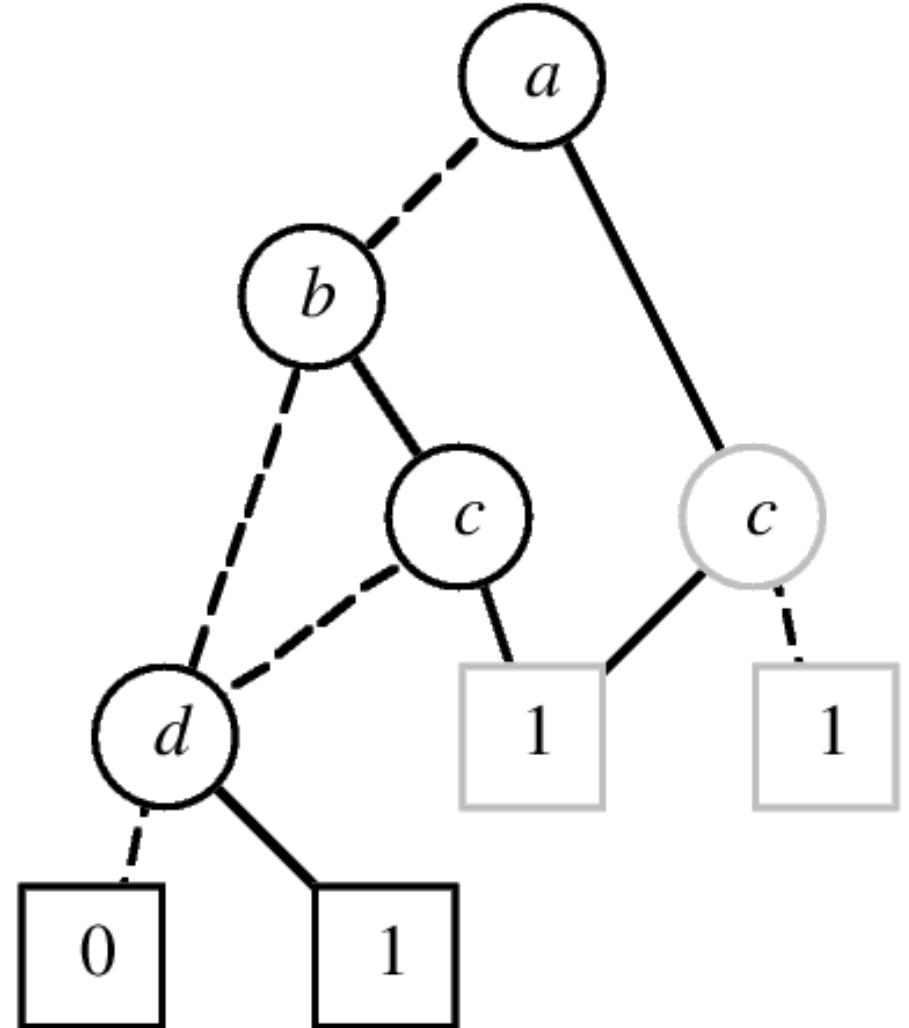
Przykład: wynik = $a \vee b \wedge c \vee d$



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

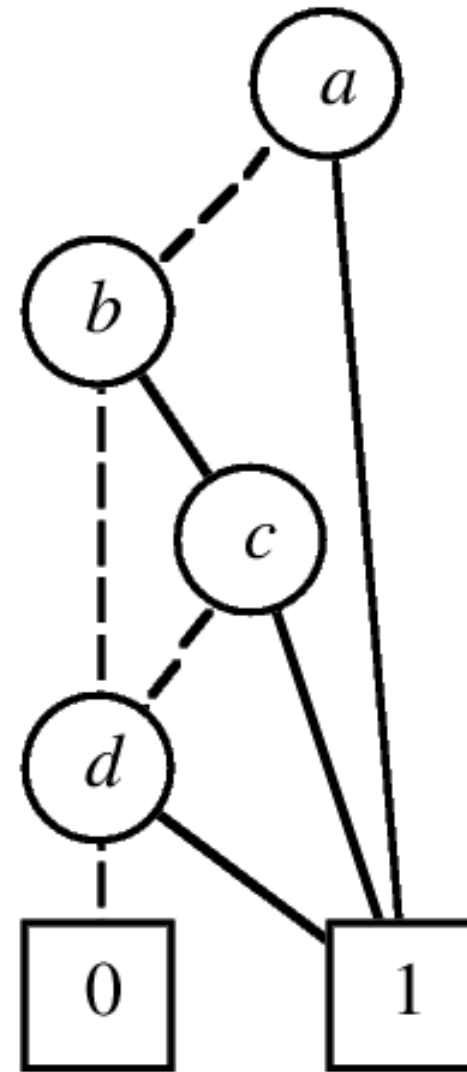
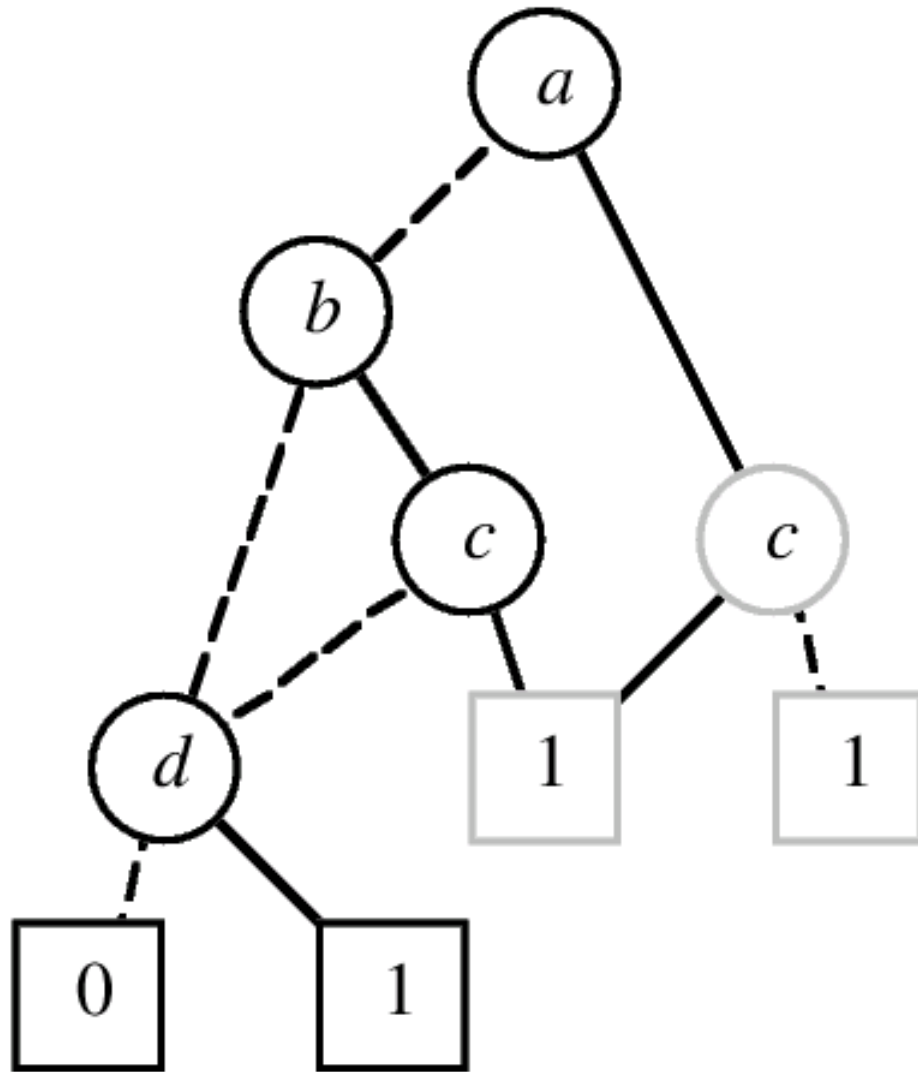


$$a \wedge \neg c \vee d$$



[Bryant 1992]

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



[Bryant 1992]

Apply(f , g , \bullet)

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

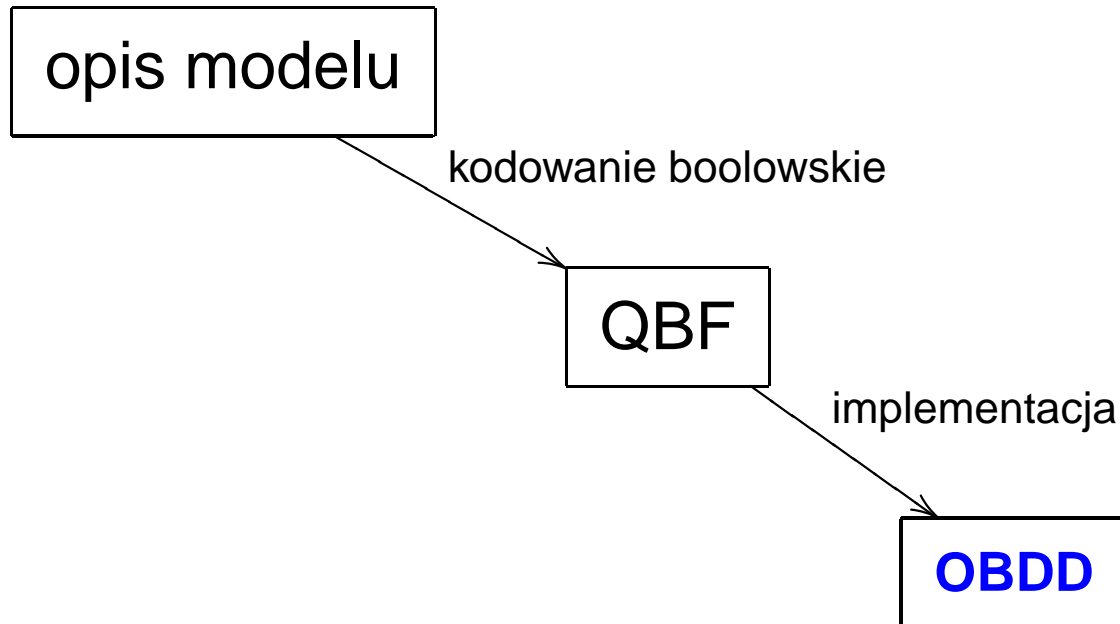
Pytanie: $f = g$?

Odmiany:

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

II. Kodowanie boolowskie

Kodowanie boolowskie



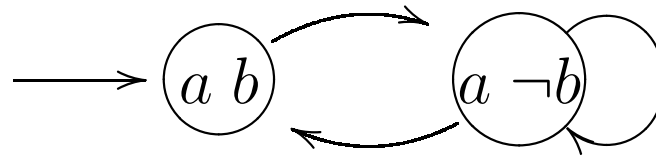
weryfikacja modelowa = operacje na OBDDs

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

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

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

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



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

$$\widehat{S}_0 = a \wedge b$$

$$\widehat{L}_p = \dots$$

struktura Kripkego \longmapsto OBDDs

ŹLE!

opis struktury K. \longmapsto OBDDs

DOBRCZE!

kompozycjonalny **opis** systemu

Procesy synchroniczne:

$$R = R_1 \wedge R_2 \wedge \dots \wedge R_n$$

Procesy asynchroniczne (model przeplotowy):

$$R = R'_1 \vee R'_2 \vee \dots \vee R'_n$$

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

Procesy asynchroniczne (model jednoczesny):

$$R = R'_1 \wedge R'_2 \wedge \dots \wedge R'_n$$

$$R'_i = R_i \vee \text{Id}_i$$

Ograniczenie do stanów osiągalnych:

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



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

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

III. Weryfikacja symboliczna

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

Niech $f : A \rightarrow A$ monotoniczna.

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

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

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

Niech $f : A \rightarrow A$ monotoniczna.

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

Przykład: $A = \mathcal{P}(S)$

$Z \mapsto \mathbf{EX} Z$

$$\mu Z. \mathbf{EX} Z = \perp = \emptyset$$

$$\nu Z. \mathbf{EX} Z = ?$$

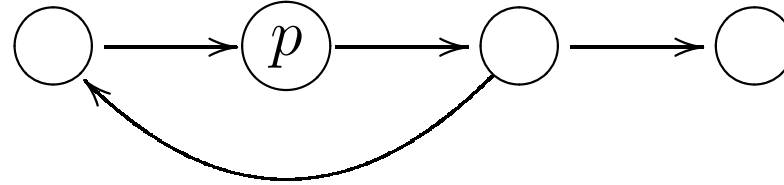
$Z \mapsto p \vee \mathbf{EX} Z$

$$\mu Z. p \vee \mathbf{EX} Z = ?$$

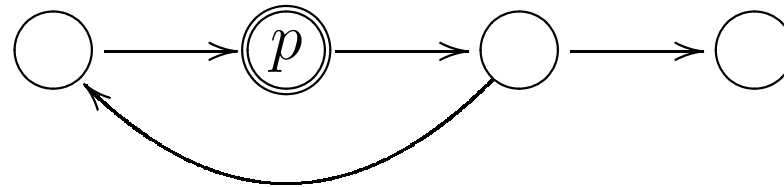
$$\mathbf{EF} p = \mu Z. p \vee \mathbf{EX} Z$$

$$Z \mapsto p \vee \mathbf{EX} Z$$

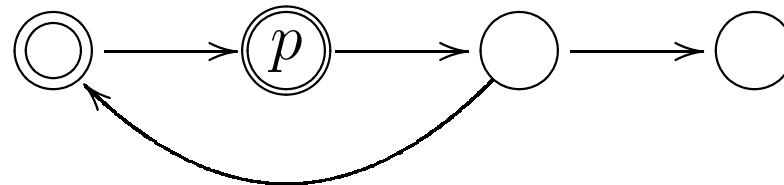
false



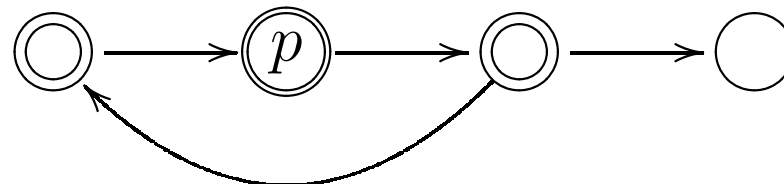
$$p \vee \mathbf{EX} \text{false} \equiv p$$



$$p \vee \mathbf{EX} p$$



$$p \vee \mathbf{EX} (p \vee \mathbf{EX} p)$$

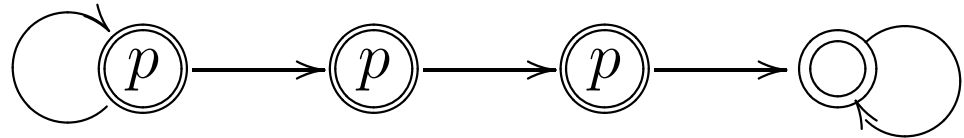


- $\mathbf{EF} \phi = \mu Z. \phi \vee \mathbf{EX} Z$ $Z \mapsto \phi \vee \mathbf{EX} Z$
- $\mathbf{AF} \phi = \mu Z. \phi \vee \mathbf{AX} Z$ $Z \mapsto \phi \vee \mathbf{AX} Z$
- $\mathbf{EG} \phi = \nu Z. \phi \wedge \mathbf{EX} Z$ $Z \mapsto \phi \wedge \mathbf{EX} Z$
- $\mathbf{AG} \phi = \nu Z.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

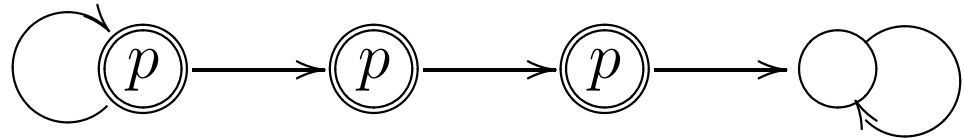
$$\mathbf{EG} p = \nu Z. p \wedge \mathbf{EX} Z$$

$$Z \mapsto p \wedge \mathbf{EX} Z$$

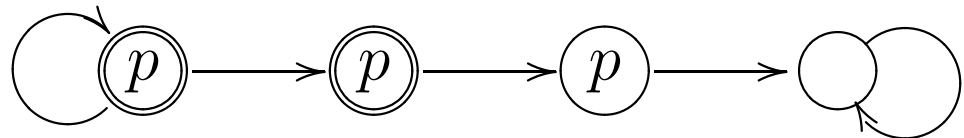
true



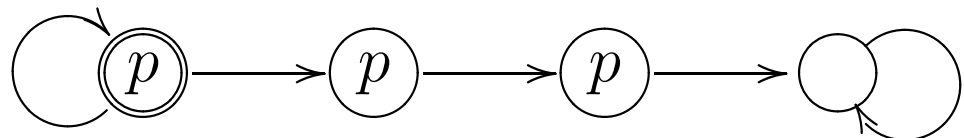
$p \wedge \mathbf{EX} \text{true} \equiv p$



$p \wedge \mathbf{EX} p$



$p \wedge \mathbf{EX} (p \wedge \mathbf{EX} p)$



Weryfikacja symboliczna

CTL (\neg , \wedge , **EX**, **E_U_**, **EG**)

(wystarczą te spójniki)

Check : CTL \mapsto OBDD

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

Weryfikacja symboliczna (EX_)

Check : CTL \rightarrow OBDD

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

Check(**EX** ϕ) := $\exists \vec{x}'. \widehat{R}(\vec{x}, \vec{x}') \wedge f(\vec{x}')$ gdzie $f = \text{Check}(\phi)$

Check(**EX** ϕ) := **EX** f

- **EX** ϕ
- **EX** Z
- **EX** f

Weryfikacja symboliczna (E_U_)

Check : CTL \rightarrow OBDD

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

Check($\mathbf{E} \phi \mathbf{U} \psi$) := $\mu Z. g \vee (f \wedge \mathbf{EX} Z)$ gdzie $f = \text{Check}(\phi)$
 $g = \text{Check}(\psi)$

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

false

$$g \vee (f \wedge \mathbf{EX} \text{false})$$

$$\equiv g$$

$$g \vee (f \wedge \mathbf{EX} (g \vee (f \wedge \mathbf{EX} \text{false})))$$

$$\equiv g \vee (f \wedge \mathbf{EX} g)$$

...

$$\equiv g \vee (f \wedge \mathbf{EX} (g \vee (f \wedge \mathbf{EX} g)))$$

\downarrow

$$\mu Z. g \vee (f \wedge \mathbf{EX} Z)$$

Weryfikacja symboliczna (EG _)

Check : CTL \rightarrow OBDD

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

Check(**EG** ϕ) := $\nu Z. f \wedge$ **EX** Z gdzie $f =$ Check(ϕ)

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

EX ϕ

E ϕ **U** ψ

EG ϕ

EX Z

E Z **U** Z'

EG Z

EX f

E f **U** g

EG f