

Praktyczne metody weryfikacji

Wykład 12: Weryfikacja probalistyczna

Motywacja:

- losowość w protokołach i algorytmach rozproszonych
- weryfikacja efektywności: przepustowość, czas dojścia, itp.
- modelowanie przy braku wiedzy
(losowość jako abstrakcja)
- opis zawodności i nieprzewidywalności
- ...

Modele probabilistyczne:

- łańcuchy z czasem dyskretnym (DTMC)
- procesy decyzyjne (MDP)
- łańcuchy z czasem ciągłym (CTMC)

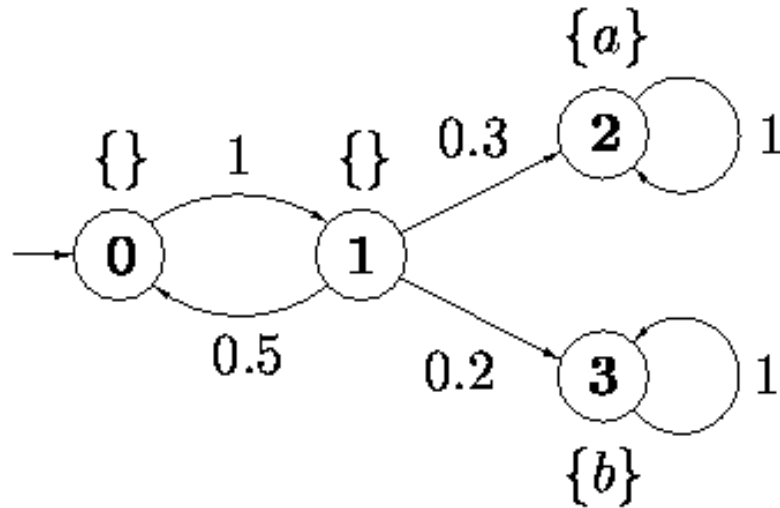
I. Czas dyskretny

Łańcuch z czasem dyskretnym:

- S – skończony zbiór stanów, $s_0 \in S$
- $\mathbf{P} : S \times S \rightarrow [0, 1]$ – macierz probabilistyczna
- $L : S \rightarrow \mathcal{P}(P)$

$$\mathbf{P} (X(k+1) = s' \mid X(k) = s) = \mathbf{P} (s, s')$$

Przykład: DTMC



$$\mathbf{P} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0.5 & 0 & 0.3 & 0.2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

dtmc

module *M*

v : [0..3] **init** 0;

□ (*v* = 0) → (*v*' = 1);

□ (*v* = 1) → 0.5 : (*v*' = 0) + 0.3 : (*v*' = 2) + 0.2 : (*v*' = 3);

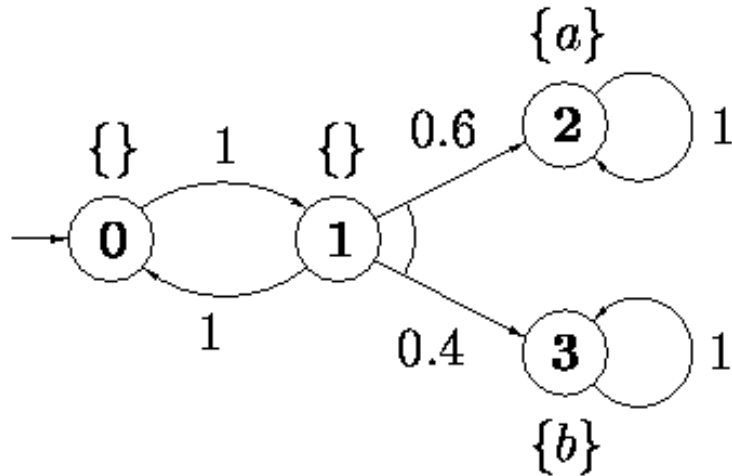
□ (*v* = 2) → (*v*' = 2);

□ (*v* = 3) → (*v*' = 3);

endmodule

[Parker 2002]

Przykład: MDP



$$\mathbf{Steps} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0.6 & 0.4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

[Parker 2002]

współbieżność \implies niedeterminizm

PCTL (Probabilistic Computation Tree Logic)

(DTMC, MDP)

$$\phi ::= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathbf{P}_{\prec p} \psi$$

$$\psi ::= \mathbf{X}\phi \mid \phi_1 \mathbf{U}^{\leq k} \phi_2 \mid \phi_1 \mathbf{U} \phi_2$$

$$\prec \in \{<, \leq, >, \geq\}$$

$\mathbf{P}_? \psi$

$$\mathbf{P}_{\prec p} \psi \equiv \mathbf{P}(\text{ścieżka ma własność } \psi) \prec p$$

$$s \models \mathbf{P}_{\prec p} \psi \equiv \mathbf{P}_s(\{\Pi \text{ sciezka z } s \mid \Pi \models \psi\}) \prec p$$

ustalmy s

$$\mathbf{P}_s (s = s_0 \rightarrow s_1 \rightarrow \dots \rightarrow s_n) = \mathbf{P} (s_0, s_1) \cdot \dots \cdot \mathbf{P} (s_{n-1}, s_n)$$

cylinder $C(s \rightarrow s_1 \rightarrow \dots \rightarrow s_n)$

$$\mathbf{P}_s (C(s \rightarrow s_1 \rightarrow \dots \rightarrow s_n)) = \mathbf{P} (s_0, s_1) \cdot \dots \cdot \mathbf{P} (s_{n-1}, s_n)$$

rozszerzamy (jednoznacznie !) \mathbf{P}_s na

najmniejsze σ -ciało zawierające wszystkie cylindry

Przykłady: jakościowy fragment logiki PCTL

$$P_{>0} (F a)$$

$$E F a$$

$$P_{=0} (F a)$$

$$\neg E F a$$

$$P_{=1} (F a)$$

$$A F a$$

$$P_{<1} (F a)$$

$$\neg A F a$$

Przykłady: jakościowy fragment logiki PCTL

$$P_{>0} (F a)$$

$$E F a$$

$$P_{=0} (F a)$$

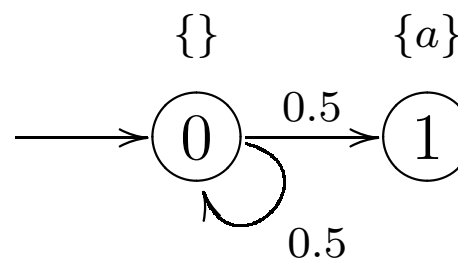
$$\neg E F a$$

$$P_{=1} (F a)$$

$$A F a$$

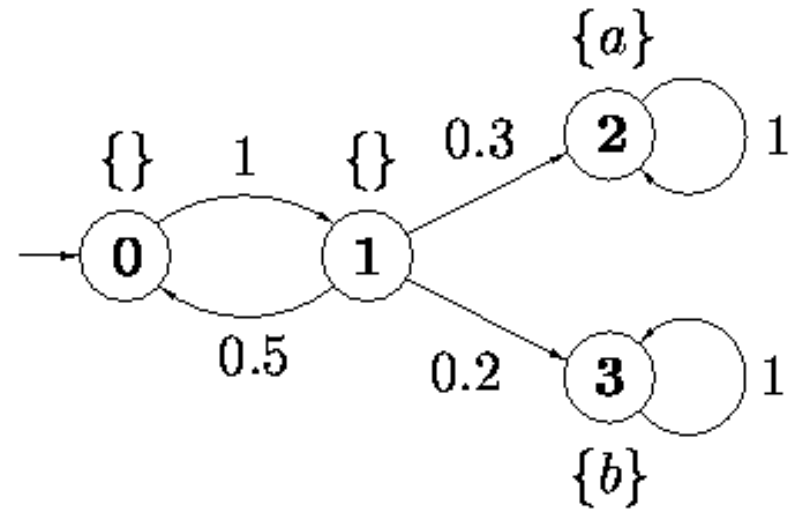
$$P_{<1} (F a)$$

$$\neg A F a$$



Pytanie: $P_{>0} \psi \equiv E \psi$?

$P_{>0} (\neg a \wedge \neg b) U a$

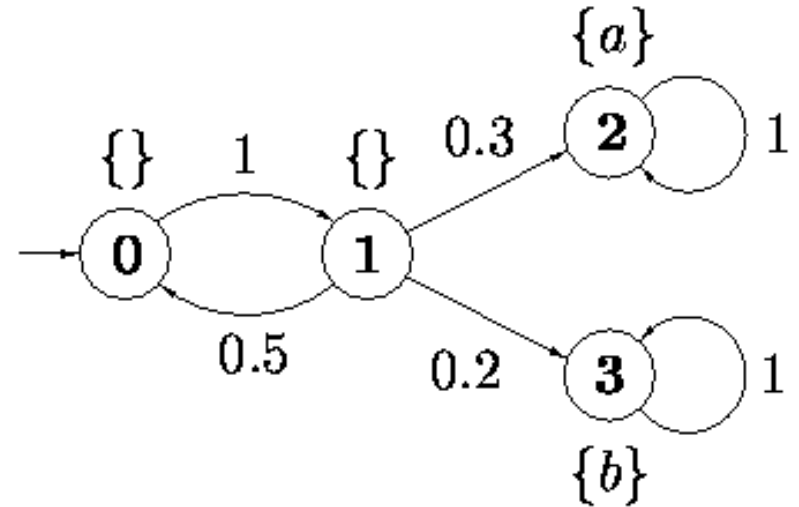


Pytanie: $P_{>0} \psi \equiv E \psi ?$

$$P_{>0} (\neg a \wedge \neg b) \mathbf{U} a$$

Pytanie: $P_{=1} \psi \equiv A \psi ?$

$$P_{=1} (\neg a \wedge \neg b) \mathbf{U} (a \vee b)$$



Pytanie: $P_{>0} \psi \equiv E \psi$?

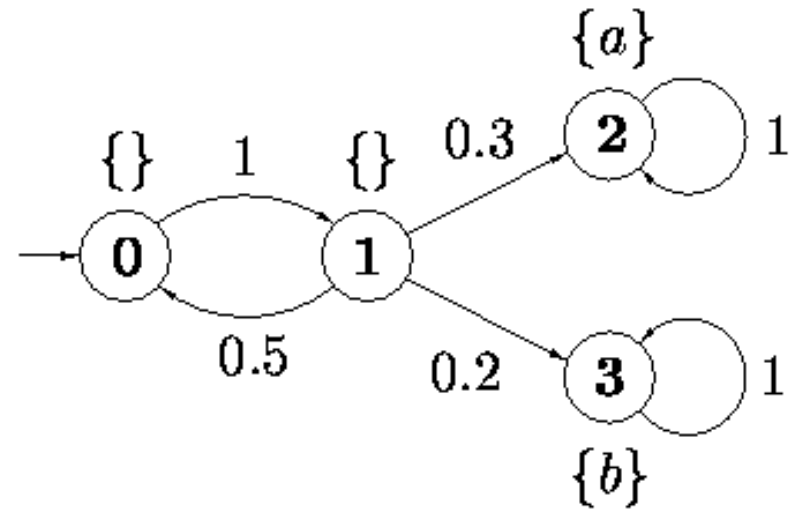
$$P_{>0} (\neg a \wedge \neg b) \mathbf{U} a$$

Pytanie: $P_{=1} \psi \equiv A \psi$?

$$P_{=1} (\neg a \wedge \neg b) \mathbf{U} (a \vee b)$$

Pytanie: $P_{<p} \neg \psi \equiv P_{>1-p} \psi$?

$$P_{>\frac{1}{4}} \mathbf{G} (\neg a \wedge \neg b) \equiv P_{<\frac{3}{4}} \mathbf{F} (a \vee b)$$



Przykłady (cd):

$$P_{=1} (F a)$$

$$P_{=0} (G \neg a)$$

$$\neg P_{>0} (G \neg a)$$

$$\bigwedge_{1 \leq i \leq 6} P_{=\frac{1}{6}} (X i)$$

$$P_{=1} (F \text{ delivered}) \wedge P_{=1} (G (\text{send} \implies P_{\geq 0.99} (F^{\leq 3} \text{ delivered})))$$

$$P_{=1} (G P_{=1} (F a))$$

$$P_{=1} (G F a)$$

$$A G A F a$$

$$A G F a$$

Silna sprawiedliwość dla $\alpha : s \rightarrow s'$:

α niedyskryminowane \equiv

$$G F (\alpha \text{ wykonalne}) \implies G F (\alpha \text{ wykonane})$$

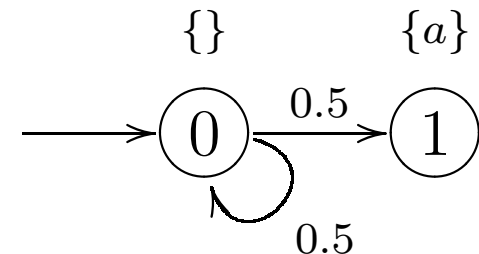
Tw.: $P_s (\alpha \text{ niedyskryminowane}) = 1$

Tw.: Sprawiedliwy CTL = jakościowy PCTL

Przykład:

$$P_{=1} (F a)$$

$$A F a$$



II. Czas ciągły

Łańcuch z czasem ciągłym:

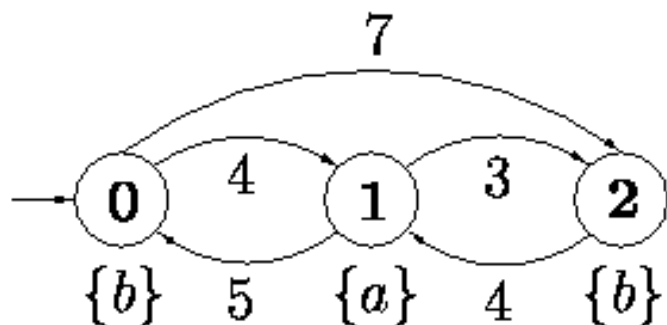
- S – skończony zbiór stanów, $s_0 \in S$
- $\mathbf{R} : S \times S \rightarrow \mathbb{R}^{\geq 0}$ – macierz intensywności
- $L : S \rightarrow \mathcal{P}(P)$

$$\mathbf{P} (s \rightarrow s' \text{ wykona się po czasie } < t) = 1 - e^{-\mathbf{R}(s,s') \cdot t}$$

$$\mathbf{P} (s, s') = \frac{\mathbf{R}(s,s')}{\sum_{s''} \mathbf{R}(s,s'')} \quad (\text{w jednym kroku}) \quad \rightsquigarrow \text{DTMC}$$

$$\text{rozkład stacjonarny:} \quad \pi_{s,t}(s') \quad \pi_s(s') = \lim_{t \rightarrow \infty} \pi_{s,t}(s')$$

Przykład: CTMC



$$\mathbf{R} = \begin{pmatrix} 0 & 4 & 7 \\ 5 & 0 & 3 \\ 0 & 4 & 0 \end{pmatrix}$$

$$\mathbf{Q} = \begin{pmatrix} -11 & 4 & 7 \\ 5 & -8 & 3 \\ 0 & 4 & -4 \end{pmatrix}$$

[Parker 2002]

$$\text{generator } \mathbf{Q}(s, s') = \begin{cases} \mathbf{R}(s, s'), & s \neq s' \\ -\sum_{s'' \neq s} \mathbf{R}(s, s''), & s = s' \end{cases}$$

CSL (Continuous Stochastic Logic)

(CTMC)

$$\phi ::= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathbf{P}_{\prec p} \psi \mid \mathbf{S}_{\prec p} \phi$$

$$\psi ::= \mathbf{X} \phi \mid \phi_1 \mathbf{U}^{\leq t} \phi_2 \mid \phi_1 \mathbf{U} \phi_2$$

$$\prec \in \{<, \leq, >, \geq\}$$

$$\mathbf{P}_? \psi, \mathbf{S}_? \psi$$

$$s \models \mathbf{P}_{\prec p} \psi \equiv \mathbf{P}_s (\{ \Pi \text{ sciezka z } s \mid \Pi \models \psi \}) \prec p$$

$$\Pi = s_0 t_0 s_1 t_1 s_2 \dots$$

$$s \models \mathbf{S}_{\prec p} \phi \equiv \sum_{s' \models \phi} \pi_s(s') \prec p$$

III. Weryfikacja

Weryfikacja probabilistyczna =

- weryfikacja nieprobabilistyczna
(weryfikacja jakościowa)

+

- obliczenia numeryczne

$M \models \phi$: Algorytm etykietuje stany podformułami ϕ

$$\phi ::= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathbf{P}_{<p} \psi$$

$$\psi ::= \mathbf{X}\phi \mid \phi_1 \mathbf{U}^{\leq k} \phi_2 \mid \phi_1 \mathbf{U} \phi_2$$

$M \models \phi$: Algorytm etykietuje stany podformułami ϕ

dla wszystkich s , obliczamy $P_s(\psi) = P_s(\{\Pi z s \mid \Pi \models \psi\})$

$$X\phi : P_s(X\phi) = \sum_{s' \models \phi} P(s, s')$$

$\phi_1 U^{\leq k} \phi_2$:

$$P_s(\phi_1 U^{\leq k} \phi_2) = \begin{cases} 0 & s \models \neg\phi_1 \wedge \neg\phi_2 \\ 1 & s \models \phi_2 \\ 0 & s \models \phi_1 \wedge \neg\phi_2, k = 0 \\ \sum_{s'} P(s, s') \cdot P_{s'}(\phi_1 U^{\leq k-1} \phi_2) & \text{wpp} \end{cases}$$

$M \models \phi$: Algorytm etykietuje stany podformułami ϕ

dla wszystkich s , obliczamy $P_s(\psi) = P_s(\{\Pi z s \mid \Pi \models \psi\})$

$\phi_1 \mathbf{U} \phi_2$:

$$x_s = \begin{cases} 0 & s \models \neg \mathbf{E} \phi_1 \mathbf{U} \phi_2 \\ 1 & s \models \neg \mathbf{E} (\phi_1 \wedge \neg \phi_2) \mathbf{U} (P_{=0} \phi_1 \mathbf{U} \phi_2) \\ \sum_{s'} P(s, s') \cdot x_{s'} & \text{wpp} \end{cases}$$

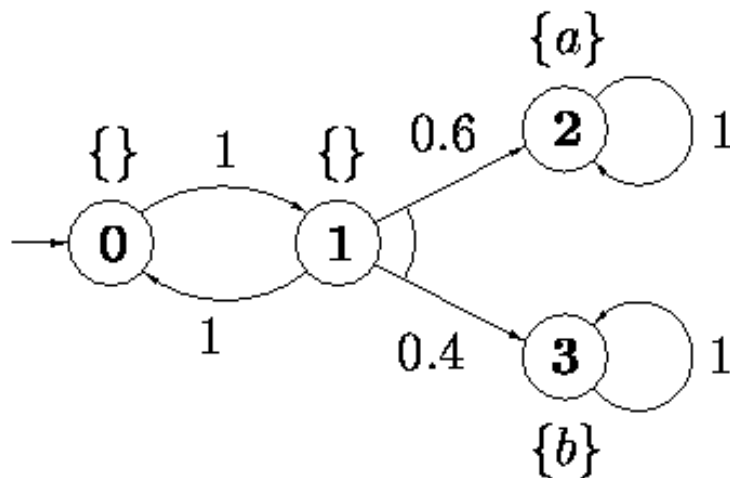
weryfikacja **jakościowa** ($P_{=0} \phi_1 \mathbf{U} \phi_2$, $P_{=1} \phi_1 \mathbf{U} \phi_2$) i **ilościowa**

Obliczenia numeryczne:

- mnożenie macierzy przez wektor
- iteracyjne rozwiązywanie układu równań liniowych
 - Jacobi
 - Gauss-Seidl
 - SOR, JOR
 - ...

(zwykle główną operacją jest mnożenie macierzy przez wektor)

?



$$\mathbf{Steps} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0.6 & 0.4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

[Parker 2002]

$P_{\prec p} X \phi$: DTMC

$P_{\prec p} \phi_1 U \phi_2$: DTMC

$P_{\prec p} \phi_1 U^{\leq t} \phi_2$:

$$P_s(\phi_1 U^{\leq t} \phi_2) = \begin{cases} 0 & s \models \neg E \phi_1 U \phi_2 \\ ? & ? \end{cases}$$

$R(s, s') := 0$, jeśli $s \models \neg E \phi_1 U \phi_2$ lub $s \models \phi_2$. Wtedy

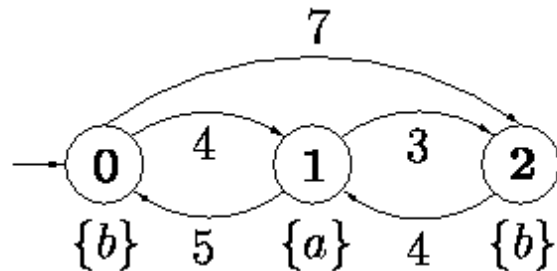
$$P_s(\phi_1 U^{\leq t} \phi_2) = \sum_{s' \models \phi_2} \pi_{s,t}(s')$$

uniformizacja

$S_{\leftarrow p} \phi$: układ równań liniowych

$$\pi \cdot \mathbf{Q} = \vec{0} \quad \sum_s \pi(s) = 1$$

Przykład:



$$\mathbf{R} = \begin{pmatrix} 0 & 4 & 7 \\ 5 & 0 & 3 \\ 0 & 4 & 0 \end{pmatrix} \quad \mathbf{Q} = \begin{pmatrix} -11 & 4 & 7 \\ 5 & -8 & 3 \\ 0 & 4 & -4 \end{pmatrix}$$

[Parker 2002]

$$\begin{aligned} -11x_0 + 5x_1 &= 0 \\ 4x_0 - 8x_1 + 4x_2 &= 0 \\ 7x_0 + 3x_1 - 4x_2 &= 0 \\ x_0 + x_1 + x_2 &= 1 \end{aligned}$$

rozwiązanie:

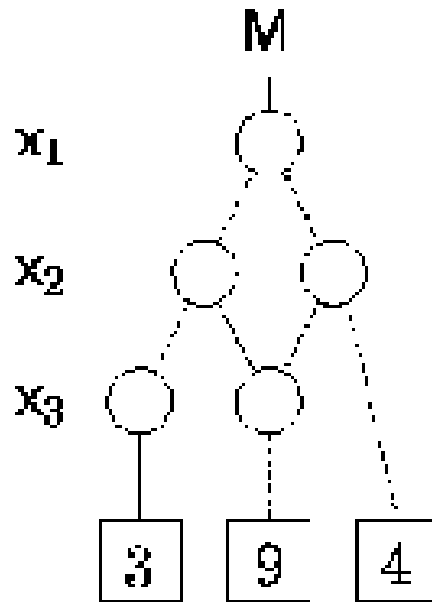
$$(x_0, x_1, x_2) = \left(\frac{5}{33}, \frac{1}{3}, \frac{17}{33} \right)$$

IV. Weryfikacja symboliczna

Co zamiast BDD?

- macierze rzadkie
- DNBDD
- PDG
- MDD
- MTBDD
- ...

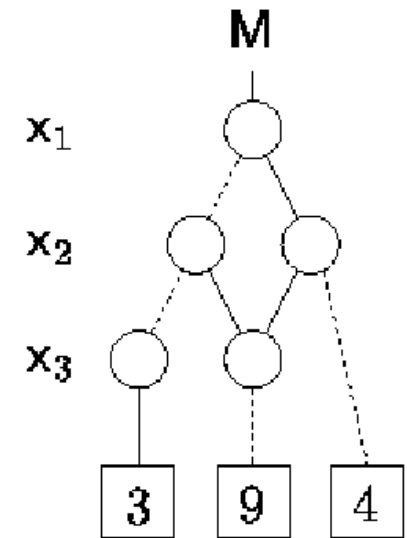
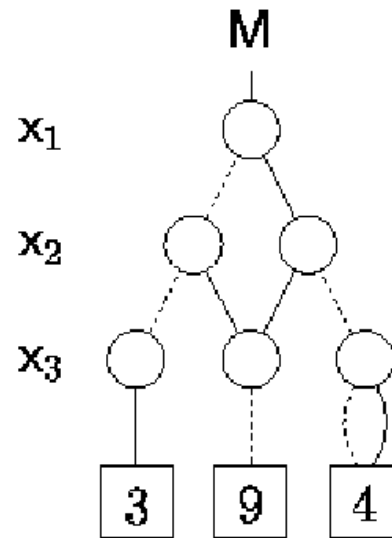
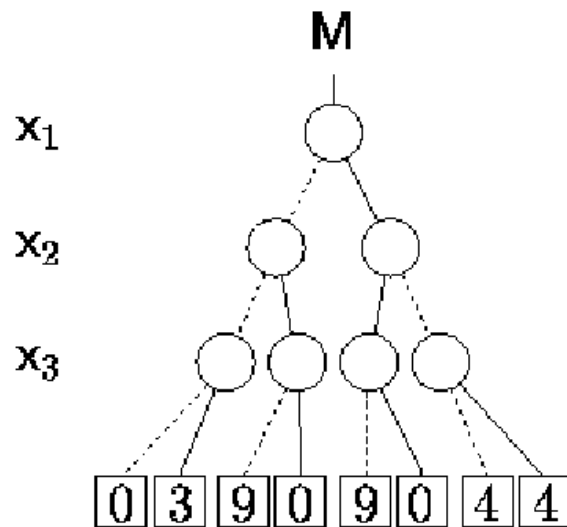
Przykład:



x_1	x_2	x_3	f_M
0	0	1	3
0	1	0	9
1	1	0	9
1	0	0	4
1	0	1	4
wpp			0

[Parker 2002]

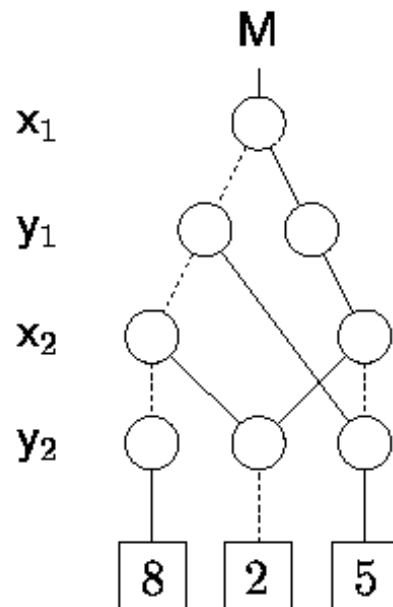
Postać kanoniczna:



[Parker 2002]

Reprezentacja macierzy (modelu):

$$M = \begin{pmatrix} 0 & 8 & 0 & 5 \\ 2 & 0 & 0 & 5 \\ 0 & 0 & 0 & 5 \\ 0 & 0 & 2 & 0 \end{pmatrix}$$

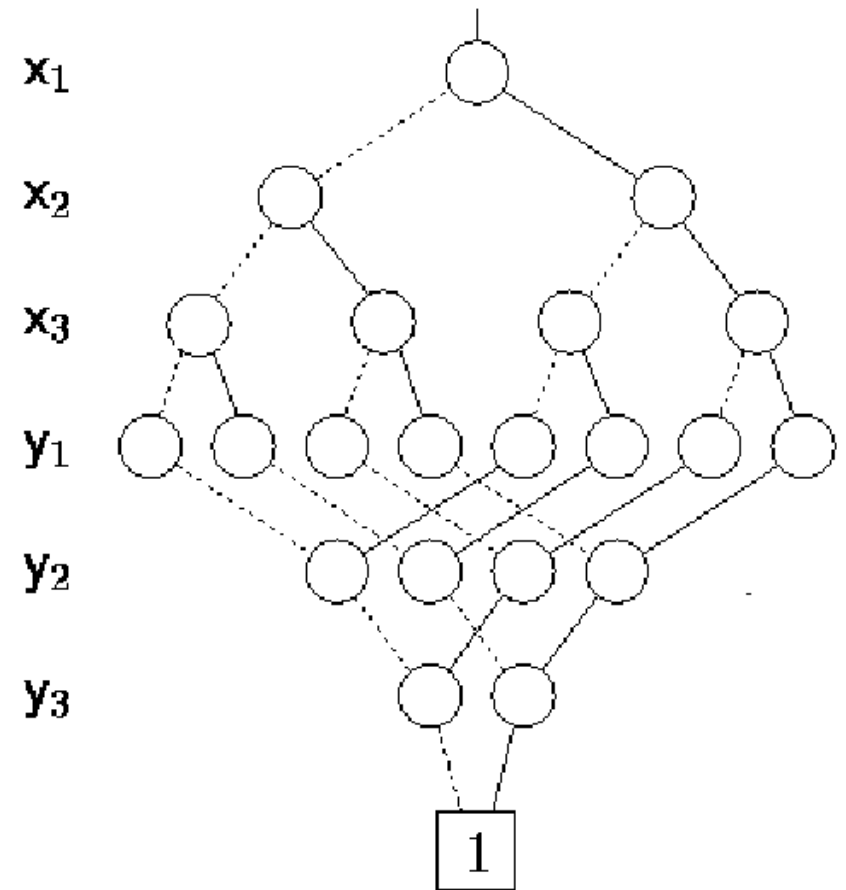
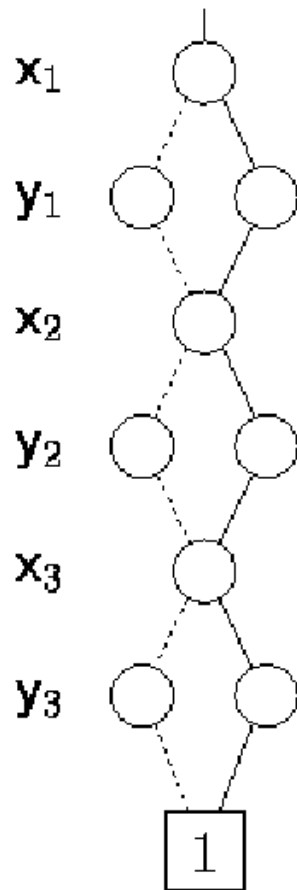


x_1	y_1	x_2	y_2	f_M	Entry in M
0	0	0	1	8	$(0, 1) = 8$
0	0	1	0	2	$(1, 0) = 2$
0	1	0	1	5	$(0, 3) = 5$
0	1	1	1	5	$(1, 3) = 5$
1	1	1	0	2	$(3, 2) = 2$
1	1	0	1	5	$(2, 3) = 5$

[Parker 2002]

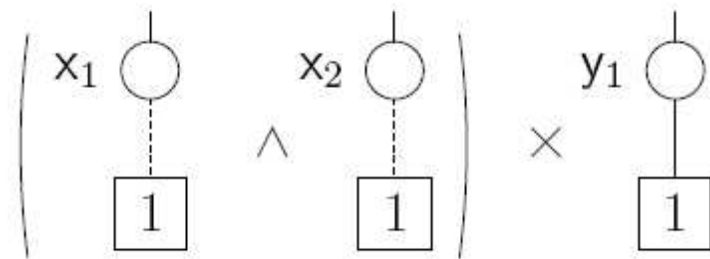
Reprezentacja wektora (rozwiązań): analogicznie

Kolejność zmiennych:

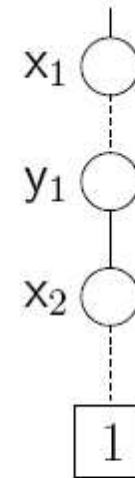


[Parker 2002]

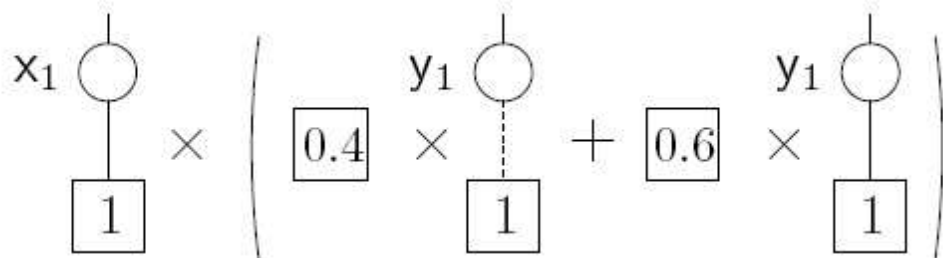
$$(v_1 = 0) \wedge (v_2 = 0) \rightarrow (v'_1 = 1)$$



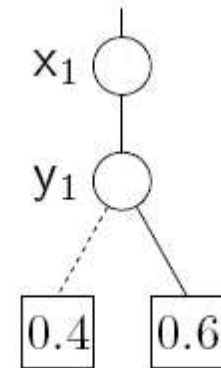
\rightarrow



$$(v_1 = 1) \rightarrow 0.4 : (v'_1 = 0) + 0.6 : (v'_1 = 1)$$



\rightarrow



[Parker 2002]

Implementacja operacji mnożenia:

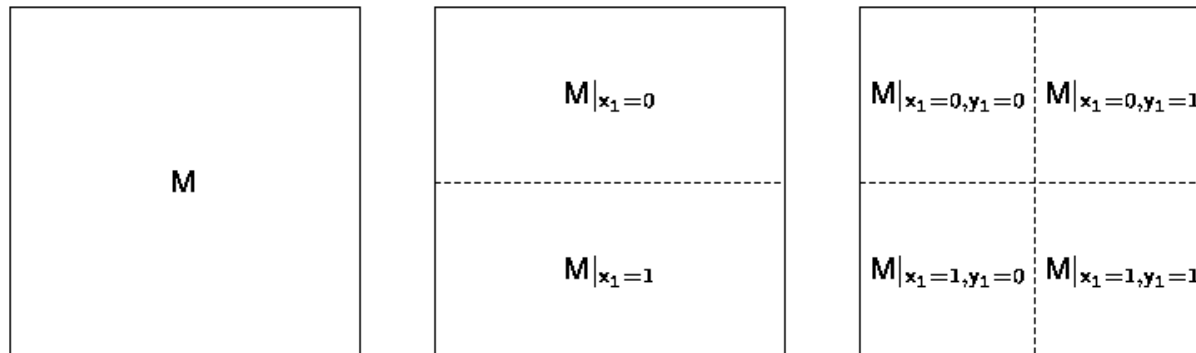
$$\begin{pmatrix} \mathbf{A}_1 & \mathbf{A}_2 \\ \mathbf{A}_3 & \mathbf{A}_4 \end{pmatrix} = \begin{pmatrix} \mathbf{B}_1 & \mathbf{B}_2 \\ \mathbf{B}_3 & \mathbf{B}_4 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{C}_1 & \mathbf{C}_2 \\ \mathbf{C}_3 & \mathbf{C}_4 \end{pmatrix} \iff$$

$$\mathbf{A}_1 = \mathbf{B}_1 \cdot \mathbf{C}_1 + \mathbf{B}_2 \cdot \mathbf{C}_3$$

$$\mathbf{A}_2 = \mathbf{B}_1 \cdot \mathbf{C}_2 + \mathbf{B}_2 \cdot \mathbf{C}_4$$

$$\mathbf{A}_3 = \mathbf{B}_3 \cdot \mathbf{C}_1 + \mathbf{B}_4 \cdot \mathbf{C}_3$$

$$\mathbf{A}_4 = \mathbf{B}_3 \cdot \mathbf{C}_2 + \mathbf{B}_4 \cdot \mathbf{C}_4$$



[Parker 2002]

Mnożenie macierzy przez **wektor**

Efektywność MTBDDs:

- reprezentacja modelu
- weryfikacja jakościowa
- weryfikacja ilościowa

Algorytm hybrydowy:

- macierz modelu jako MTBDD
- wektor (rozwiązania) jawnie

MTBDD < macierz rzadka < hybrydowy < ...

Stop!

Zamiast podsumowania: czego nie było ?

- SAT i jego dalsze zastosowania, np. UMC
- weryfikacja kompozycyjna
- weryfikacja parametryczna i nieskończeniostanowa
(regularna)
- weryfikacja software'u
- bogatsze logiki, np. rachunek μ
- nic poza weryfikacją modelową