Praktyczne metody weryfikacji

Wykład 13: Weryfikacja probalistyczna

Motywacja:

- losowość w protokołach i algorytmach rozproszonych
- opis zawodności
- weryfikacja ilościowa
- weryfikacja efektywności: przepustowość, czas dojścia, itp.
- weryfikacja bezpieczeństwa
- ...

Modele probabilistyczne:

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

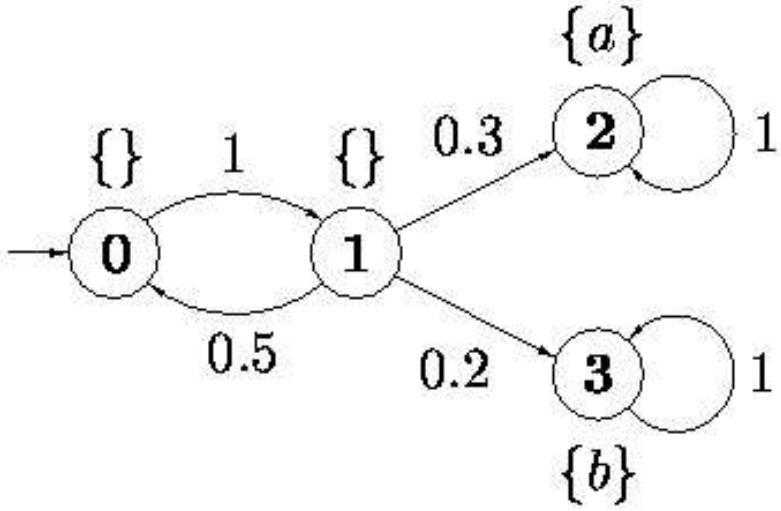
I. Czas dyskretny

Łańcuch z czasem dyskretnym:

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

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

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;

[] $(v = 0) \rightarrow (v' = 1)$;

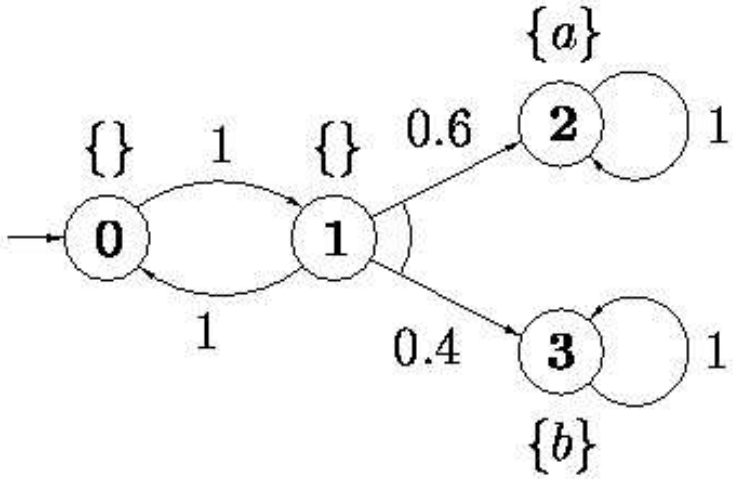
[] $(v = 1) \rightarrow 0.5 : (v' = 0) + 0.3 : (v' = 2) + 0.2 : (v' = 3)$;

[] $(v = 2) \rightarrow (v' = 2)$;

[] $(v = 3) \rightarrow (v' = 3)$;

endmodule

Przykład: MDP



$$\mathbf{Steps} = \left(\begin{array}{cccc} 0 & \mathbf{1} & 0 & 0 \\ \hline \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0.6 & 0.4 \\ \hline 0 & 0 & \mathbf{1} & 0 \\ \hline 0 & 0 & 0 & \mathbf{1} \end{array}\right)$$

PCTL (Probabilistic Computation Tree Logic) (DTMC, MDP)

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

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

$\prec \in \{<, \leq, >, \geq\}$ $\qquad$ $\mathsf{P}_?\,\psi$

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

$s \vDash \mathsf{P}_{\prec p}\,\psi \quad \equiv \quad \mathsf{P}_s\,(\,\{\Pi \text{ sciezka z } s \mid \Pi \vDash \psi\}\,) \prec p$

ustalmy s

$$\mathsf{P}_s\left(s = s_0 \to s_1 \to \ldots \to s_n \right) = \mathsf{P}\left(s_0, s_1\right) \cdot \ldots \cdot \mathsf{P}\left(s_{n-1}, s_n\right)$$

cylinder $C\left(s \to s_1 \to \ldots \to s_n \right)$

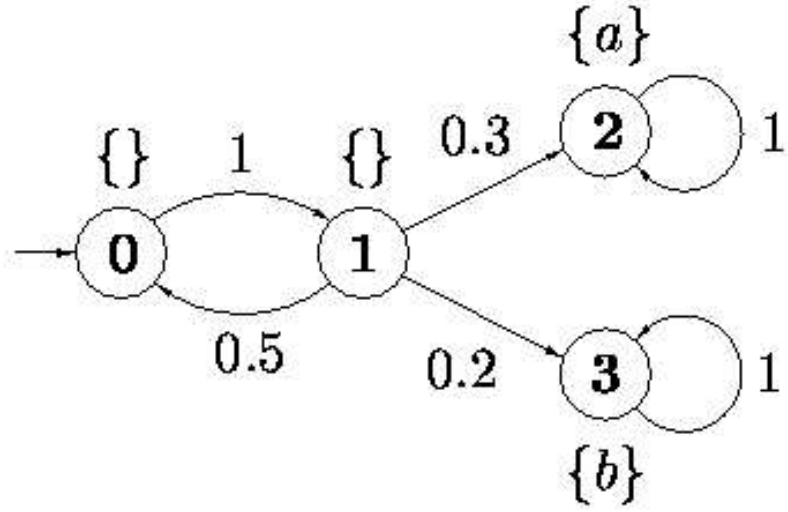
$$\mathsf{P}_s\left(C\left(s \to s_1 \to \ldots \to s_n \right) \right) = \mathsf{P}\left(s_0, s_1\right) \cdot \ldots \cdot \mathsf{P}\left(s_{n-1}, s_n\right)$$

najmniejsze σ-ciało zawierają wszystkie cylindry

rozszerzamy (jednoznacznie !) P_s na σ-ciało

Pytanie: $\mathsf{P}_{>0}\,\psi \quad \equiv \quad \mathsf{E}\,\psi$?

$\mathsf{P}_{>0}\,(\neg a \wedge \neg b)\,\mathsf{U}\,a$



Pytanie: $\mathsf{P}_{=1}\,\psi \quad \equiv \quad \mathsf{A}\,\psi$?

$\mathsf{P}_{=1}\,(\neg a \wedge \neg b)\,\mathsf{U}\,(a \vee b)$

Pytanie: $\mathsf{P}_{\prec p}\,\neg\psi \quad \equiv \quad \mathsf{P}_{\succ 1-p}\,\psi$?

$\mathsf{P}_{>\frac{1}{4}}\,\mathsf{G}\,(\neg a \wedge \neg b) \quad \equiv \quad \mathsf{P}_{<\frac{3}{4}}\,\mathsf{F}\,(a \vee b)$

II. Czas ciągły

Łańcuch z czasem ciągłym:

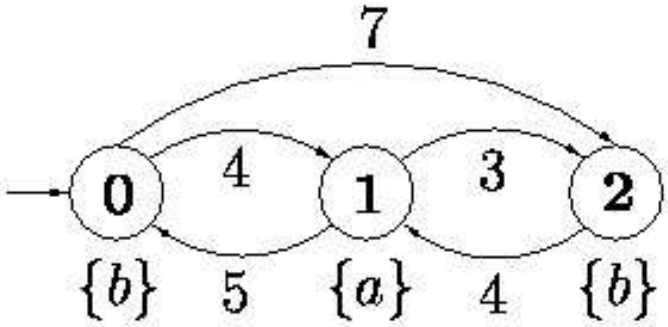
- S – skończony zbiór stanów, $s_0 \in S$
- $\mathbf{R} : S \times S \to \mathbb{R}^{\geq 0}$ – macierz intensywności
- $L : S \to \mathcal{P}(P)$

$$\mathsf{P}\left(s \to s' \text{ wykona sie po czasie } < t \right) = 1 - e^{-\mathbf{R}(s,s') \cdot t}$$

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

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

Przykład: CTMC



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

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)

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

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

$\prec \in \{<, \leq, >, \geq\}$ $\qquad$ $\mathsf{P}_?\,\psi,\ \ \mathsf{S}_?\,\psi$

$$s \vDash \mathsf{P}_{\prec p}\,\psi \quad \equiv \quad \mathsf{P}_s\,(\,\{\Pi \text{ sciezka z } s \mid \Pi \vDash \psi\}\,) \prec p$$

$$\Pi \;=\; s_0\ t_0\ s_1\ t_1\ s_2\ \ldots$$

$$s \vDash \mathsf{S}_{\prec p}\,\phi \quad \equiv \quad \sum_{s' \vDash \phi}\ \pi_s(s') \prec p$$

III. Weryfikacja

Weryfi kacja probabilistyczna =

– weryfi kacja nieprobabilistyczna

(weryfi kacja jakościowa)

+

– obliczenia numeryczne

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

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

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

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

dla wszystkich s, obliczamy $\mathsf{P}_s(\psi) = \mathsf{P}_s(\{\Pi \text{ z } s \mid \Pi \models \psi\})$

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

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

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

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

dla wszystkich s, obliczamy $\mathsf{P}_s(\psi) = \mathsf{P}_s(\{\Pi \text{ z } s \mid \Pi \models \psi\})$

$\phi_1 \,\mathsf{U}\, \phi_2$:

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

weryfi kacja jakościowa ($\mathsf{P}_{=0}\, \phi_1 \,\mathsf{U}\, \phi_2$, $\mathsf{P}_{=1}\, \phi_1 \,\mathsf{U}\, \phi_2$) 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)

$\mathsf{P}_{\prec p}\ \mathsf{X}\,\phi$: DTMC

$\mathsf{P}_{\prec p}\,\phi_1\,\mathsf{U}\,\phi_2$: DTMC

$\mathsf{P}_{\prec p}\,\phi_1\,\mathsf{U}^{\leq t}\,\phi_2$:

$$\mathsf{P}_s\left(\phi_1\,\mathsf{U}^{\leq t}\,\phi_2\right) = \begin{cases} 0 & s \models \neg\,\mathsf{E}\,\phi_1\,\mathsf{U}\,\phi_2 \\ ? & ? \end{cases}$$

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

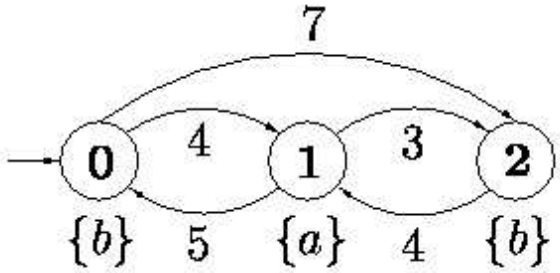
$$\mathsf{P}_s\left(\phi_1\,\mathsf{U}^{\leq t}\,\phi_2\right) = \sum_{s' \models \phi_2} \pi_{s,t}(s')$$

uniformizacja

$S_{\prec p}\,\phi$: układ równań liniowych

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

Przykład:



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

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

rozwiązanie:

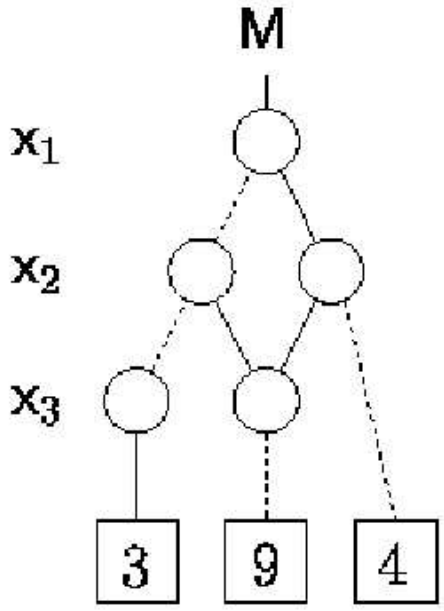
$$(x_0, x_1, x_2) = (\tfrac{5}{33}, \tfrac{1}{3}, \tfrac{17}{33})$$

IV. MTBDD

- BDD
- MTBDD
- MDD
- …

Przykład:

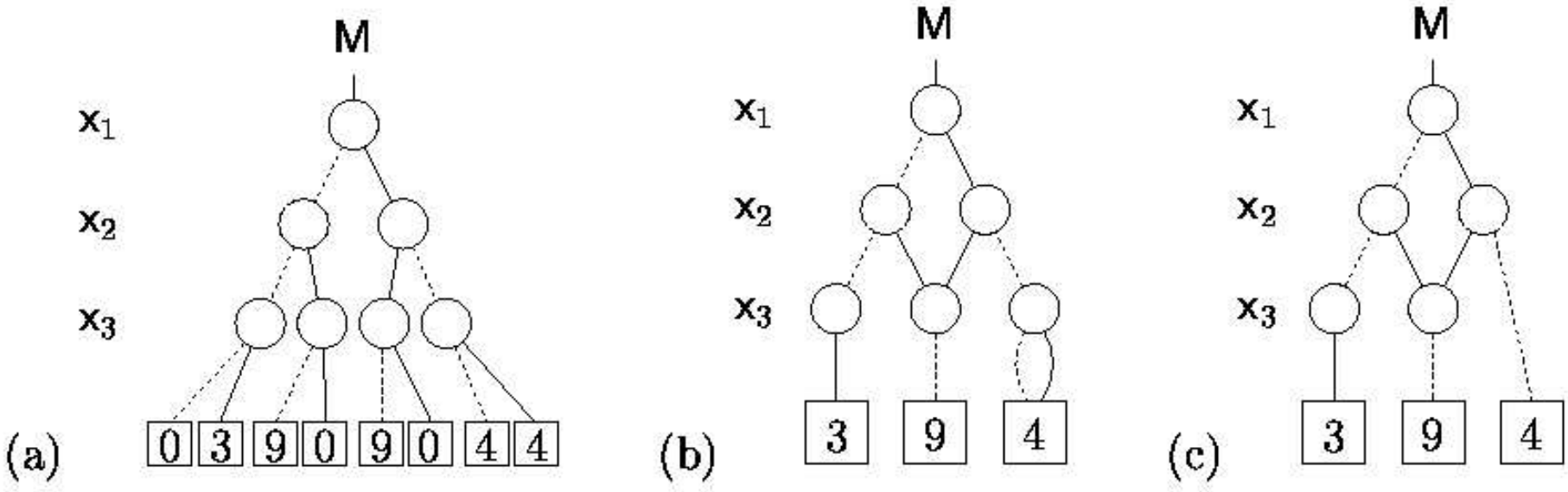
(a)



(b)

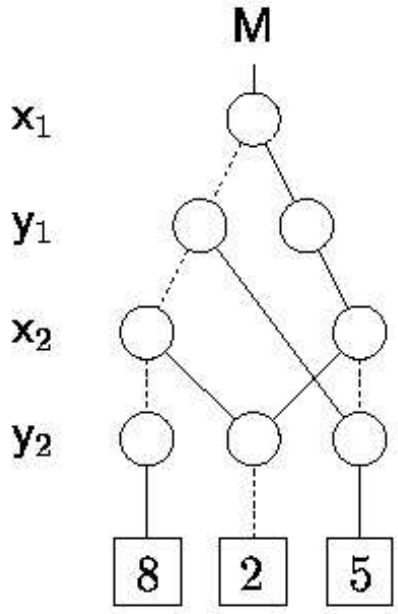
x_1	x_2	x_3	f_M
0	0	1	3
0	1	0	9
1	1	0	9
1	0	0	4
1	0	1	4
	wpp		0

Postać kanoniczna:



Reprezentacja macierzy (modelu):

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

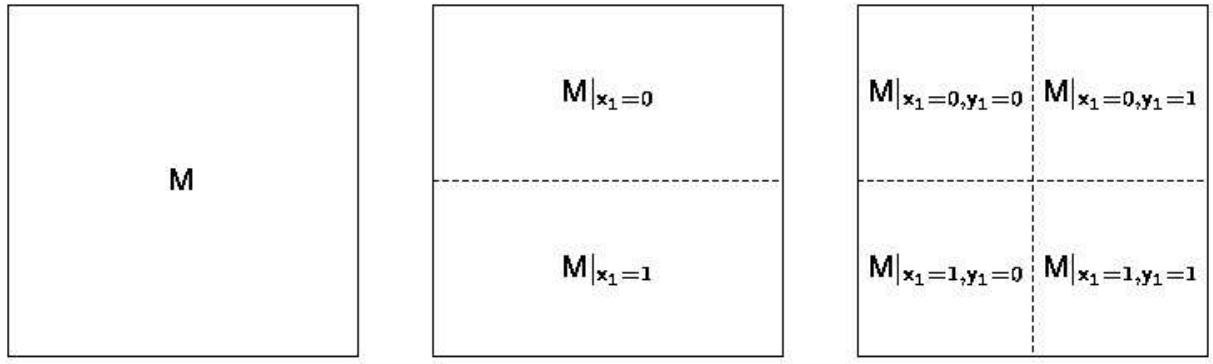


x_1	y_1	x_2	y_2	f_M	Entry in M
0	0	0	1	8	$(0,1) = 8$
0	0	1	0	2	$(1,0) = 2$
0	1	0	1	5	$(0,3) = 5$
0	1	1	1	5	$(1,3) = 5$
1	1	1	0	2	$(3,2) = 2$
1	1	0	1	5	$(2,3) = 5$

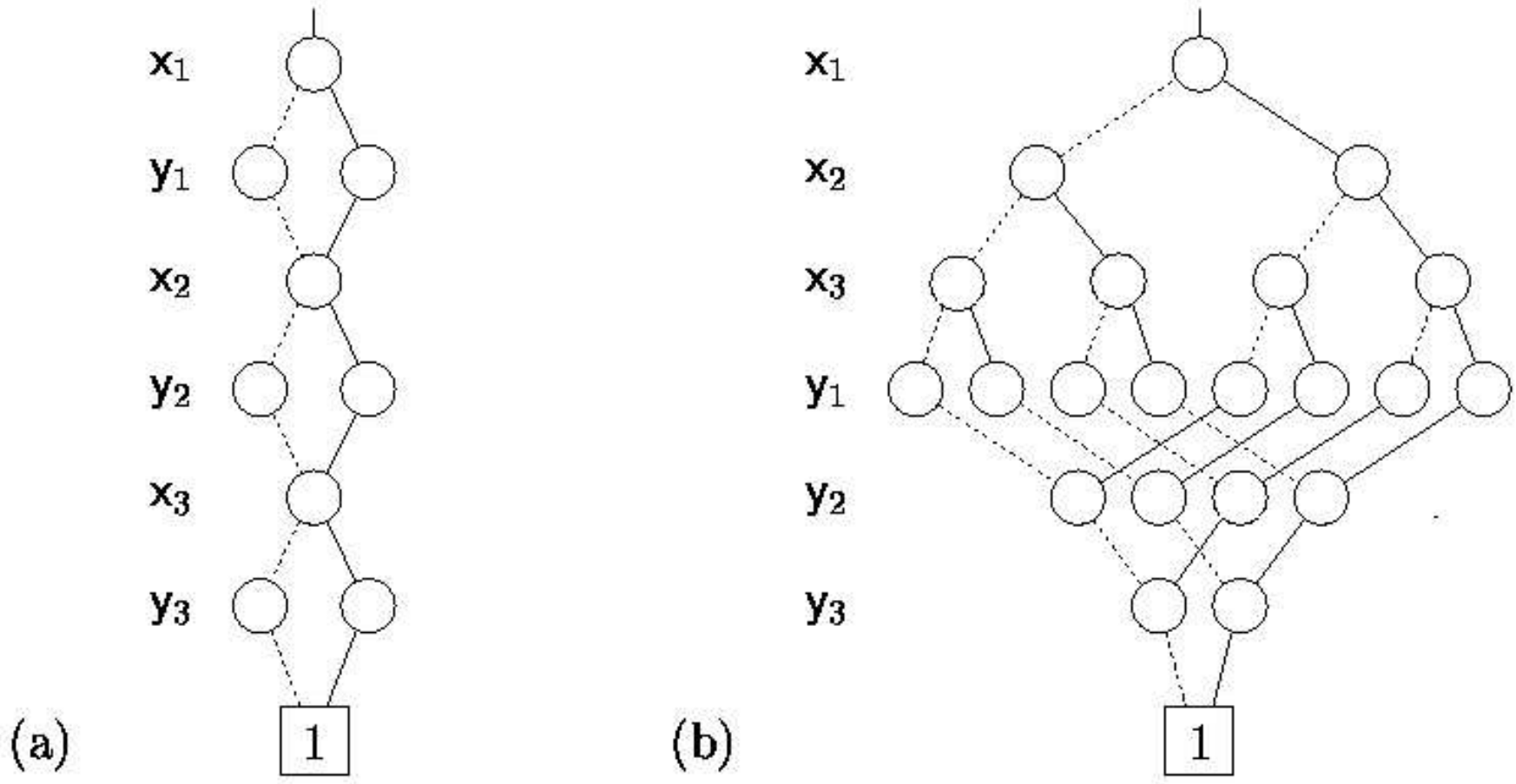
Reprezentacja wektora (rozwiązań): analogicznie

Implementacja operacji mnożenia:

$$\begin{pmatrix} \mathbf{A}_1 & \mathbf{A}_2 \\ \mathbf{A}_3 & \mathbf{A}_4 \end{pmatrix} = \begin{pmatrix} \mathbf{B}_1 & \mathbf{B}_2 \\ \mathbf{B}_3 & \mathbf{B}_4 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{C}_1 & \mathbf{C}_2 \\ \mathbf{C}_3 & \mathbf{C}_4 \end{pmatrix} \quad \Longleftrightarrow \quad \begin{aligned} \mathbf{A}_1 &= \mathbf{B}_1 \cdot \mathbf{C}_1 + \mathbf{B}_2 \cdot \mathbf{C}_3 \\ \mathbf{A}_2 &= \mathbf{B}_1 \cdot \mathbf{C}_2 + \mathbf{B}_2 \cdot \mathbf{C}_4 \\ \mathbf{A}_3 &= \mathbf{B}_3 \cdot \mathbf{C}_1 + \mathbf{B}_4 \cdot \mathbf{C}_3 \\ \mathbf{A}_4 &= \mathbf{B}_3 \cdot \mathbf{C}_2 + \mathbf{B}_4 \cdot \mathbf{C}_4 \end{aligned}$$



Kolejność zmiennych:



Efektywność MTBDDs:

- reprezentacja modelu
- weryfi kacja jakościowa
- weryfi kacja ilościowa

Algorytm hybrydowy:

- macierz modelu jako MTBDD
- wektor (rozwiązania) jawnie

Stop!

Zamiast podsumowania: czego nie był o ?

– SAT i jego dalsze zastosowania, np. UMC

– weryfi kacja kompozycjonalna

– weryfi kacja parametryczna i nieskończeniestanowa (regularna)

– weryfi kacja software'u

– abstrakcja i jej uszczegółowianie

– bogatsze logiki, np. rachunek μ

– nic poza weryfi kacją modelową