

Weryfikacja wspomagana komputerowo

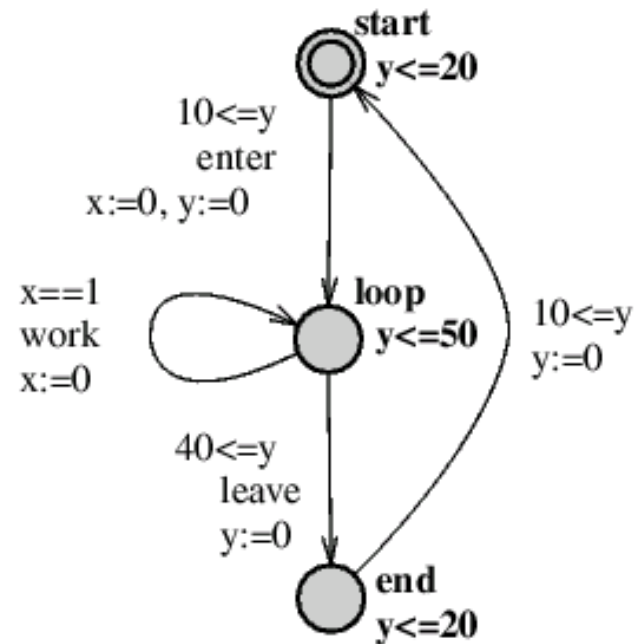
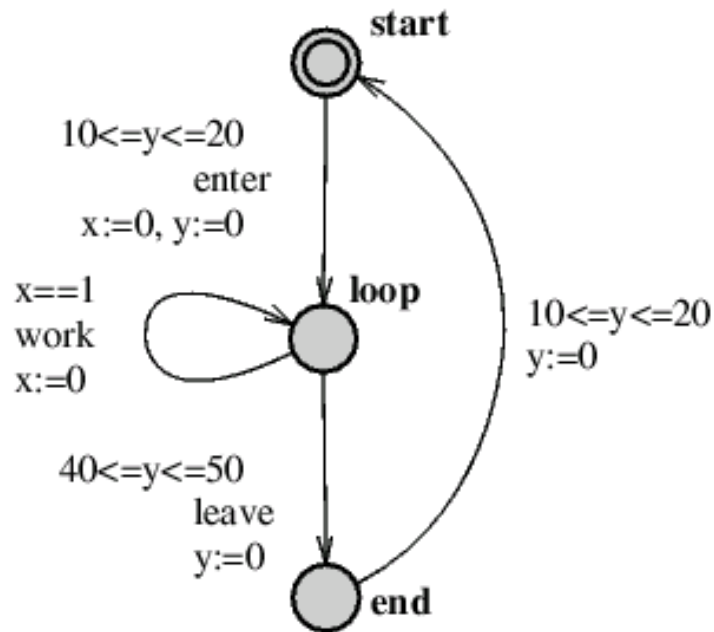
Wykład 13: Automaty czasowe

Jak modelować upływ czasu ?

- czas dyskretny lub **ciągły**
- trwanie tranzycji lub **upływ czasu** między tranzycjami
- różne modele:
 - **automaty czasowe** \mapsto **czasowa struktura Kripkego**
 - czasowe sieci Petri'ego
 - czasowe algebry procesów
- logiki czasowe: **TCTL, TLTL, ...**

I. Modele czasowe

Automaty czasowe



[Bengtsson, Yi 2004]

Zegary : $x \in \mathcal{C}$

Dozory, niezmienniki : $\Psi(\mathcal{C})$

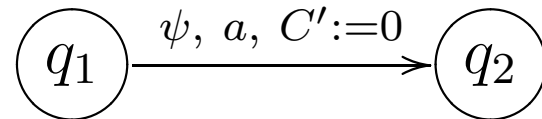
$$\psi ::= x \prec c \mid \psi_1 \wedge \psi_2 \mid x_1 - x_2 \prec c$$

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

$$c \in \mathbb{Q}^+ \quad (c \in \mathbb{N})$$

Relacja przejścia $\rho \subseteq Q \times \Sigma \times \Psi(\mathcal{C}) \times \mathcal{P}(\mathcal{C}) \times Q$

$$\langle q_1, a, \psi, \mathcal{C}', q_2 \rangle \in \rho$$



Słowo czasowe : $\langle t_1, a_1 \rangle \langle t_2, a_2 \rangle \dots$ (żywotność)

nie-Zeno : $\sum_i t_i$ nieograniczony

Wartościowanie zegarów : $v \in (\mathbb{R}^+)^{\mathcal{C}}$ $\forall x \in \mathcal{C}. v_0(x) = 0$

Bieg automatu : $\langle q_0, v_0 \rangle \xrightarrow{t_1} \langle q_0, v_0 + t_1 \rangle \xrightarrow{a} \langle q_1, v_1 \rangle \xrightarrow{t_2} \dots$

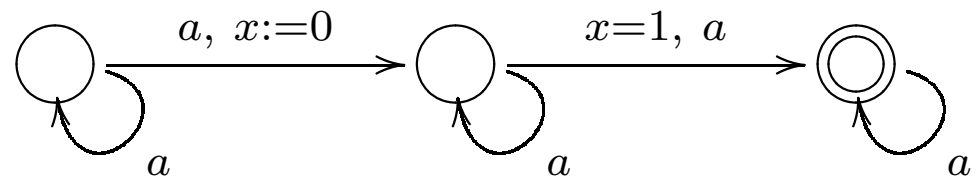
$v_0 \models \text{niezm}(q_0)$ $v_0 + t_1 \models \text{niezm}(q_0)$ $v_1 \models \text{niezm}(q_1)$

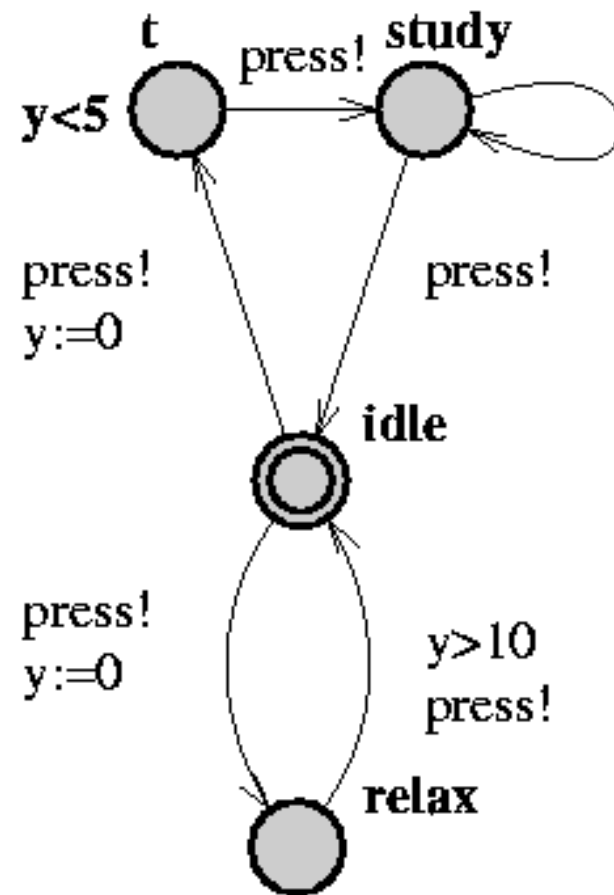
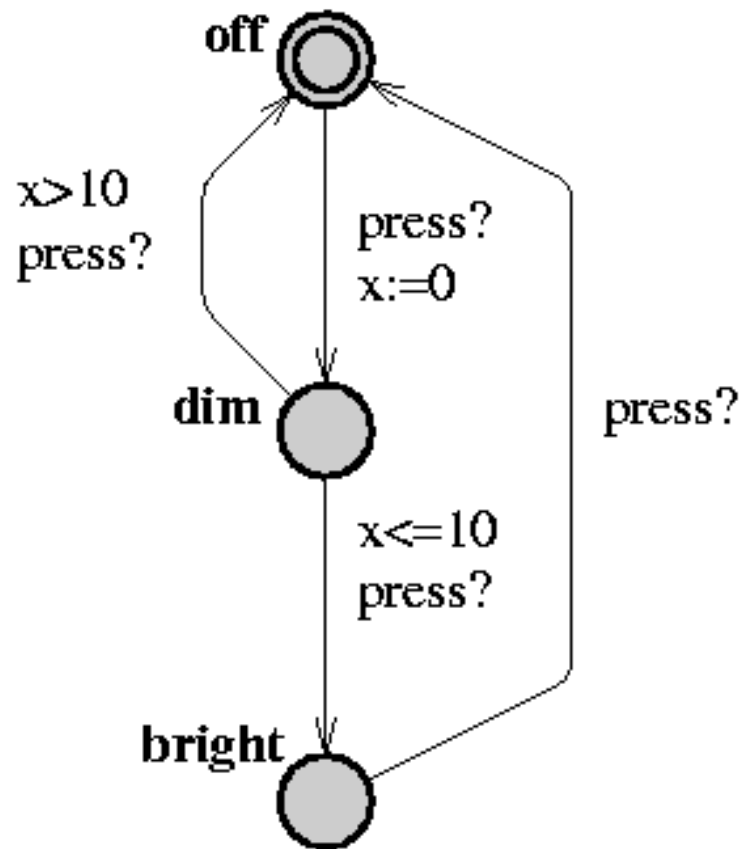
$\langle q_0, a, \psi, \mathcal{C}', q_1 \rangle \in \rho$ $v_0 + t_1 \models \psi$ $v_1 = (v_0 + t_1)[C' := 0]$

Warianty:

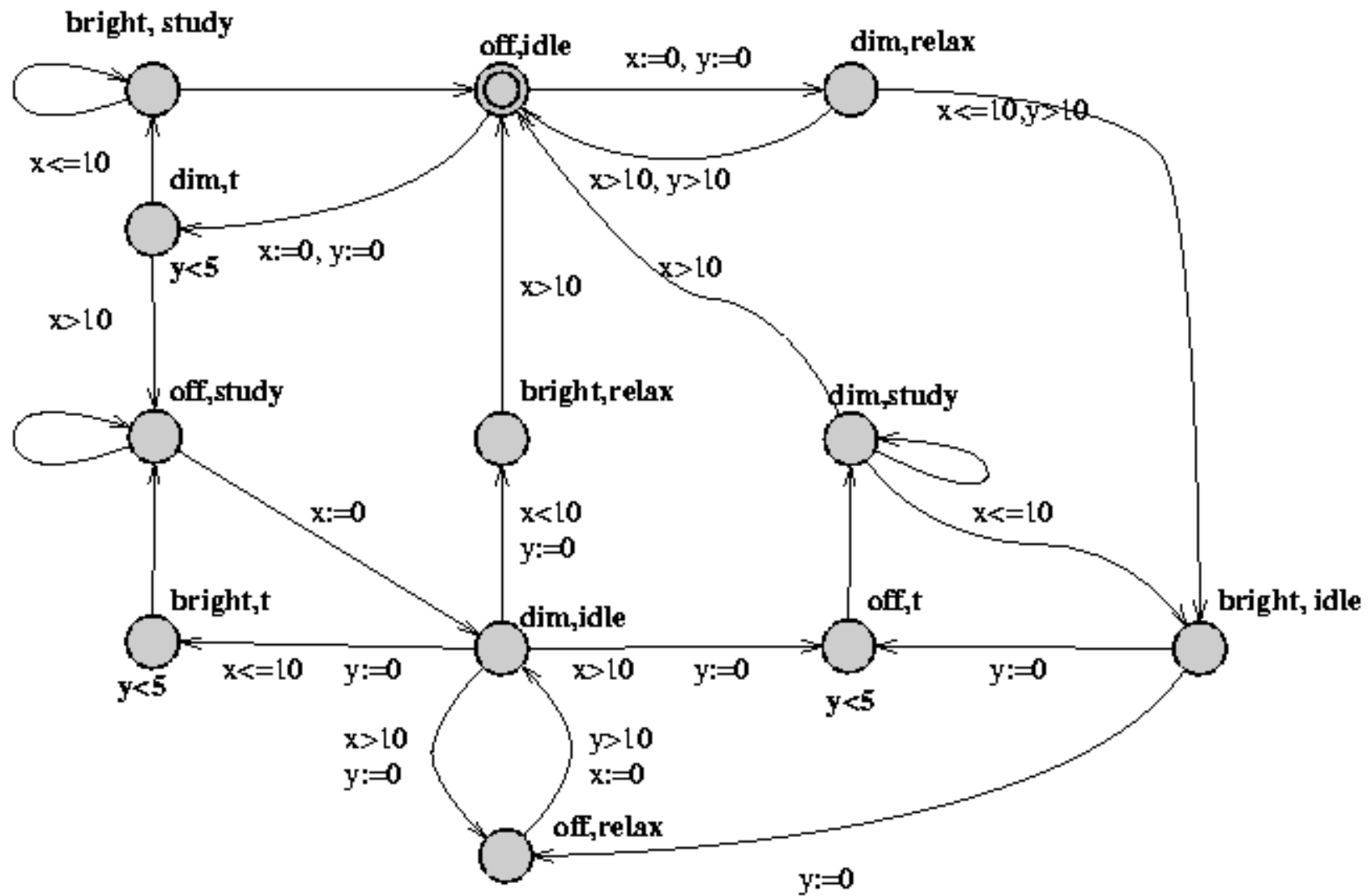
- bez niezmienników
- bez dozorów postaci $x_i - x_j \prec c$
- bez etykiet

2 rodzaje tranzycji: $\rightarrow i \overset{t}{\rightsquigarrow}$





[Bengtsson, Yi 2004]



[Bengtsson, Yi 2004]

Blokada: nie istnieje t t. że

$$\langle q, v \rangle \overset{t}{\rightsquigarrow} \langle q, v + t \rangle \xrightarrow{a}$$

Blokada czasowa: dodatkowo, nie istnieje $t > 0$ t. że

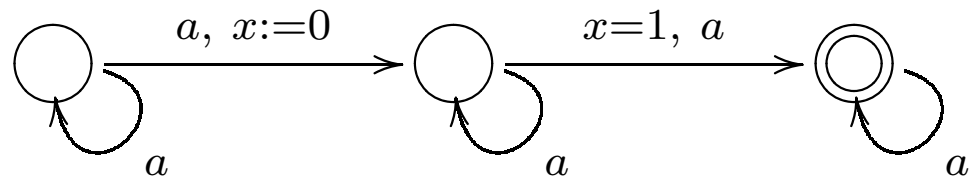
$$\langle q, v \rangle \overset{t}{\rightsquigarrow} \langle q, v + t \rangle$$

Pilność (niezmienniki)

automaty	pustość	uniwersalność
bezczasowe	NLOGSPACE	PSPACE
czasowe	PSPACE	nierozstrzygalna

- $L(A) \subseteq L(B)$
- tylko 1 zegar
- słowa skończone lub ω -słowa

Brak uzupełnienia :



$L(\mathcal{A}_1) \cap L(\mathcal{A}_2) ?$

$M(\mathcal{A})$

- stany: $\langle q, v \rangle \in Q \times (\mathbb{R}^+)^c$
- stany pocz.: $\langle q_0, v_0 \rangle$
- tranzycje: $\langle q, v \rangle \overset{t}{\rightsquigarrow} \langle q, v + t \rangle$ $\langle q, v \rangle \overset{a}{\rightarrow} \langle q', v' \rangle$
- $L(\langle q, v \rangle) = L(q) \cup \{\psi : v \models \psi\}$

determinizm: $s \overset{t}{\rightsquigarrow} s', s \overset{t}{\rightsquigarrow} s'' \implies s' = s''$

gęstość: $s \overset{t_1+t_2}{\rightsquigarrow} s' \iff \exists s''. s \overset{t_1}{\rightsquigarrow} s'' \overset{t_2}{\rightsquigarrow} s'$

II. Regiony i strefy

$$v \sim w \iff$$

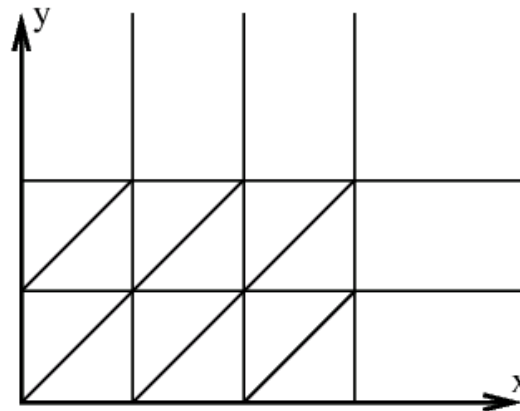
$$- \text{ albo } v(x) > c_x \text{ i } w(x) > c_x \text{ albo } \lfloor v(x) \rfloor = \lfloor w(x) \rfloor$$

$$- v(x) \leq c_x \implies (\langle v(x) \rangle = 0 \iff \langle w(x) \rangle = 0)$$

$$- v(x) \leq c_x \text{ i } v(y) \leq c_y \implies$$

$$(\langle v(x) \rangle \leq \langle v(y) \rangle \iff \langle w(x) \rangle \leq \langle w(y) \rangle)$$

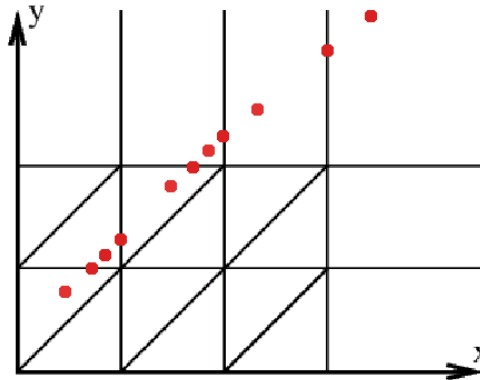
$$v, w \in (\mathbb{R}^+)^c$$



Liczba regionów:

$$\leq |\mathcal{C}|! \cdot 2^{|\mathcal{C}|-1} \cdot \left(\prod_{x \in \mathcal{C}} (2 \cdot c_x + 2) \right) = \mathcal{O}(2^{(|\mathcal{C}| \cdot \log(|\mathcal{C}| \cdot c_{\max}))})$$

$r \rightsquigarrow r'$

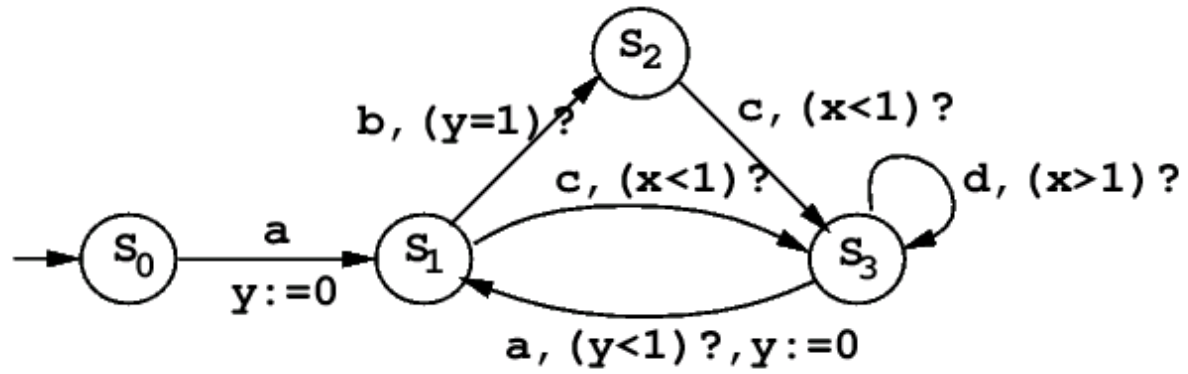


Automat „regionowy” $R(\mathcal{A})$

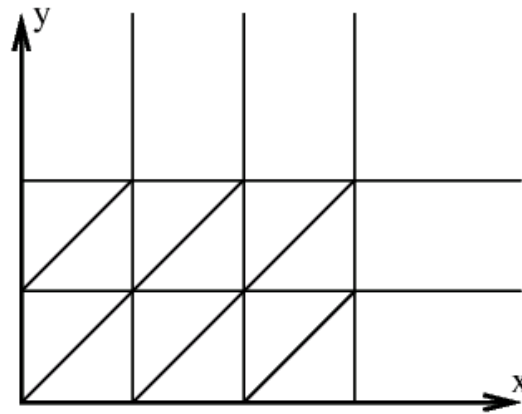
- stany: (q, r)
- tranzycje: $(q_1, r_1) \xrightarrow{a} (q_2, r_2) \iff \exists r, \langle q_1, a, \psi, \mathcal{C}', q_2 \rangle \in \rho$
 - $r_1 \rightsquigarrow r$
 - $r \models \psi \quad (r \subseteq \psi)$
 - $r_2 = r[\mathcal{C}' := 0]$

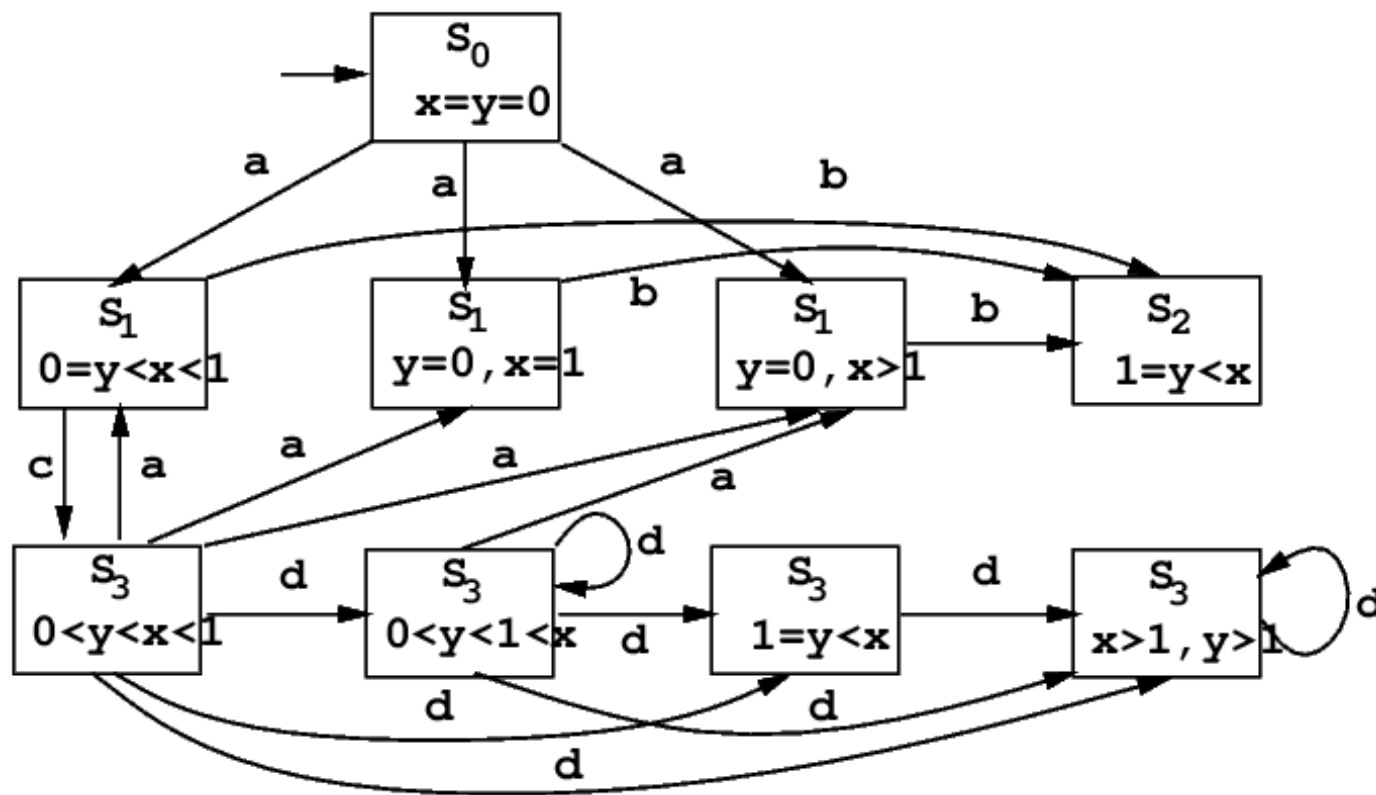
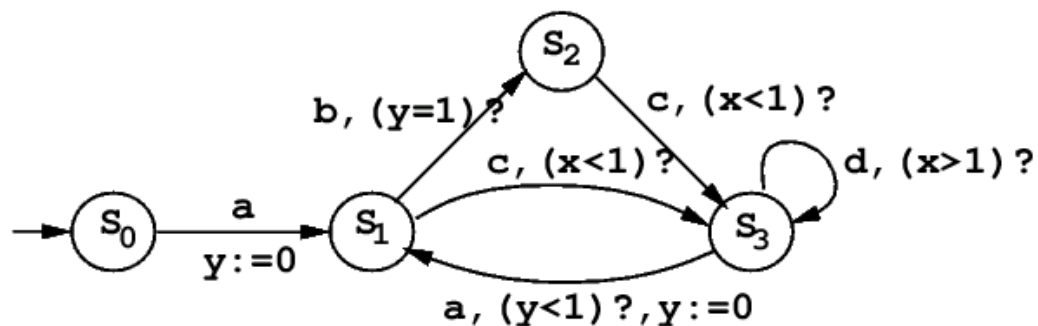
automat „symboliczny”, abstrakcyjny

$$L(R(\mathcal{A})) = \text{untime}(L(\mathcal{A}))$$



[Alur, Dill 1994]

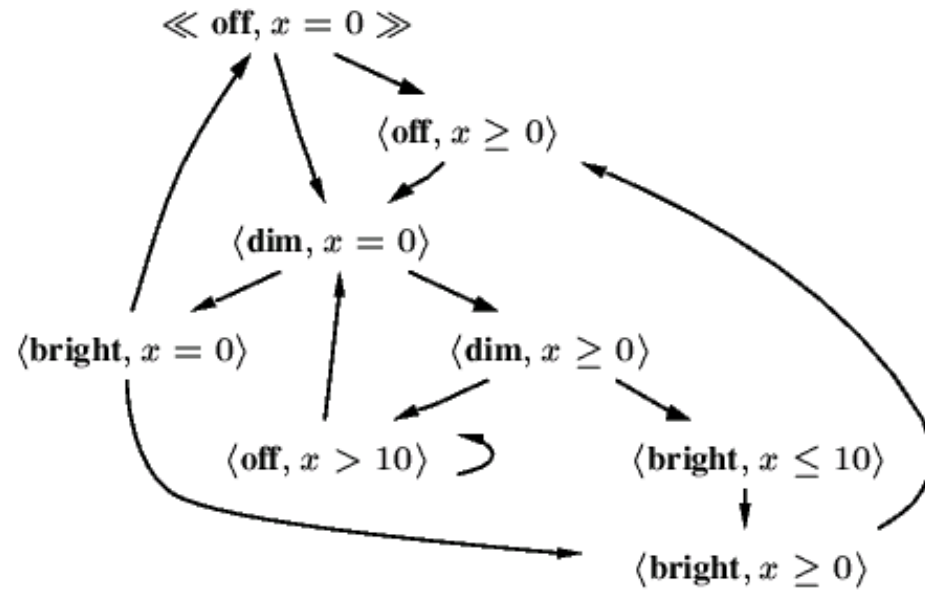
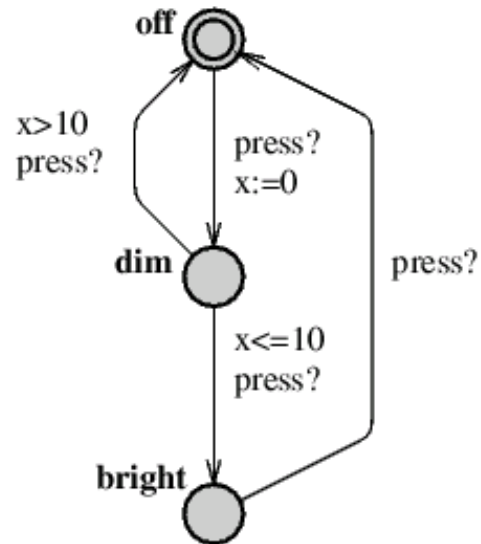




[Alur, Dill 1994]

Automat „strefowy” $Z(A)$

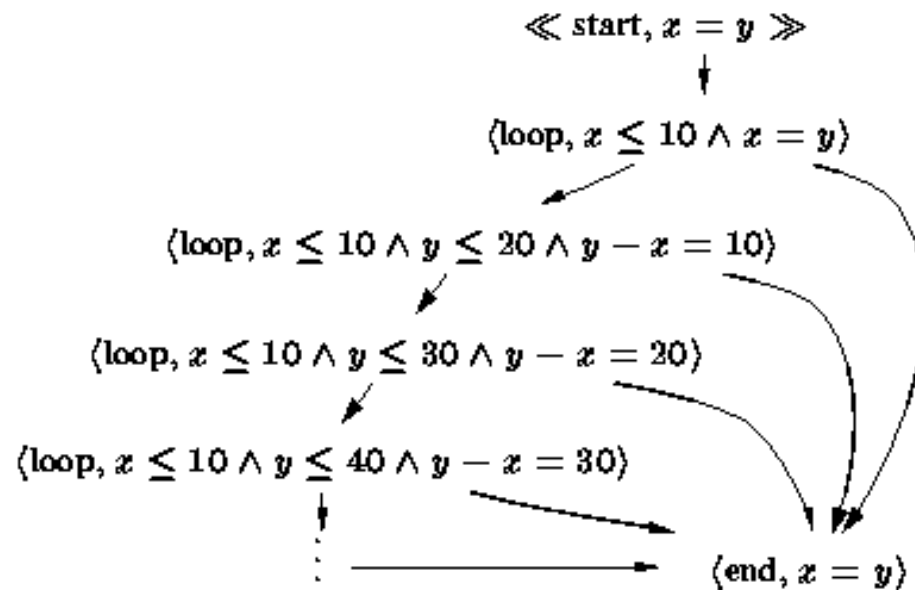
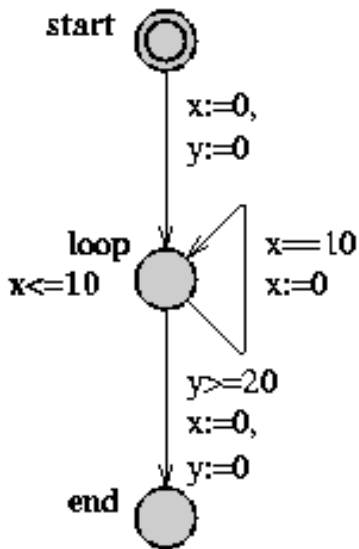
- stany: (q, ψ)
- tranzycje:
 - $(q, \psi) \rightsquigarrow (q, \psi \rightsquigarrow \wedge \text{niezm}(q))$
 - $(q_1, \psi_1) \xrightarrow{a} (q_2, (\psi_1 \wedge \psi)[\mathcal{C}' := 0] \wedge \text{niezm}(q_2))$
jeśli $\langle q_1, a, \psi, \mathcal{C}', q_2 \rangle \in \rho$

$Z(\mathcal{A})$ 

[Bengtsson, Yi 2004]

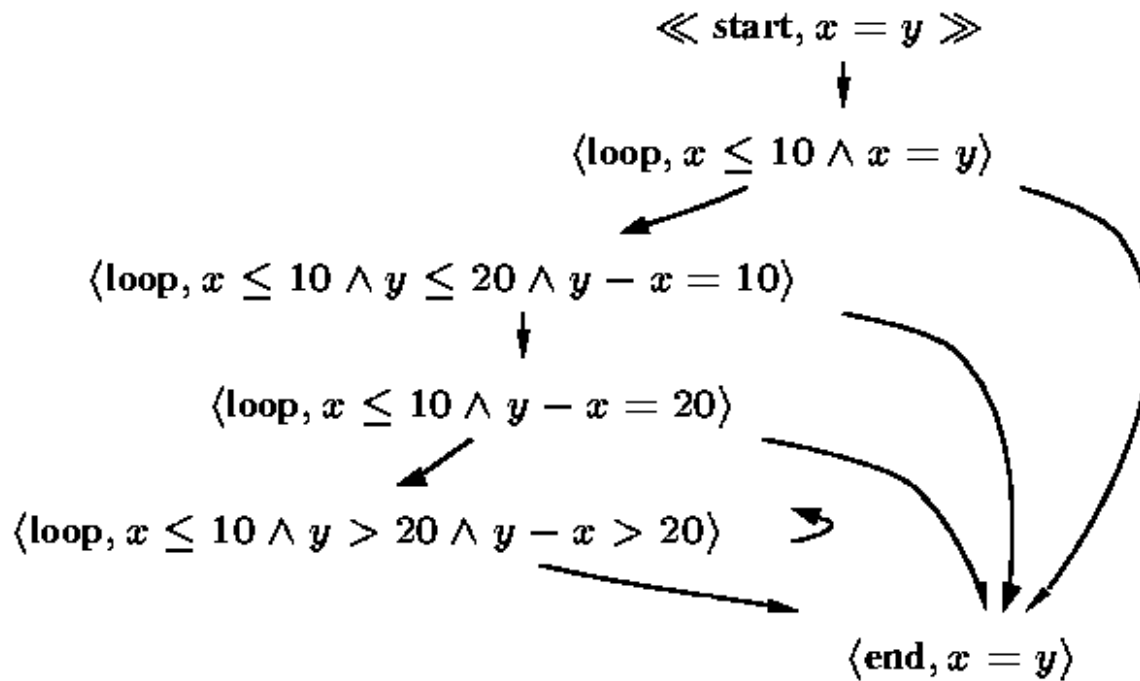
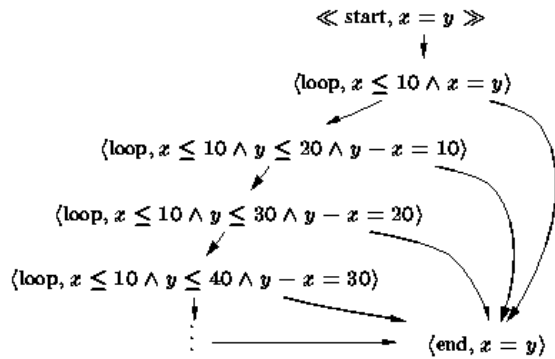
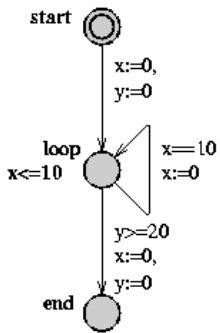
 $R(\mathcal{A})$ ma > 50 stanów !

$Z(\mathcal{A})$ o nieskończenie wielu stanach



[Bengtsson, Yi 2004]

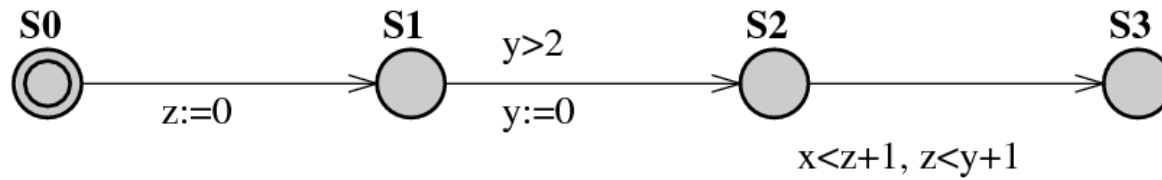
Przykład – po znormalizowaniu



[Bengtsson, Yi 2004]

normalizacja nie zawsze jest poprawna! (dozory różnicowe)

Niepoprawność normalizacji



[Bengtsson, Yi 2004]

$$\langle S_2, x-y > 2 \wedge x > 2 \rangle \xrightarrow{\text{normalizacja}} \langle S_2, x-y > 1 \wedge x > 1 \rangle$$

I. Logiki czasowe

$M(\mathcal{A})$

- stany: $\langle q, v \rangle \in Q \times (\mathbb{R}^+)^c$
- stany pocz.: $\langle q_0, v_0 \rangle$
- tranzycje: $\langle q, v \rangle \xrightarrow{t} \langle q, v + t \rangle$ $\langle q, v \rangle \xrightarrow{a} \langle q', v' \rangle$
- $L(\langle q, v \rangle) = L(q) \cup \{\psi : v \models \psi\}$

determinizm: $s \xrightarrow{t} s', s \xrightarrow{t} s'' \implies s' = s''$

gęstość: $s \xrightarrow{t_1+t_2} s' \iff \exists s''. s \xrightarrow{t_1} s'' \xrightarrow{t_2} s'$

Rozszerzamy CTL*_{-X}

formuły stanowe:

 $s \models \phi$

$$\phi ::= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \mathbf{E} \psi$$

formuły ścieżkowe:

 $\Pi \models \psi$

$$\psi ::= \phi \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \psi_1 \mathbf{U}_I \psi_2$$

 I – przedziałnp. $\prec c$, $\prec \in \{<, \leq, >, \geq, =\}$

$$M \models \phi \quad M(\mathcal{A}) \models \phi \quad \mathcal{A} \models \phi$$

ścieżka: $\Pi = s_0 \xrightarrow{t_0} s'_0 \xrightarrow{a_0} s_1 \xrightarrow{t_1} s'_1 \xrightarrow{a_1} \dots$ ($\sum_i t_i$ nieogr.)

sygnał: $\Pi = \cdot \xrightarrow{a_0} t_0 \xrightarrow{a_1} t_0 + t_1 \dots$

$s_0 \models \phi_1 \mathbf{U}_I \phi_2$ wtw gdy $\exists \Pi$ j. w., $t \in I$.

$$\Pi^t \models \phi_2 \wedge \forall 0 < t' < t. \Pi^{t'} \models \phi_1$$

Uwaga: kwantyfikacja po $t \in \mathbb{R}^+$

TLTL (MTL):

$$\mathbf{G} (p \implies \mathbf{F}_{=1} q)$$

$$\mathbf{F}_{\leq 10} p \wedge \mathbf{F}_{\geq 5} p \qquad \mathbf{F}_{\langle 5,10 \rangle} p$$

$$\mathbf{G} \mathbf{F}_{\leq 1} p$$

TCTL:

$$\mathbf{AG} (p \implies \mathbf{AF}_{\leq 3} q)$$

$$\mathbf{AG} (p \implies \mathbf{AF} q \wedge x \leq 3)$$

$\phi \in \dots$	$M \models \phi$	spełnialność ϕ
LTL	PSPACE	PSPACE
CTL	P	EXPTIME

$\phi \in \dots$	$M(\mathcal{A}) \models \phi$	spełnialność ϕ
TLTL (MTL)	nierozstrzygalna	nierozstrzygalna
TCTL	PSPACE	nierozstrzygalna

- TLTL: punktualność (MITL)
- TLTL: słowa skończone lub ω -słowa
- TLTL: semantyka punktowa
- TCTL: 1 lub 2 zegary

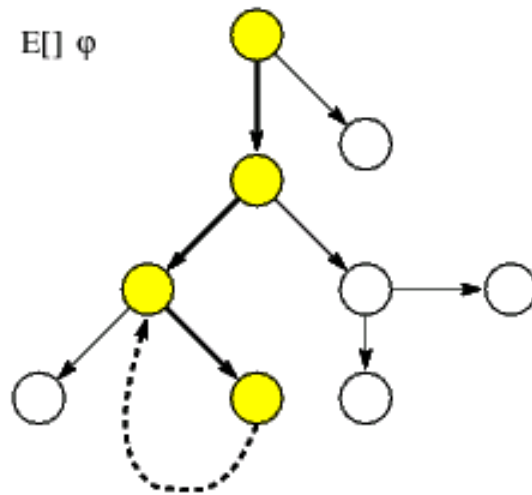
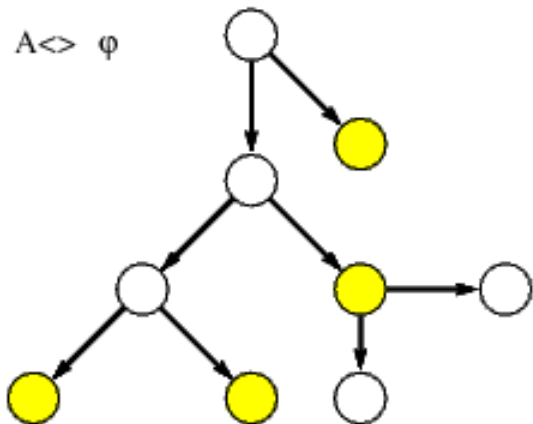
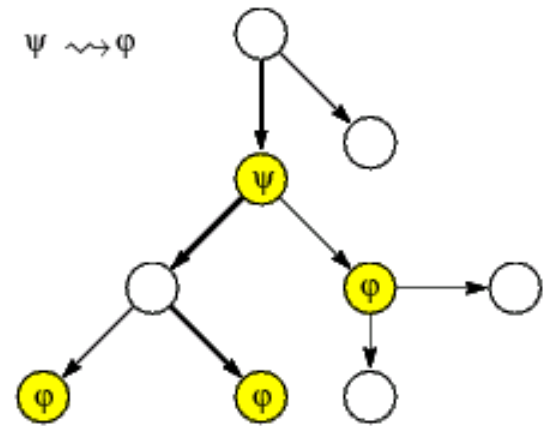
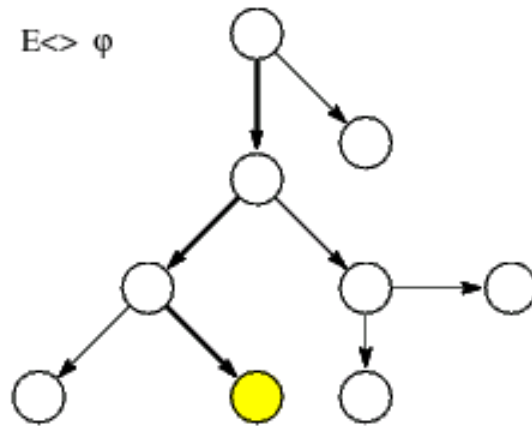
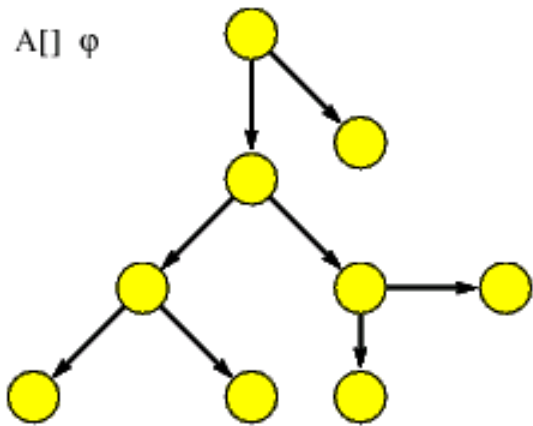
TLTL:

$$\mathbf{G} (p \implies x. \mathbf{F} (q \wedge y. \mathbf{F} (r \wedge y < 5 \wedge x \leq 10)))$$

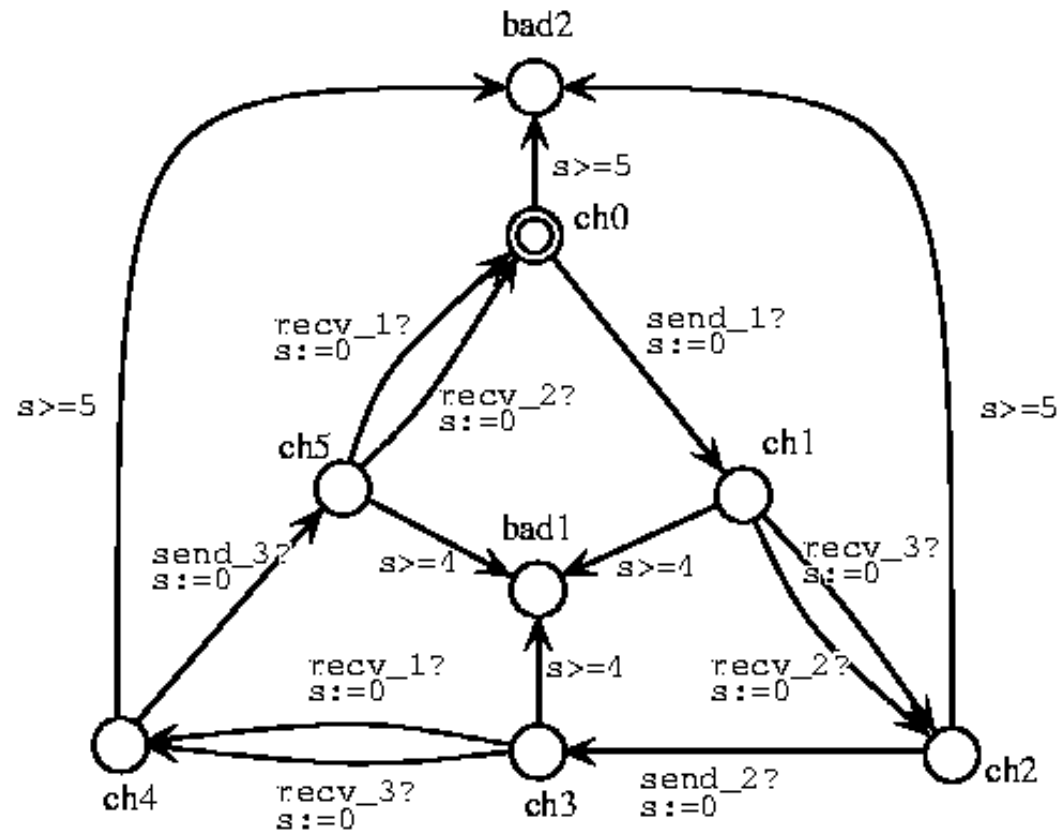
$$x. \mathbf{F} (p \wedge x \leq 1 \wedge \mathbf{G} (x \leq 1 \implies p))$$

TCTL:

$$\mathbf{EF} x. (p \wedge \mathbf{EF} (q \wedge \mathbf{EF} (r \wedge x < 5)))$$



Automaty testujące



```

PASSED:= {}
WAIT:= {(l0, D0)}
repeat
  begin
    get (l, D) from WAIT
    if (l, D) ⊨ φ then return “YES”
    else if D ⊈ D' for all (l, D') ∈ PASSED then
      begin
        add (l, D) to PASSED      (*)
        NEXT:={ (ls, Ds) : (l, D) ~→ (ls, Ds) ∧ Ds ≠ ∅ }
        for all (ls', Ds') in NEXT do
          put (ls', Ds') to WAIT
        end
      end
    end
  until WAIT={ }
return “NO”

```

[Bengtsson, Yi 2004]

II. DBMs

Difference-Bound Matrix

DBM = reprezentacja strefy

$$x_i - x_j \prec_{ij} c_{ij}$$

$$\prec_{ij} \in \{<, \leq\}$$

$$x_i - x_j \prec_{ij} c_{ij}$$

$$\mapsto -c_{ji} \prec_{ji} x_i - x_j \prec_{ij} c_{ij}$$

$$x_j - x_i \prec_{ji} c_{ji}$$

$$x_i - 0 \prec_{i0} c_{i0}$$

$$\mapsto -c_{0i} \prec_{0i} x_i \prec_{i0} c_{i0}$$

$$0 - x_i \prec_{0i} c_{0i}$$

strefa:

$$\{x < 20, y \leq 20, y - x = 10, \dots\}$$

$$\{x - 0 < 20, y - 0 \leq 20, y - x \leq 10, x - y \leq -10, 0 - z < 5\}$$

macierz ją reprezentująca:

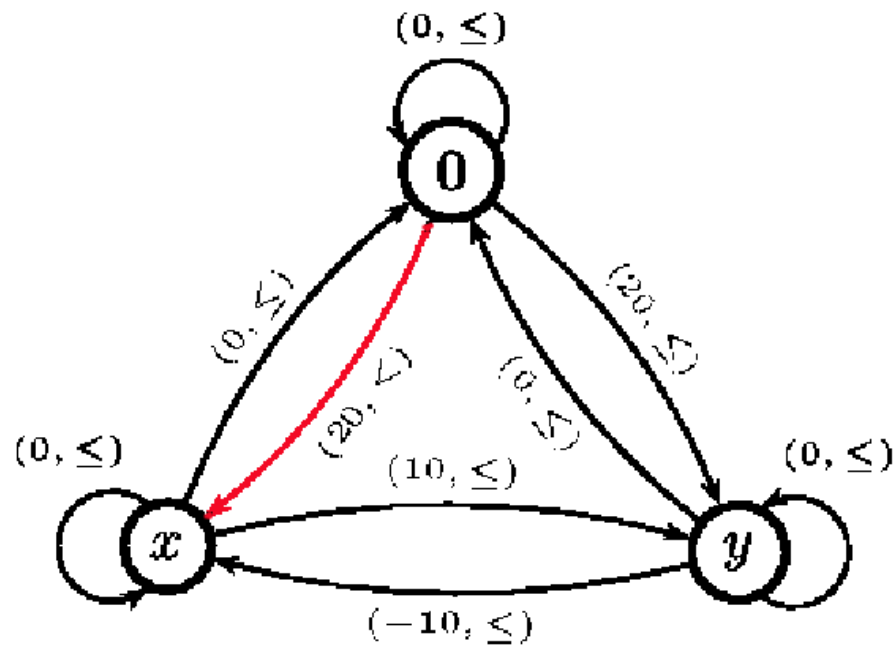
$$\begin{pmatrix} (0, \leq) & (0, \leq) & (0, \leq) & (5, <) \\ (20, <) & (0, \leq) & (-10, \leq) & \infty \\ (20, \leq) & (10, \leq) & (0, \leq) & \infty \\ \infty & \infty & \infty & (0, \leq) \end{pmatrix}$$

[Bengtsson, Yi 2004]

strefa:

$$\{x - 0 < 20, y - 0 \leq 20, y - x \leq 10, x - y \leq -10\}$$

graf ją reprezentujący:

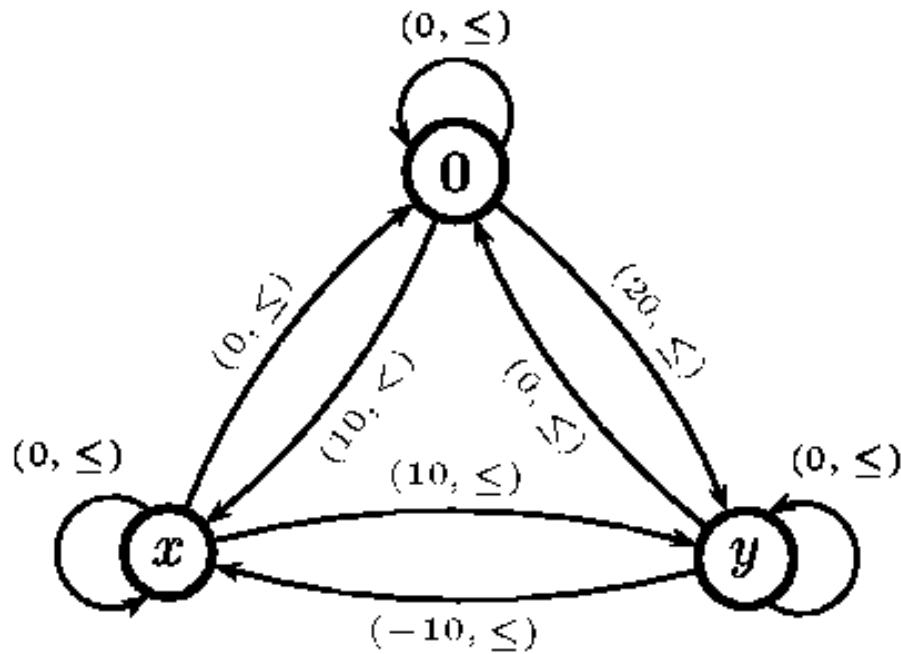


[Bengtsson, Yi 2004]

strefa:

$$\{x - 0 < 20, y - 0 \leq 20, y - x \leq 10, x - y \leq -10\}$$

graf **kanoniczny** ją reprezentujący:



[Bengtsson, Yi 2004]

$$x_i - x_j \prec_{ij} c_{ij}$$

$$\prec_{ij} \in \{<, \leq\}$$

$$c'_{ij} := c_{ij} + c_{jk}$$
$$\prec'_{ik} := \begin{cases} \leq & \text{gdy } \prec_{ij} = \leq \wedge \prec_{jk} = \leq \\ < & \text{w p.p.} \end{cases}$$

jeśli $\langle c'_{ik}, \prec'_{ik} \rangle$ silniejsze niż $\langle c_{ik}, \prec_{ik} \rangle$ to zastąp
(∞ jest zawsze słabsze)

Czas $O(n^3)$

Operacje na strefach (macierzach):

– $D \neq \emptyset$? \iff nie ma cyklu < 0

$$-c_{ji} \prec_{ji} x_i - x_j \prec_{ij} c_{ij} \quad -c_{ji} \prec' c_{ij}$$

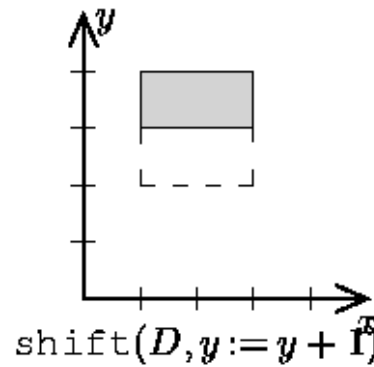
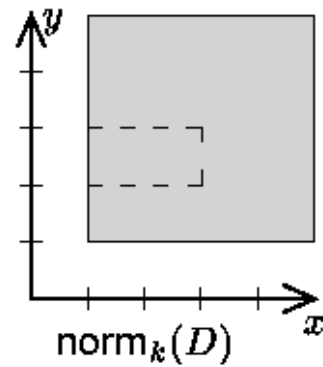
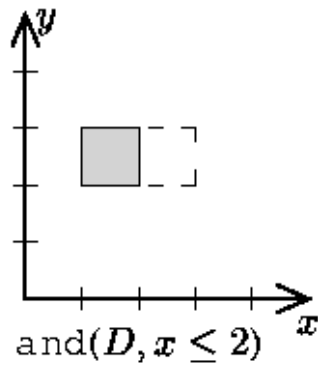
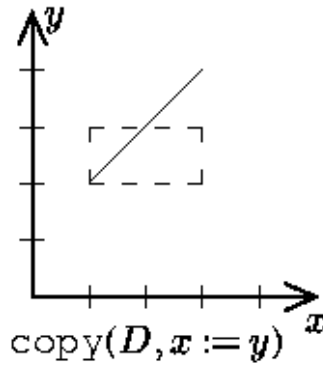
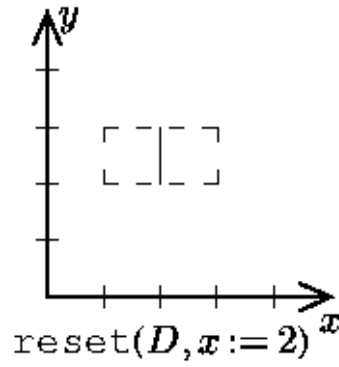
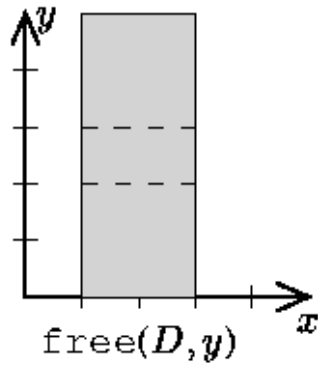
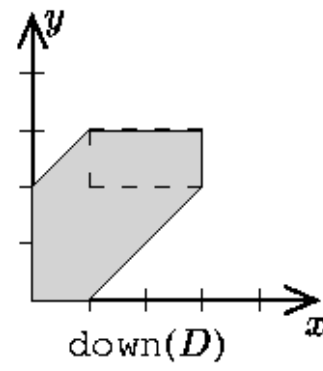
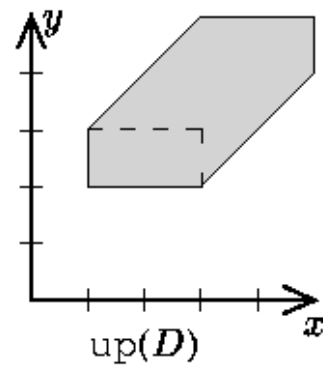
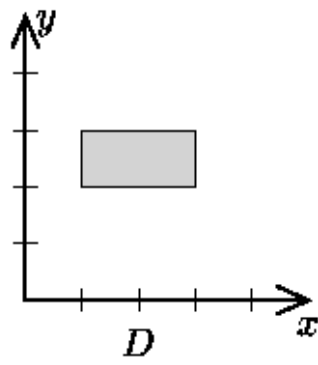
– $D \subseteq D'$?

– $D \rightsquigarrow \text{up}(D) \quad \text{down}(D)$

– $D \wedge \psi \quad D_1 \wedge D_2$

– $D[C' := 0]$

– ...



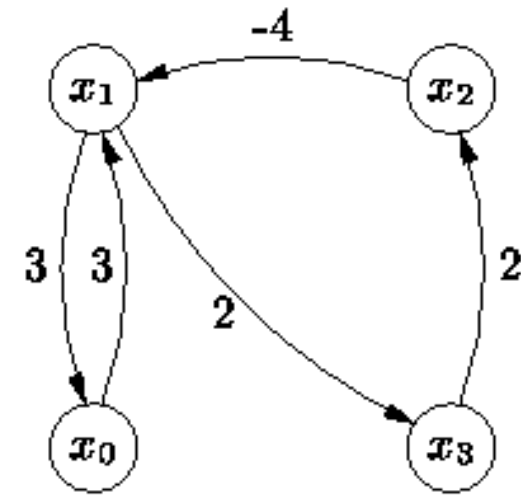
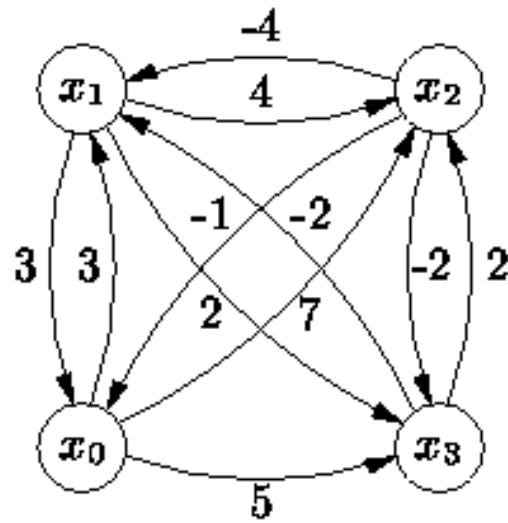
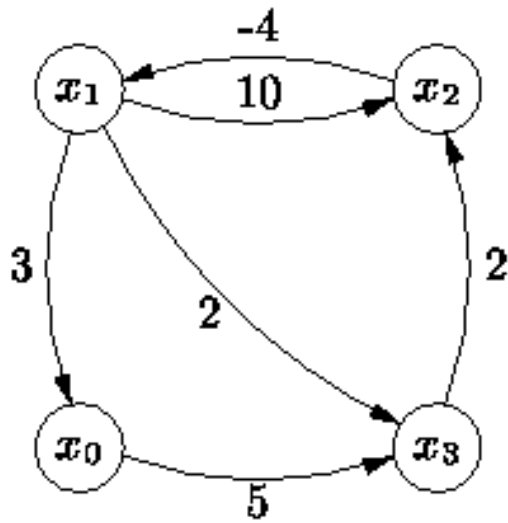
[Bengtsson, Yi 2004]

Operacje na strefach c.d.:

- $D_1 \vee D_2$

- ...

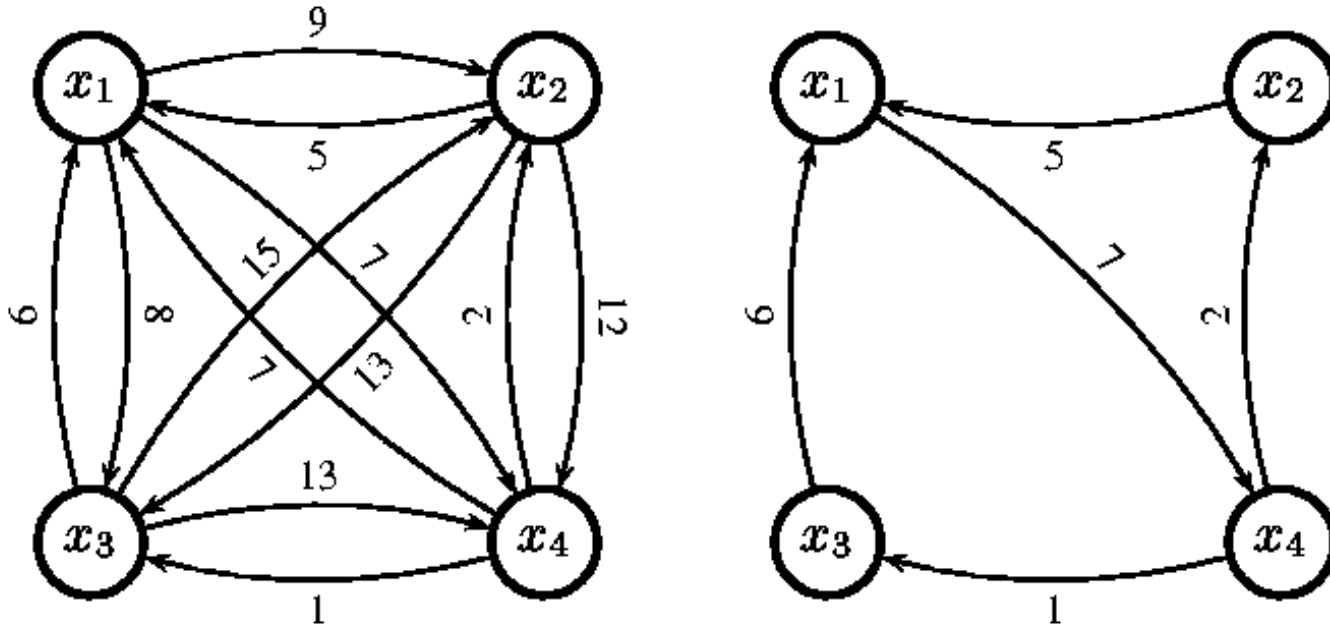
Reprezentacja minimalna



[Bengtsson, Yi 2004]

kanoniczność reprezentacji

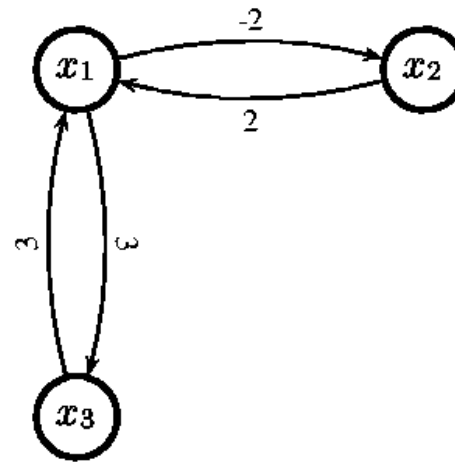
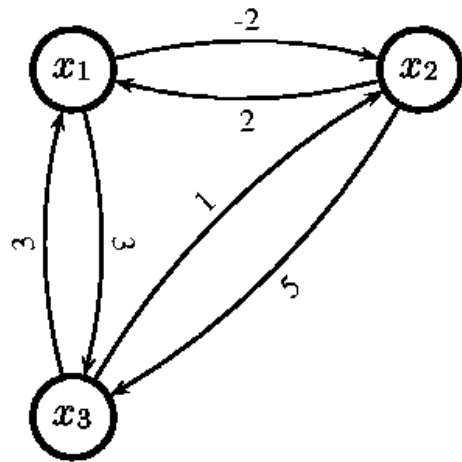
Reprezentacja minimalna



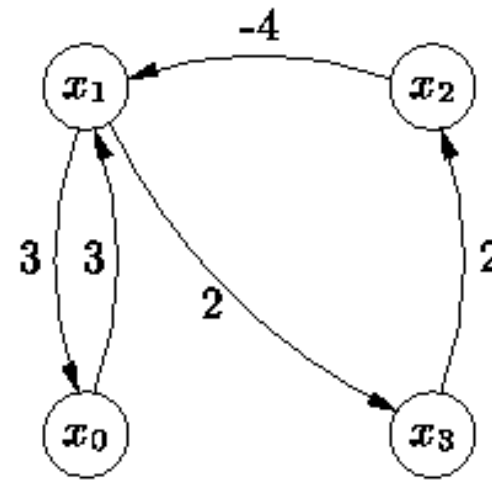
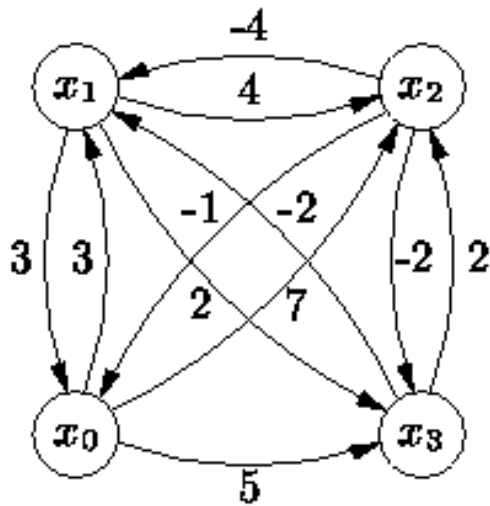
[Bengtsson, Yi 2004]

- eliminacja krawędzi nadmiarowych, gdy nie ma 0-cykli
- usunięcie krawędzi nadmiarowej nie wpływa na pozostałe

Reprezentacja minimalna (0-cykle)



[Bengtsson, Yi 2004]



III. CDDs

```

PASSED:= {}
WAIT:= {(l0, D0)}
repeat
  begin
    get (l, D) from WAIT
    if (l, D) ⊨ φ then return “YES”
    else if D ⊈ D' for all (l, D') ∈ PASSED then
      begin
        add (l, D) to PASSED (*)
        NEXT:= {(ls, Ds) : (l, D) ~> (ls, Ds) ∧ Ds ≠ ∅}
        for all (ls', Ds') in NEXT do
          put (ls', Ds') to WAIT
        end
      end
    end
  until WAIT= {}
return “NO”

```

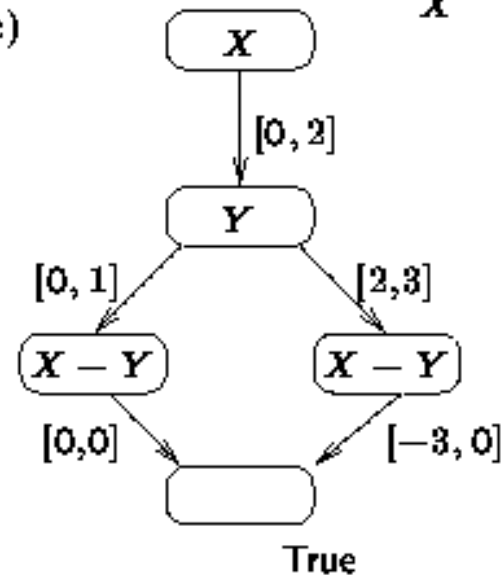
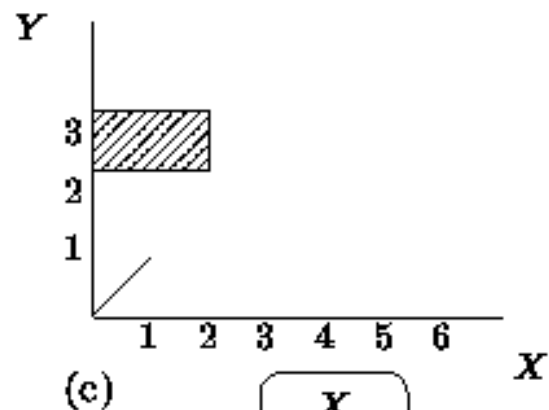
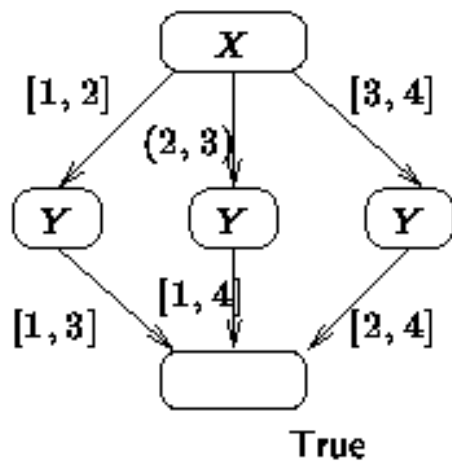
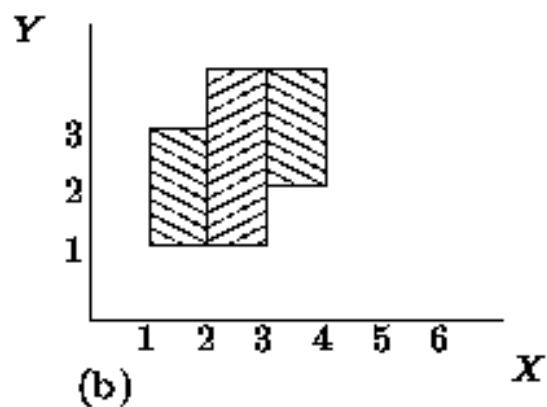
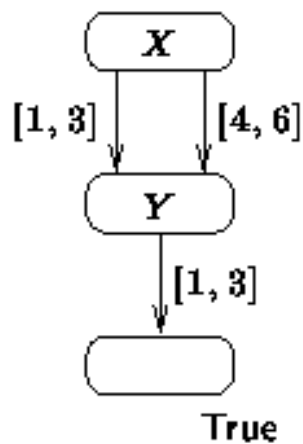
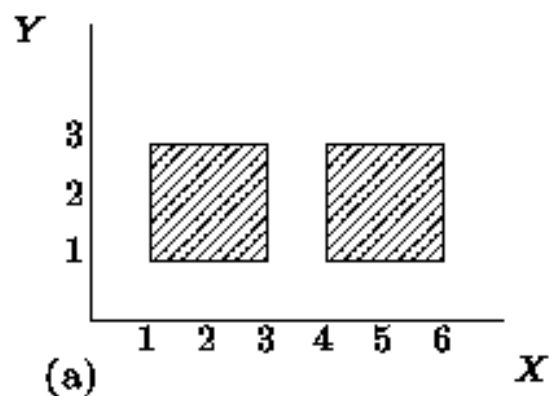


bardziej symbolicznie ?

Różne czasowe adaptacje BDDs:

- IDD
- DDD
- CDD
- ...

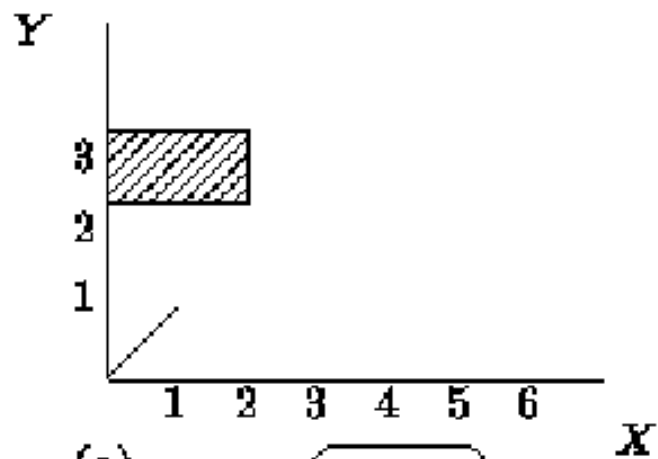
CDD = suma skończenie wielu stref



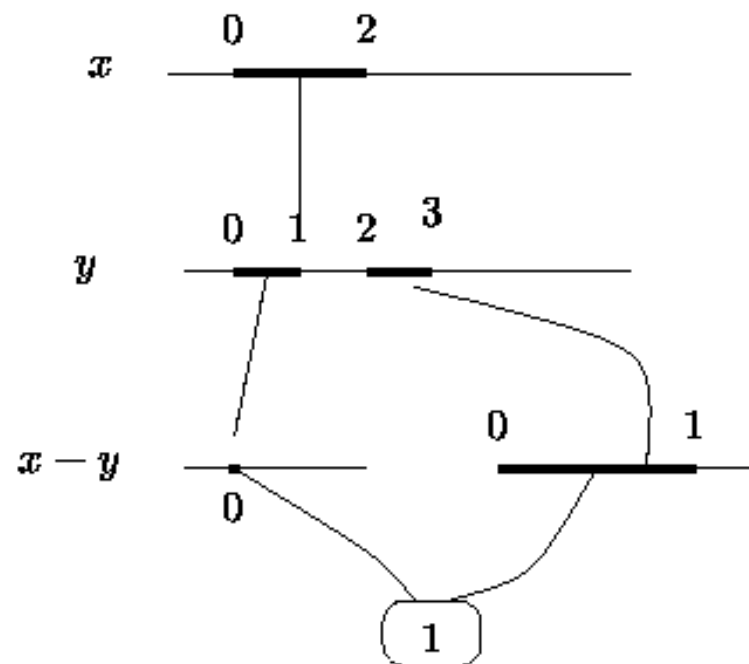
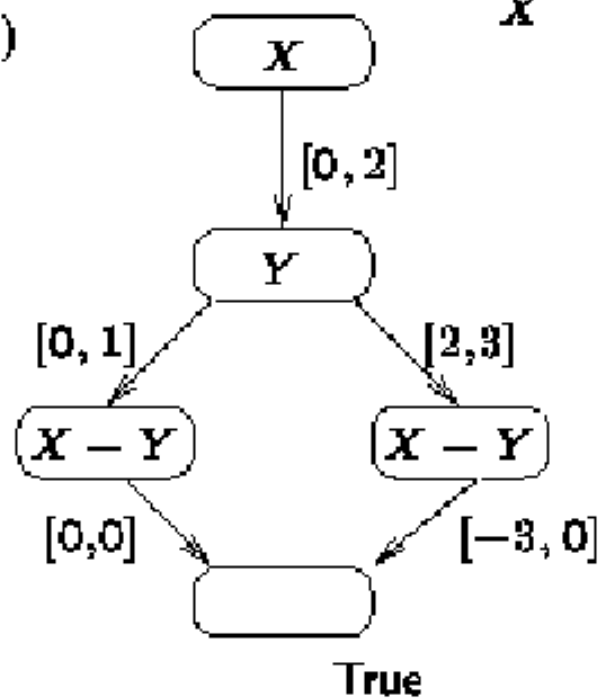
[Larsen, Pearson, Weise, Yi 1999]

CDD (zamiast porządkowej definicji :)

- przestrzega porządku
- następniki wyznaczają podział \mathbb{R} na odcinki

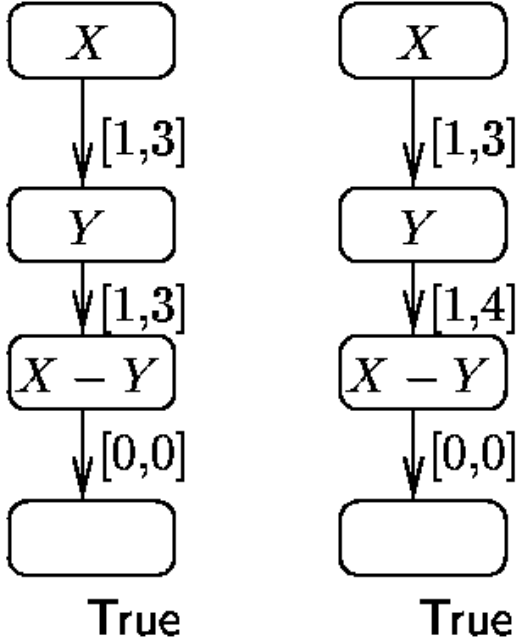
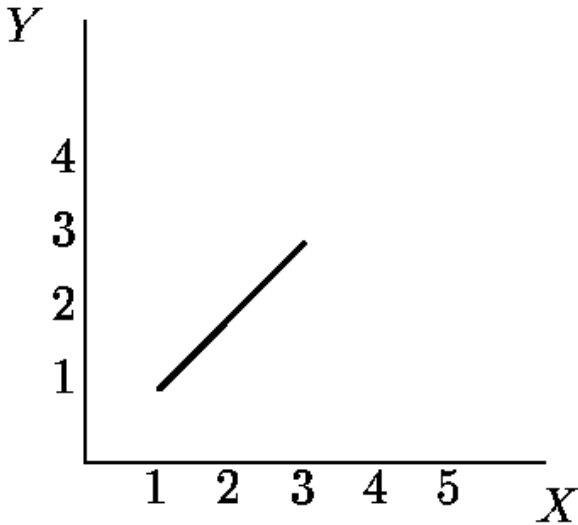


(c)



[Larsen, Pearson, Weise, Yi 1999]

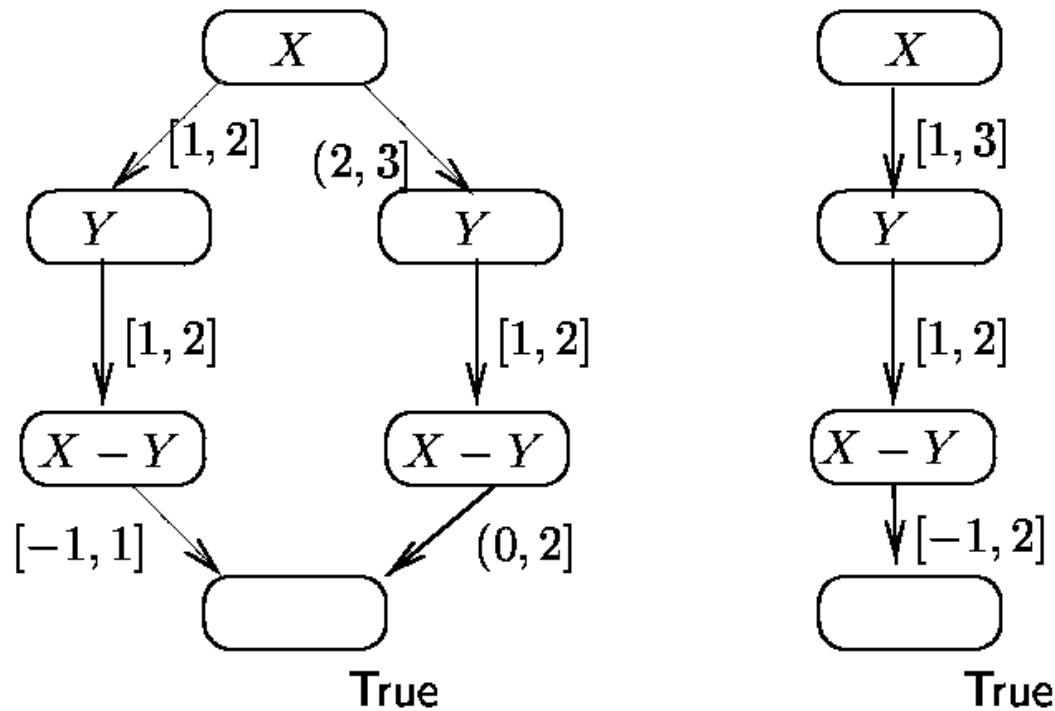
Brak kanoniczności !



[Larsen, Pearson, Weise, Yi 1999]

Dodatkowe założenie:
każda ścieżka jest „kanonicznym DBM'em”.

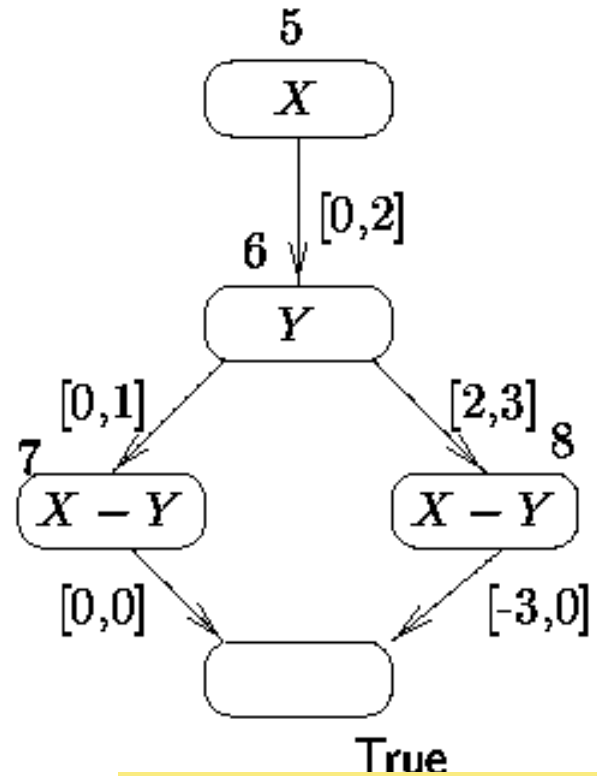
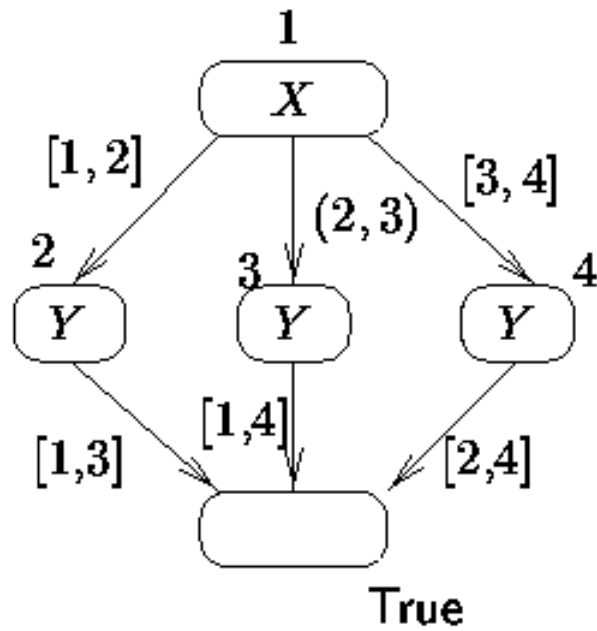
Wciąż brak kanoniczności !



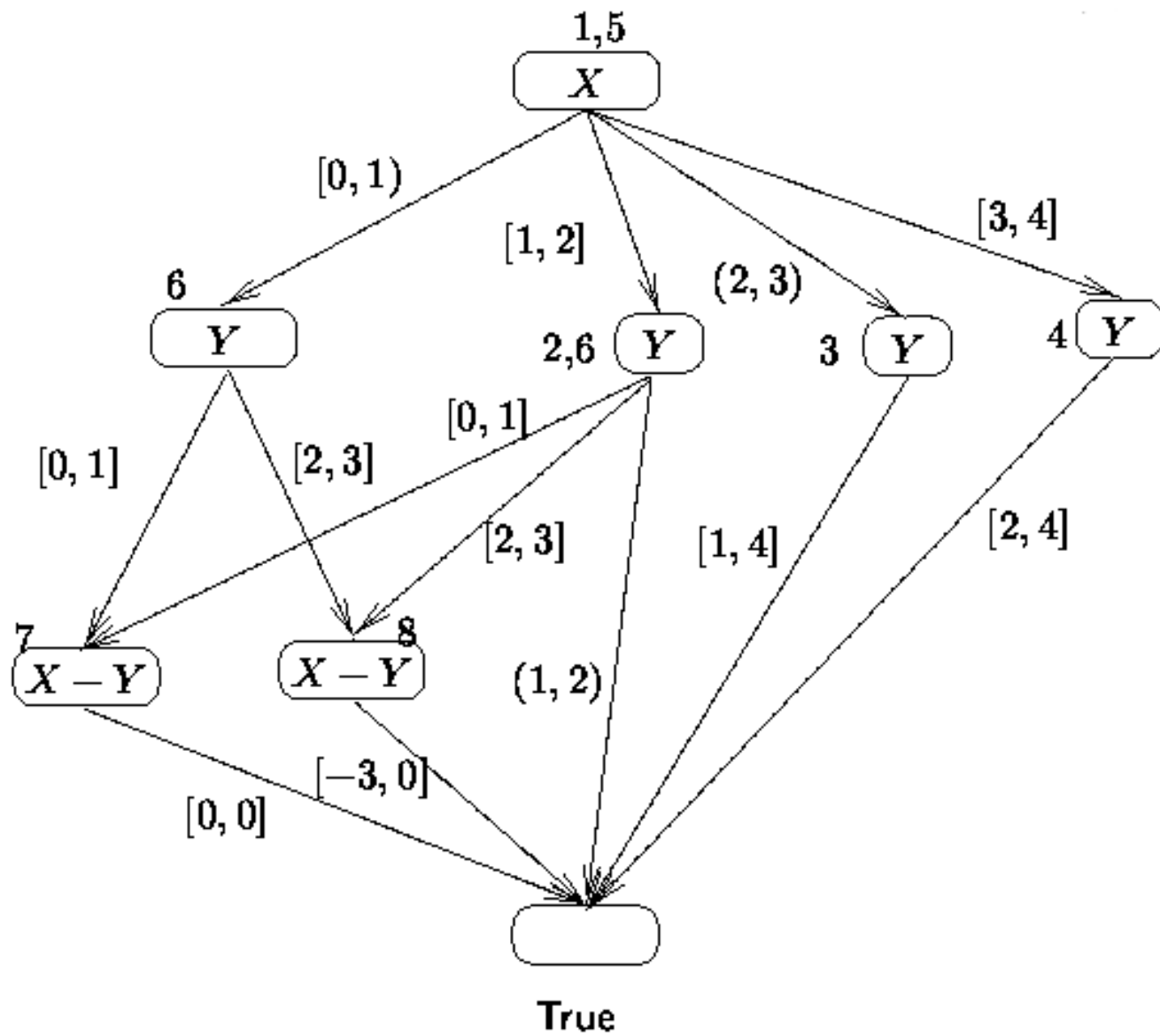
[Larsen, Pearson, Weise, Yi 1999]

Operacje na CDDs – przykład

$op(D_1, D_2)$



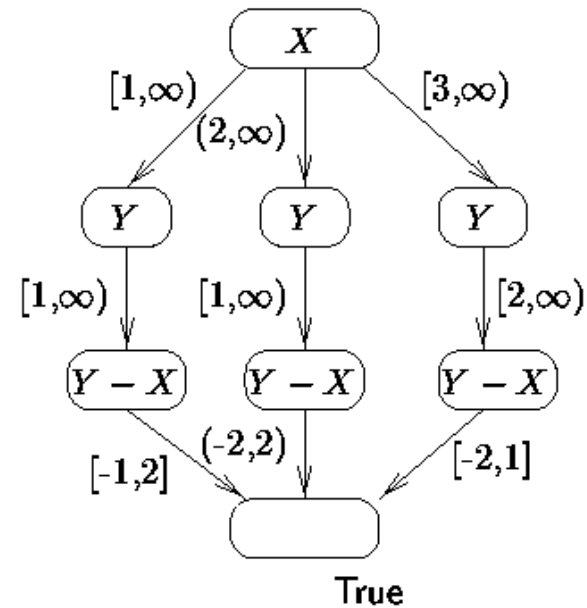
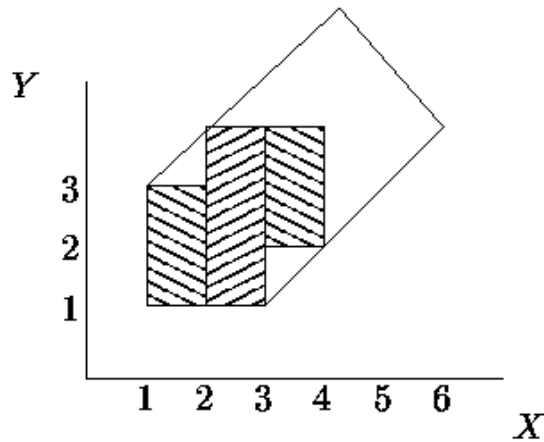
[Larsen, Pearson, Weise, Yi 1999]



[Larsen, Pearson, Weise, Yi 1999]

Operacije na CDDs

- $D_1 \subseteq D_2 \iff D_1 \cap \neg D_2 = \emptyset$
- $D \rightsquigarrow$



- $D[C' := 0]$

[Larsen, Pearson, Weise, Yi 1999]