Praktyczne metody weryfikacji

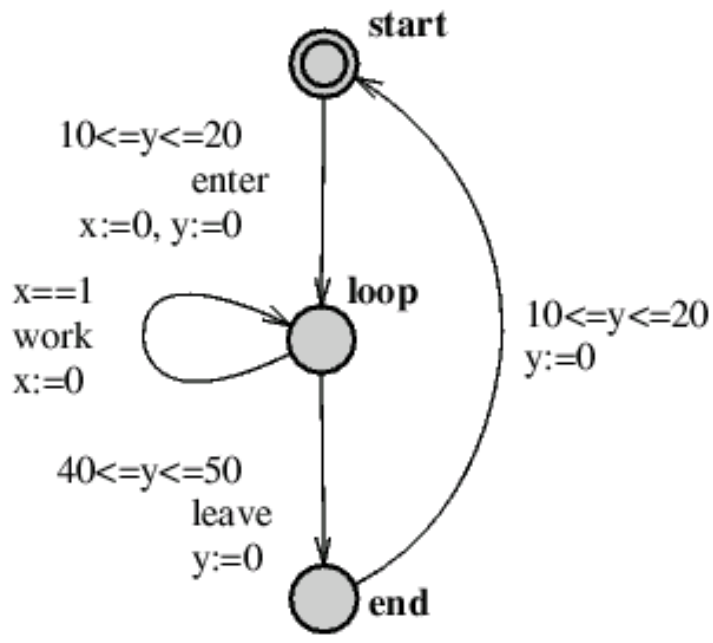
Wykład 11: Automaty czasowe

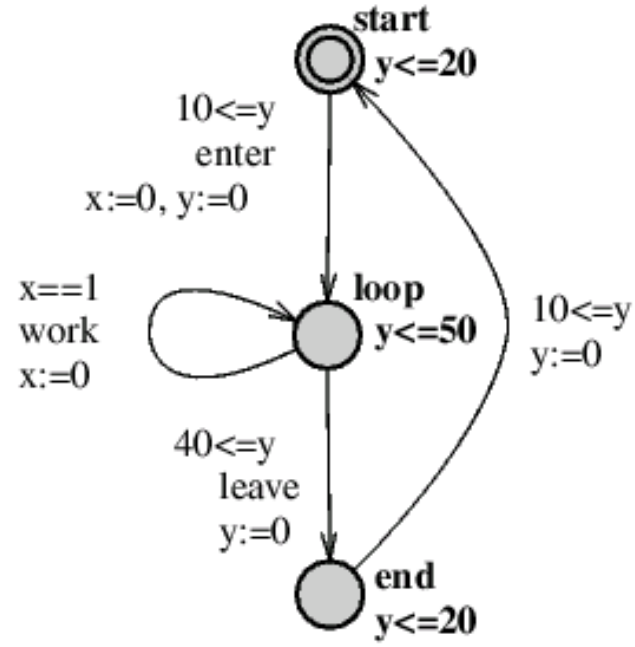
Jak modelować upływ czasu ?

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

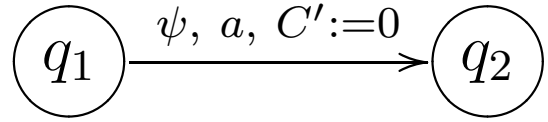
Dozory, niezmiennniki : $\Psi(\mathcal{C})$

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

$\prec \in \{<, \leq, >, \geq\}$
$c \in \mathbb{Q}^+ \quad (c \in \mathbb{N})$

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 : $\langle t_1, a_1 \rangle \langle t_2, a_2 \rangle \ \ldots$ (żywotność)

nie-Zeno : $\Sigma_i t_i$ nieograniczony

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

Bieg automatu : $\langle q_0, v_0 \rangle \overset{t_1}{\rightsquigarrow} \langle q_0, v_0 + t_1 \rangle \overset{a}{\longrightarrow} \langle q_1, v_1 \rangle \overset{t_2}{\rightsquigarrow} \ \ldots$

$v_0 \vDash \mathrm{niezm}(q_0)$ $v_0 + t_1 \vDash \mathrm{niezm}(q_0)$ $v_1 \vDash \mathrm{niezm}(q_1)$

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

Warianty:

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

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

Blokada: nie istnieje t t. że

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

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

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

Pilność (niezmienniki)

Złożoność

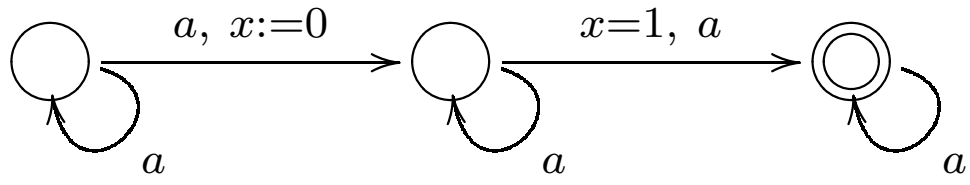
automaty	pustość	uniwersalność
bezczasowe	NLOGSPACE	PSPACE
czasowe	PSPACE	nierozstrzygalna

– $L(A) \subseteq L(B)$

– tylko 1 zegar

– słowa skończone lub ω-słowa

Brak uzupełnienia :



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

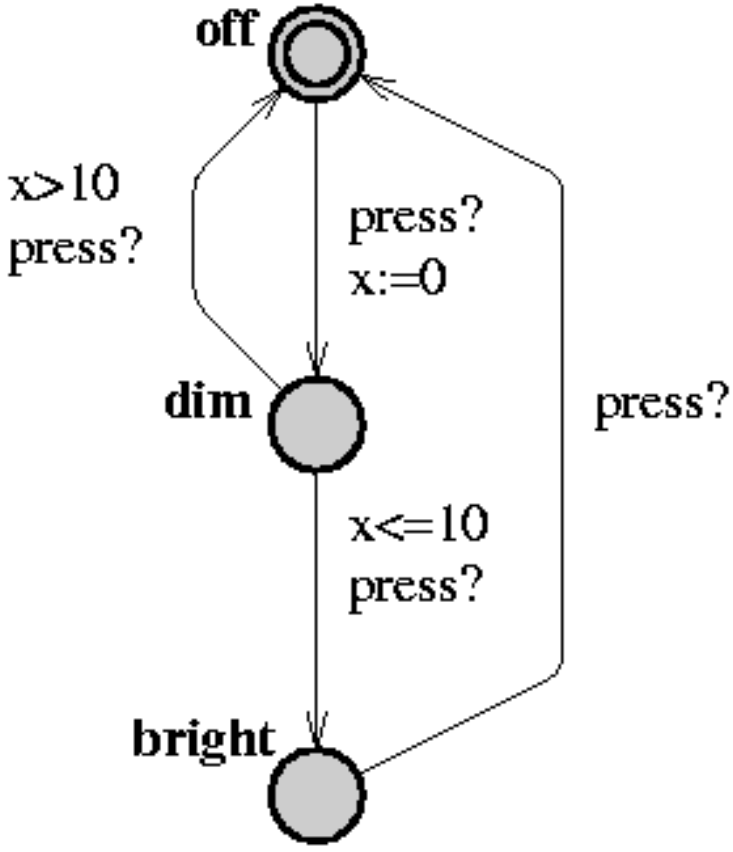
Struktura Kripkego

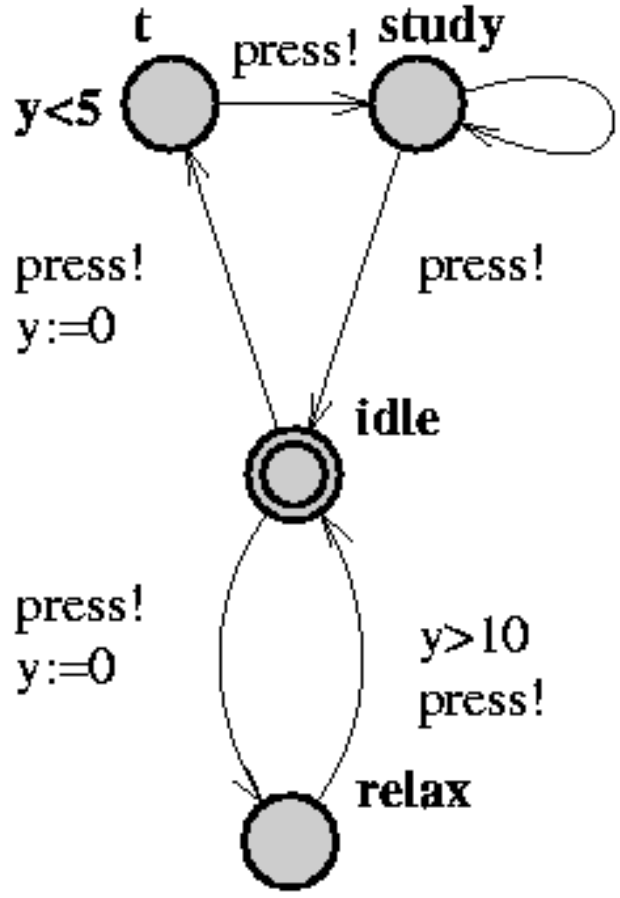
M(A)

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

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

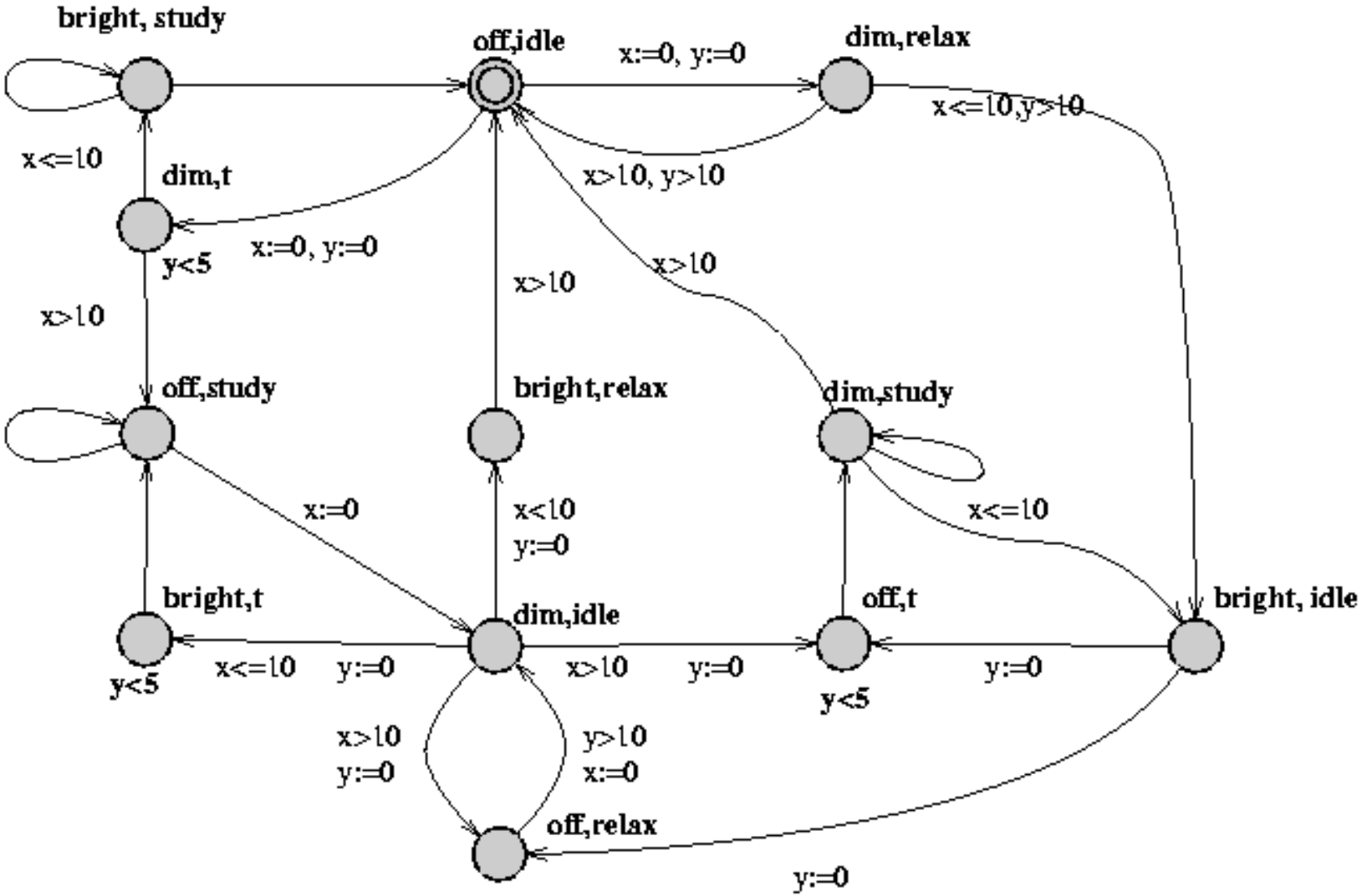
gęstość: $s \overset{t_1+t_2}{\rightsquigarrow} s' \iff \exists s''.\ s \overset{t_1}{\rightsquigarrow} s'' \overset{t_2}{\rightsquigarrow} s'$





[Bengtsson, Yi 2004]

w UPPAALu



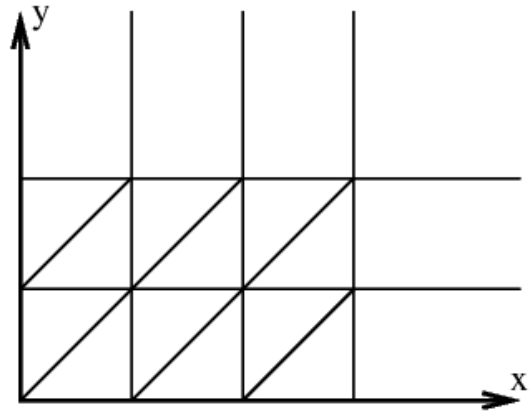
[Bengtsson, Yi 2004]

II. Regiony i strefy

$v \sim w \iff$

- albo $v(x) > c_x$ i $w(x) > c_x$ albo $\lfloor v(x) \rfloor = \lfloor w(x) \rfloor$
- $v(x) \leq c_x \implies (\langle v(x) \rangle = 0 \iff \langle w(x) \rangle = 0)$
- $v(x) \leq c_x$ i $v(y) \leq c_y \implies$

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

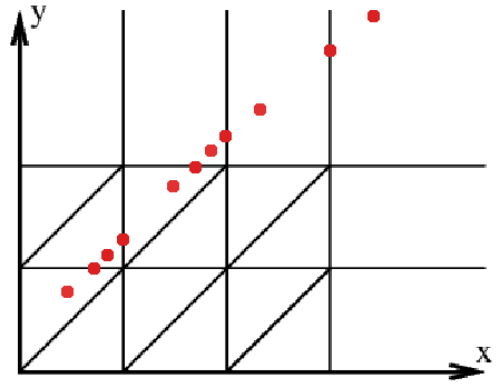


[Bengtsson, Yi 2004]

Liczba regionów:

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

$r \rightsquigarrow r'$



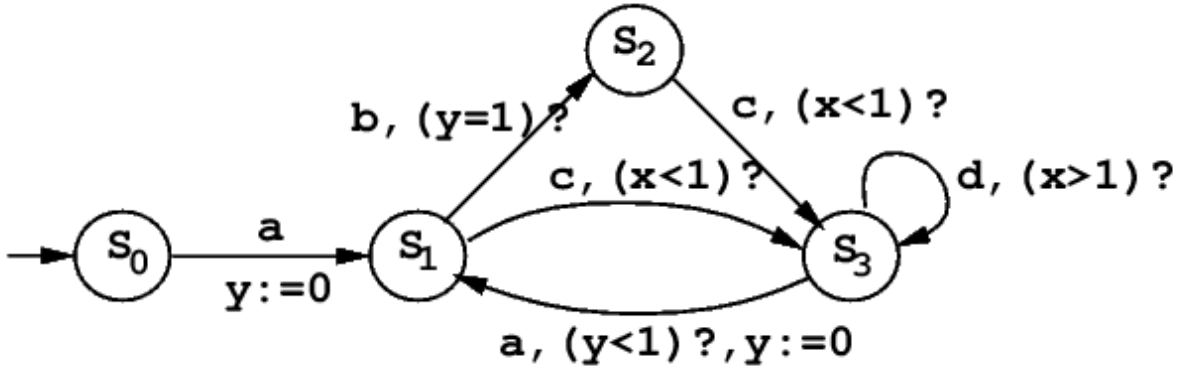
Automat „regionowy” R(A)

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

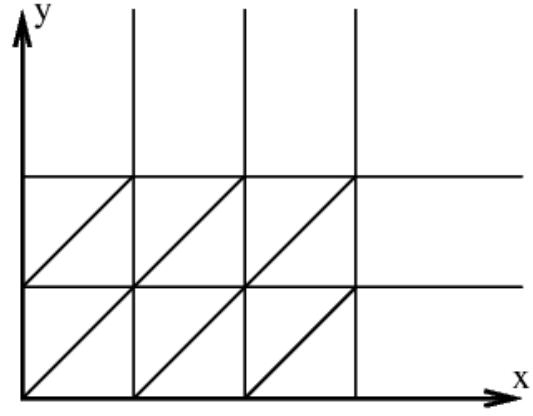
automat „symboliczny”

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

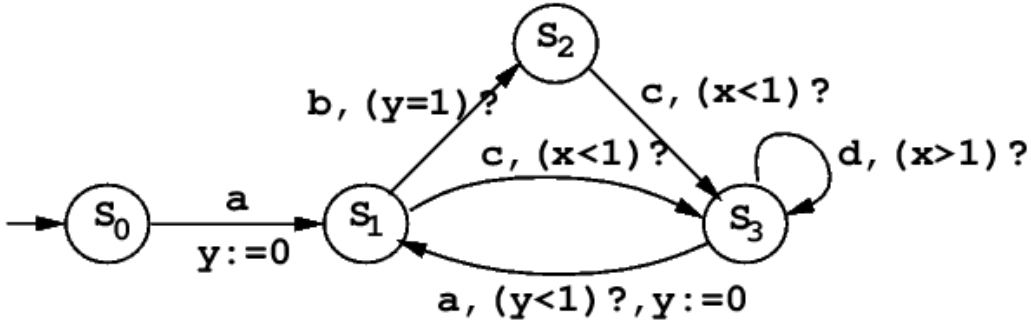
Przykład

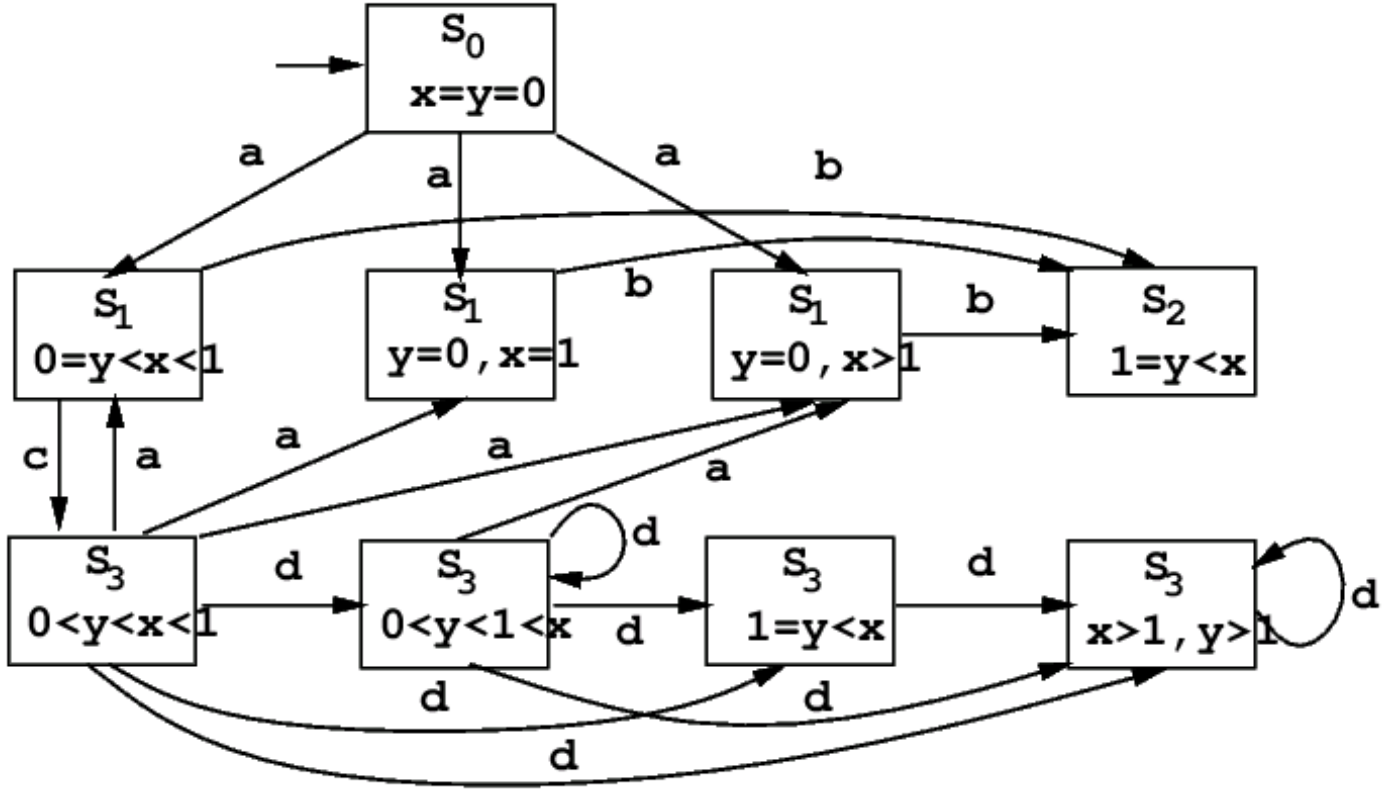


[Alur, Dill 1994]



Przykład





[Alur, Dill 1994]

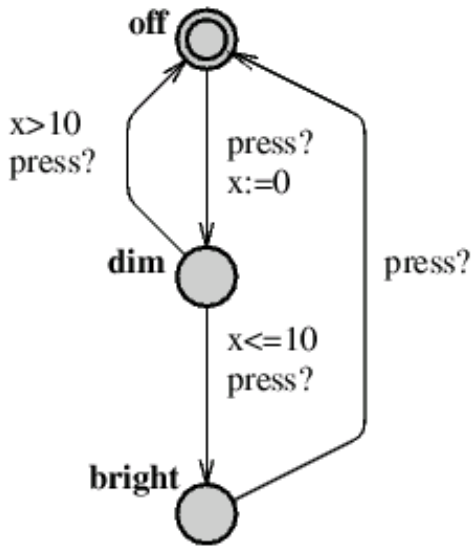
Automat „strefowy” Z(A)

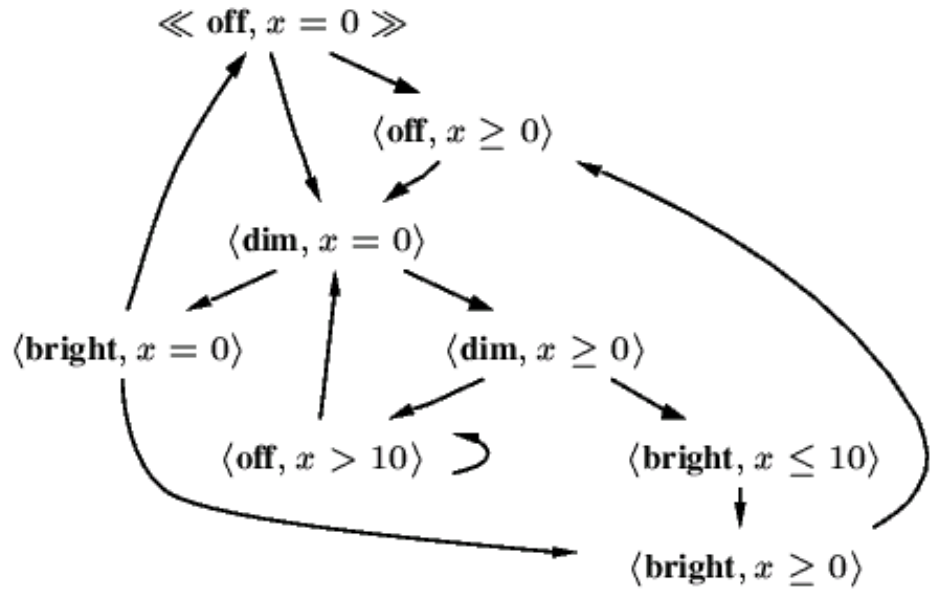
- stany: (q, ψ)
- tranzycje:
  - $(q, \psi) \rightsquigarrow (q, \psi^{\rightsquigarrow} \wedge \mathrm{niezm}(q))$
  - $(q_1, \psi_1) \xrightarrow{a} (q_2, (\psi_1 \wedge \psi)[\mathcal{C}' := 0] \wedge \mathrm{niezm}(q_2))$

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

Przykład

$Z(\mathcal{A})$



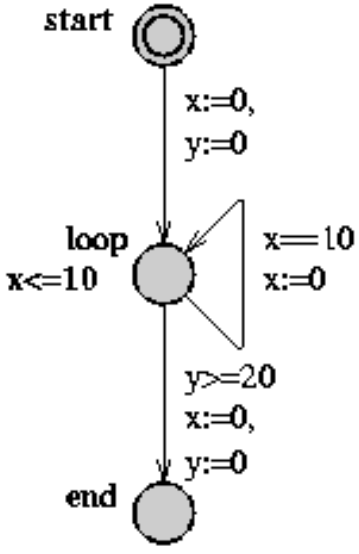


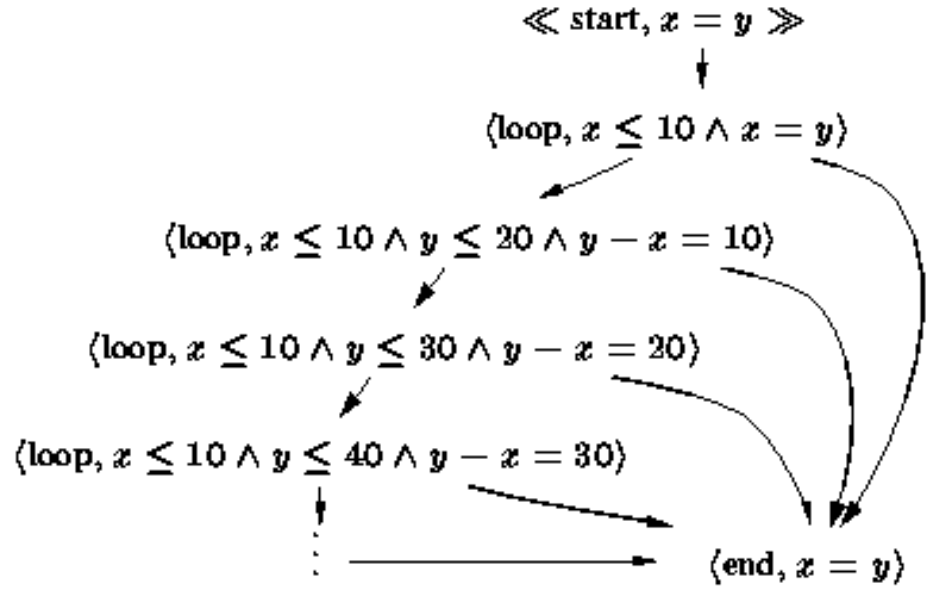
[Bengtsson, Yi 2004]

$R(\mathcal{A})$ ma > 50 stanów !

Przykład

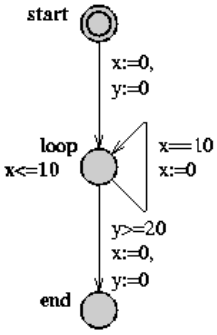
$Z(\mathcal{A})$ o nieskończenie wielu stanach

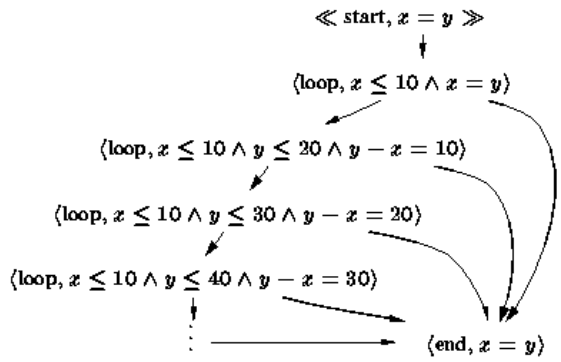


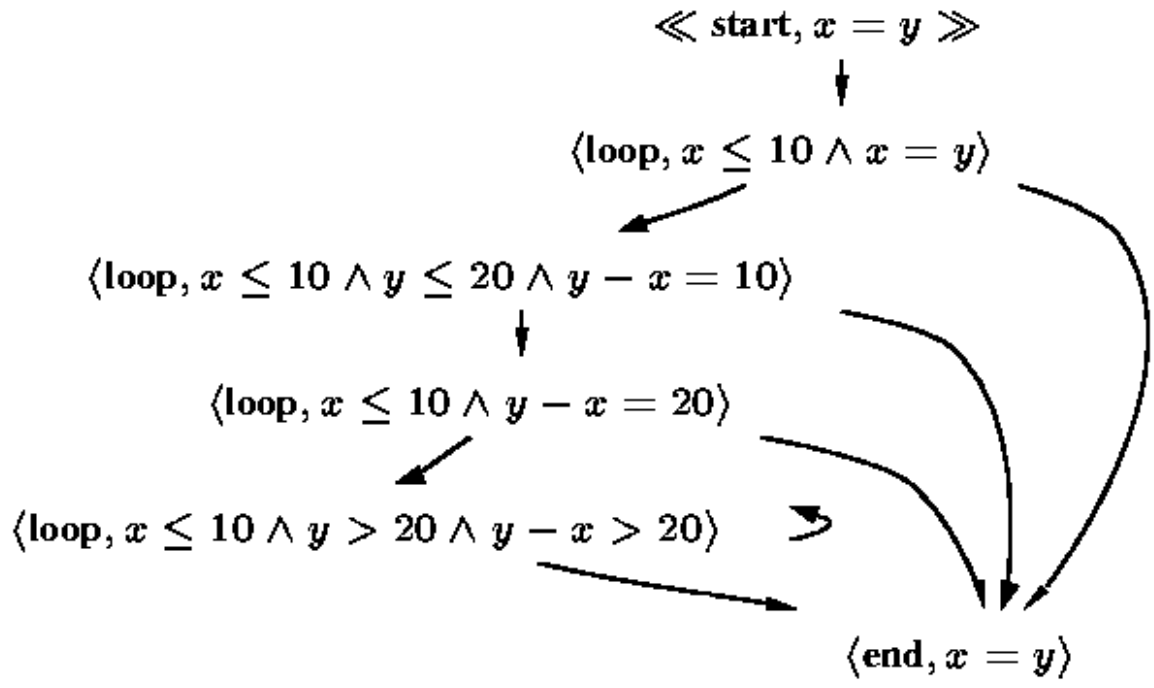


[Bengtsson, Yi 2004]

Przykład – po znormalizowaniu



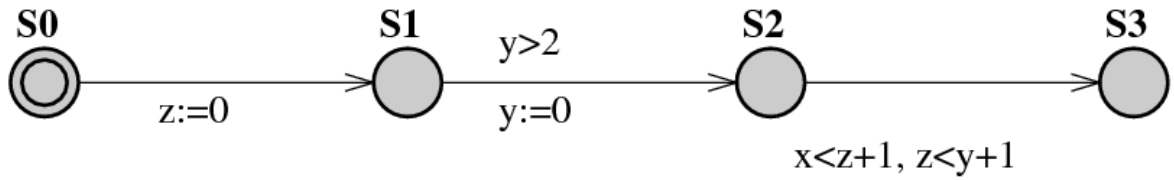




[Bengtsson, Yi 2004]

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

Struktura Kripkego

M(A)

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

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

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

Rozszerzamy CTL$^*_{-X}$

formuły stanowe: $s \models \phi$

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

formuły ścieżkowe: $\Pi \models \psi$

$$\psi \quad ::= \quad \phi \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \psi_1 \,\mathsf{U}_I\, \psi_2$$

I – przedział

np. $\prec c$, $\quad \prec \in \{<, \leq, >, \geq, =\}$

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

ścieżka: $\Pi = s_0 \overset{t_0}{\rightsquigarrow} s_0' \xrightarrow{a_0} s_1 \overset{t_1}{\rightsquigarrow} s_1' \xrightarrow{a_1} \ldots$ $(\Sigma_i\, t_i$ nieogr.)

sygnał: $\Pi = \quad \cdot \overset{a_0}{\text{———}} t_0 \overset{a_1}{\text{———————}} t_0 + t_1 \cdots$

$s_0 \models \phi_1 \,\mathsf{U}_I\, \phi_2$ 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 $t \in \mathbb{R}^+$

Przykłady

TLTL (MTL):

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

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

$$\mathsf{G}\ \mathsf{F}_{\leq 1}\, p$$

TCTL:

$$\mathsf{AG}\,(p \implies \mathsf{AF}_{\leq 3}\, q) \qquad\qquad \mathsf{AG}\,(p \implies \mathsf{AF}\, q \wedge x \leq 3)$$

Złożoność

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

Złożoność

$\phi \in \ldots$	$M(\mathcal{A}) \models \phi$	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

Zegary w formułach

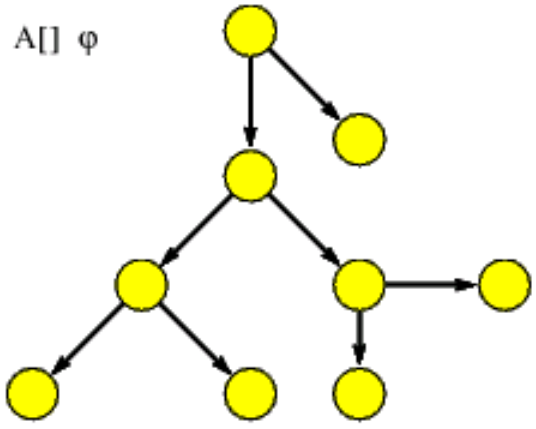
TLTL:

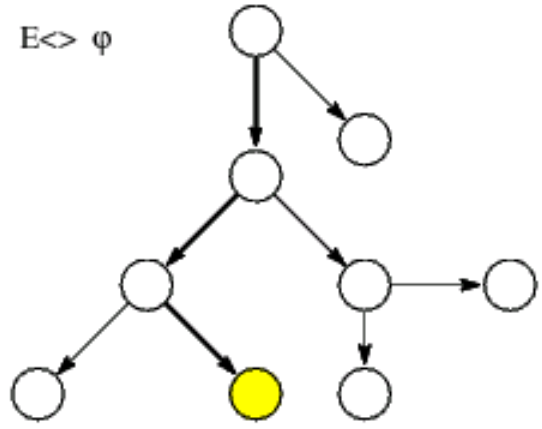
$$\mathsf{G}\left(p \implies x.\ \mathsf{F}\left(q \ \wedge\ y.\mathsf{F}\left(r \ \wedge\ y < 5 \ \wedge\ x \leq 10\right)\right)\right)$$

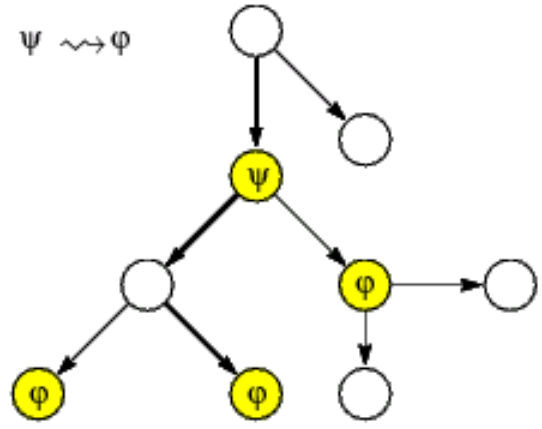
$$x.\ \mathsf{F}\left(p \ \wedge\ x \leq 1 \ \wedge\ \mathsf{G}\left(x \leq 1 \implies p\right)\right)$$

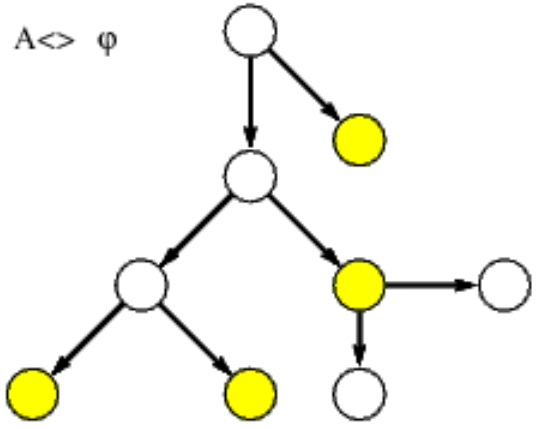
TCTL:

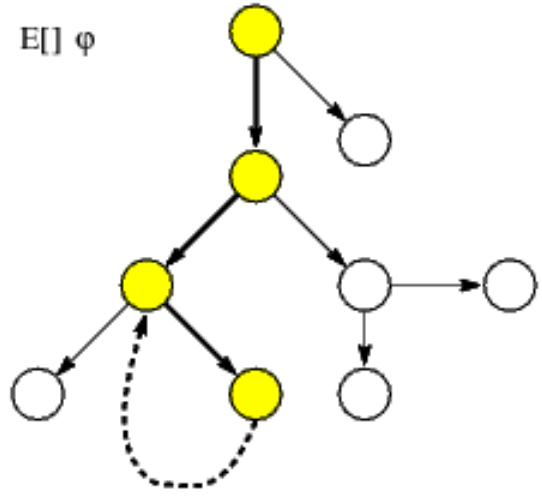
$$\mathsf{EF}\, x.\ \left(p \ \wedge\ \mathsf{EF}\left(q \ \wedge\ \mathsf{EF}\left(r \ \wedge\ x < 5\right)\right)\right)$$


A[] φ

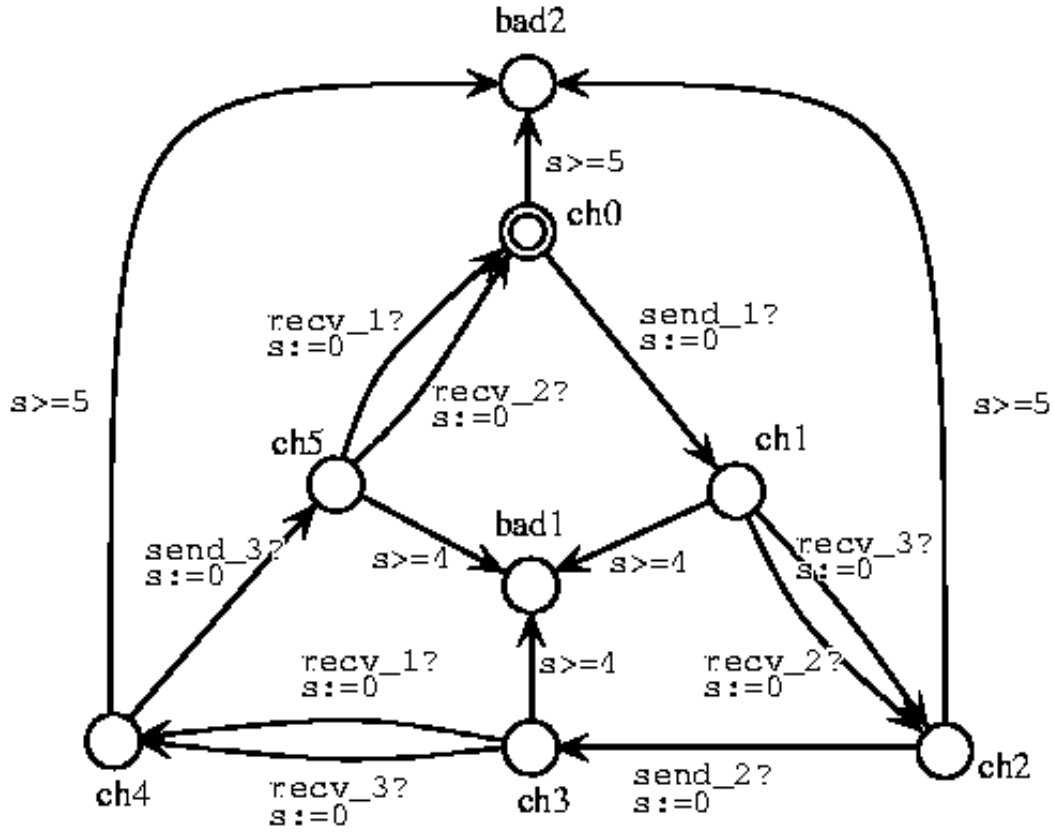

E<> φ


ψ ⇝ φ
ψ
φ
φ
φ


A<> φ


E[] φ

Automaty testujące



```
PASSED:= {}
WAIT:= {(l_0, D_0)}
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:={(l_s, D_s) : (l, D) ⇝ (l_s, D_s) ∧ D_s ≠ ∅}
                    for all (l_s', D_s') in NEXT do
                            put (l_s', D_s') to WAIT
                  end
        end
until WAIT={}
return "NO"
```

[Bengtsson, Yi 2004]

II. DBMs

Difference-Bound Matrix

DBM = reprezentacja strefy

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

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

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

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

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

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

strefa:

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

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

macierz ją reprezentująca:

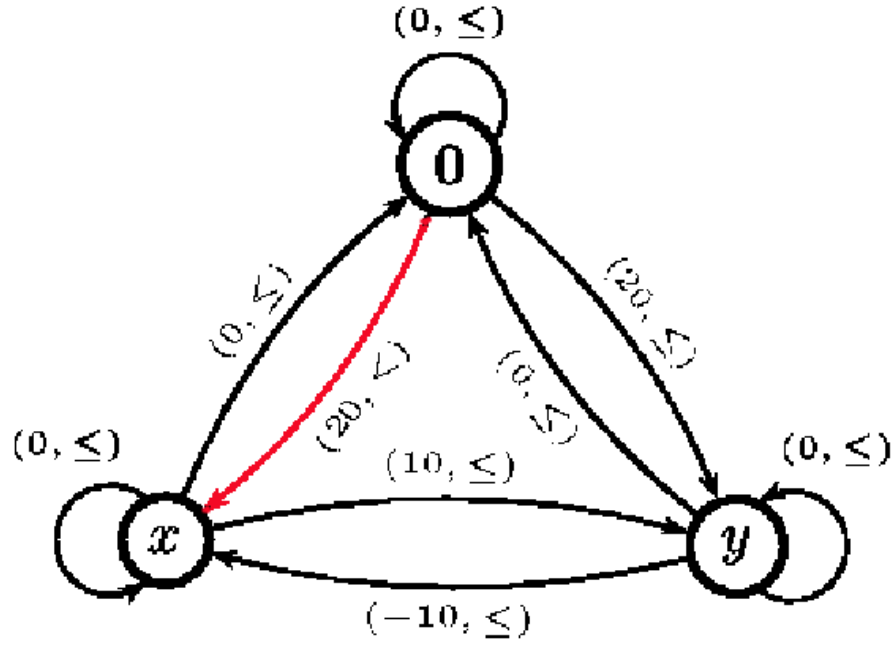
$$\begin{pmatrix} (0,\leq) & (0,\leq) & (0,\leq) & (5,<) \\ (20,<) & (0,\leq) & (-10,\leq) & \infty \\ (20,\leq) & (10,\leq) & (0,\leq) & \infty \\ \infty & \infty & \infty & (0,\leq) \end{pmatrix}$$

[Bengtsson, Yi 2004]

strefa:

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

graf ją reprezentujący:

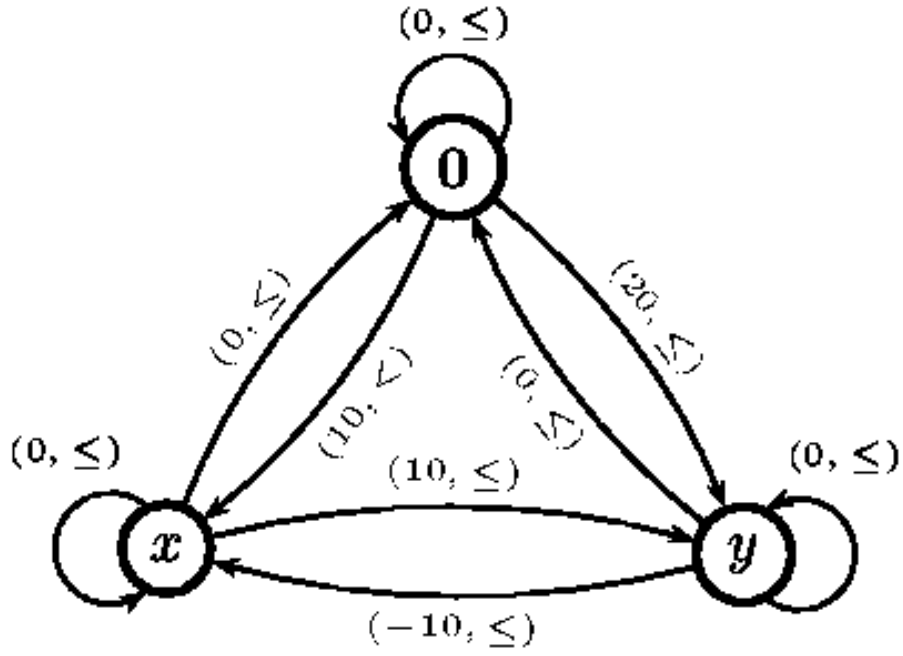


[Bengtsson, Yi 2004]

strefa:

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

graf kanoniczny ją reprezentujący:



[Bengtsson, Yi 2004]

Kanonizacja

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

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

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

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

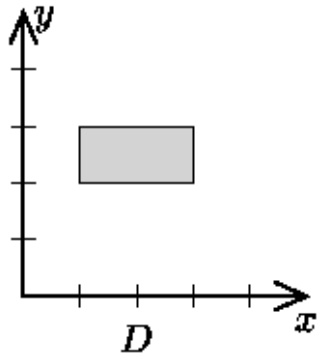
Czas $\mathcal{O}(n^3)$

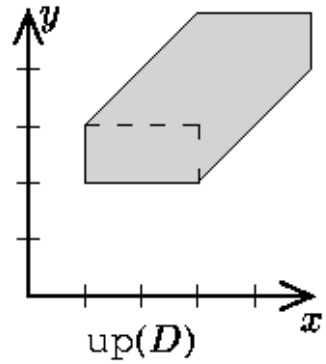
Operacje na strefach (macierzach):

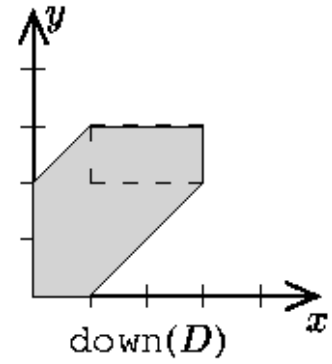
- $D \neq \emptyset$? $\iff$ nie ma cyklu < 0

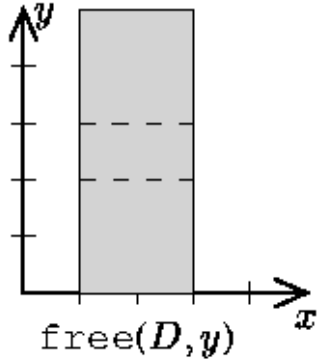
$$-c_{ji} \prec_{ji} x_i - x_j \prec_{ij} c_{ij} \qquad\qquad -c_{ji} \prec' c_{ij}$$

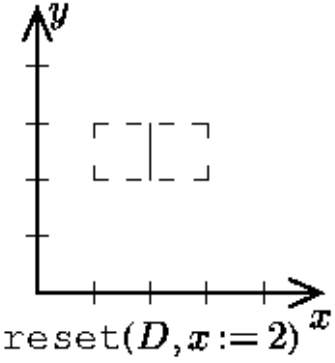
- $D \subseteq D'$?
- $D^{\rightsquigarrow}$ $\quad \mathrm{up}(D)$ $\quad \mathrm{down}(D)$
- $D \wedge \psi$ $\quad D_1 \wedge D_2$
- $D[\mathcal{C}' := 0]$
- ...

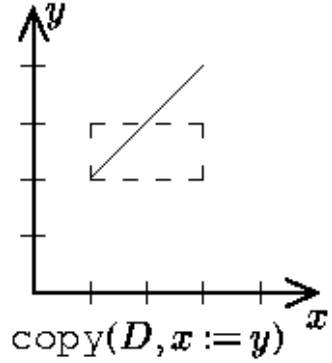


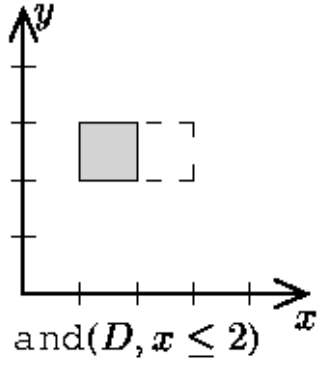


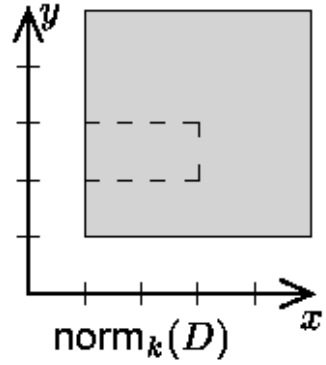


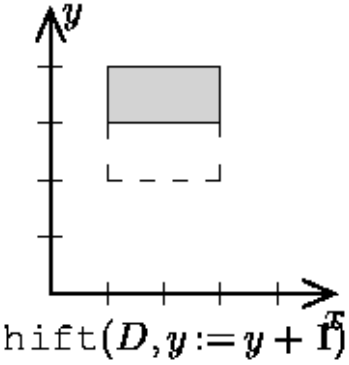










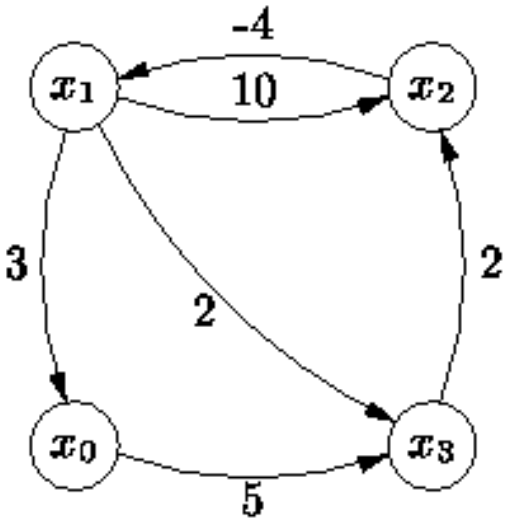


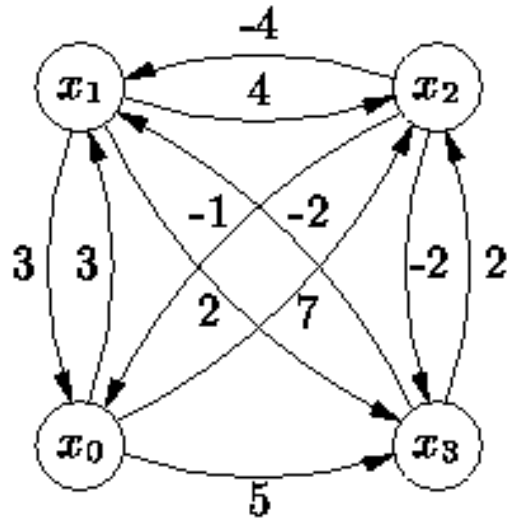
[Bengtsson, Yi 2004]

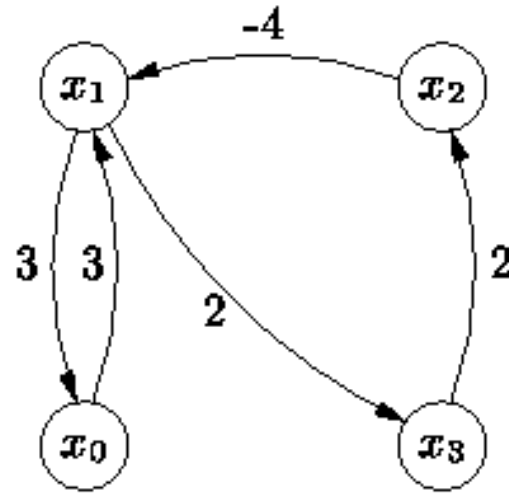
Operacje na strefach c.d.:

- $D_1 \vee D_2$
- $\ldots$

Reprezentacja minimalna

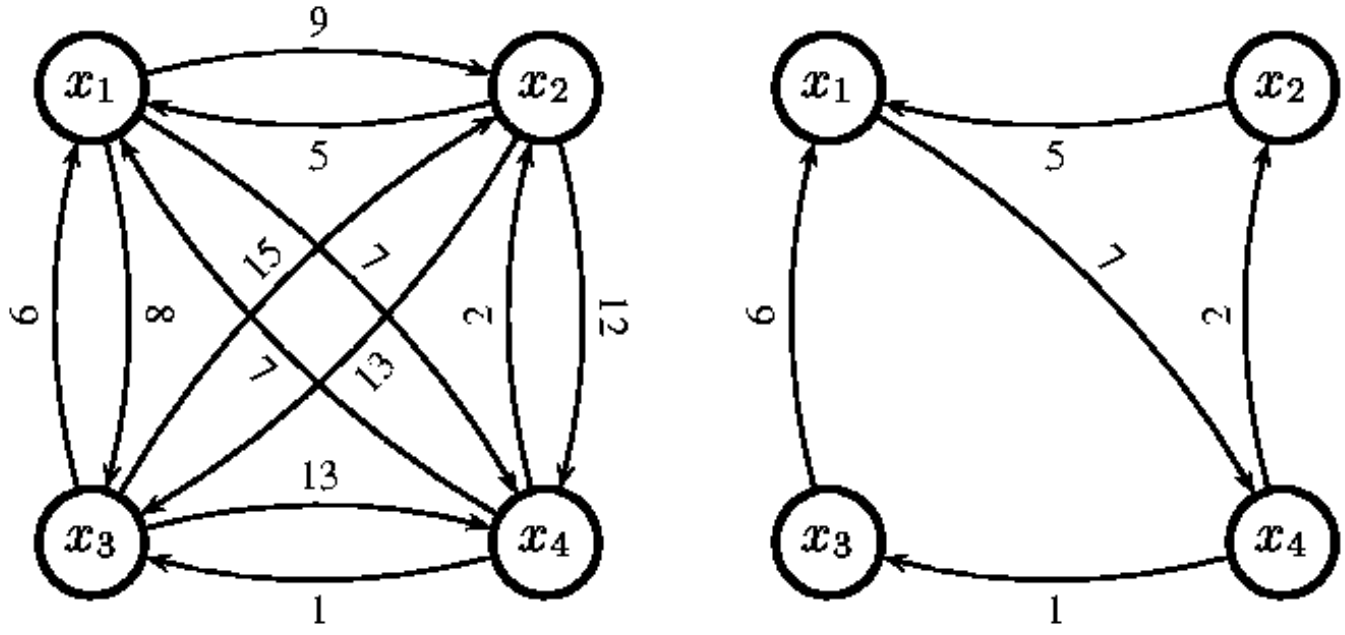






kanoniczność reprezentacji

Reprezentacja minimalna

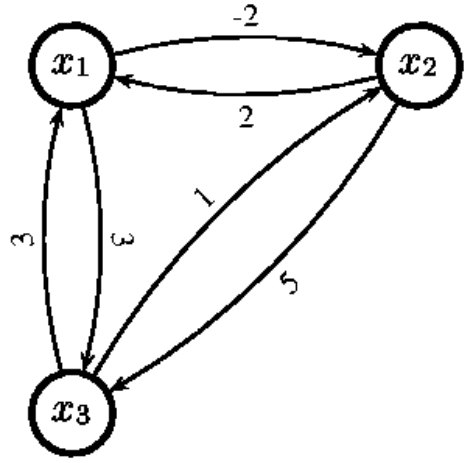


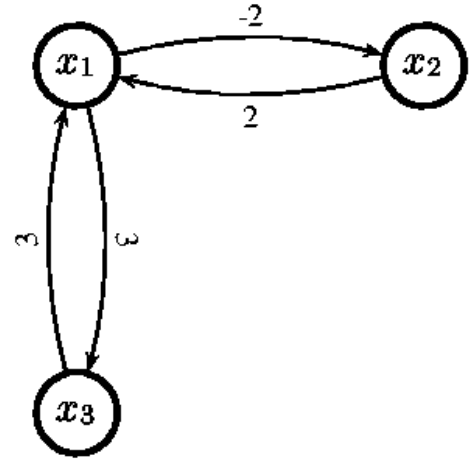
[Bengtsson, Yi 2004]

– eliminacja krawędzi nadmiarowych, gdy nie ma 0-cykli

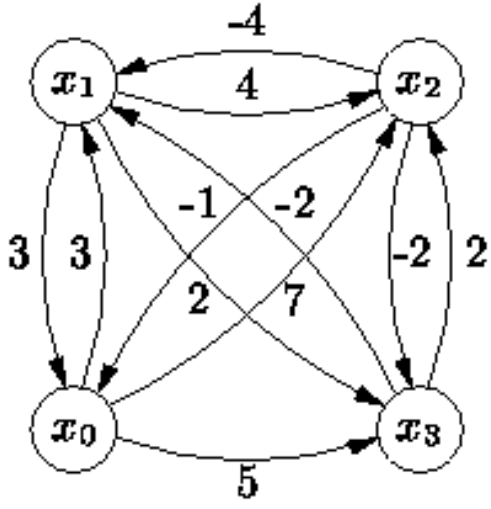
– usunięcie krawędzi nadmiarowej nie wpływa na pozostałe

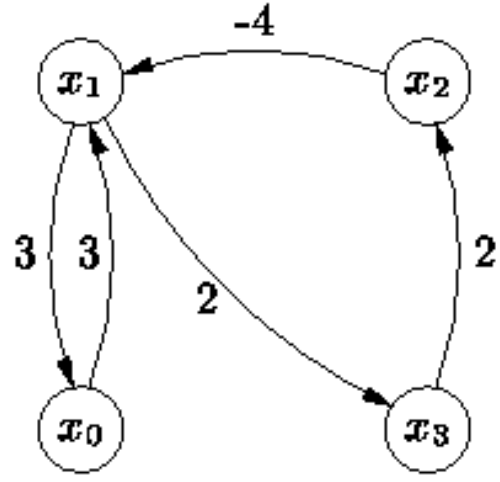
Reprezentacja minimalna (0-cykle)





[Bengtsson, Yi 2004]





III. CDDs

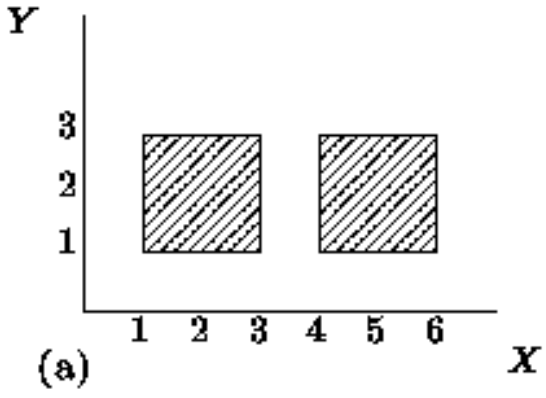
```
PASSED:= {}
WAIT:= {(l_0, D_0)}
repeat
        begin
        get (l, D) from WAIT
        if (l, D) ⊨ φ then return "YES"
        else if D ⋢ D' for all (l, D') ∈ PASSED then
                begin
                add (l, D) to PASSED          (*)
                NEXT:={(l_s, D_s) : (l, D) ⇝ (l_s, D_s) ∧ D_s ≠ ∅}
                for all (l_s', D_s') in NEXT do
                        put (l_s', D_s') to WAIT
                end
        end
until WAIT={}
return "NO"
```

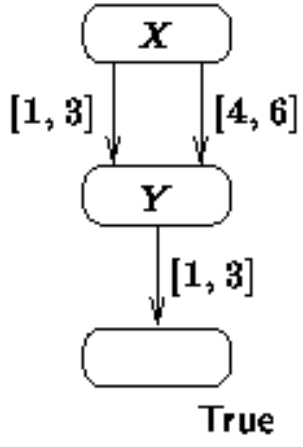
bardziej symbolicznie ?

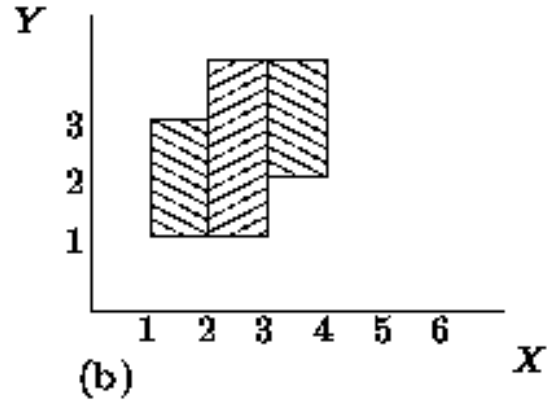
Różne czasowe adaptacje BDDs:

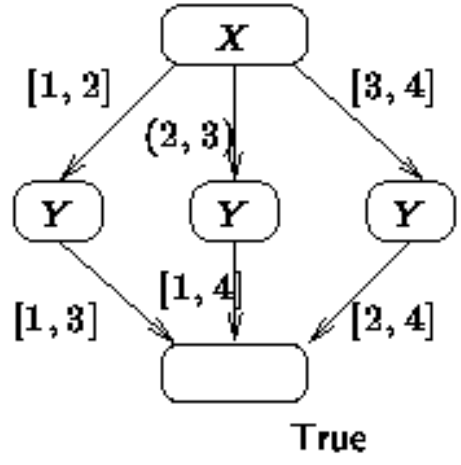
- IDD
- DDD
- CDD
- ...

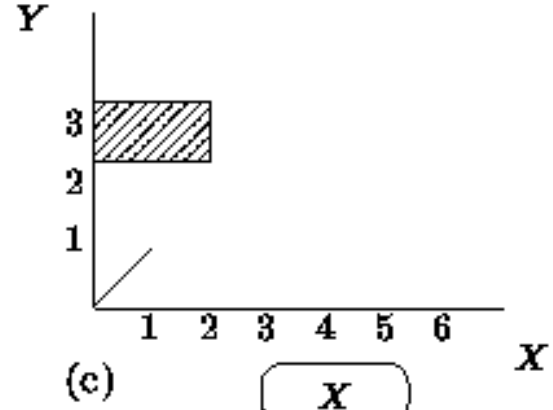
CDD = suma skończenie wielu stref

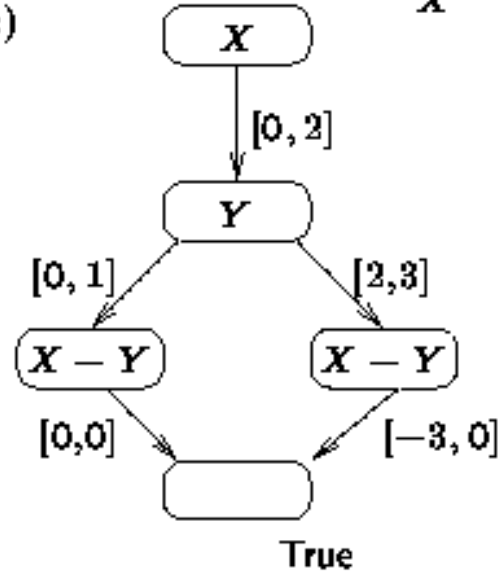








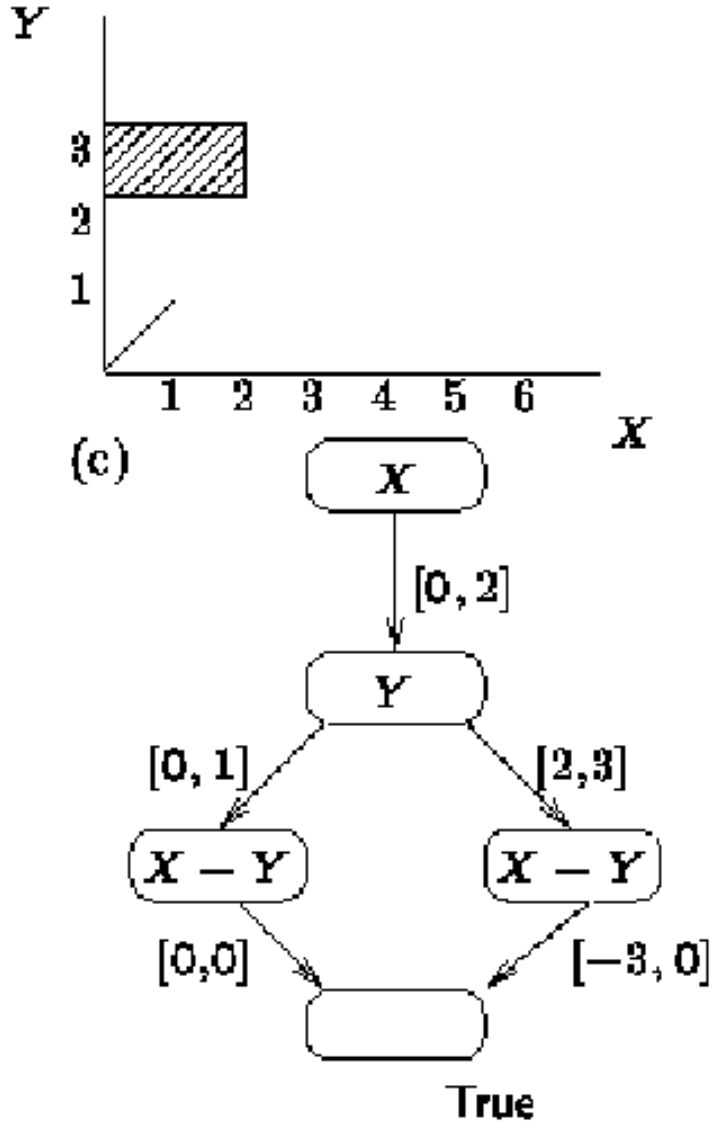


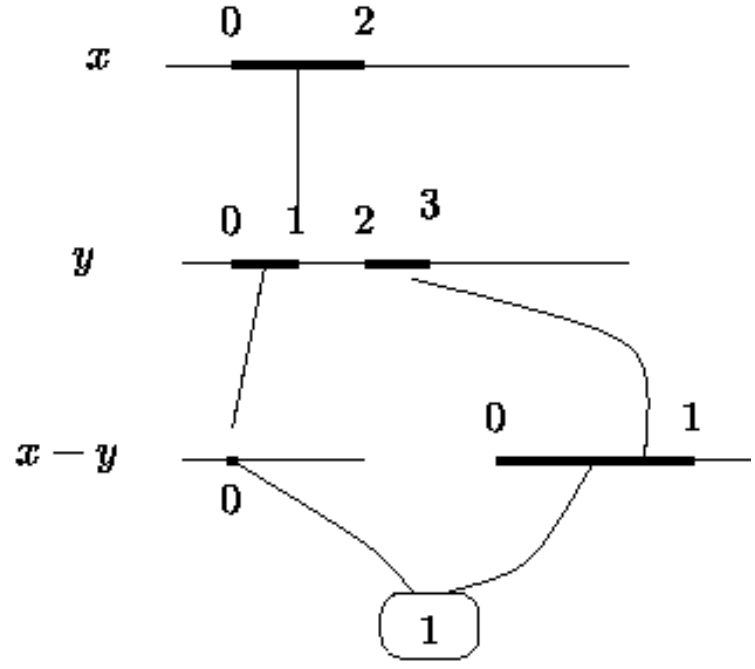


[Larsen, Pearson, Weise, Yi 1999]

CDD (zamiast porządnej definicji :)

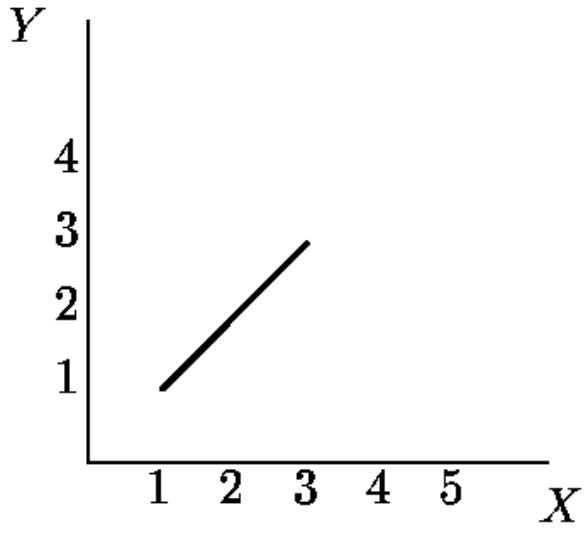
- przestrzega porządku
- następniki wyznaczają podział $\mathbb{R}$ na odcinki

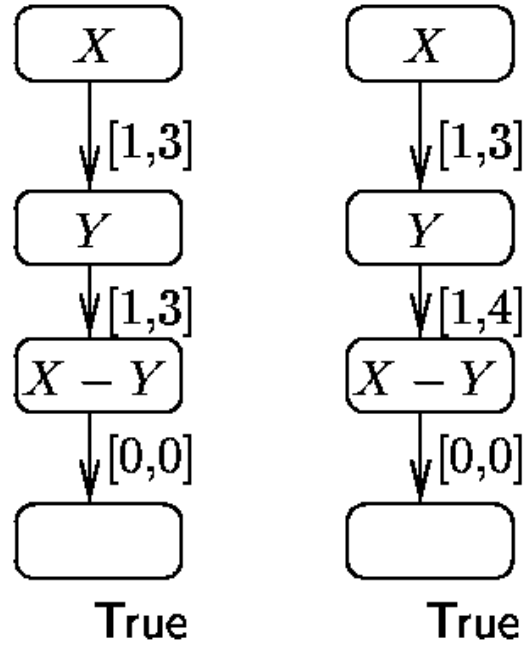




[Larsen, Pearson, Weise, Yi 1999]

Brak kanoniczności !

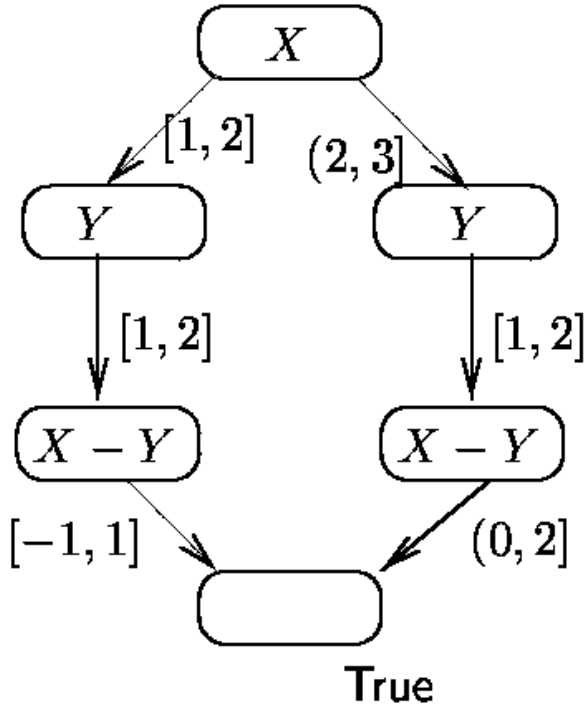


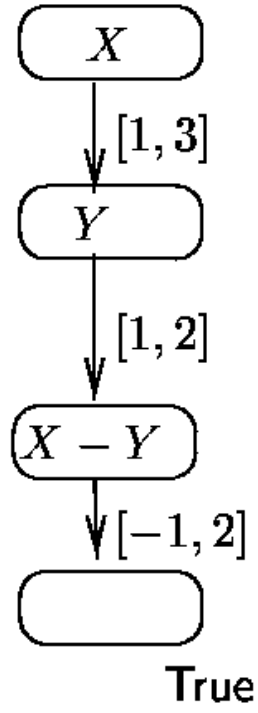


[Larsen, Pearson, Weise, Yi 1999]

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

Wciąż brak kanoniczności !

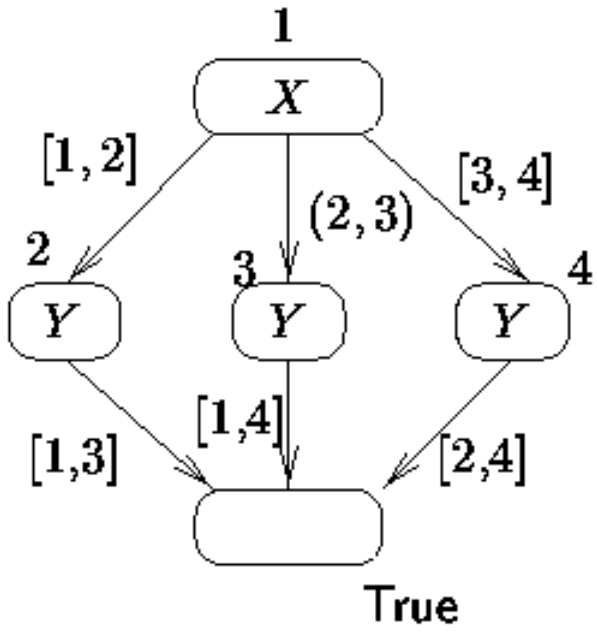


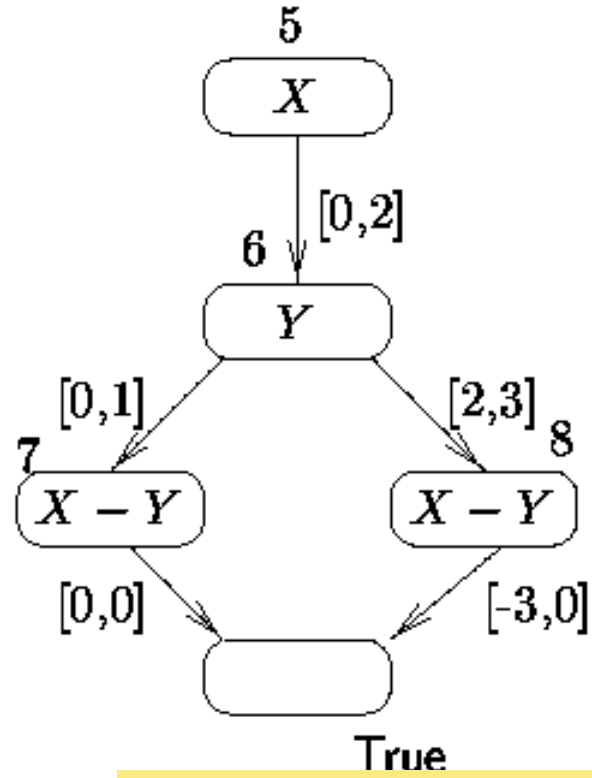


[Larsen, Pearson, Weise, Yi 1999]

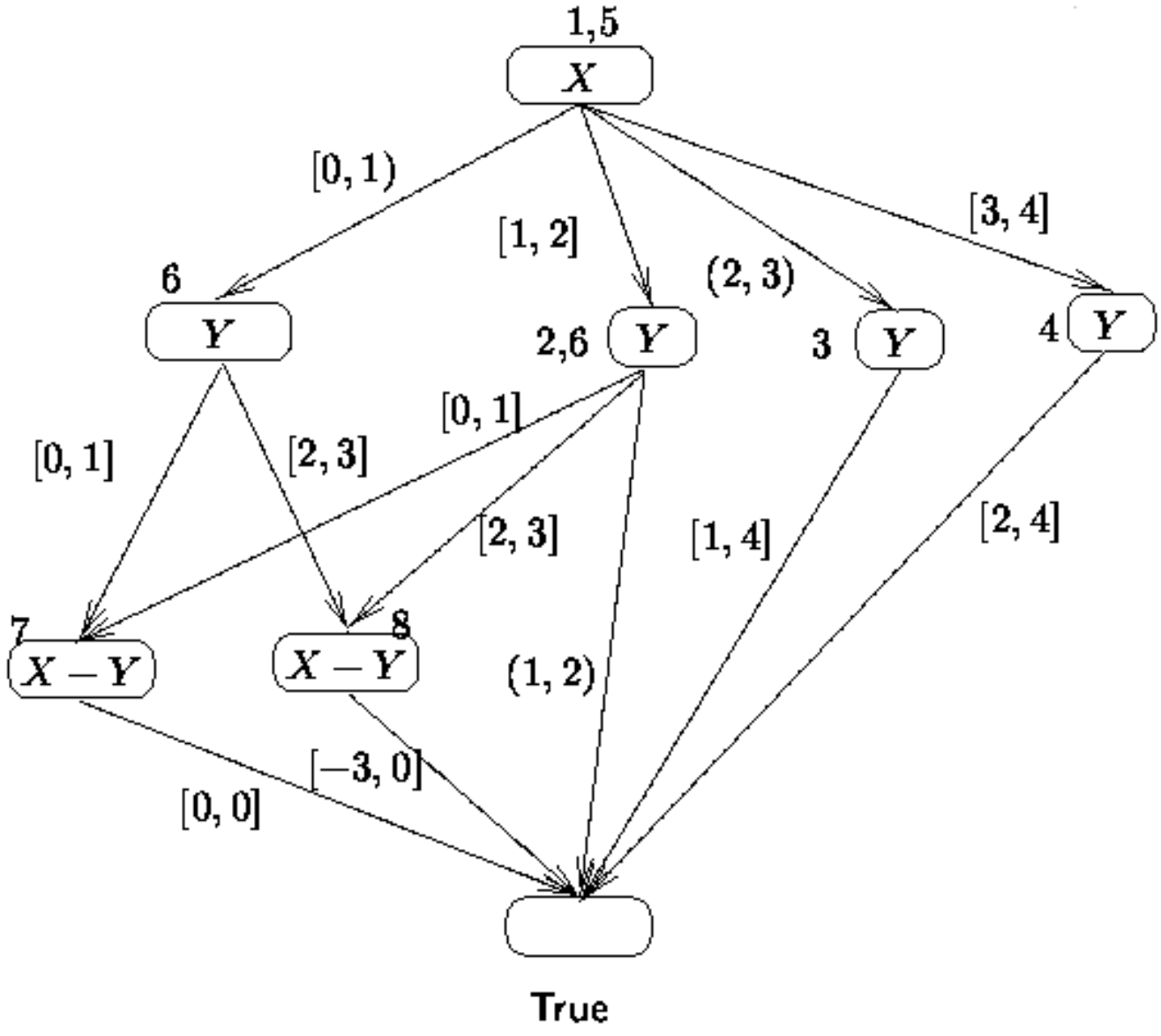
Operacje na CDDs – przykład

$\mathrm{op}(D_1, D_2)$





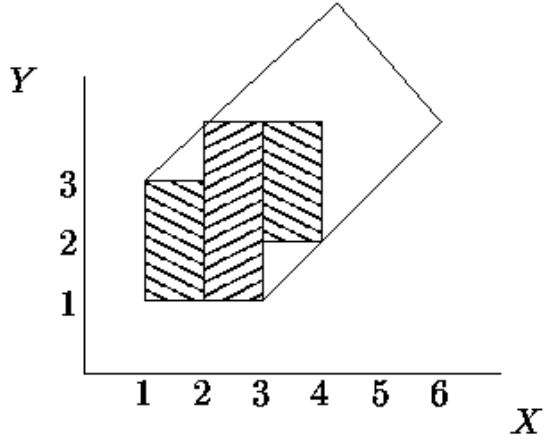
[Larsen, Pearson, Weise, Yi 1999]

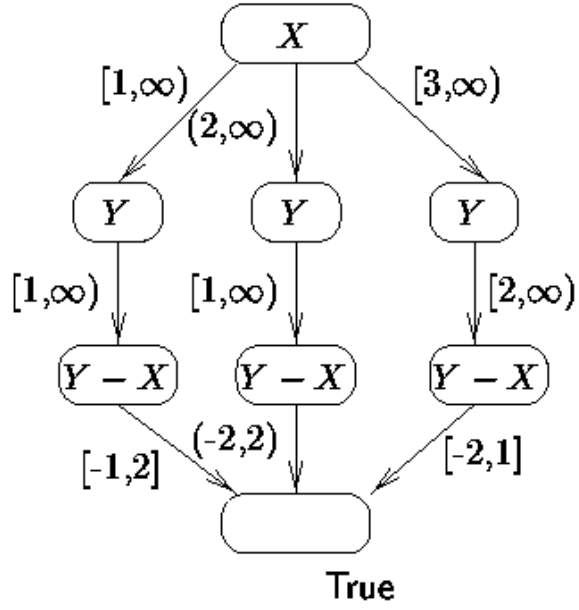


[Larsen, Pearson, Weise, Yi 1999]

Operacje na CDDs

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





[Larsen, Pearson, Weise, Yi 1999]

- $D[\mathcal{C}' := 0]$