Praktyczne metody weryfikacji

Wykład 11: Weryfikacja czasowa

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: $\Pi \models \psi$

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

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

Wariant: $\psi_1 \,\mathsf{U}_I\, \psi_2$, I – przedział

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

ścieżki: $\Pi = s_0 \overset{t_0}{\rightsquigarrow} s_0' \xrightarrow{a_0} s_1 \overset{t_1}{\rightsquigarrow} s_1' \xrightarrow{a_1} \ldots$

$\Sigma_i\, t_i$ nieograniczony

$s_0 \models \phi_1 \,\mathsf{U}_{\prec c}\, \phi_2$ wtw gdy $\exists \Pi$ j. w., $t \prec c$.

$$\Pi(t) \models \phi_2 \ \wedge\ \forall 0 < t' < t.\ \Pi(t') \models \phi_1$$

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

Przykłady

TLTL:

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

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

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

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	nierozstrzygalna	nierozstrzygalna
TCTL	PSPACE	nierozstrzygalna

- TLTL: słowa skończone lub ω-słowa
- TLTL: semantyka punktowa
- TCTL: 1 lub 2 zegary

Zegary w formułach

TLTL:

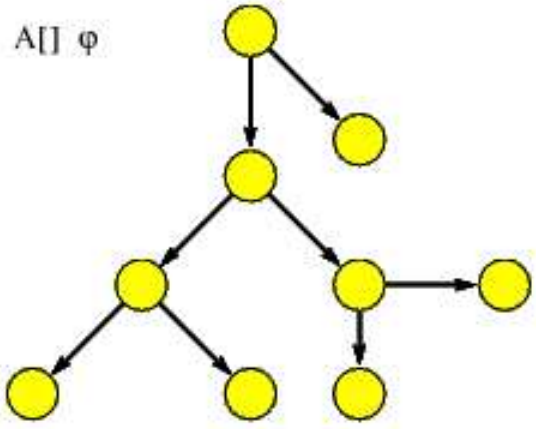
$$\mathsf{G}\, x.\ \big(p \implies \mathsf{F}\, y.\ (q \ \wedge\ y < x{+}5)\big)$$

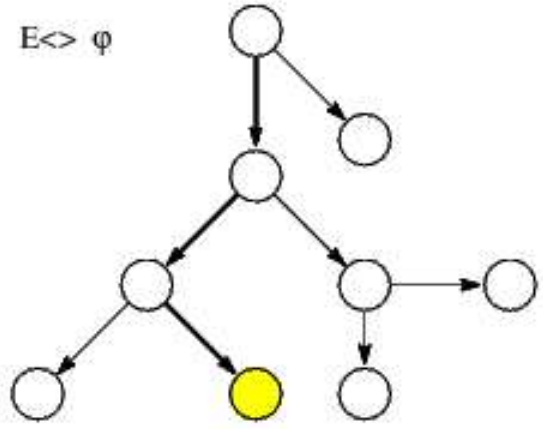
$$\mathsf{G}\, \big(p \implies y.\ \mathsf{F}\, (q \ \wedge\ y < 5)\big)$$

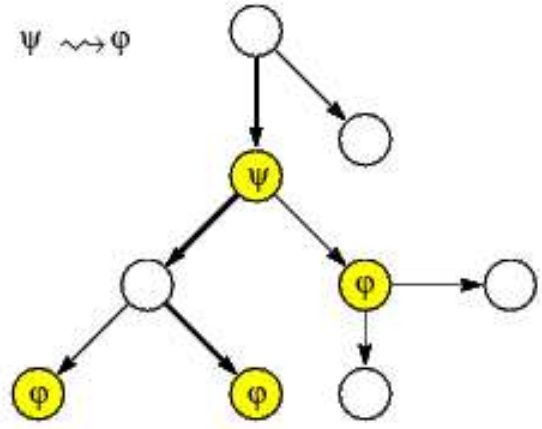
$$x.\ \mathsf{F}\, \big(p \ \wedge\ x \leq 1 \ \wedge\ \mathsf{G}\, (x \leq 1 \implies p)\big)$$

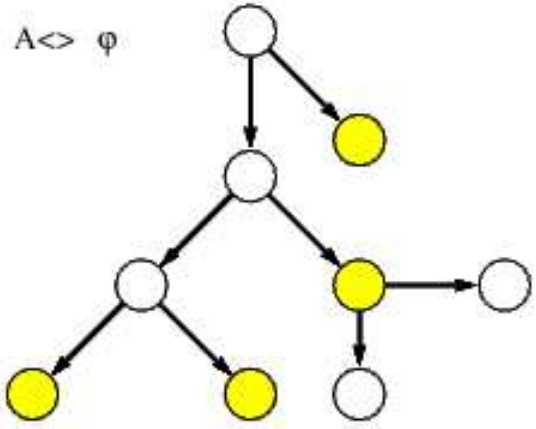
TCTL:

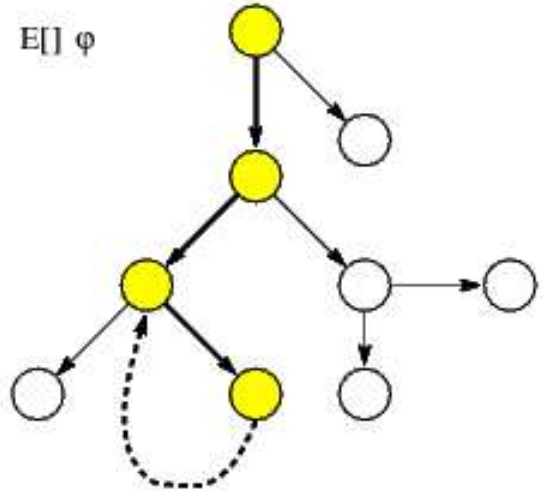
$$\mathsf{EF}\, x.\ \big(p \ \wedge\ \mathsf{EF}\, (q \ \wedge\ \mathsf{EF}\, (r \ \wedge\ x < 5))\big)$$


A[] φ

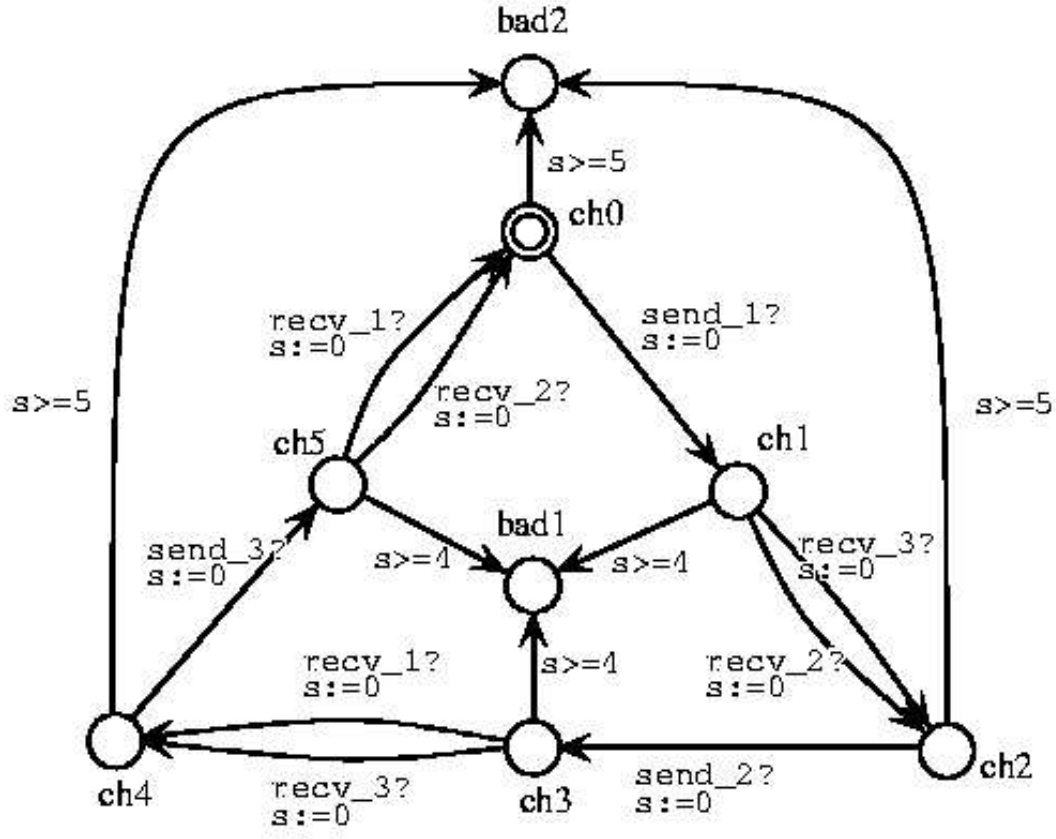

E<> φ


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"
```

II. DBMs

Difference-Bound Matrix

DBM = reprezentacja strefy

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

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

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

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

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

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

strefa:

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

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

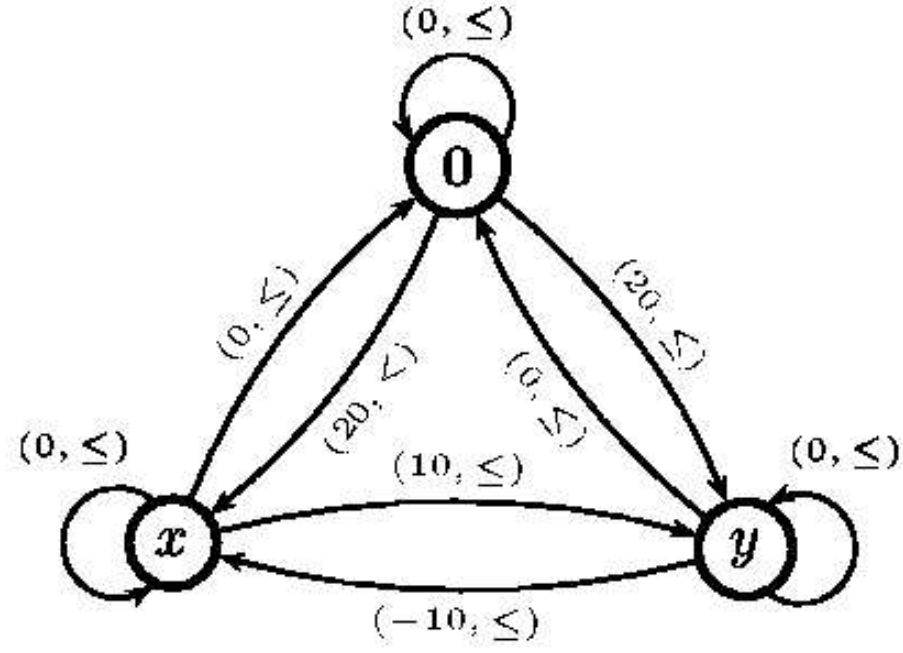
macierz ją reprezentująca:

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

strefa:

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

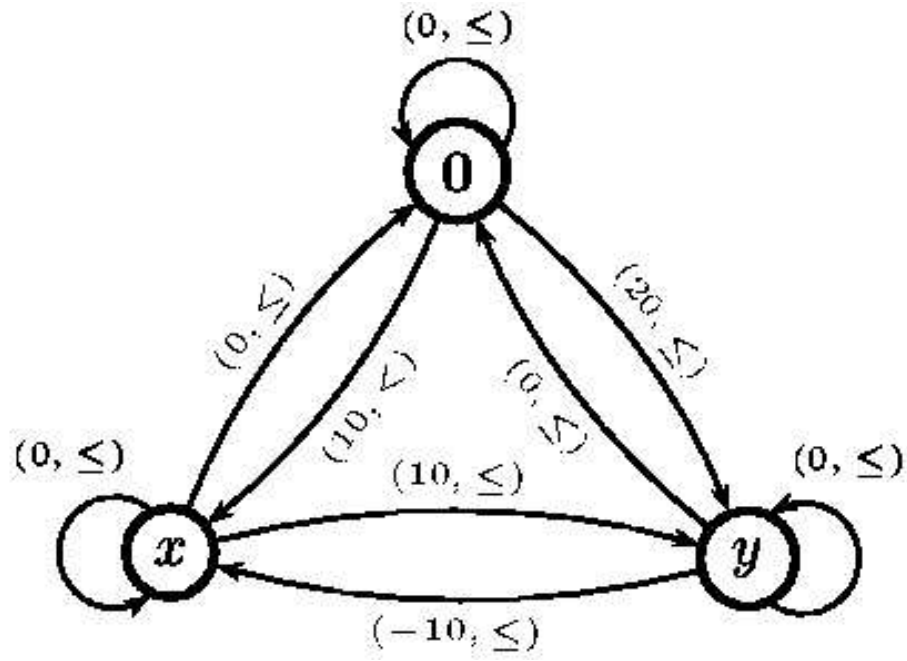
graf ją reprezentujący:



strefa:

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

graf kanoniczny ją reprezentujący:



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)

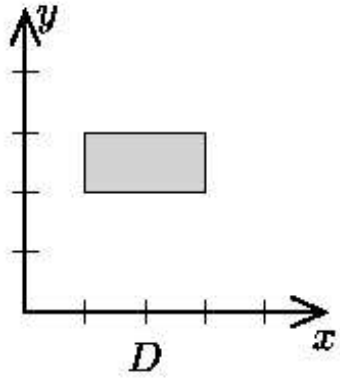
Czas $\mathcal{O}(n^3)$

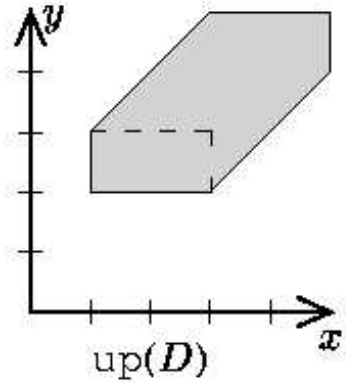
Operacje na strefach (macierzach):

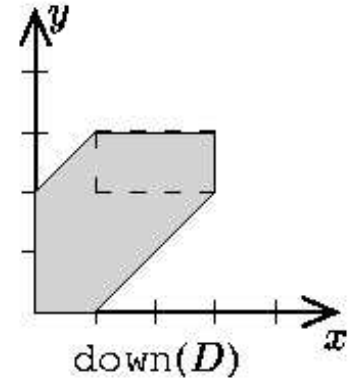
- $D \neq \emptyset$? $\iff$ nie ma cyklu < 0

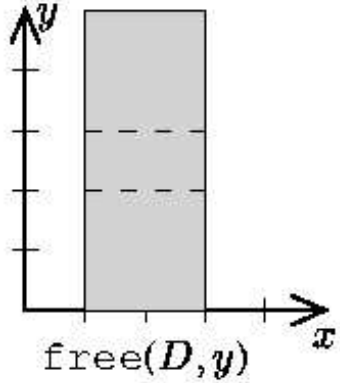
$$-c_{ji} \prec_{ji} x_i - x_j \prec_{ij} c_{ij} \qquad\qquad -c_{ji} \prec' c_{ij}$$

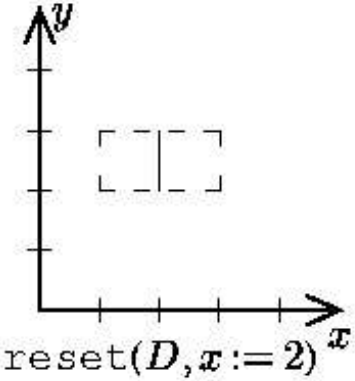
- $D \subseteq D'$?
- $D^{\rightsquigarrow}$ $\quad \mathrm{up}(D)$ $\quad \mathrm{down}(D)$
- $D \wedge \psi$ $\quad D_1 \wedge D_2$
- $D[\mathcal{C}' := 0]$
- ...

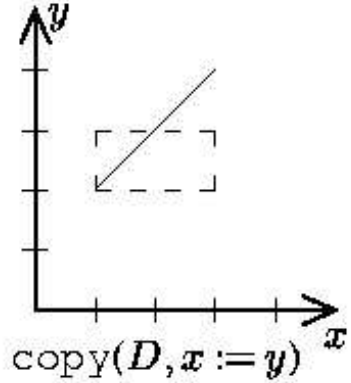

y
x
D

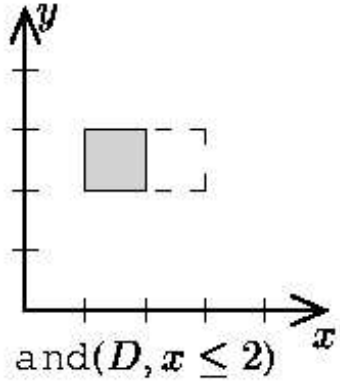

y
x
up(D)

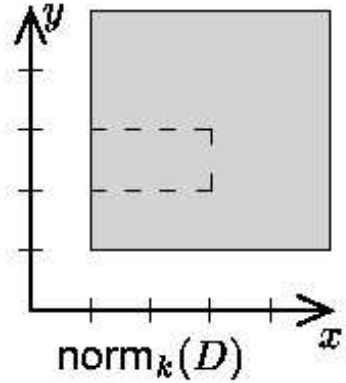

y
x
down(D)

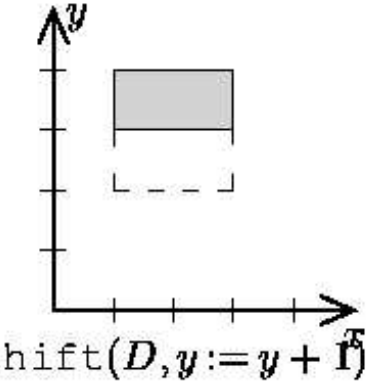

y
x
free(D, y)


y
x
reset(D, x := 2)


y
x
copy(D, x := y)


y
x
and(D, x ≤ 2)

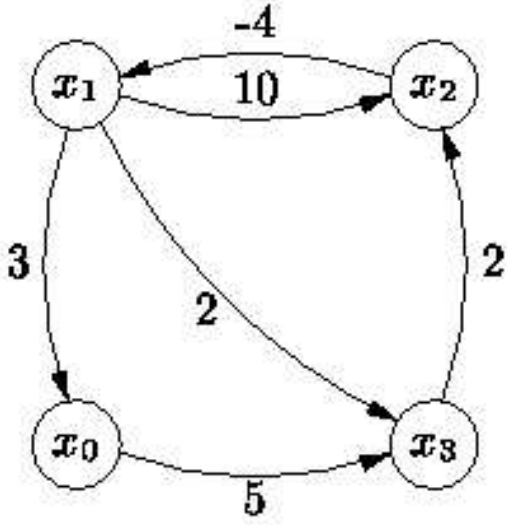

y
x
norm_k(D)

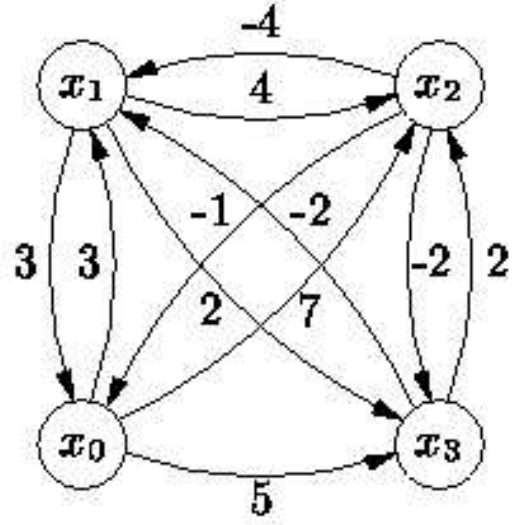

y
x
shift(D, y := y + 1)

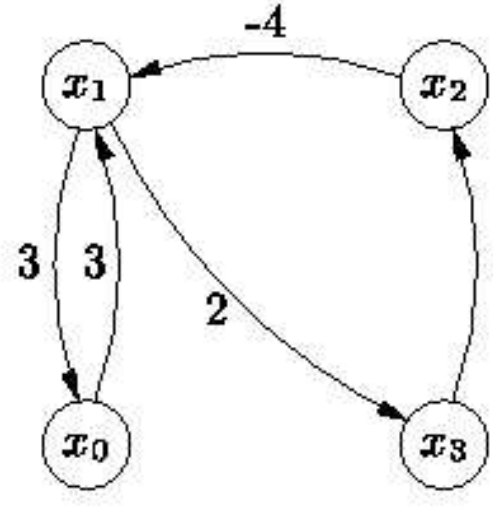
Operacje na strefach c.d.:

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

Reprezentacja minimalna

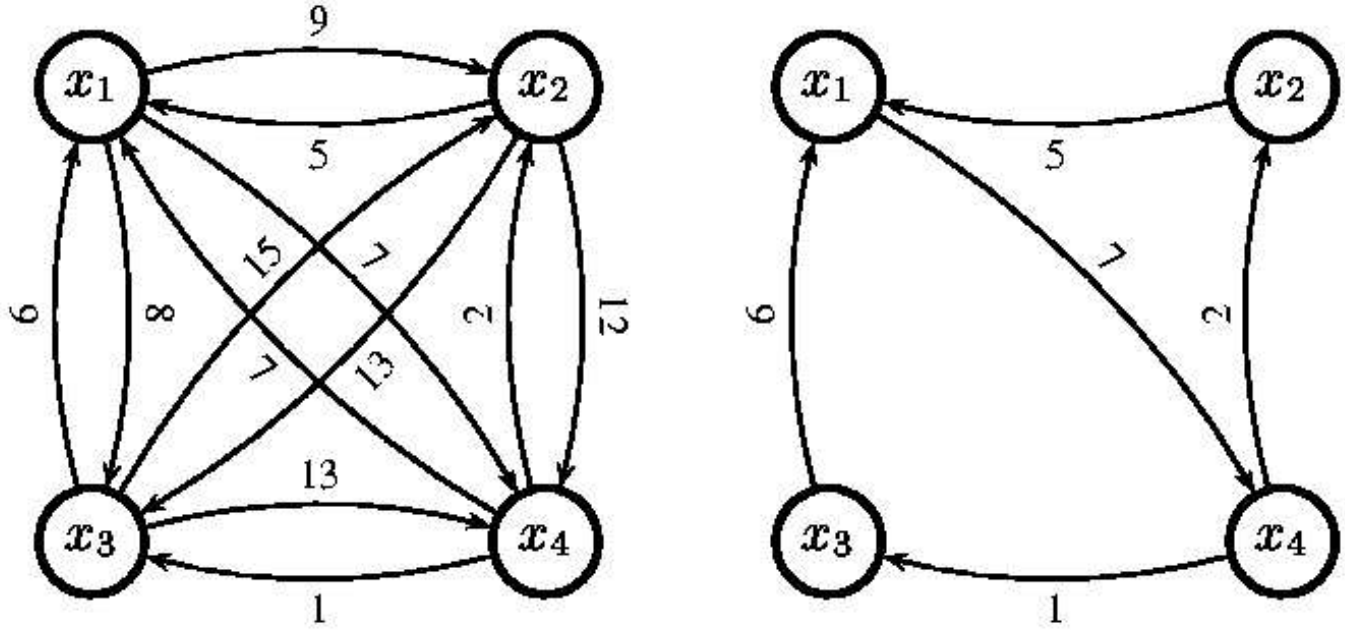






kanoniczność reprezentacji

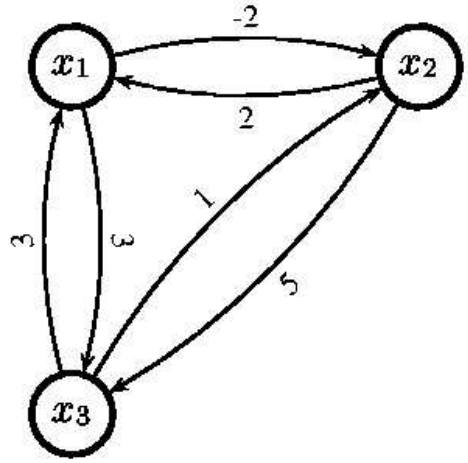
Reprezentacja minimalna

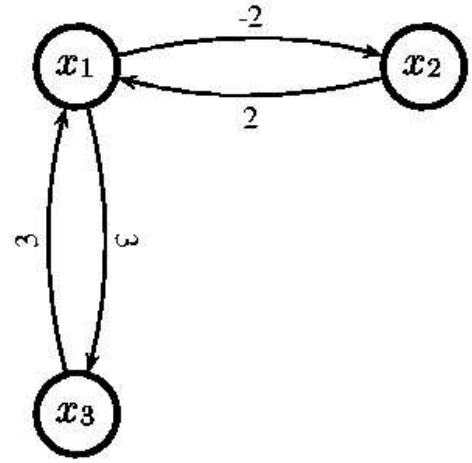


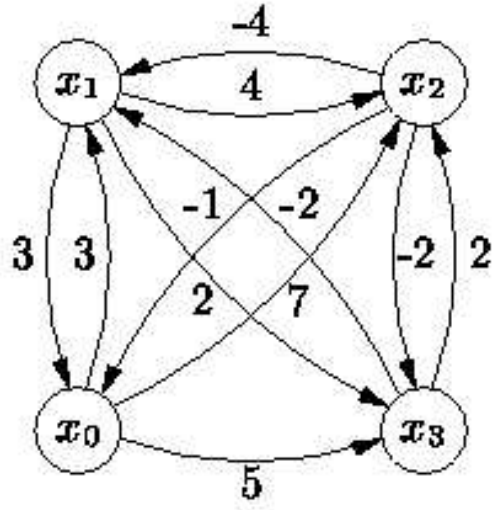
– eliminacja krawędzi nadmiarowych, gdy nie ma 0-cykli

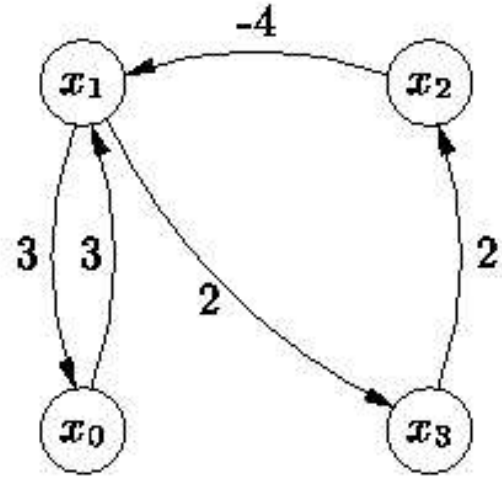
– usunięcie krawędzi nadmiarowej nie wpływa na pozostałe

Reprezentacja minimalna gdy są 0-cykle









III. CDDs

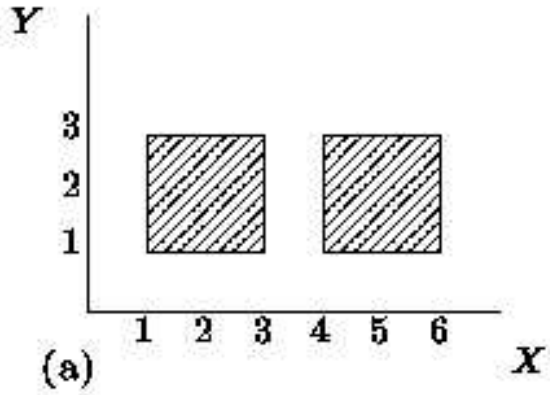
```
PASSED:= {}
WAIT:= {(l_0, D_0)}
repeat
        begin
          get (l, D) from WAIT
          if (l, D) ⊨ φ then return "YES"
          else if D ⋢ D' for all (l, D') ∈ PASSED then
                  begin
                    add (l, D) to PASSED          (*)
                    NEXT:={(l_s, D_s) : (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"
```

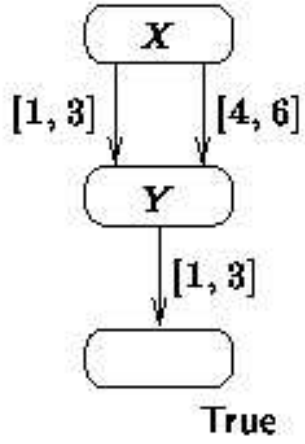
bardziej symbolicznie ?

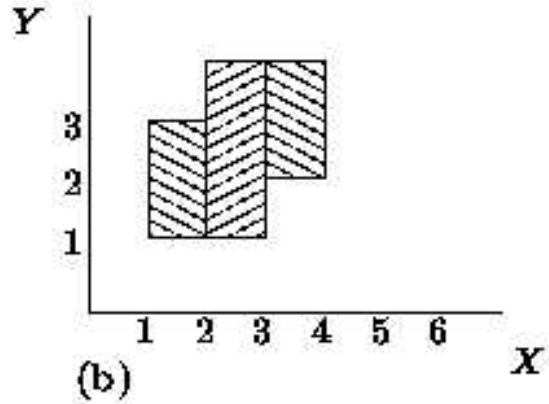
Różne czasowe adaptacje BDDs:

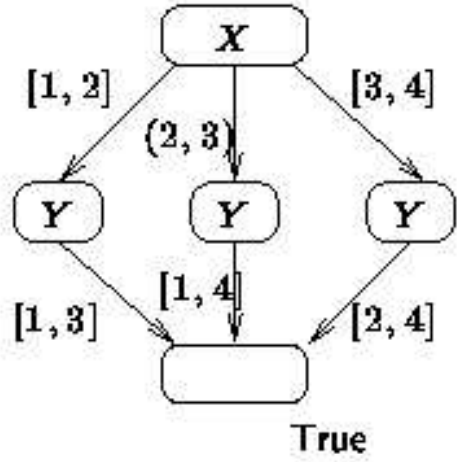
- IDD
- DDD
- CDD
- ...

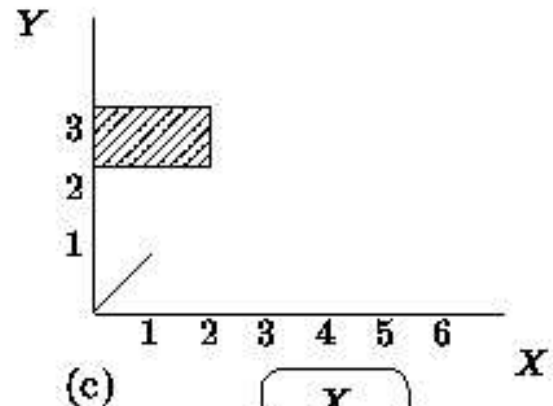
CDD = suma skończenie wielu stref

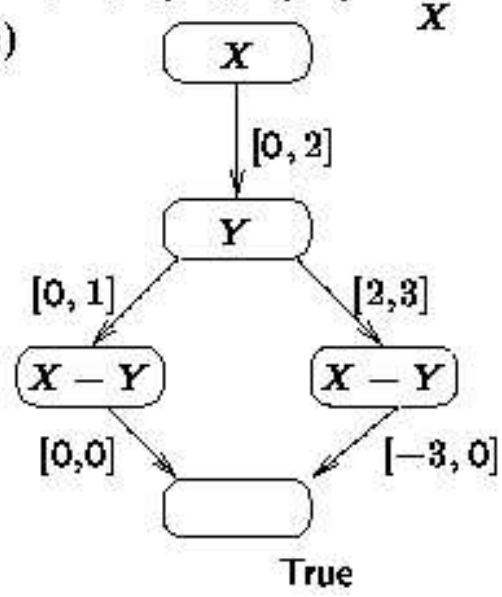






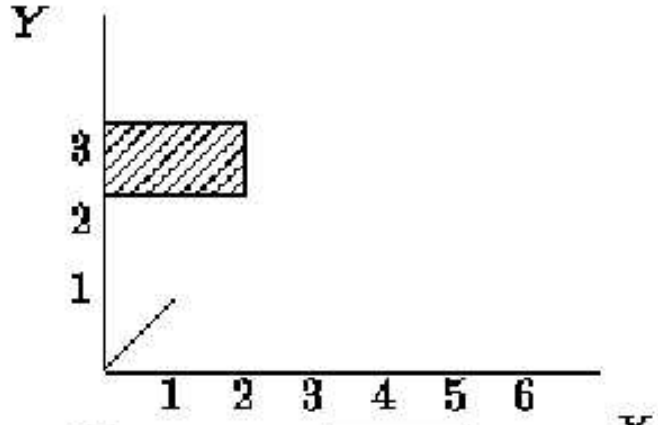




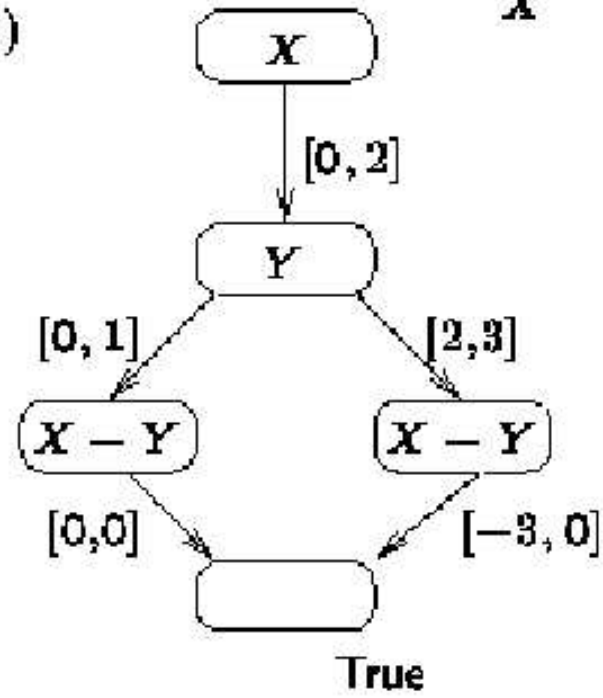


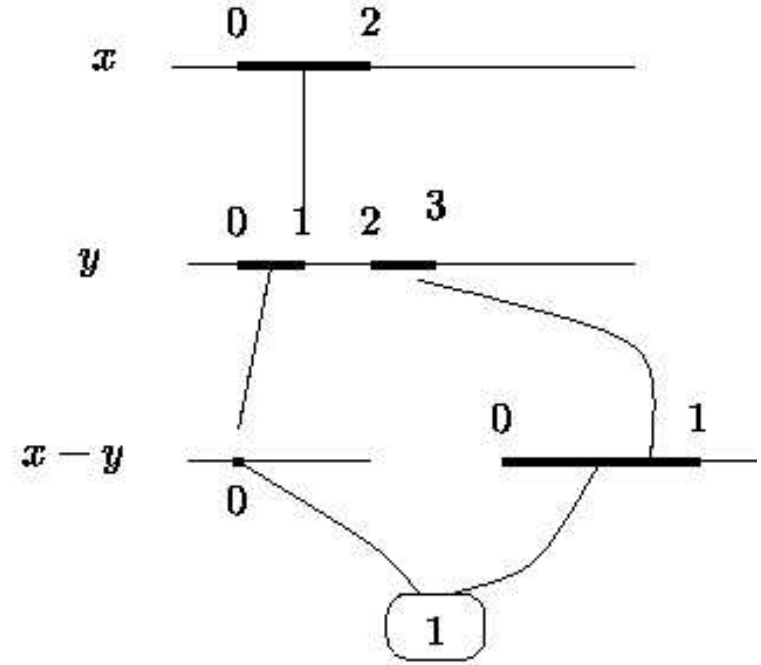
CDD (zamiast porządnej defi nicji :)

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

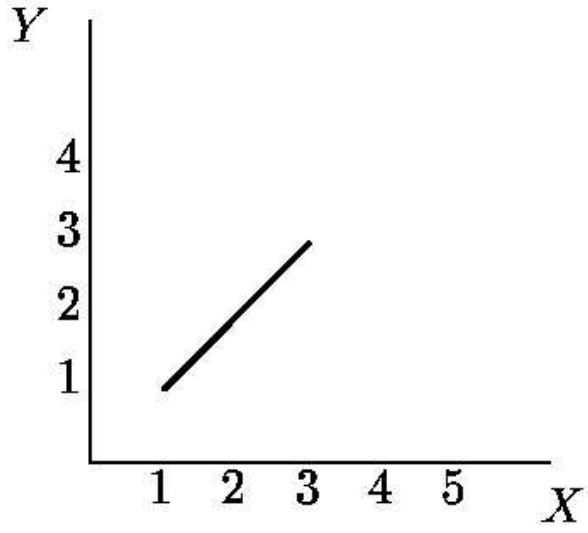


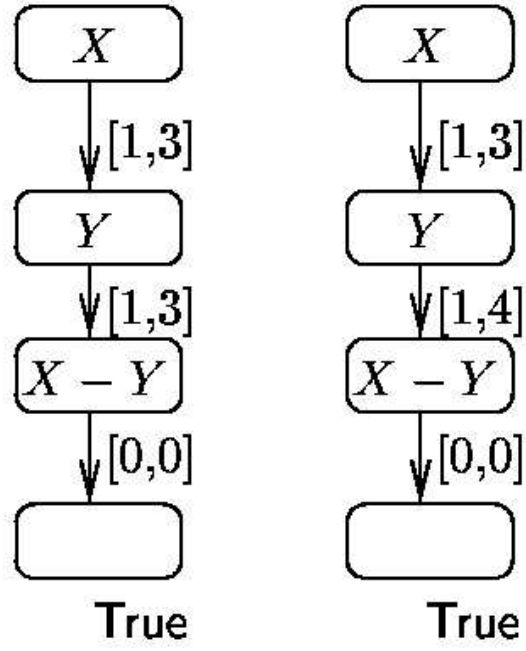
(c)





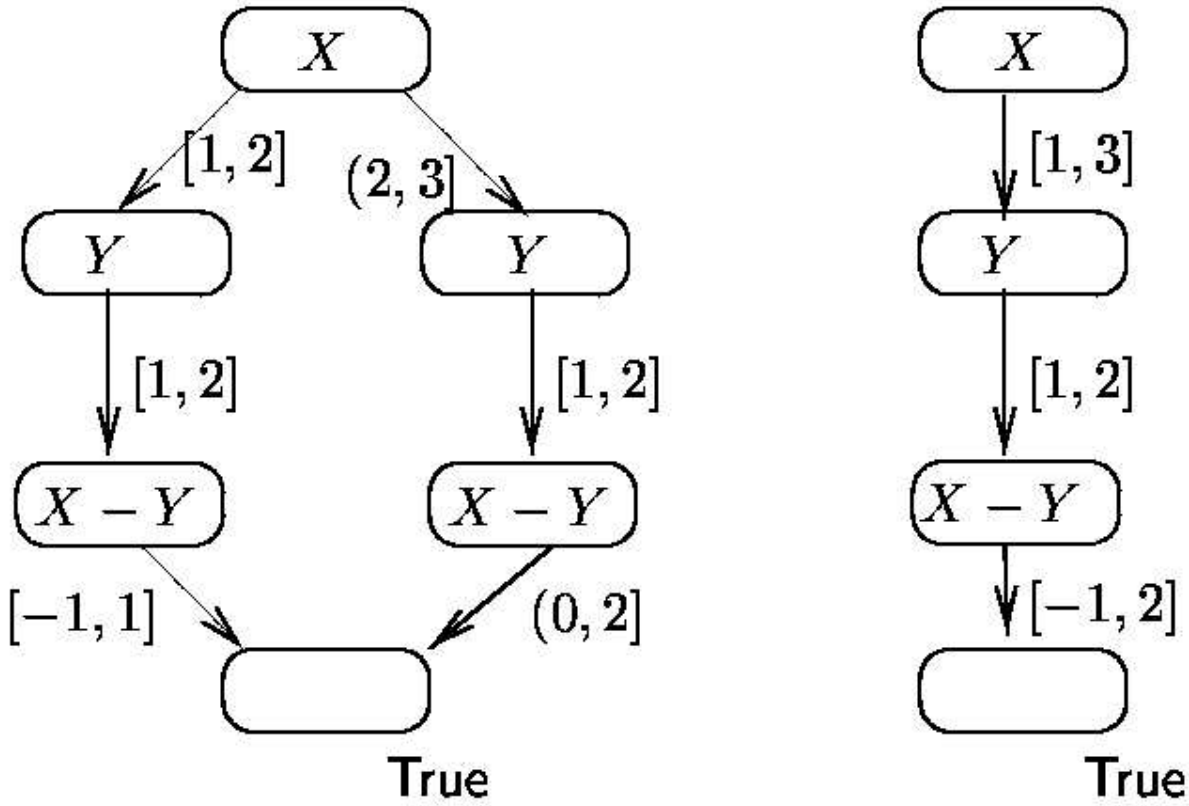
Brak kanoniczności !





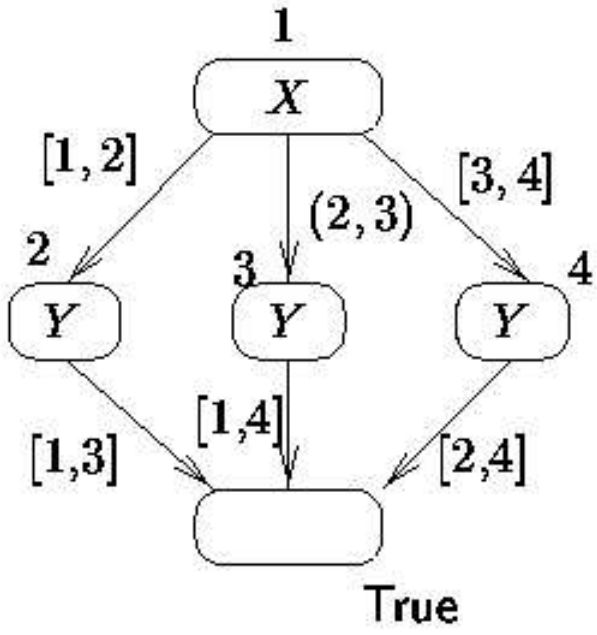
Dodatkowe założenie: każda ścieżka jest kanoniczna.

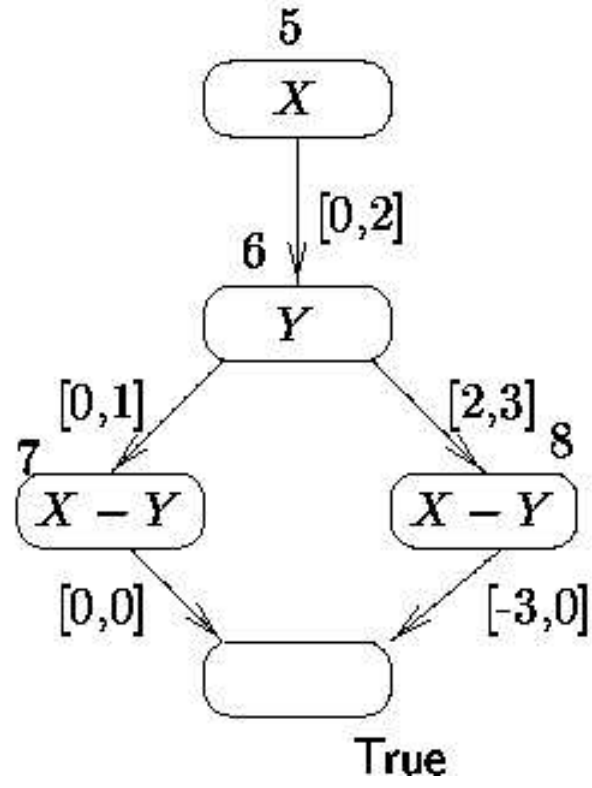
Wciąż brak kanoniczności !

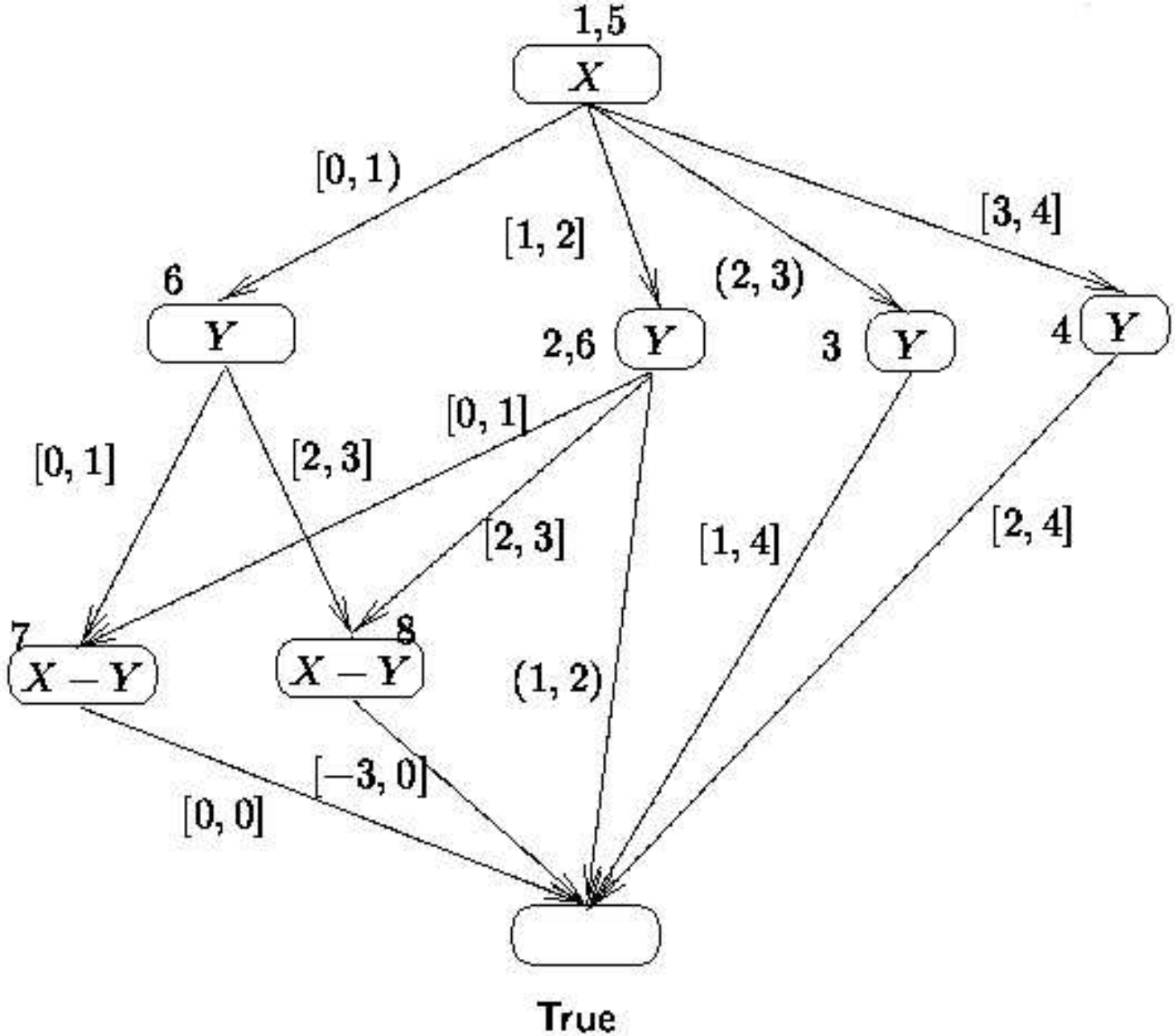


Operacje na CDDs – przykł ad

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

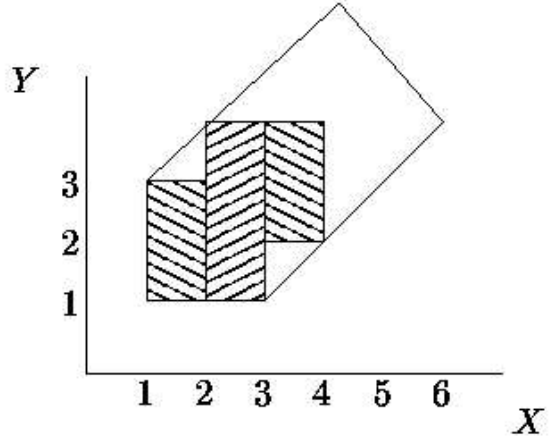


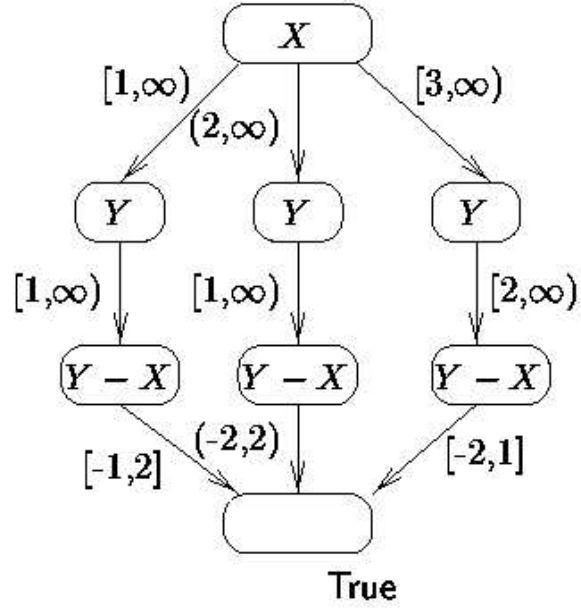



1,5
X
[0, 1)
[1, 2]
(2, 3)
[3, 4]
6
Y
2,6
Y
3
Y
4
Y
[0, 1]
[2, 3]
[0, 1]
[2, 3]
[1, 4]
[2, 4]
7
X − Y
8
X − Y
(1, 2)
[−3, 0]
[0, 0]
True

Operacje na CDDs

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





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