Praktyczne metody weryfikacji

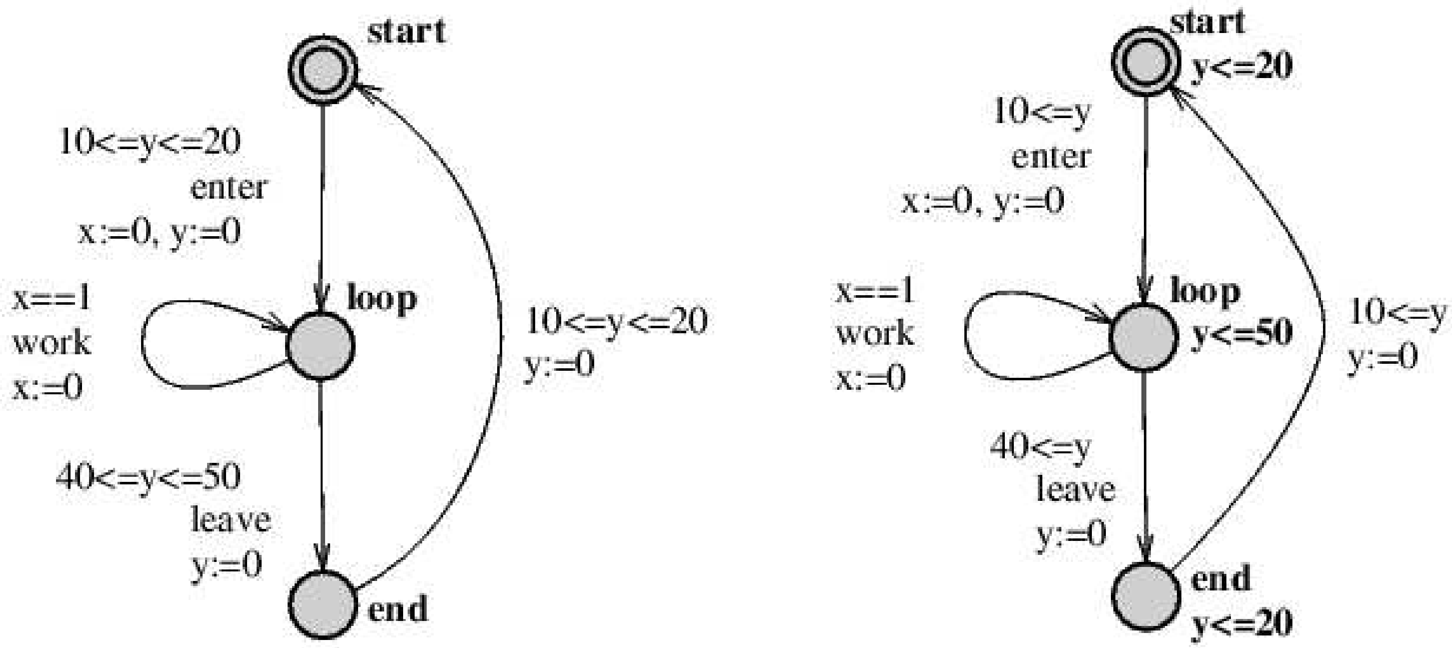
Wykład 10: Automaty czasowe

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



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

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

$$q_1 \xrightarrow{\psi,\ a,\ C':=0} q_2$$

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 : $\langle q_0, v_0\rangle \overset{t_1}{\leadsto} \langle q_0, v_0 + t_1\rangle \xrightarrow{a} \langle q_1, v_1\rangle \overset{t_2}{\leadsto} \ldots$

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

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

Warianty:

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

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

Blokada: nie istnieje t t. że

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

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

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

Pilność (niezmienniki)

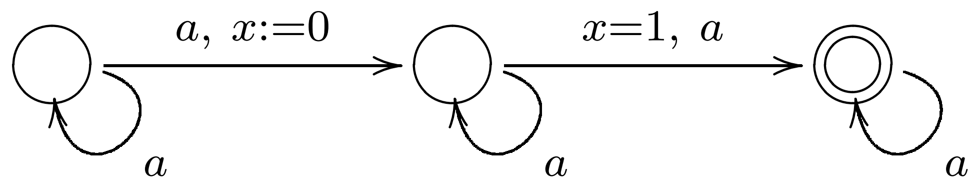
automaty	pustość	uniwersalność
bezczasowe	NLOGSPACE	PSPACE
czasowe	PSPACE	nierozstrzygalna

– $L(A) \subseteq L(B)$

– tylko 1 zegar

– słowa skończone lub ω-słowa

Brak uzupełnienia :



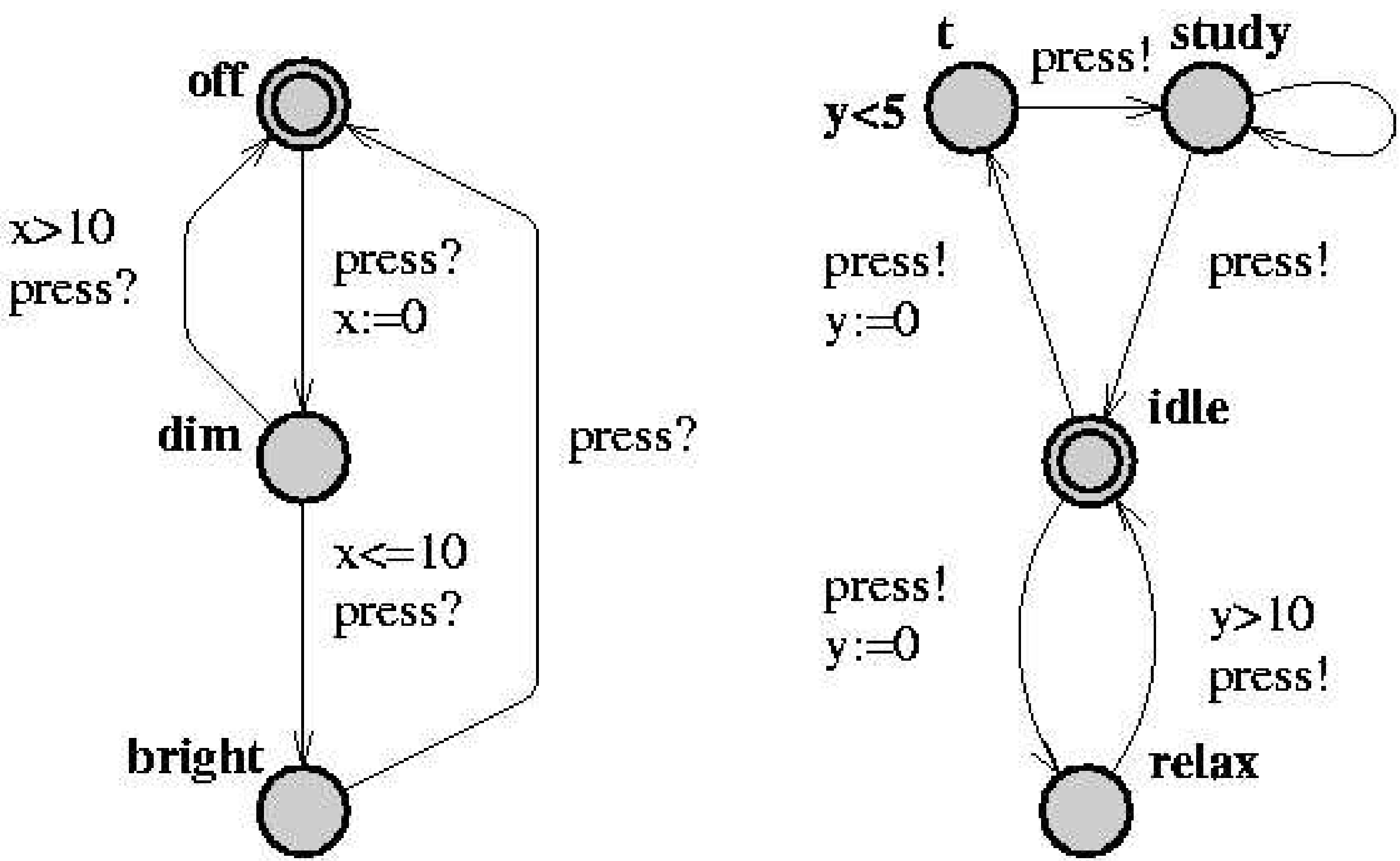
$L(\mathcal{A}_1)\ \cap\ L(\mathcal{A}_2)$ **?**

M(A)

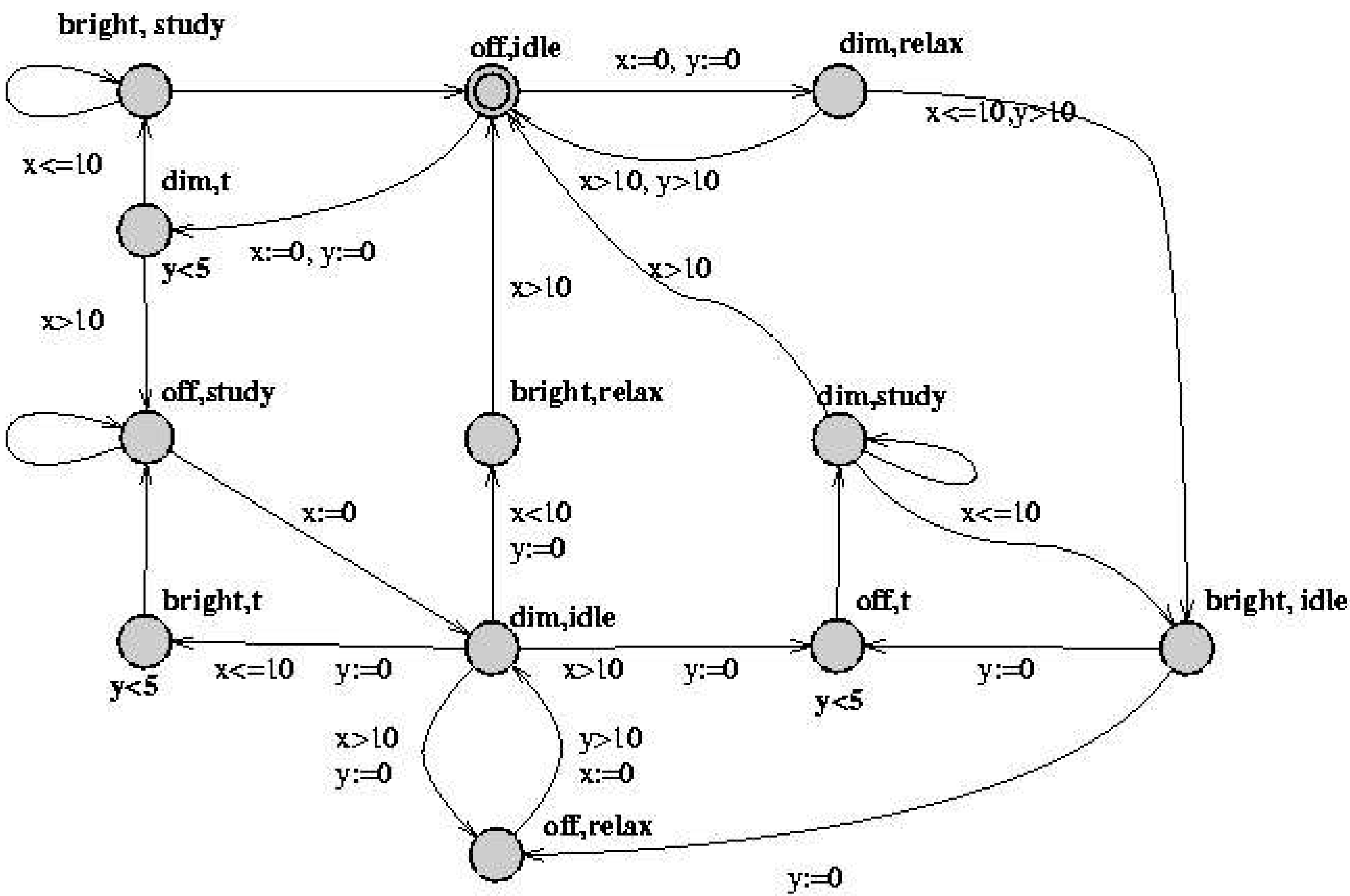
- stany: $\langle q, v\rangle \in Q \times (\mathbb{R}^+)^{\mathcal{C}}$
- stany pocz.: $\langle q_0, v_0\rangle$
- tranzycje: $\langle q, v\rangle \overset{t}{\rightsquigarrow} \langle q, v+t\rangle$ $\quad\quad$ $\langle q, v\rangle \xrightarrow{a} \langle q', v'\rangle$
- $L(\langle q, v\rangle) =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

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

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


off
x>10
press?
press?
x:=0
dim
press?
x<=10
press?
bright
t
y<5
press!
study
press!
y:=0
press!
idle
press!
y:=0
y>10
press!
relax

w UPPAALu

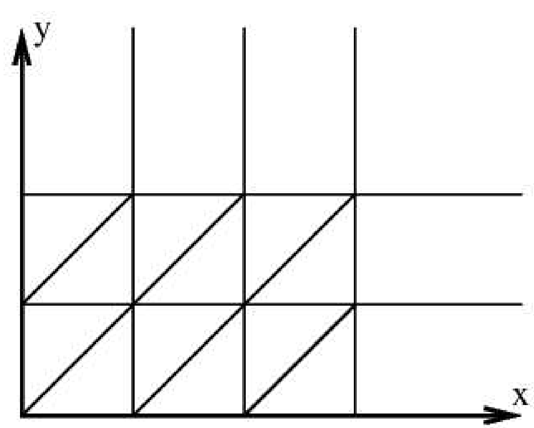

bright, study
off,idle
x:=0, y:=0
dim,relax
x<=10,y>10
x<=10
dim,t
x>10, y>10
x:=0, y:=0
y<5
x>10
x>10
x>10
off,study
bright,relax
dim,study
x:=0
x<10
y:=0
x<=10
bright,t
dim,idle
off,t
bright, idle
y<5
x<=10
y:=0
x>10
y:=0
y:=0
y<5
x>10
y:=0
y>10
x:=0
off,relax
y:=0

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 $v(y) \leq c_y \implies$

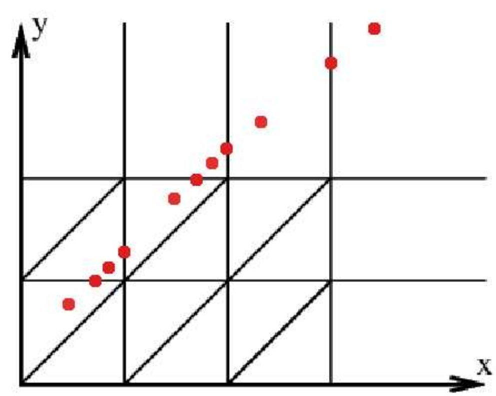
$$(\langle v(x) \rangle \leq \langle v(y) \rangle \iff \langle w(x) \rangle \leq \langle w(y) \rangle)$$



Liczba regionów:

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

$r \rightsquigarrow r'$

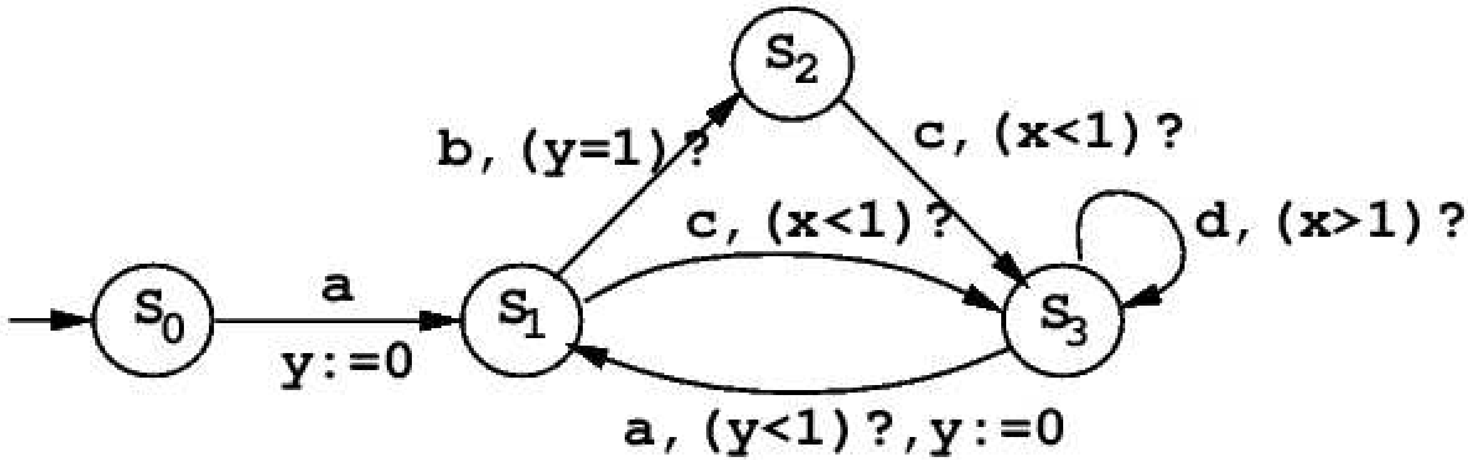


Automat „regionowy” R(A)

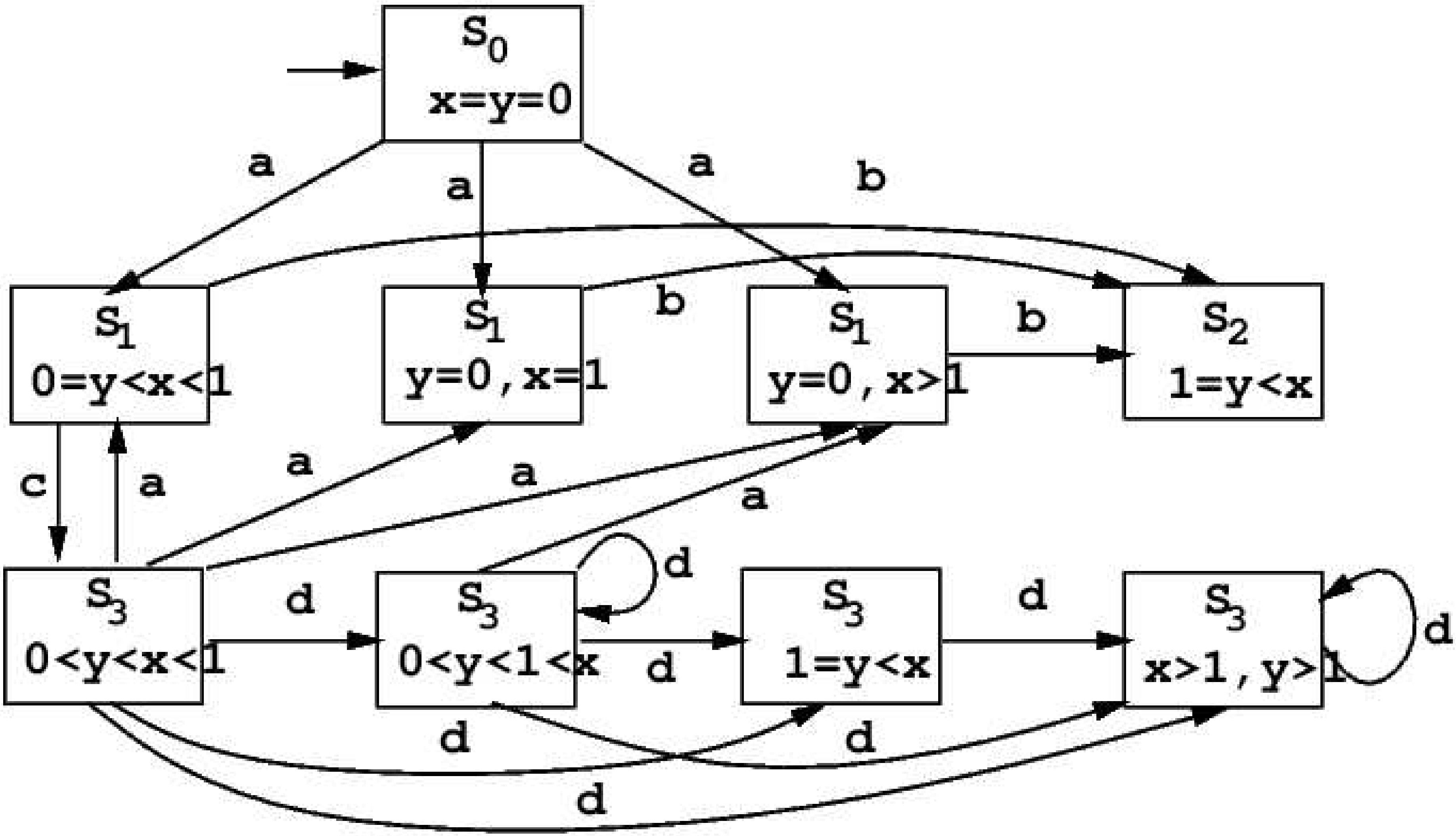
- stany: (q, r)
- tranzycje: $(q_1, r_1) \xrightarrow{a} (q_2, r_2) \iff \exists r,\ \langle q_1, a, \psi, \mathcal{C}', q_2 \rangle \in \rho$
  - $r_1 \rightsquigarrow r$
  - $r \models \psi \quad (r \subseteq \psi)$
  - $r_2 = r[\mathcal{C}' := 0]$

automat „symboliczny” $\qquad L(R(\mathcal{A})) = \mathrm{untime}(L(\mathcal{A}))$

Przykład



Przykład



S_0
x=y=0
a
a
a
b
S_1
0=y<x<1
S_1
y=0,x=1
b
S_1
y=0,x>1
b
S_2
1=y<x
c
a
a
a
a
d
S_3
0<y<x<1
d
S_3
0<y<1<x
d
S_3
1=y<x
d
S_3
x>1,y>1
d
d
d
d

Automat „strefowy” Z(A)

– stany: (q, ψ)

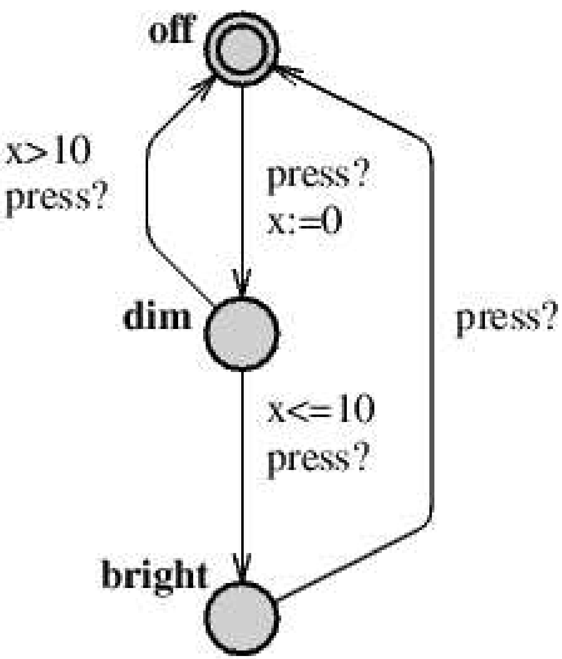
– tranzycje:

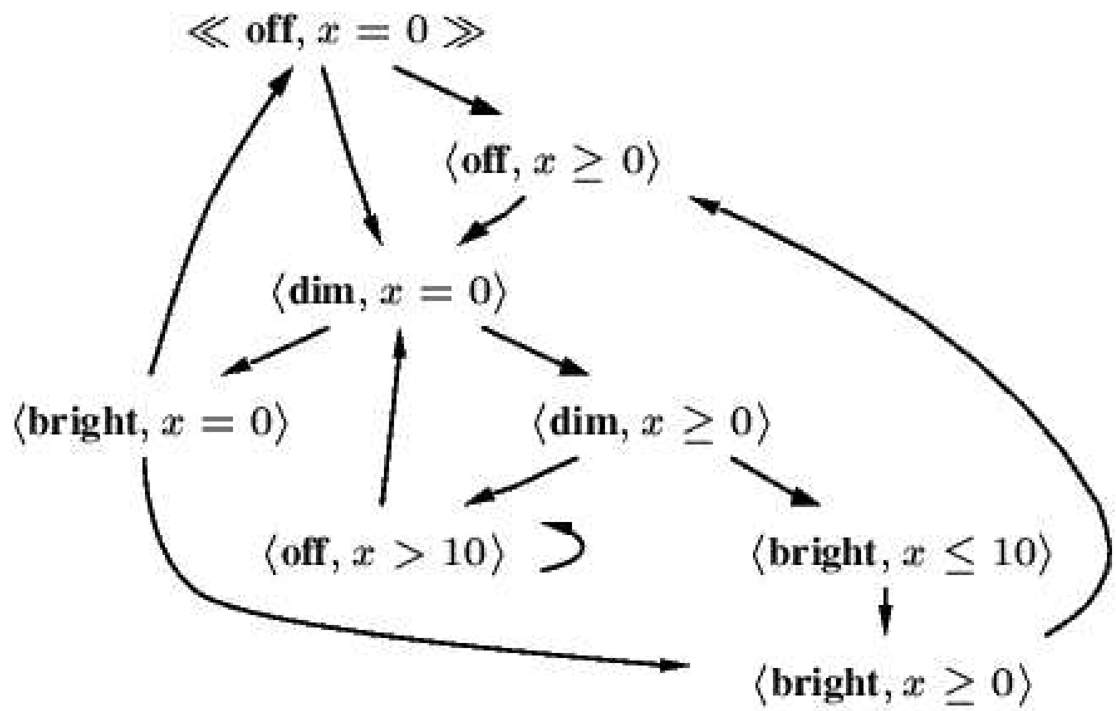
  – $(q, \psi) \rightsquigarrow (q, \psi^{\rightsquigarrow} \wedge \mathrm{niezm}(q))$

  – $(q_1, \psi_1) \xrightarrow{a} (q_2, (\psi_1 \wedge \psi)[\mathcal{C}' := 0] \wedge \mathrm{niezm}(q_2))$

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

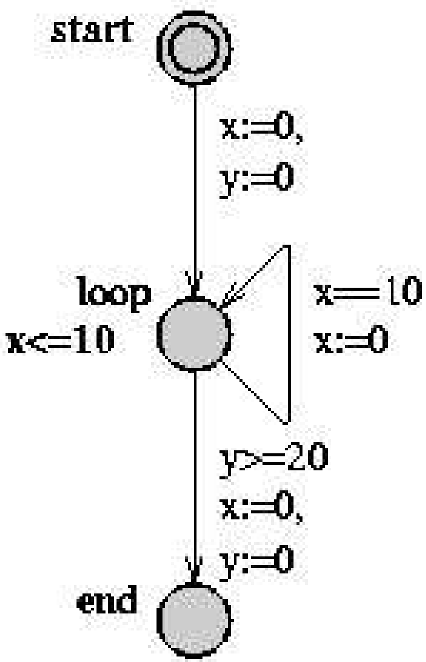
$Z(\mathcal{A})$

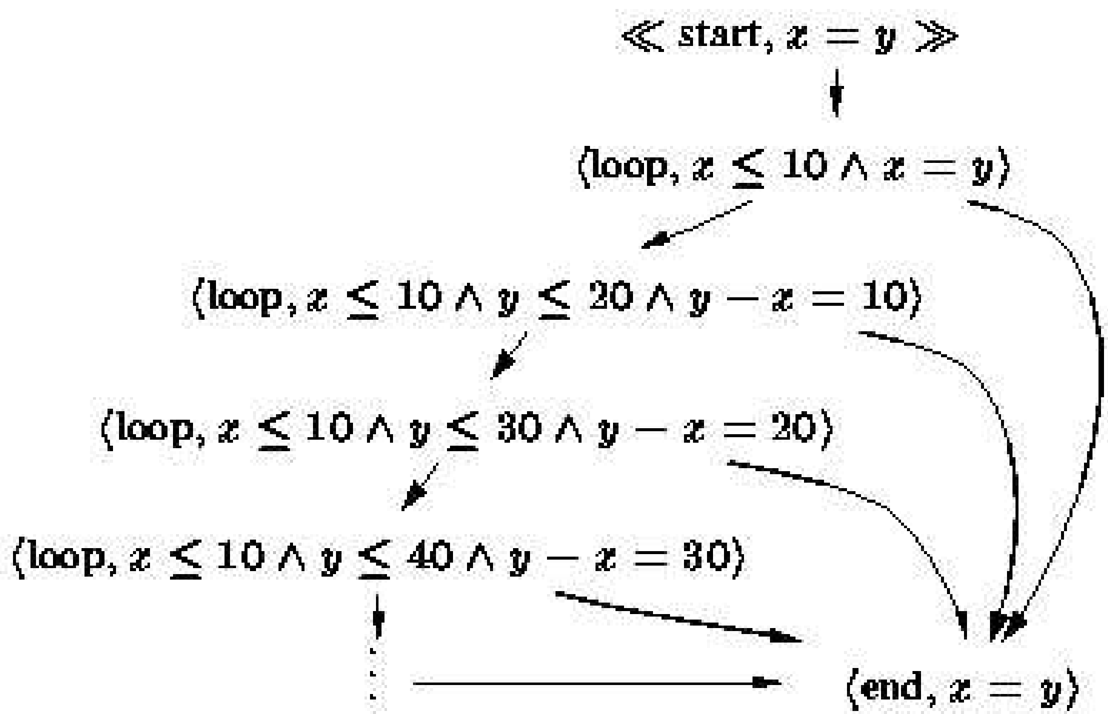




$R(\mathcal{A})$ ma > 50 stanów !

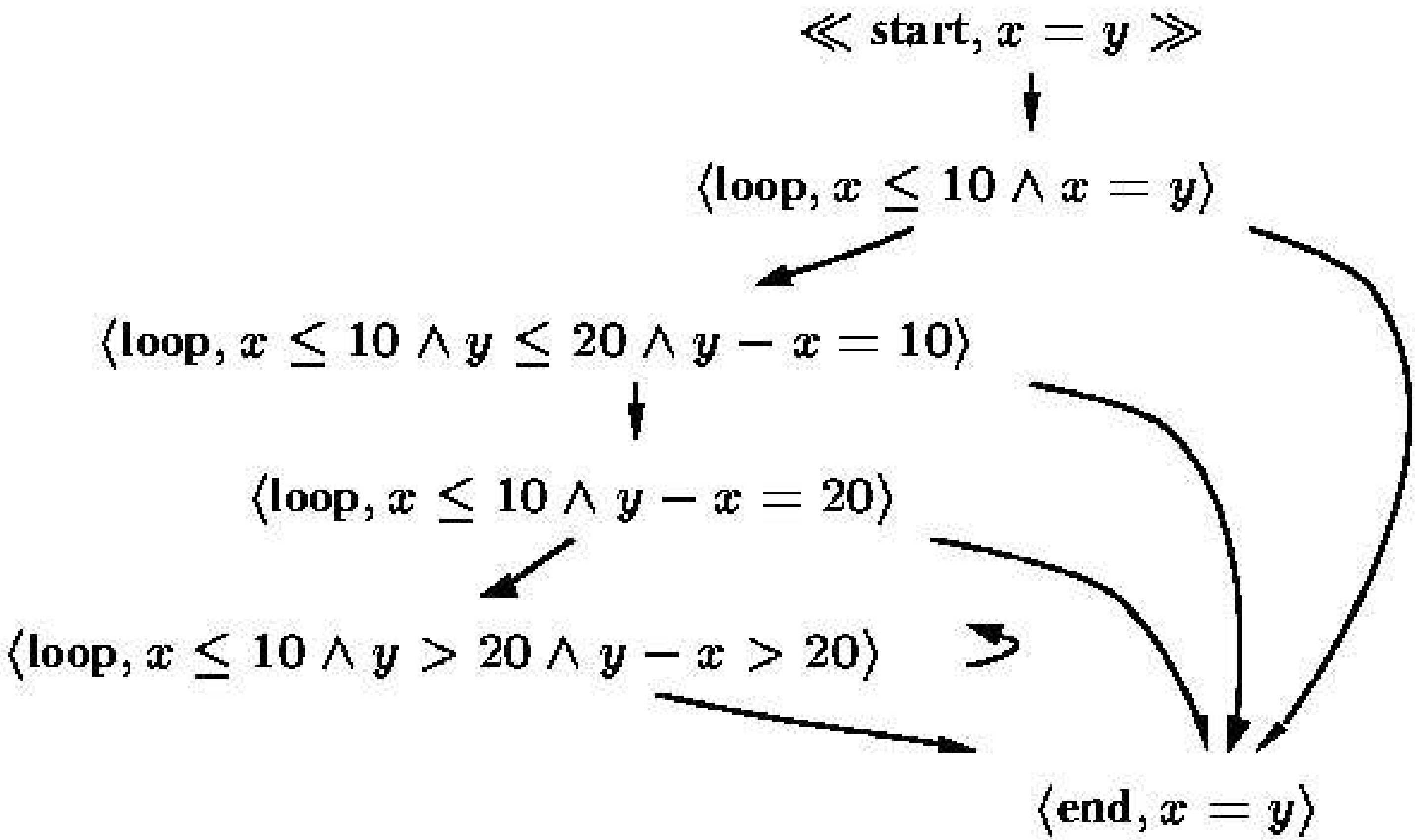
$Z(\mathcal{A})$ o nieskończenie wielu stanach





Przykład

$Z(\mathcal{A})$ po znormalizowaniu



III. Logiki czasowe

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

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:

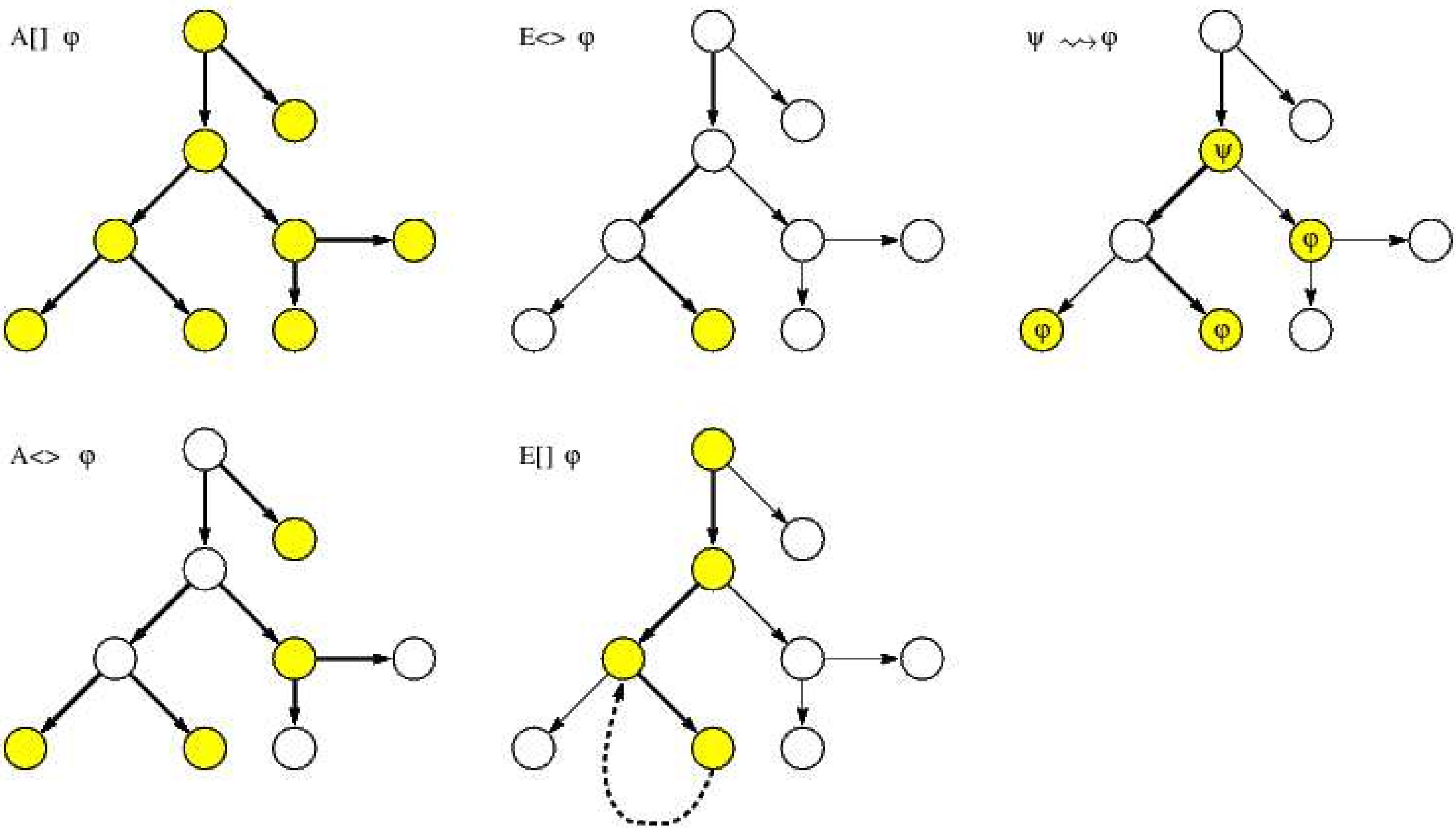
$$\mathsf{G}\, x.\ \big(p \implies \mathsf{F}\, y.\ (q \ \wedge\ y < x{+}5)\big)$$

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

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

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