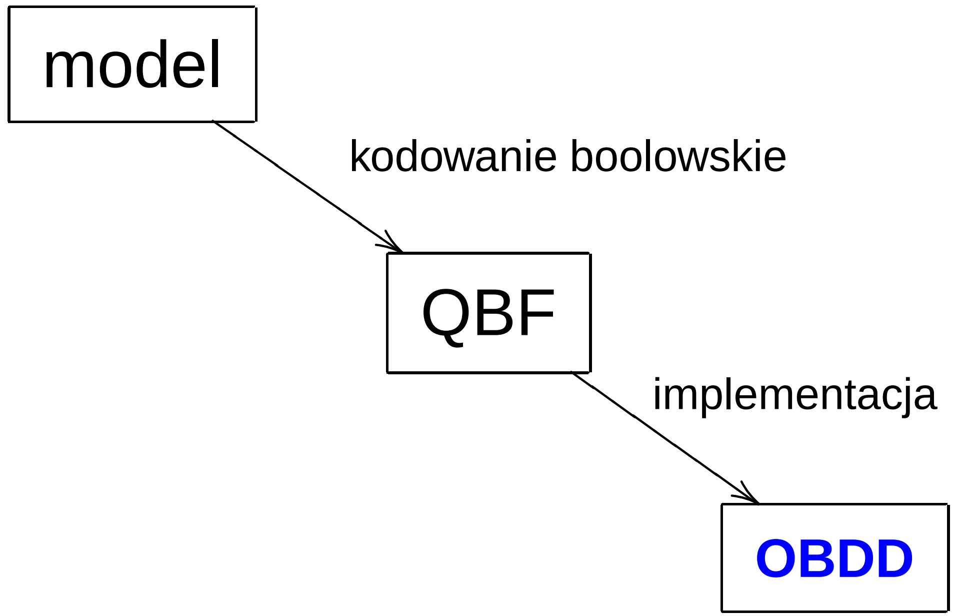
Praktyczne metody weryfikacji

Wykład 8: Weryfikacja symboliczna (II)

Symboliczna weryfikacja modelowa



weryfikacja modelowa = operacje na OBDDs

I. Weryfikacja modelowa

Przypomnienie

Punkty stałe w kracie zupełnej $\langle A, \leq \rangle$.

Niech $f : A \to A$ monotoniczna.

- najmniejszy p.s.: $\perp \leq f(\perp) \leq f^2(\perp) \leq \ldots \leadsto \mu Z.\, f(Z)$
- największy p.s.: $\top \geq f(\top) \geq f^2(\top) \geq \ldots \leadsto \nu Z.\, f(Z)$

Gdy A skończony, kres osiągamy po $\leq |A|$ krokach.

Przypomnienie

Punkty stałe w kracie zupełnej $\langle A, \leq \rangle$.

Niech $f : A \to A$ monotoniczna.

- najmniejszy p.s.: $\perp \leq f(\perp) \leq f^2(\perp) \leq \ldots \;\leadsto\; \mu Z.\, f(Z)$
- największy p.s.: $\top \geq f(\top) \geq f^2(\top) \geq \ldots \;\leadsto\; \nu Z.\, f(Z)$

Przykład: $A \;=\; \mathcal{P}(S)$

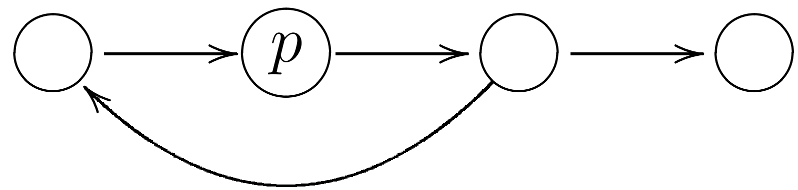
$Z \mapsto \mathsf{EX}\, Z$ $\quad\quad \mu Z.\, \mathsf{EX}\, Z \;=\; \perp = \emptyset$ $\quad\quad \nu Z.\, \mathsf{EX}\, Z \;=\;$ **?**

$Z \mapsto p \vee \mathsf{EX}\, Z$ $\quad\quad \mu Z.\, p \vee \mathsf{EX}\, Z \;=\;$ **?**

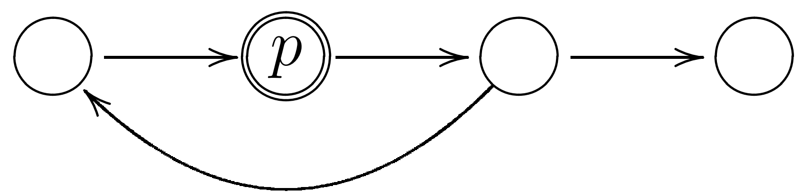
Przykład

$$\mathsf{EF}\,p \quad = \quad \mu Z.\, p \vee \mathsf{EX}\, Z$$

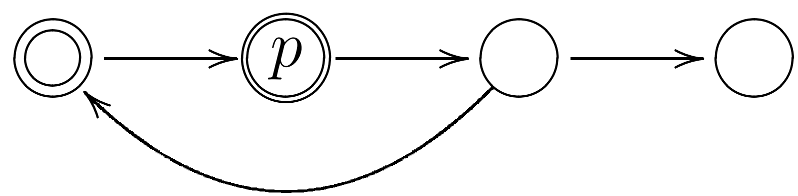
$\texttt{false}$



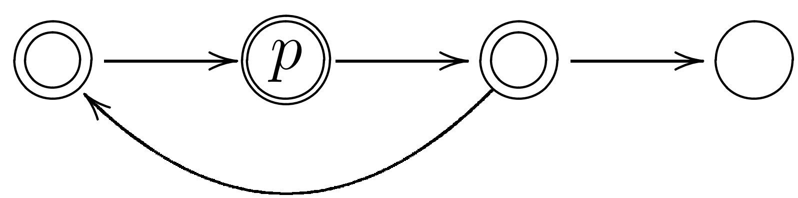
$p \vee \mathsf{EX}\,\texttt{false} \equiv p$



$p \vee \mathsf{EX}\, p$



$p \vee \mathsf{EX}\,(p \vee \mathsf{EX}\, p)$

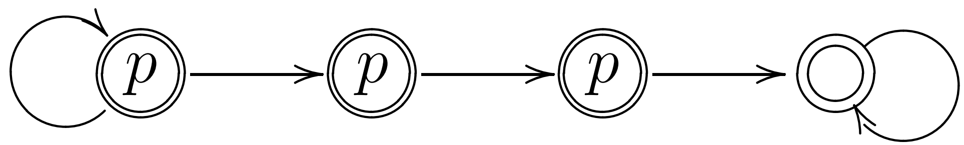


- $\mathsf{EF}\,\phi \;=\; \mu Z.\,\phi \vee \mathsf{EX}\,Z$ $\quad Z \mapsto \phi \vee \mathsf{EX}\,Z$
- $\mathsf{AF}\,\phi \;=\; \mu Z.\,\phi \vee \mathsf{AX}\,Z$ $\quad Z \mapsto \phi \vee \mathsf{AX}\,Z$
- $\mathsf{EG}\,\phi \;=\; \nu Z.\,\phi \wedge \mathsf{EX}\,Z$ $\quad Z \mapsto \phi \wedge \mathsf{EX}\,Z$
- $\mathsf{AG}\,\phi \;=\; \nu Z.\,\phi \wedge \mathsf{AX}\,Z$ $\quad Z \mapsto \phi \wedge \mathsf{AX}\,Z$
- $\mathsf{E}\,\phi\,\mathsf{U}\,\psi \;=\; \mu Z.\,\psi \vee \phi \wedge \mathsf{EX}\,Z$ $\quad Z \mapsto \psi \vee (\phi \wedge \mathsf{EX}\,Z)$
- $\mathsf{A}\,\phi\,\mathsf{U}\,\psi \;=\; \mu Z.\,\psi \vee \phi \wedge \mathsf{AX}\,Z$ $\quad Z \mapsto \psi \vee (\phi \wedge \mathsf{AX}\,Z)$
- ...

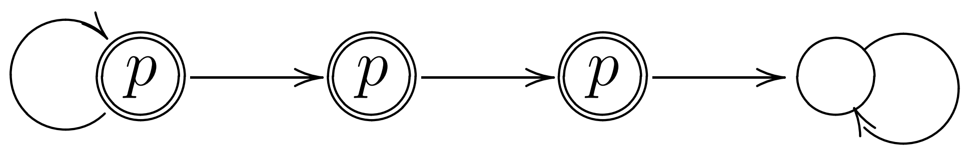
Przykład

$$\mathsf{EG}\,p \;=\; \nu Z.\,\phi \wedge \mathsf{EX}\,Z$$

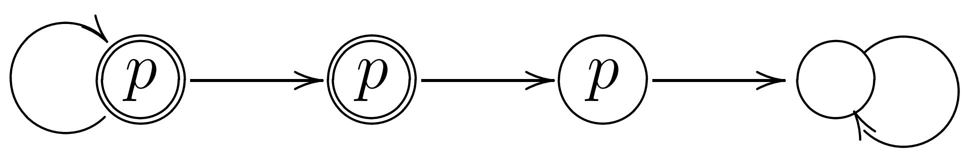
$\mathtt{true}$



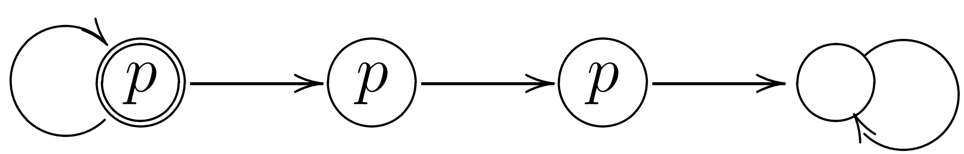
$p \wedge \mathsf{EX}\,\mathtt{true} \;\equiv\; p$



$p \wedge \mathsf{EX}\,p$



$p \wedge \mathsf{EX}\,(p \wedge \mathsf{EX}\,p)$



CTL ($\neg$, $\wedge$, **EX**, **E_U_**, **EG)** (wystarczą te spójniki)

$$\mathrm{Check} : \text{CTL} \mapsto \text{OBDD}$$

$$\boxed{\mathrm{Check}(\phi) \;\; \text{reprezentuje} \;\; \{s \mid s \models \phi\}}$$

Check : CTL $\rightarrow$ OBDD

$\boxed{\mathrm{Check}(\phi) \text{ reprezentuje } \{s \mid s \vDash \phi\}}$

$\mathrm{Check}(\mathsf{EX}\,\phi) \quad := \quad \exists \vec{x}'.\, \widehat{R}(\vec{x}, \vec{x}') \wedge f(\vec{x}')$ gdzie $f = \mathrm{Check}(\phi)$

$\mathrm{Check}(\mathsf{EX}\,\phi) \quad := \quad \mathsf{EX}\, f$

- $\mathsf{EX}\,\phi$
- $\mathsf{EX}\,Z$
- $\mathsf{EX}\,f$

Weryfikacja symboliczna (E _ U _)

$\mathrm{Check} : \mathsf{CTL} \to \mathsf{OBDD}$

$\boxed{\mathrm{Check}(\phi) \text{ reprezentuje } \{s \mid s \models \phi\}}$

$$\mathrm{Check}(\mathsf{E}\,\phi\,\mathsf{U}\,\psi) \;:=\; \mu Z.\, g \vee (f \wedge \mathsf{EX}\, Z) \qquad \text{gdzie} \quad f = \mathrm{Check}(\phi), \quad g = \mathrm{Check}(\psi)$$

$$Z \mapsto g \vee (f \wedge \exists \vec{x}'.\, \widehat{R}(\vec{x}, \vec{x}') \wedge Z[\vec{x}'/\vec{x}])$$

$$\begin{array}{lcl}
\mathtt{false} & & \\
g \vee (f \wedge \mathsf{EX}\, \mathtt{false}) & \equiv & g \\
g \vee (f \wedge \mathsf{EX}\, (g \vee (f \wedge \mathsf{EX}\, \mathtt{false}))) & \equiv & g \vee (f \wedge \mathsf{EX}\, g) \\
\ldots & \equiv & g \vee (f \wedge \mathsf{EX}\, (g \vee (f \wedge \mathsf{EX}\, g
\end{array}$$

$$\downarrow$$

$$\mu Z.\, g \vee (f \wedge \mathsf{EX}\, Z)$$

Weryfikacja symboliczna (EG _)

Check : CTL $\longrightarrow$ OBDD

$\boxed{\mathrm{Check}(\phi) \text{ reprezentuje } \{s \mid s \models \phi\}}$

$\mathrm{Check}(\text{EG}\,\phi) \quad := \quad \nu Z.\ f \wedge \text{EX}\,Z$ gdzie $f = \mathrm{Check}(\phi)$

$$Z \mapsto f \wedge \exists \vec{x}'.\ \widehat{R}(\vec{x}, \vec{x}') \wedge Z[\vec{x}'/\vec{x}]$$

EX ϕ	E ϕ U ψ	EG ϕ
EX Z	E Z U Z'	EG Z
EX f	E f U g	EG f

II. Sprawiedliwość

$\mathbf{F} = \{\psi_1, \ldots, \psi_n\}$, $\psi_i \in$ CTL $\qquad \mapsto \quad F = \{Z_1, \ldots, Z_n\}$

$s \models_{\mathbf{F}} p \iff p \in L(s) \wedge \exists$ sprawiedliwa Π z s

$s \models_{\mathbf{F}} \mathsf{A}\,\phi\,\mathsf{U}\,\psi \iff \forall$ sprawiedliwej Π z s . $\Pi \models \phi\,\mathsf{U}\,\psi$

$s \models_{\mathbf{F}} \mathsf{E}\,\phi\,\mathsf{U}\,\psi \iff \exists$ sprawiedliwa Π z s . $\Pi \models \phi\,\mathsf{U}\,\psi$

$s \models_{\mathbf{F}} \mathsf{AX}\,\phi \iff \forall$ sprawiedliwej Π z s . $\Pi \models \mathsf{X}\,\phi$

$s \models_{\mathbf{F}} \mathsf{EX}\,\phi \iff \exists$ sprawiedliwa Π z s . $\Pi \models \mathsf{X}\,\phi$

$\mathbf{F} = \{h_1, \ldots, h_n\}$, $h_i \in$ OBDD

$\mathbf{F} = \{\psi_1, \ldots, \psi_n\}$, $\psi_i \in$ CTL $\quad\mapsto\quad F = \{Z_1, \ldots, Z_n\}$

$\{s \mid s \models_{\mathbf{F}}$ EG $\phi\}$ = największy Z t. że jeśli $s \in Z$, to

- $s \models \phi$
- $\forall i \leq n \,.\, \exists s' \,.\, s \to \ldots \to s' \in Z_i$, $s' \neq s$, wszystkie stany po drodze spełniają ϕ

EG ϕ $= \nu Z.\, \phi \wedge \bigwedge_{i=1}^{n}$ EX E ϕ U $(\psi_i \wedge Z)$ (alternacja!)

Tw.:

$$\mathsf{EG}\,\phi \;=\; \nu Z.\, \phi \;\wedge\; \bigwedge_{i=1}^{n} \mathsf{EX}\; \mathsf{E}\,\phi\,\mathsf{U}\,(\psi_i \wedge Z)$$

Dowód:

$$\mathsf{EG}\,\phi \;=\; \phi \;\wedge\; \bigwedge_{i=1}^{n} \mathsf{EX}\; \mathsf{E}\,\phi\,\mathsf{U}\,(\psi_i \wedge \mathsf{EG}\,\phi)$$

$$Z \;=\; \phi \;\wedge\; \bigwedge_{i=1}^{n} \mathsf{EX}\; \mathsf{E}\,\phi\,\mathsf{U}\,(\psi_i \wedge Z) \;\Longrightarrow\; Z \subseteq \mathsf{EG}\,\phi$$

Sprawiedliwa w. symboliczna (EG _)

Check : CTL $\rightarrow$ OBDD

$\boxed{\mathrm{Check}(\phi) \text{ reprezentuje } \{s \mid s \vDash \phi\}}$

$\mathbf{F} = \{\psi_1, \ldots, \psi_n\}$, $\psi_i \in$ CTL $\quad \mapsto \quad F = \{h_1, \ldots, h_n\}$, $h_i \in$ OBDD

$\mathrm{Check}(\mathsf{EG}\,\phi) \quad := \quad \nu Z.\ f \ \wedge\ \bigwedge_{i=1}^{n} \mathsf{EX}\ \mathsf{E}\, f\, \mathsf{U}\, (h_i \wedge Z)$

gdzie $\quad f = \mathrm{Check}(\phi)$

$$Z \mapsto f \wedge \bigwedge_{i=1}^{n} \mathsf{EX}\ \mathsf{E}\,\phi\,\mathsf{U}\,(h_i \wedge Z)$$

Sprawiedliwa w. symboliczna

$$\texttt{fair} \quad := \quad \mathrm{Check}(\,\mathsf{EG}\,\texttt{true})$$

$$\mathrm{Check}(\,\mathsf{EX}\,\phi) \quad := \quad \exists \vec{x}'.\, \widehat{R}(\vec{x}, \vec{x}') \wedge f(\vec{x}') \wedge \texttt{fair}(\vec{x}')$$

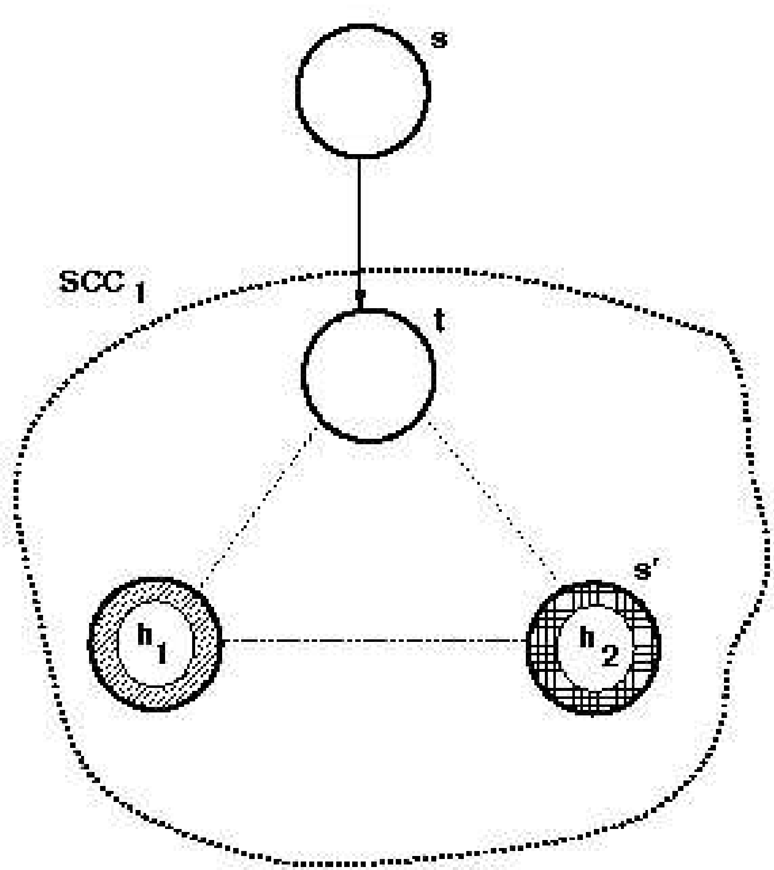
gdzie $f = \mathrm{Check}(\phi)$

$$\mathrm{Check}(\,\mathsf{E}\,\phi\,\mathsf{U}\,\psi) \quad := \quad \mu Z.\, (g \wedge \texttt{fair}) \vee (f \wedge \mathsf{EX}\, Z)$$

gdzie $f = \mathrm{Check}(\phi)$
$g = \mathrm{Check}(\psi)$

III. (Kontr)przykłady

kontrprzykład dla AF ϕ = przykład dla EG $\neg\phi$



kontrprzykład dla $\mathrm{AF}\,\phi$ = przykład dla $\mathrm{EG}\,\neg\phi$

kontrprzykład dla $\mathrm{AG}\,\phi$ = przykład dla $\mathrm{EF}\,\neg\phi$

(sprawiedliwy przykład to zawsze nieskończona scieżka)

kontrprzykład dla $\mathrm{EF}\,\phi$ = **?**

kontrprzykład dla $\mathrm{EG}\,\phi$ = **?**

Jak obliczyć **symbolicznie** przykład dla:

- EG ϕ
- E ϕ U ψ
- EX ϕ ?

Przykład dla E _ U _

Obliczenie E f U g:

$$Q_0 \subseteq Q_1 \subseteq \ldots \qquad (1 \leq i \leq n)$$

$s \in Q_j \iff$ można dojść „po f" z s do g w $\leq j$ krokach

Obliczenie przykładu:

– niech j minimalne t. że $s \in Q_j$

– zrekonstruuj $s = s_j \to s_{j-1} \to \ldots \to s_0 \in g$

Jak obliczyć **symbolicznie** sprawiedliwy przykład dla:

- EG ϕ
- E ϕ U ψ
- EX ϕ ?

$$\text{EG}\, f \;=\; \nu Z.\, f \;\wedge\; \bigwedge_{i=1}^{n} \text{EX E}\, f\, \text{U}\, (h_i \wedge Z)$$

ostatnia iteracja $Z \;\mapsto\; f \;\wedge\; \bigwedge_{i=1}^{n} \text{EX E}\, f\, \text{U}\, (h_i \wedge Z)$:

obliczenie $\text{E}\, f\, \text{U}\, (h_i \wedge Z)$: $\quad Z = \text{EG}\, f$

$$Q_0^i \;\subseteq\; Q_1^i \;\subseteq\; \ldots \qquad (1 \leq i \leq n)$$

$s \in Q_j^i \iff$ można dojść „po f” z s do $(h_i \wedge \text{EG}\, f)$

w $\leq j$ krokach

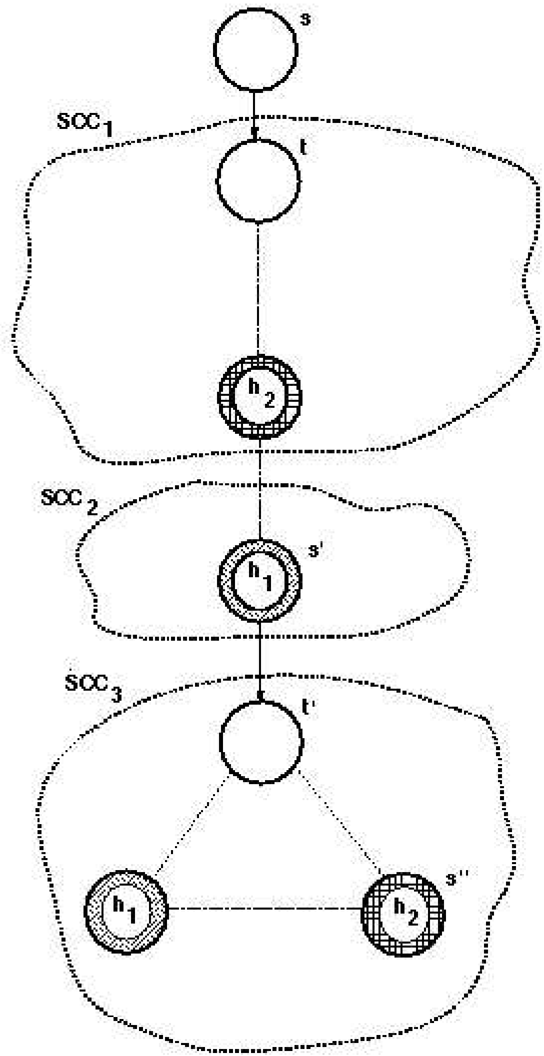
Sprawiedliwy przykład dla EG _

$$\mathsf{EG}\, f \;=\; \nu Z.\; f \;\wedge\; \bigwedge_{i=1}^{n} \mathsf{EX}\; \mathsf{E}\, f\, \mathsf{U}\, (h_i \wedge Z)$$

$s := s_0$ stan początkowy
$I := \{1, \ldots, n\}$
powtarzaj
znajdź t t. że $s \to t$, $t \in Q^i_j$, $i \in I$, j minimalne
zrekonstruuj $t = t_j \to t_{j-1} \to \ldots \to t_0 \in (h_i \wedge \mathsf{EG}\, f)$
$I := I \setminus \{i \mid t_0 \in h_i\}$
$s := t_0$ $\qquad I := I \setminus \{i \mid t \in Q^i_j\}$
aż $I = \emptyset$

$s' := s \qquad \mapsto \qquad$ ścieżka $s_0 \to \ldots \to s'$

Sprawiedliwy przykład dla EG _



Sprawiedliwy przykład dla EG _

$$\text{EG}\, f \;=\; \nu Z.\, f \;\wedge\; \bigwedge_{i=1}^{n} \text{EX E}\, f \,\text{U}\, (h_i \wedge Z)$$

mamy ścieżkę $s_0 \to \ldots \to s'$ niech $t =$ pierwsze t_0

(a) jesli $s' \models$ EX E f U $\{t\}$ stop

w p. p. restart: $s_0 := s'$, $I := \{1, \ldots, n\}$

ulepszenie:

(b) oblicz E f U $\{t\}$

gdy tylko $\neg(s \models$ E f U $\{t\})$, restart: $s_0 := s$, $I := \{1, \ldots, n\}$

Sprawiedliwy przykład dla $\mathsf{E}\_\mathsf{U}\_$, $\mathsf{EX}\_$

Przykład dla $\mathsf{E}\,\phi\,\mathsf{U}\,(\psi \wedge \texttt{fair})$ lub $\mathsf{EX}\,(\phi \wedge \texttt{fair})$ uzupełniamy o sprawiedliwy przykład dla $\mathsf{EG}\,\texttt{true}$.

IV. Jak oblicza się EX f ?

$$\text{EX}\, f \;:=\; \exists \vec{x}'.\ \widehat{R}(\vec{x}, \vec{x}') \wedge f(\vec{x}')$$

operacja $\exists\wedge(g, h, V) \;:=\; \exists V.\ g \wedge h$ (V – zbiór zmiennych)

$\widehat{R}(x_1, \ldots, x_m, x'_1, \ldots, x'_m)$

$f(x_1, \ldots, x_m) \;\mapsto\; f'(x'_1, \ldots, x'_m)$ $x_i \leq x_j \iff x'_i \leq x'_j$

$$\text{EX}\, f \;=\; \exists\wedge(\widehat{R}, f', \{x'_1, \ldots, x'_m\})$$

$\exists\wedge(\,f,\ g, V)$ $\qquad$ $(\,\exists V.\ f \wedge g\,)$

- f, g końcowe: $\mathrm{val}(\exists\wedge(f, g, V)) \ := \ \mathrm{val}(f) \wedge \mathrm{val}(g)$
- f końcowe, g nie: $\exists\wedge(f, g, V) \ := \ \texttt{false}$ albo $\exists V.\ g$
- $x = \mathrm{var}(f) \leq \mathrm{var}(g)$:

  $l := \exists\wedge(f|_{x\leftarrow 0}, g|_{x\leftarrow 0}, V)$, $\qquad h := \exists\wedge(f|_{x\leftarrow 1}, g|_{x\leftarrow 1}, V)$

  - $x \in V$: $\quad \exists\wedge(f, g, V) \ := \ l \vee h$
  - $x \notin V$: $\quad \mathrm{lo}(\exists\wedge(f, g, V)) \ := \ l \qquad \mathrm{hi}(\exists\wedge(f, g, V)) := h$

$$f \bullet g \ = \ \neg x \wedge (f|_{x\leftarrow 0} \bullet g|_{x\leftarrow 0}) \ \vee \ x \wedge (f|_{x\leftarrow 1} \bullet g|_{x\leftarrow 1})$$

$$\mathsf{EX}\, f \;:=\; \exists \vec{x}'.\, \widehat{R}(\vec{x},\vec{x}') \wedge f(\vec{x}')$$

Model synchroniczny: $\widehat{R} \;=\; \widehat{R}_1 \;\wedge\; \widehat{R}_2 \wedge \;\ldots\; \wedge\; \widehat{R}_n$

Model asynchroniczny: $\widehat{R} \;=\; R'_1 \;\vee\; R'_2 \vee \;\ldots\; \vee\; R'_n$

$$R'_i \;=\; \widehat{R}_i \wedge\; \bigwedge_{j \neq i} \mathrm{Id}_j$$

Czy da się wykorzystać tę dodatkową strukturę ?

Model asynchroniczny: $\widehat{R} \;=\; R'_1 \;\vee\; R'_2 \vee \;\ldots\; \vee\; R'_n$

$$R'_i \;=\; \widehat{R}_i \wedge \; \bigwedge_{j \neq i} x_j = x'_j$$

$$\exists \vec{x}'.\ \widehat{R} \wedge f(\vec{x}') \quad \equiv \quad \exists \vec{x}'.\ (R'_1 \wedge f(\vec{x}')) \;\vee\; \ldots \;\vee\; (R'_n \wedge f(\vec{x}'))$$

$$\equiv \quad \big(\exists \vec{x}'.\ R'_1 \wedge f(\vec{x}')\big) \;\vee\; \ldots \;\vee\; \big(\exists \vec{x}'.\ R'_n \wedge f(\vec{x}')\big)$$

$$\exists \vec{x}'.\ R'_i \wedge f(\vec{x}') \quad \equiv \quad \exists \vec{x}'.\ \widehat{R}_i \wedge \big(\bigwedge_{j \neq i} x_j = x'_j\big) \wedge f(\vec{x}')$$

$$\equiv \quad \exists x'_i.\ \widehat{R}_i(\vec{x}, x'_i) \wedge f(x_1, \ldots, x_{i-1}, x'_i, x_{i+1}, \ldots, x_m)$$

Model synchroniczny: $\widehat{R} \;=\; \widehat{R}_1 \wedge \widehat{R}_2 \wedge \ldots \wedge \widehat{R}_n$

$$\exists \vec{x}'.\, \widehat{R}_1(\vec{x}, \vec{x}') \;\wedge\; \ldots \;\wedge\; \widehat{R}_n(\vec{x}, \vec{x}') \;\wedge\; f(\vec{x}')$$

– relacje $\widehat{R}_i$ są lokalne

– „wczesna" kwantyfikacja

– heurystyki

Przykład: licznik 3-bitowy

$$
\begin{aligned}
\widehat{R}_0(\vec{x}, x'_0) &= (x'_0 = \neg x_0) \\
\widehat{R}_1(\vec{x}, x'_1) &= (x'_1 = x_0 \text{ xor } x_1) \\
\widehat{R}_2(\vec{x}, x'_2) &= (x'_2 = (x_0 \wedge x_1) \text{ xor } x_2)
\end{aligned}
$$

$$\exists x'_2 \exists x'_1 \exists x'_0 .\ f(x'_0, x'_1, x'_2) \ \wedge\ \widehat{R}_0(\vec{x}, x'_0) \ \wedge\ \widehat{R}_1(\vec{x}, x'_1) \ \wedge\ \widehat{R}_2(\vec{x}, x'_2)$$

$$\exists x'_2 \Big(\exists x'_1 \exists x'_0 .\ f(x'_0, x'_1, x'_2) \ \wedge\ \widehat{R}_0(\vec{x}, x'_0) \ \wedge\ \widehat{R}_1(\vec{x}, x'_1)\Big) \ \wedge\ \widehat{R}_2(\vec{x}, x'_2)$$

$$\exists x'_2 \Big(\exists x'_1 \Big(\exists x'_0 .\ f(x'_0, x'_1, x'_2) \ \wedge\ \widehat{R}_0(\vec{x}, x'_0)\Big) \ \wedge\ \widehat{R}_1(\vec{x}, x'_1)\Big) \ \wedge\ \widehat{R}_2(\vec{x}, x'_2)$$

$$\Big(\exists x'_1 \Big(\exists x'_0 .\ f(x'_0, x'_1, x'_2) \ \wedge\ \widehat{R}_0(x_0, x'_0)\Big) \ \wedge\ \widehat{R}_1(x_0, x_1, x'_1)\Big) \wedge \widehat{R}_2(x_0, x_1, x_2,$$

Przykład

$$\exists x_2' \quad \Big(\exists x_1' \quad \Big(\exists x_0' \quad f(x_0', x_1', x_2') \ \wedge\ \widehat{R}_0(x_0, x_0')\Big)$$
$$\wedge \qquad \widehat{R}_1(x_0, x_1, x_1')\Big)$$
$$\wedge \qquad \widehat{R}_2(x_0, x_1, x_2, x_2')$$

- ciąg operacji $\exists\wedge$
- optymalna kolejność procesów (a nie zmiennych):
  - szybka eliminacja zmiennych ($\exists$)
  - wolne wprowadzanie zmiennych

Co jeszcze można policzyć za pomocą OBDD ?

- $L_\omega(\mathcal{A}) \neq \emptyset$ sprawiedliwy EG `true`
- weryfikacja LTL
- $L_\omega(\mathcal{A}_1) \subseteq L_\omega(\mathcal{A}_2)$
- blokady, stany osiągalne
- równoważność (bi)symulacyjna
- weryfikacja rachunku μ
- ...