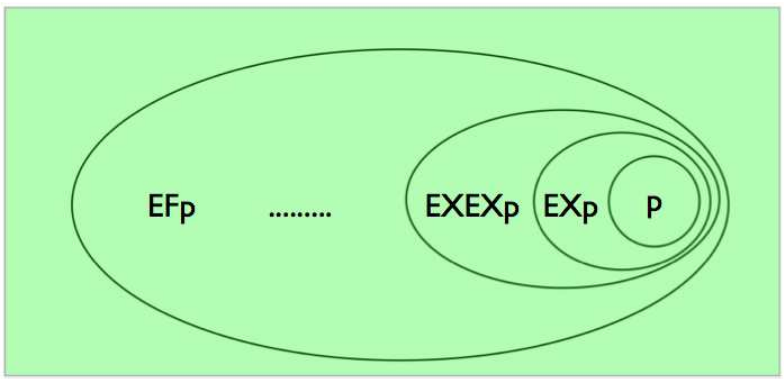
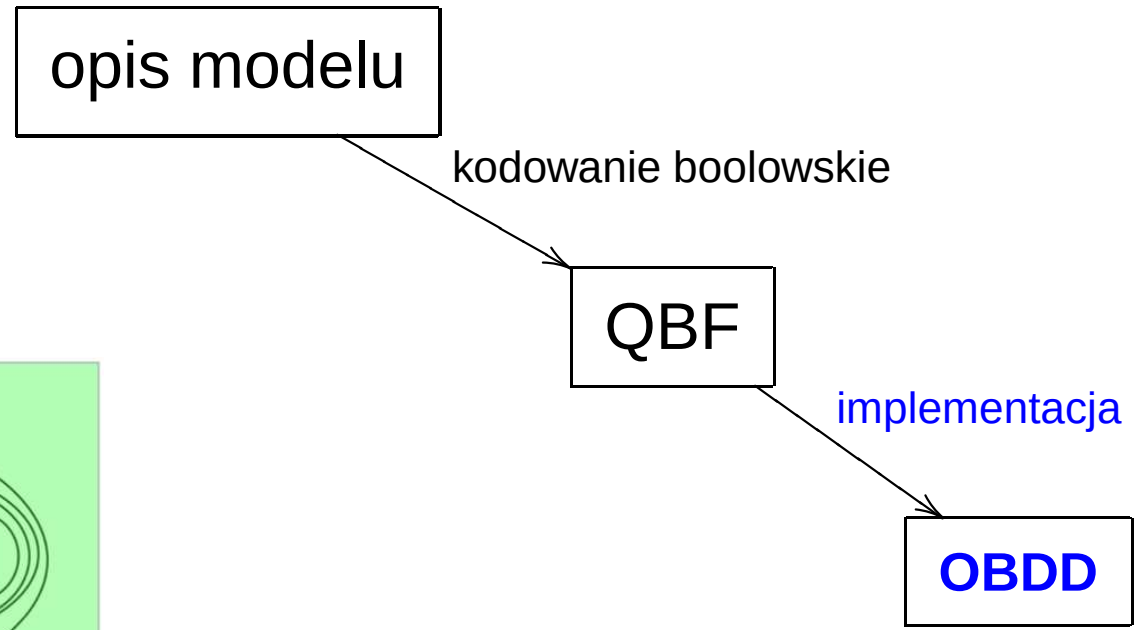
Weryfikacja wspomagana komputerowo

Wykład 7: Weryfikacja symboliczna II

Symboliczna weryfikacja modelowa





weryfikacja modelowa = operacje na OBDDs

I. Sprawiedliwość

II. (Kontr)przykłady

III. Jak oblicza się EX f ?

I. Sprawiedliwość

Sprawiedliwy CTL

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

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

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

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

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

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

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

Sprawiedliwy EG

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

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

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

Sprawiedliwy EG

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

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

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

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

Sprawiedliwy EG

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

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

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

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

$\mathsf{EG}\,\phi \;=\; \nu Z.\, \phi \wedge \bigwedge_{i=1}^{n} \mathsf{EX}\,\mu Y.(\psi_i \wedge Z) \vee (\phi \wedge \mathsf{EX}\,Y)$ alternacja!

Sprawiedliwy EG

Tw.:

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

Dowód:

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

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

Sprawiedliwa w. symboliczna (EG _)

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

$\mathrm{Check}(\phi)$ reprezentuje $\{s \mid s \models_{\mathbf{F}} \phi\}$

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

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

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

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

Sprawiedliwa w. symboliczna

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

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

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

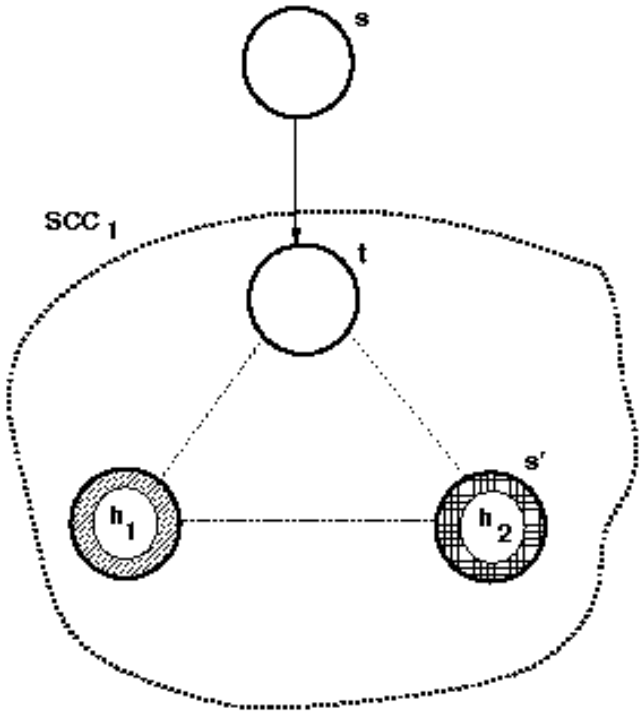
$$\text{Check}(\,\mathsf{E}\,\phi\,\mathsf{U}\,\psi) \quad := \quad \mu Z.\ (g \wedge \texttt{fair}) \vee (f \wedge \mathsf{EX}\, Z)$$

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

II. (Kontr)przykłady

Kontrprzykład

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



[Clarke, Grumberg, Long 1994]

Kontrprzykład

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

Kontrprzykład symbolicznie

Jak obliczyć **symbolicznie** przykład dla:

- $\mathsf{EG}\,\phi$
- $\mathsf{E}\,\phi\,\mathsf{U}\,\psi$
- $\mathsf{EX}\,\phi$?

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

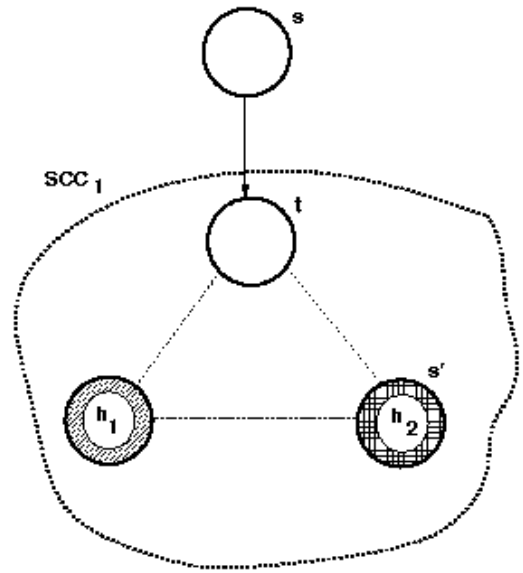
Obliczenie przykładu dla $s \vDash$ E f U g:

- niech j minimalne t. że $s \in Q_j$
- zrekonstruuj $s = s_j \to s_{j-1} \to \ldots \to s_0 \in g$

Kontrprzykład symbolicznie

Jak obliczyć **symbolicznie** sprawiedliwy przykład dla:

- $\mathrm{EG}\,\phi$
- $\mathrm{E}\,\phi\,\mathrm{U}\,\psi$
- $\mathrm{EX}\,\phi$?



[Clarke, Grumberg, Long 1994]

Sprawiedliwy przykład dla EG _

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

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

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

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

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

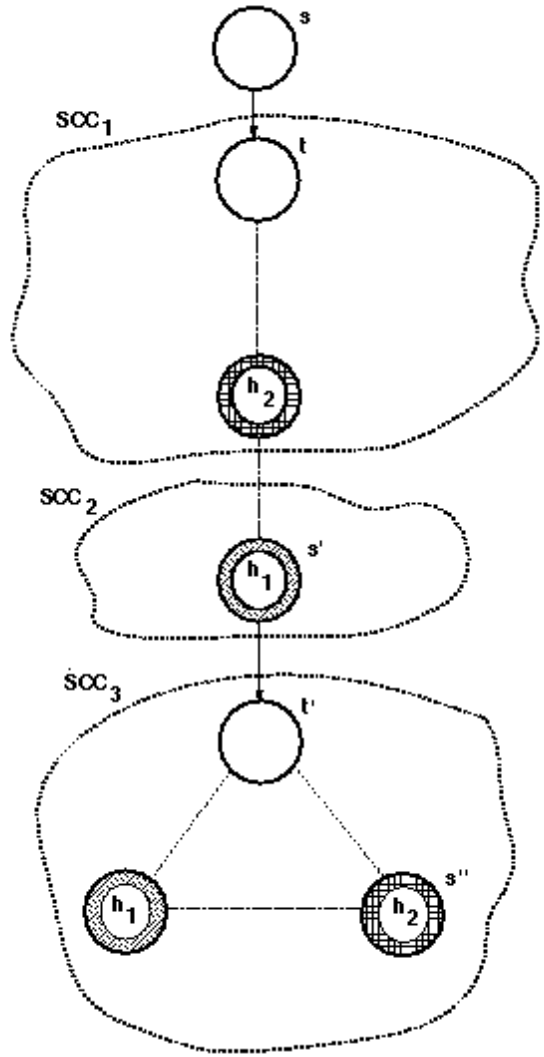
w $\leq j$ krokach

Sprawiedliwy przykład dla EG

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

$s := s_0$ stan początkowy
$I := \{1, \ldots, n\}$
powtarzaj
znajdź t t. że $s \to t, \quad t \in Q_j^i, \quad i \in I, \quad j$ minimalne
zrekonstruuj $t = t_j \to t_{j-1} \to \ldots \to t_0 \ \in (h_i \wedge \mathsf{EG}\, f)$
$I := I \setminus \{i \mid t_0 \in h_i\}$
$s := t_0$
$I := I \setminus \{i \mid t \in Q_j^i\}$
aż $I = \emptyset$
$s' := s \qquad \mapsto \qquad$ ścieżka $s_0 \to \ldots \to s'$

Sprawiedliwy przykład dla EG _



[Clarke, Grumberg, Long 1994]

Sprawiedliwy przykład dla EG _

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

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

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

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

ulepszenie:

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

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

Sprawiedliwy przykład dla E _ U _, EX _

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

III. Jak oblicza się EX f ?

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

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

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

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

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

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

- 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 $\exists V.\ g$
- $x = \mathrm{var}(f) = \mathrm{var}(g)$:

  $l := \exists\wedge(\mathrm{lo}(f), \mathrm{lo}(g), V), \quad h := \exists\wedge(\mathrm{hi}(f), \mathrm{hi}(g), V)$

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

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

R nie jest monolityczna

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

Model synchroniczny: $\quad R \;=\; R_1 \;\wedge\; R_2 \wedge \;\ldots\; \wedge\; R_n$

Model asynchroniczny: $\quad R \;=\; R'_1 \;\vee\; R'_2 \vee \;\ldots\; \vee\; R'_n$

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

Czy da się wykorzystać tę dodatkową strukturę ?

Model asynchroniczny: $R = R'_1 \vee R'_2 \vee \ldots \vee R'_n$

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

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

$$\equiv \left(\exists \vec{x'}.\ R'_1 \wedge f(\vec{x'})\right) \vee \ldots \vee \left(\exists \vec{x'}.\ R'_n \wedge f(\vec{x'})\right)$$

$$\exists \vec{x'}.\ R'_i \wedge f(\vec{x'}) \equiv \exists \vec{x'}.\ R_i \wedge \left(\bigwedge_{j \neq i} x_j = x'_j\right) \wedge f(\vec{x'})$$

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

Model synchroniczny: $R = R_1 \wedge R_2 \wedge \ldots \wedge R_n$

$$\exists \vec{x}'.\ R_1(\vec{x}, \vec{x}') \wedge \ldots \wedge R_n(\vec{x}, \vec{x}') \wedge f(\vec{x}')$$

- relacje R_i są lokalne
- „wczesna” kwantyfikacja
- heurystyki

Przykład: licznik 3-bitowy

$$
\begin{aligned}
R_0(\vec{x}, x'_0) &= (x'_0 = \neg x_0) \\
R_1(\vec{x}, x'_1) &= (x'_1 = x_0 \text{ xor } x_1) \\
R_2(\vec{x}, x'_2) &= (x'_2 = (x_0 \wedge x_1) \text{ xor } x_2)
\end{aligned}
$$

$$\exists x'_2 \exists x'_1 \exists x'_0.\ f(x'_0, x'_1, x'_2) \ \wedge\ R_0(\vec{x}, x'_0) \ \wedge\ R_1(\vec{x}, x'_1) \ \wedge\ R_2(\vec{x}, x'_2)$$

$$\exists x'_2 \big(\exists x'_1 \exists x'_0.\ f(x'_0, x'_1, x'_2) \ \wedge\ R_0(\vec{x}, x'_0) \ \wedge\ R_1(\vec{x}, x'_1)\big) \ \wedge\ R_2(\vec{x}, x'_2)$$

$$\exists x'_2 \big(\exists x'_1 \big(\exists x'_0.\ f(x'_0, x'_1, x'_2) \ \wedge\ R_0(\vec{x}, x'_0)\big) \ \wedge\ R_1(\vec{x}, x'_1)\big) \ \wedge\ R_2(\vec{x}, x'_2)$$

$$\big(\exists x'_1 \big(\exists x'_0.\ f(x'_0, x'_1, x'_2) \ \wedge\ R_0(x_0, x'_0)\big) \ \wedge\ R_1(x_0, x_1, x'_1)\big) \wedge R_2(x_0, x_1, x_2, x$$

Przykład

$$\exists x'_2 \quad \big(\exists x'_1 \quad \big(\exists x'_0 \quad f(x'_0, x'_1, x'_2) \ \wedge \ R_0(x_0, x'_0)\big) \quad \wedge \quad R_1(x_0, x_1, x'_1)\big) \quad \wedge \quad R_2(x_0, x_1, x_2, x'_2)$$

– 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 $\mathsf{EG}\,\mathtt{true}$
- weryfikacja LTL
- $L_\omega(\mathcal{A}_1) \subseteq L_\omega(\mathcal{A}_2)$ — $\mathcal{A}_1 \times \mathcal{A}_2 \vDash \mathsf{A}\,(\mathsf{G}\,\mathsf{F}\,q_1 \implies \mathsf{G}\,\mathsf{F}\,q_2)$
- weryfikacja rachunku μ
- stany osiągalne, zakleszczenie
- równoważność (bi)symulacyjna
- ...