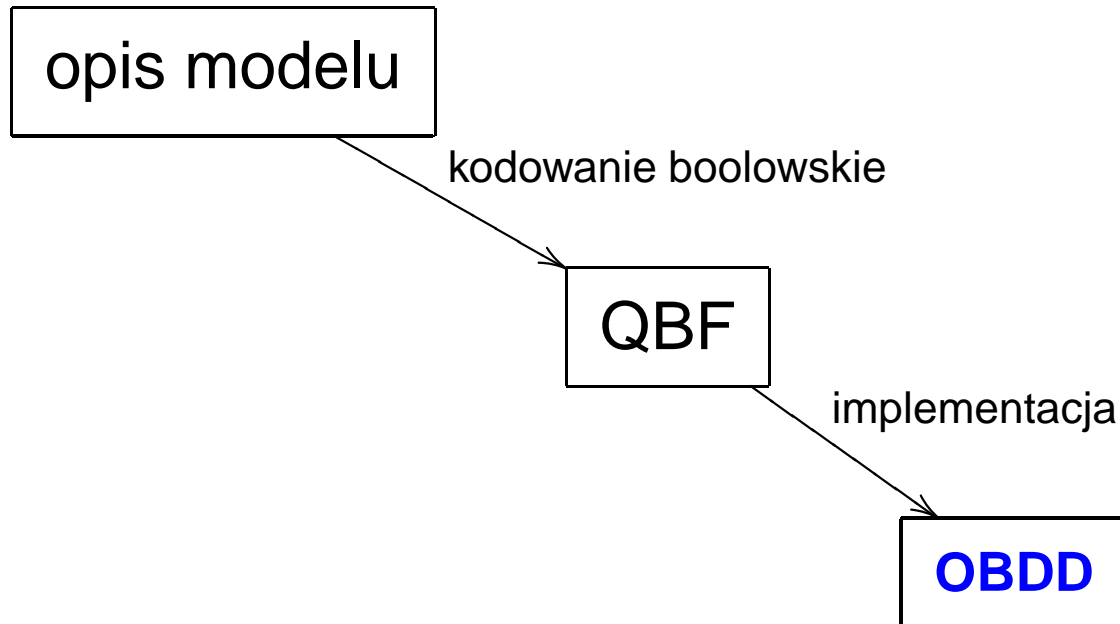


Praktyczne metody weryfikacji

Wykład 8: Weryfikacja symboliczna (II)

Symboliczna weryfikacja modelowa



weryfikacja modelowa = operacje na OBDDs

I. Weryfikacja modelowa

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

Niech $f : A \rightarrow A$ monotoniczna.

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

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

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

Niech $f : A \rightarrow A$ monotoniczna.

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

Przykład: $A = \mathcal{P}(S)$

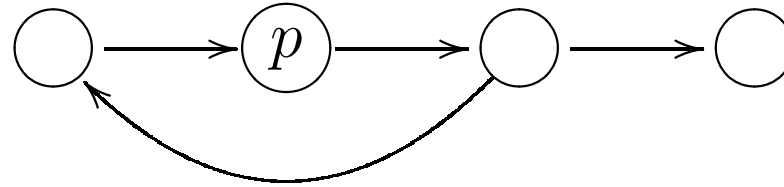
$$Z \mapsto \mathbf{EX} Z \qquad \mu Z. \mathbf{EX} Z = \perp = \emptyset \qquad \nu Z. \mathbf{EX} Z = ?$$

$$Z \mapsto p \vee \mathbf{EX} Z \qquad \mu Z. p \vee \mathbf{EX} Z = ?$$

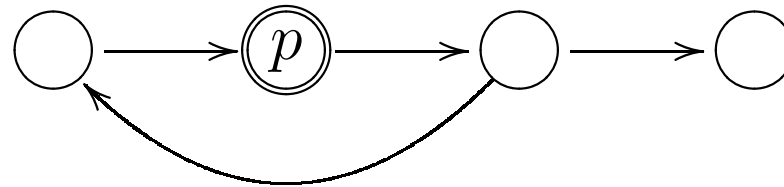
$$\mathbf{EF} p = \mu Z. p \vee \mathbf{EX} Z$$

$$Z \mapsto p \vee \mathbf{EX} Z$$

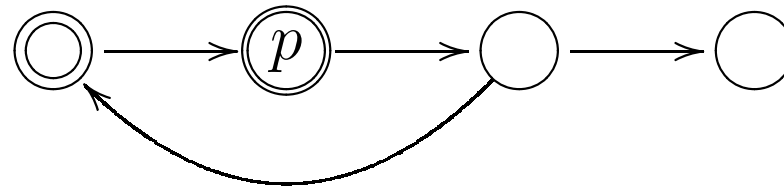
false



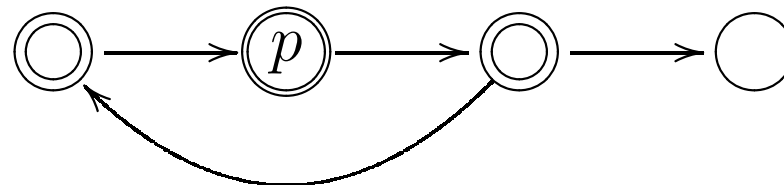
$$p \vee \mathbf{EX} \text{false} \equiv p$$



$$p \vee \mathbf{EX} p$$



$$p \vee \mathbf{EX} (p \vee \mathbf{EX} p)$$

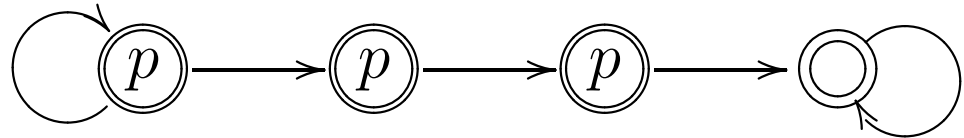


- $\mathbf{EF} \phi = \mu Z. \phi \vee \mathbf{EX} Z$ $Z \mapsto \phi \vee \mathbf{EX} Z$
- $\mathbf{AF} \phi = \mu Z. \phi \vee \mathbf{AX} Z$ $Z \mapsto \phi \vee \mathbf{AX} Z$
- $\mathbf{EG} \phi = \nu Z. \phi \wedge \mathbf{EX} Z$ $Z \mapsto \phi \wedge \mathbf{EX} Z$
- $\mathbf{AG} \phi = \nu Z.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

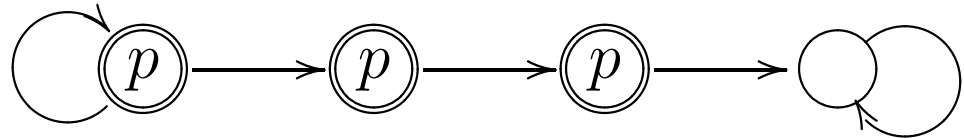
$$\mathbf{EG} p = \nu Z. p \wedge \mathbf{EX} Z$$

$$Z \mapsto p \wedge \mathbf{EX} Z$$

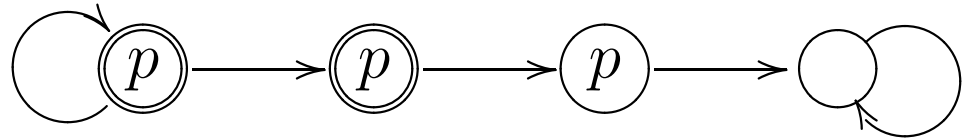
true



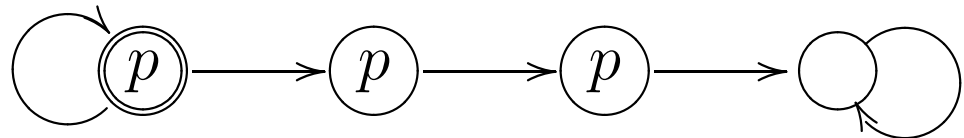
$p \wedge \mathbf{EX} \text{true} \equiv p$



$p \wedge \mathbf{EX} p$



$p \wedge \mathbf{EX} (p \wedge \mathbf{EX} p)$



Weryfikacja symboliczna

CTL (\neg , \wedge , **EX**, **E_U_**, **EG**)

(wystarczą te spójniki)

Check : CTL \mapsto OBDD

Check(ϕ) reprezentuje $\{s \mid s \models \phi\}$

Weryfikacja symboliczna (EX_)

Check : CTL \rightarrow OBDD

Check(ϕ) reprezentuje $\{s \mid s \models \phi\}$

Check(**EX** ϕ) := $\exists \vec{x}'. \widehat{R}(\vec{x}, \vec{x}') \wedge f(\vec{x}')$ gdzie $f = \text{Check}(\phi)$

Check(**EX** ϕ) := **EX** f

- **EX** ϕ
- **EX** Z
- **EX** f

Weryfikacja symboliczna (E_U_)

Check : CTL \rightarrow OBDD

Check(ϕ) reprezentuje $\{s \mid s \models \phi\}$

Check($\mathbf{E} \phi \mathbf{U} \psi$) := $\mu Z. g \vee (f \wedge \mathbf{EX} Z)$ gdzie $f = \text{Check}(\phi)$
 $g = \text{Check}(\psi)$

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

false

$$g \vee (f \wedge \mathbf{EX} \text{false})$$

$$\equiv g$$

$$g \vee (f \wedge \mathbf{EX} (g \vee (f \wedge \mathbf{EX} \text{false})))$$

$$\equiv g \vee (f \wedge \mathbf{EX} g)$$

...

$$\equiv g \vee (f \wedge \mathbf{EX} (g \vee (f \wedge \mathbf{EX} g)))$$

\downarrow

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

Weryfikacja symboliczna (EG _)

Check : CTL \rightarrow OBDD

Check(ϕ) reprezentuje $\{s \mid s \models \phi\}$

Check(**EG** ϕ) := $\nu Z. f \wedge \mathbf{EX} Z$ gdzie $f = \text{Check}(\phi)$

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

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

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

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

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

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

$$s \models_{\mathbf{F}} \mathbf{A} \mathbf{X} \phi \quad \iff \quad \forall \text{sprawiedliwej } \Pi z s . \Pi \models \mathbf{X} \phi$$

$$s \models_{\mathbf{F}} \mathbf{E} \mathbf{X} \phi \quad \iff \quad \exists \text{sprawiedliwa } \Pi z s . \Pi \models \mathbf{X} \phi$$

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

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

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

– $s \models \phi$

– $\forall i \leq n . \exists s' . s \rightarrow \dots \rightarrow s' \in Z_i, \quad s' \neq s,$ wszystkie stany

po drodze spełniają ϕ

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

Tw.:

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

Dowód:

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

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

Sprawiedliwa w. symboliczna (EG _)

Check : CTL \rightarrow OBDD

Check(ϕ) reprezentuje $\{s \mid s \models \phi\}$

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

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

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

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

Sprawiedliwa w. symboliczna

$$\text{fair} := \text{Check}(\text{EG true})$$

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

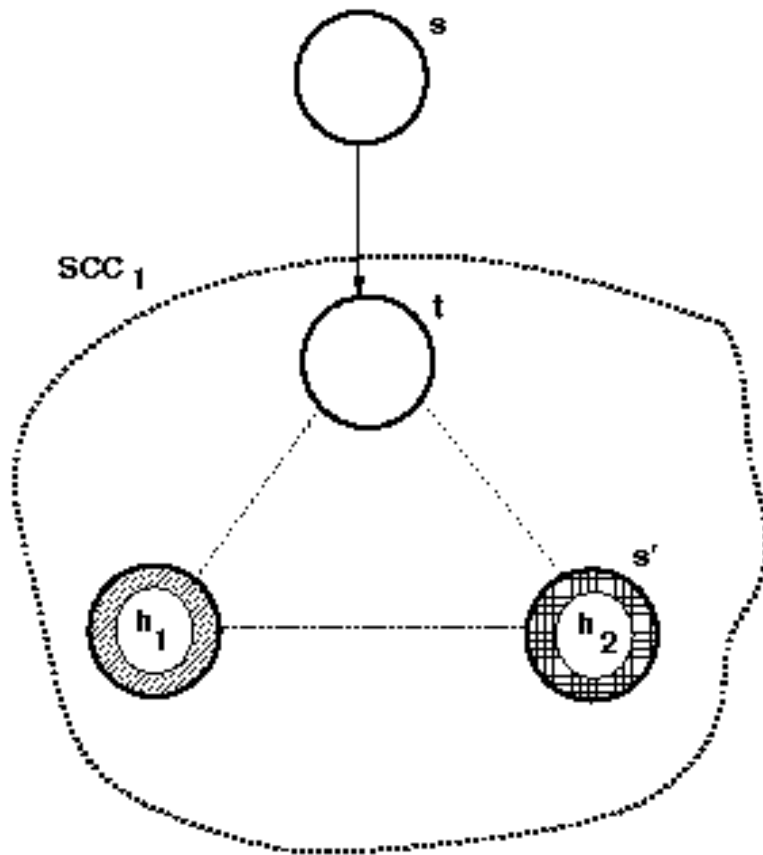
gdzie $f = \text{Check}(\phi)$

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

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

III. (Kontr)przykłady

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



[Clarke, Grumberg, Long 1994]

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

kontrprzykład dla $AG \phi$ = przykład dla $EF \neg \phi$

(sprawiedliwy przykład to zawsze nieskończona ścieżka)

kontrprzykład dla $EF \phi$ = ?

kontrprzykład dla $EG \phi$ = ?

Jak obliczyć **symbolicznie** przykład dla:

– $EG \phi$

– $E \phi U \psi$

– $EX \phi ?$

Obliczenie $E \cup g$:

$$Q_0 \subseteq Q_1 \subseteq \dots \quad (1 \leq i \leq n)$$

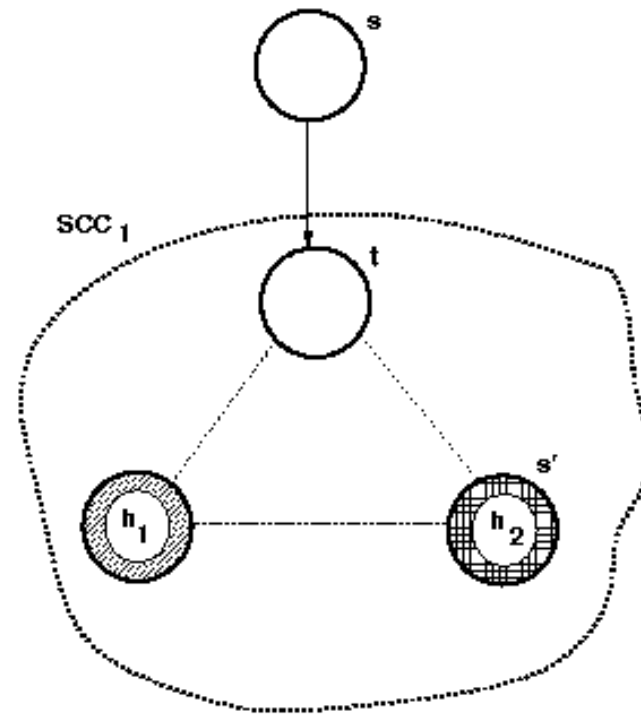
$s \in Q_j \iff$ można dojść „po f ” z s do g w $\leq j$ krokach

Obliczenie przykładu:

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

Jak obliczyć **symbolicznie** sprawiedliwy przykład dla:

- $EG \phi$
- $E \phi U \psi$
- $EX \phi ?$



[Clarke, Grumberg, Long 1994]

Sprawiedliwy przykład dla EG

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

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

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

$$Q_0^i \subseteq Q_1^i \subseteq \dots \quad (1 \leq i \leq n)$$

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

w $\leq j$ krokach

Sprawiedliwy przykład dla EG

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

$s := s_0$ stan początkowy

$I := \{1, \dots, n\}$

powtarzaj

znajdź t t. że $s \rightarrow t$, $t \in Q_j^i$, $i \in I$, j minimalne

zrekonstruuuj $t = t_j \rightarrow t_{j-1} \rightarrow \dots \rightarrow t_0 \in (h_i \wedge \mathbf{EG} f)$

$I := I \setminus \{i \mid t_0 \in h_i\}$

$s := t_0$

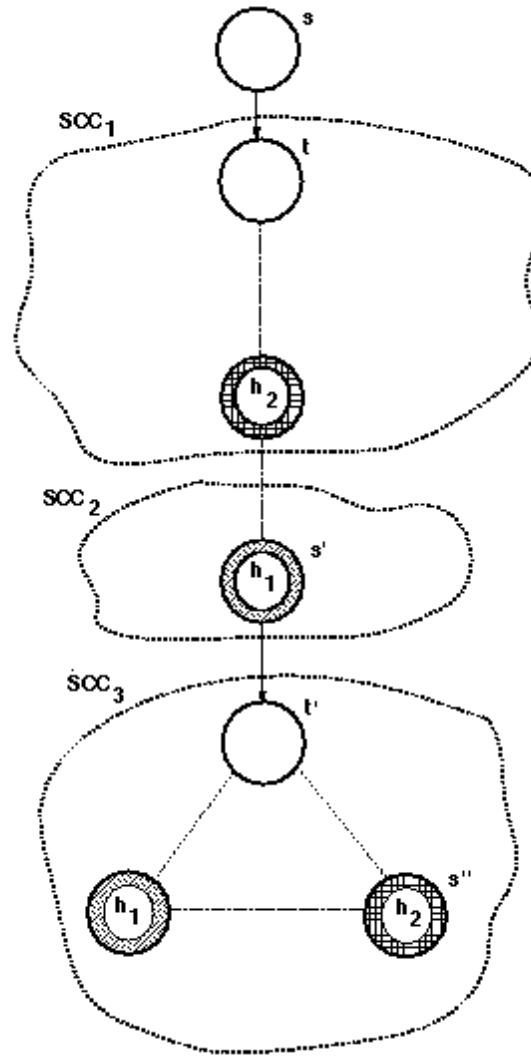
$I := I \setminus \{i \mid t \in Q_j^i\}$

aż $I = \emptyset$

$s' := s$

\mapsto ścieżka $s_0 \rightarrow \dots \rightarrow s'$

Sprawiedliwy przykład dla EG_



[Clarke, Grumberg, Long 1994]

Sprawiedliwy przykład dla EG

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

mamy ścieżkę $s_0 \rightarrow \dots \rightarrow s'$ niech t = pierwsze t_0

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

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

ulepszenie:

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

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

Sprawiedliwy przykład dla $E_U_$, $EX_$

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

IV. Jak oblicza się $EX f$?

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

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

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

$$f(x_1, \dots, x_m) \mapsto f'(x'_1, \dots, x'_m)$$

$$x_i \leq x_j \iff x'_i \leq x'_j$$

$$\mathbf{EX} f = \exists \wedge(\widehat{R}, f', \{x'_1, \dots, x'_m\})$$

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

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

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

$$- x \in V: \quad \exists\wedge(f, g, V) := l \vee h$$

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

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

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

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

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

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

Czy da się wykorzystać tę dodatkową strukturę ?

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

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

$$\begin{aligned} \exists \vec{x}'. \widehat{R} \wedge f(\vec{x}') &\equiv \exists \vec{x}'. (R'_1 \wedge f(\vec{x}')) \vee \dots \vee (R'_n \wedge f(\vec{x}')) \\ &\equiv (\exists \vec{x}'. R'_1 \wedge f(\vec{x}')) \vee \dots \vee (\exists \vec{x}'. R'_n \wedge f(\vec{x}')) \end{aligned}$$

$$\begin{aligned} \exists \vec{x}'. R'_i \wedge f(\vec{x}') &\equiv \exists \vec{x}'. \widehat{R}_i \wedge (\bigwedge_{j \neq i} x_j = x'_j) \wedge f(\vec{x}') \\ &\equiv \exists x'_i. \widehat{R}_i(\vec{x}, x'_i) \wedge f(x_1, \dots, x_{i-1}, x'_i, x_{i+1}, \dots, x_m) \end{aligned}$$

Model synchroniczny: $\hat{R} = \hat{R}_1 \wedge \hat{R}_2 \wedge \dots \wedge \hat{R}_n$

$$\exists \vec{x}'. \hat{R}_1(\vec{x}, \vec{x}') \wedge \dots \wedge \hat{R}_n(\vec{x}, \vec{x}') \wedge f(\vec{x}')$$

- relacje \hat{R}_i są lokalne
- „wczesna” kwantyfikacja
- heurystyki

Przykład: licznik 3-bitowy

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

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

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

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

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

$$\begin{aligned} \exists x'_2 & \left(\exists x'_1 \left(\exists x'_0 \left(f(x'_0, x'_1, x'_2) \wedge \widehat{R}_0(x_0, x'_0) \right) \right. \right. \\ & \quad \left. \left. \wedge \widehat{R}_1(x_0, x_1, x'_1) \right) \right) \\ & \quad \wedge \widehat{R}_2(x_0, x_1, x_2, x'_2) \end{aligned}$$

- 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
- $L_\omega(\mathcal{A}_1) \subseteq L_\omega(\mathcal{A}_2)$ $\mathcal{A}_1 \times \mathcal{A}_2 \models A (G F q \implies G F q')$
- weryfikacja rachunku μ
- blokady, stany osiągalne
- równoważność (bi)symulacyjna
- ...