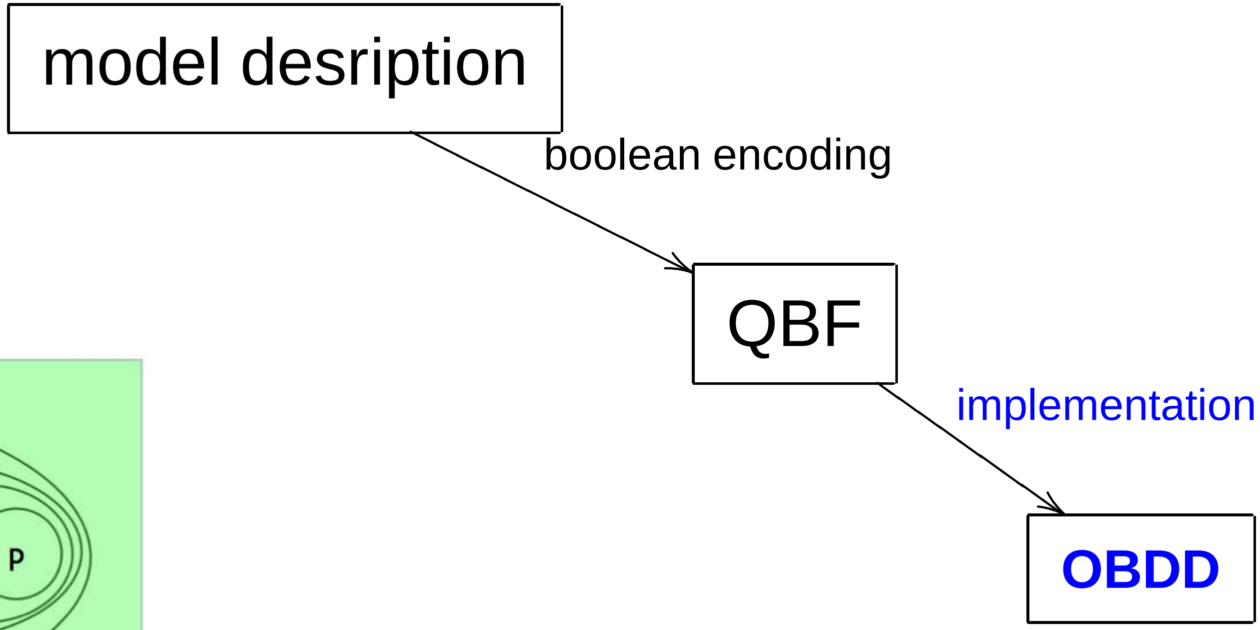
Computer aided verification

Lecture 7: Symbolic verification II

Symbolic model checking



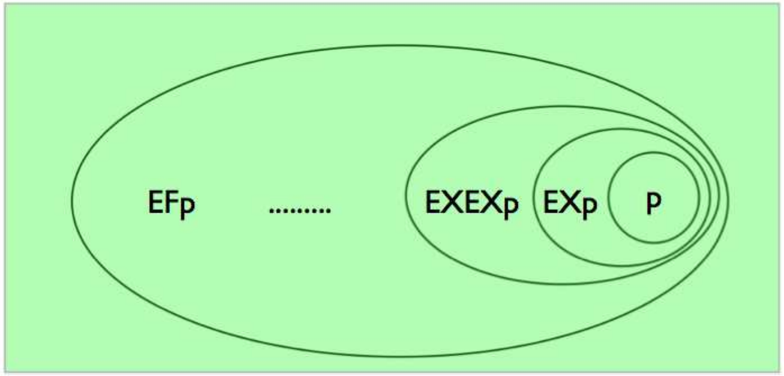
model desription

boolean encoding

QBF

implementation

OBDD



model checking = operations on OBDDs

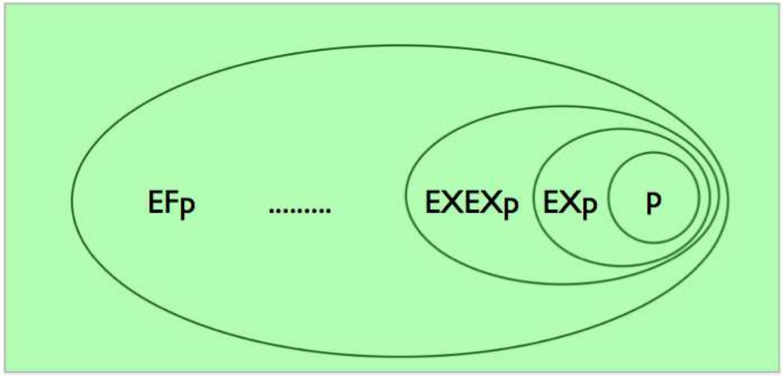
0. Symbolic verification

I. Fairness

II. (Counter)examples

III. How to compute EX f ?

0. Symbolic verification



o

Reminder

Fixed points in a complete lattice $\langle A, \leq \rangle$.

Let $f : A \to A$ monotonic.

- the least f.p.: $\bot \leq f(\bot) \leq f^2(\bot) \leq \ldots \ \rightsquigarrow \ \mu Z.\ f(Z)$
- the greatest f.p.: $\top \geq f(\top) \geq f^2(\top) \geq \ldots \ \rightsquigarrow \ \nu Z.\ f(Z)$

When A finite, the fixed points are reached after $\leq |A|$ iterations.

Reminder

Fixed points in a complete lattice $\langle A, \leq \rangle$.

Let $f : A \to A$ monotonic.

- the least f.p.: $\bot \leq f(\bot) \leq f^2(\bot) \leq \ldots \; \rightsquigarrow \; \mu Z.\; f(Z)$
- the greatest f.p.: $\top \geq f(\top) \geq f^2(\top) \geq \ldots \; \rightsquigarrow \; \nu Z.\; f(Z)$

Example: $\langle A, \leq \rangle \; = \; \langle \mathcal{P}(S), \subseteq \rangle$

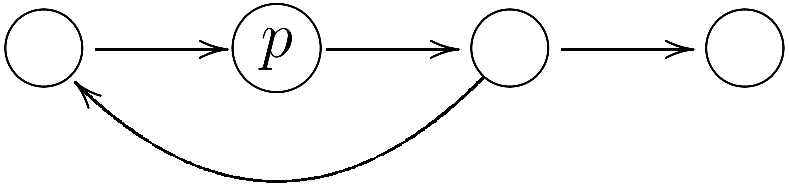
$Z \mapsto \; \text{EX}\, Z$ $\qquad$ $\mu Z.\, \text{EX}\, Z \; = \bot = \emptyset$ $\qquad$ $\nu Z.\, \text{EX}\, Z \; = \;$ **?**

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

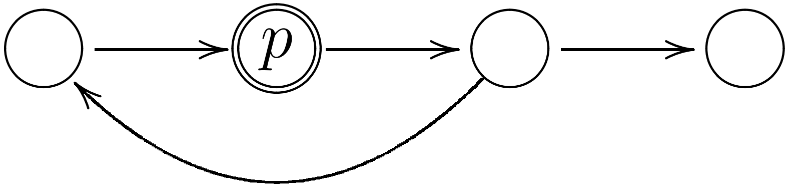
Example

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

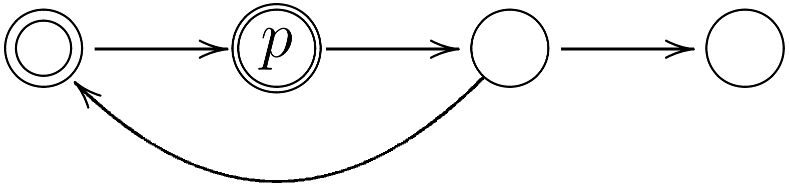
$\mathtt{false}$



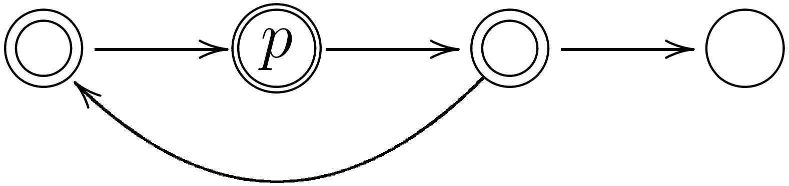
$p \vee \mathsf{EX}\, \mathtt{false} \equiv p$



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



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



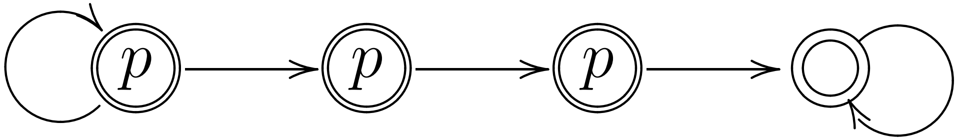
CTL via fixed points

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

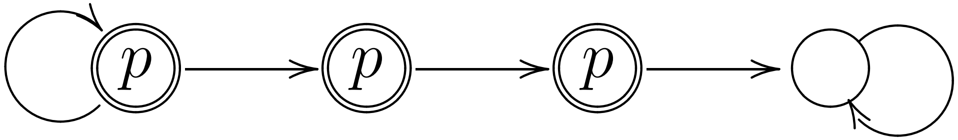
Example

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

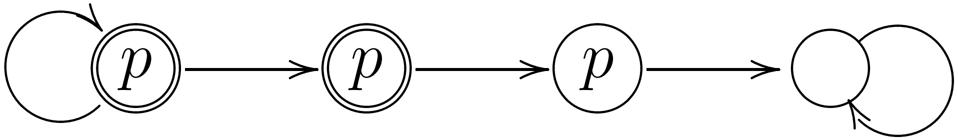
$\mathtt{true}$



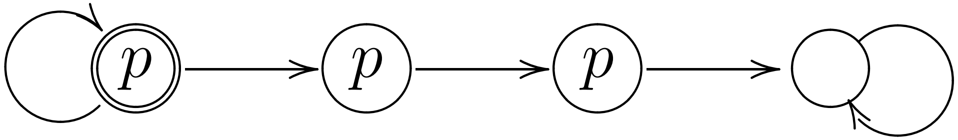
$p \wedge \mathsf{EX}\,\mathtt{true} \;\equiv p$



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



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



Symbolic model checking

CTL ($\neg$, $\wedge$, **EX**, **E _ U _**, **EG)** (these connectives are sufficient)

Check : CTL $\mapsto$ OBDD

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

Example: $\mathrm{Check}(p)$ represents L_p

The order of variables is often crucial!

Symbolic model checking (EX _)

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

$\mathrm{Check}(\phi)$ represents $\{s \mid s \vDash \phi\}$

$$\mathrm{Check}(\,\text{EX}\,\phi) \;:=\; \exists \vec{x}'.\; R(\vec{x}, \vec{x}') \wedge f[\vec{x}'/\vec{x}] \qquad \text{where } \; f = \mathrm{Check}(\phi)$$

$$\mathrm{Check}(\,\text{EX}\,\phi) \;:=\; \text{EX}\, f$$

$\text{EX}\,\phi$

$\text{EX}\,Z$

$\text{EX}\,f$

Order of variables

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

$$\vec{x} = x_1, x_2, \ldots, x_m$$

$$x_1 < x_1' < x_2 < x_2' < \ldots < x_m < x_m'$$

Symbolic model checking (E _ U _)

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

$$\boxed{\mathrm{Check}(\phi) \;\; \textsf{represents} \;\; \{s \mid s \models \phi\}}$$

$$\mathrm{Check}(\,\mathsf{E}\,\phi\,\mathsf{U}\,\psi) \quad := \quad \mu Z.\, g \vee (f \wedge \mathsf{EX}\, Z) \qquad \textsf{where} \quad \begin{array}{r@{}l} f &= \mathrm{Check}(\phi) \\ g &= \mathrm{Check}(\psi) \end{array}$$

$$h \mapsto g \vee (f \wedge \mathsf{EX}\, h)$$

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

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

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

Symbolic model checking (EG _)

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

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

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

$$h \mapsto f \wedge \text{EX}\, h$$

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

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

I. Fairness

Fair CTL

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

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

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

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

$$s \models_{\mathbf{F}} \ \mathsf{AX}\, \phi \iff \forall\ \text{fair}\ \Pi\ \text{from}\ s\ .\ \ \Pi \models \ \mathsf{X}\, \phi$$

$$s \models_{\mathbf{F}} \ \mathsf{EX}\, \phi \iff \exists\ \text{fair}\ \Pi\ \text{from}\ s\ .\ \ \Pi \models \ \mathsf{X}\, \phi$$

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

Fair EG

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

EG ϕ $= \{s \mid s \models_{\mathbf{F}}$ EG $\phi\} =$ the greatest Z s.t. if $s \in Z$ then

- $s \models \phi$
- $\forall i \leq n \;.\; \exists s' \;.\; s \rightarrow \ldots \rightarrow s' \in Z_i \cap Z$, $s' \neq s$, all intermediate states satisfy ϕ

Fair EG

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

EG ϕ $= \{s \mid s \vDash_{\mathbf{F}}$ EG $\phi\}$ $=$ the greatest Z s.t. if $s \in Z$ then

- $s \vDash \phi$
- $\forall i \leq n \,.\, \exists s' \,.\, s \to \ldots \to s' \in Z_i \cap Z$, $s' \neq s$, all intermediate states satisfy ϕ

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

Fair EG

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

EG ϕ $=$ $\{s \mid s \models_{\mathbf{F}}$ EG $\phi\}$ $=$ the greatest Z s.t. if $s \in Z$ then

- $s \models \phi$
- $\forall i \leq n \,.\, \exists s' \,.\, s \rightarrow \ldots \rightarrow s' \in Z_i \cap Z$, $s' \neq s$, all intermediate states satisfy ϕ

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

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

Fair EG

Thm:

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

Proof:

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

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

Fair symbolic model checking (EG _)

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

$\boxed{\mathrm{Check}(\phi) \;\; \text{represents} \;\; \{s \mid s \vDash_{\mathbf{F}} \phi\}}$

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

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

where $\;f = \mathrm{Check}(\phi)$

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

Fair symbolic model checking

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

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

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

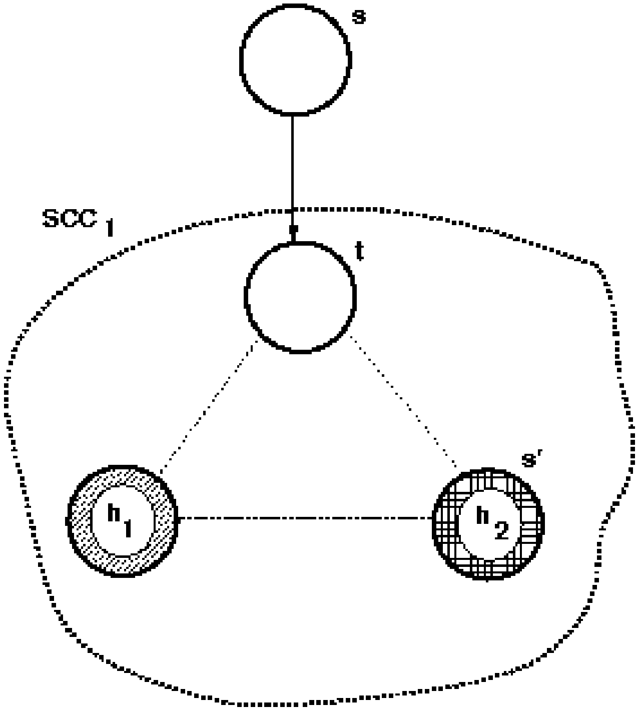
$$\mathrm{Check}(\,\mathsf{E}\,\phi\,\mathsf{U}\,\psi) \quad := \quad \mu Z.\ (g \wedge \texttt{fair}) \vee (f \wedge \mathsf{EX}\,Z)$$

$$\text{where} \quad \begin{aligned} f &= \mathrm{Check}(\phi) \\ g &= \mathrm{Check}(\psi) \end{aligned}$$

II. (Counter)examples

Counterexample

counterexample for AF ϕ = example for EG $\neg\phi$



[Clarke, Grumberg, Long 1994]

Counterexample

counterexample for AF ϕ = example for EG $\neg\phi$

counterexample for AG ϕ = example for EF $\neg\phi$

(fair counterexample is always an infinite path)

Counterexample

counterexample for AF ϕ = example for EG $\neg\phi$

counterexample for AG ϕ = example for EF $\neg\phi$

(fair counterexample is always an infinite path)

counterexample for EF ϕ = **?**

counterexample for EG ϕ = **?**

Symbolic counterexample

How to compute an example for:

- EG ϕ
- E ϕ U ψ
- EX ϕ

symbolically ?

Example for E _ U _

Computation of E f U g:

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

$s \in Q_j \iff g$ may be reached from s "via f" by $\leq j$ transitions

Computing an example for $s \models$ E f U g:

– let j minimal s.t. $s \in Q_j$

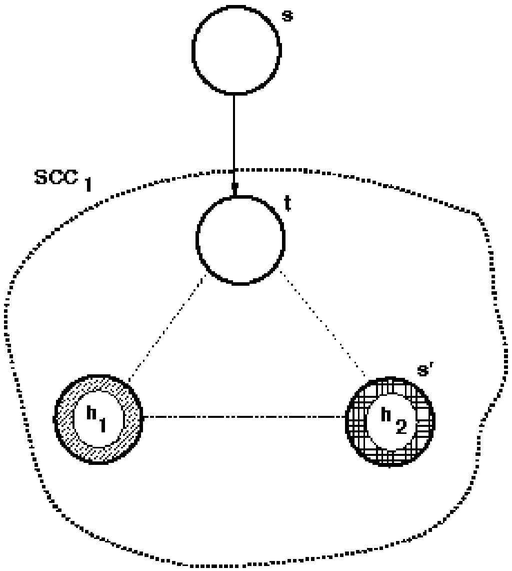
– reconstruct $s = s_j \to s_{j-1} \to \ldots \to s_0 \in g$

Symbolic counterexample

How to compute a fair example for:

- EG ϕ
- E ϕ U ψ
- EX ϕ

symbolically ?



[Clarke, Grumberg, Long 1994]

Fair example for EG _

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

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

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

$$Q^i_0 \;\subseteq\; Q^i_1 \;\subseteq\; \ldots \qquad (1 \leq i \leq n)$$

$s \in Q^i_j \;\Longleftrightarrow\; (h_i \wedge \mathsf{EG}\, f)$ may be reached from s ”via f”

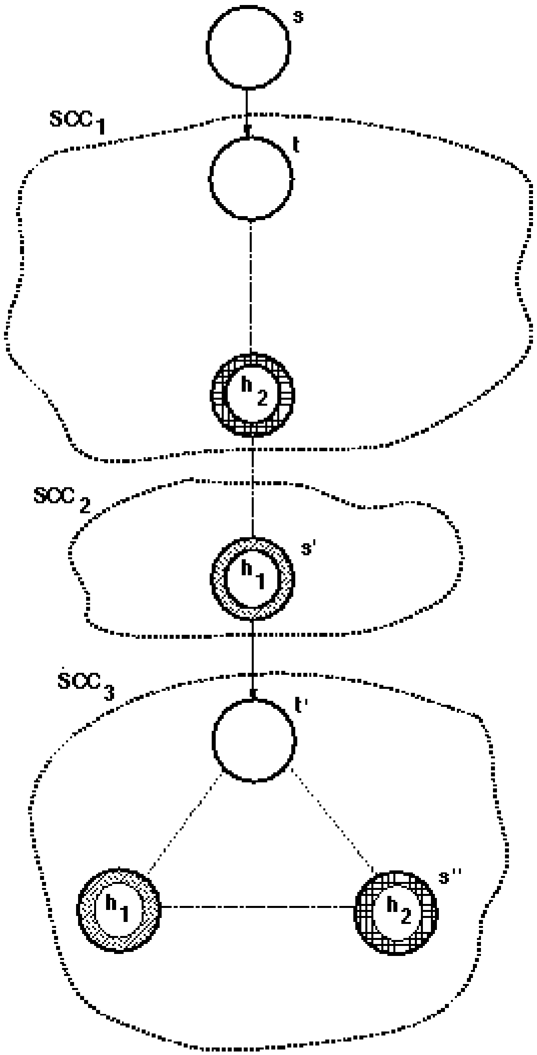
by $\leq j$ transitions

Fair example for EG _

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

```
$s := s_0$ initial state
$I := \{1, \ldots, n\}$
repeat
    find $t$ s.t. $s \rightarrow t$,   $t \in Q^i_j$,   $i \in I$,   $j$ minimal
    reconstruct $t = t_j \rightarrow t_{j-1} \rightarrow \ldots \rightarrow t_0 \in (h_i \wedge \mathsf{EG}\, f)$
    $I := I \setminus \{i \mid t_0 \in h_i\}$
    $s := t_0$                                        $I := I \setminus \{i \mid t \in Q^i_j\}$
until $I = \emptyset$
$s' := s$                    $\mapsto$     path $s_0 \rightarrow \ldots \rightarrow s'$
```

Fair example for EG _



[Clarke, Grumberg, Long 1994]

Fair example for EG _

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

we have a path $s_0 \rightarrow \ldots \rightarrow s'$ let $t =$ the first t_0

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

otherwise restart: $s_0 := s'$, $I := \{1, \ldots, n\}$

improvement:

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

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

Fair example for E _ U _, EX _

Example for $\mathsf{E}\,\phi\,\mathsf{U}\,(\psi \wedge \texttt{fair})$ or $\mathsf{EX}\,(\phi \wedge \texttt{fair})$ extend with a fair example for $\mathsf{EG}\,\texttt{true}$.

III. How to compute EX f ?

EX f by AndExist

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

operation $\exists\wedge(g, h, V) \;:=\; \exists V.\, g \wedge h$ (V – set of variables)

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

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

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

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

- f, g leaves: $\mathrm{val}(\exists\wedge(f, g, V)) \ := \ \mathrm{val}(f) \wedge \mathrm{val}(g)$
- f a leaf, g not: $\exists\wedge(f, g, V) \ := \ \texttt{false} \ \text{or} \ \exists V.\ g$
- $x = \mathrm{var}(f) = \mathrm{var}(g)$:

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

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

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

R is not monolytic

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

Synchronous model: $R \;=\; R_1 \;\wedge\; R_2 \wedge \;\ldots\; \wedge\; R_n$

Asynchronous model: $R \;=\; R'_1 \;\vee\; R'_2 \vee \;\ldots\; \vee\; R'_n$

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

Can one profit from this additional structure ?

Asynchronous model: $R \;=\; R'_1 \,\vee\, R'_2 \vee \,\ldots\, \vee\, R'_n$

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

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

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

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

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

Synchronous model: $R \;=\; R_1 \;\wedge\; R_2 \wedge\; \ldots \;\wedge\; R_n$

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

– relations R_i are local

– „early” quantification

– heuristics

Example: 3-bit counter

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

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

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

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

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

$$R_2(x_0, x_1, x_2, x'_2)$$

Example: 3-bit counter

$$\begin{array}{l}
\exists x'_2 \quad \big(\exists x'_1 \quad \big(\exists x'_0 \quad f(x'_0, x'_1, x'_2) \;\wedge\; R_0(x_0, x'_0)\big) \\
\qquad\qquad\qquad \wedge \qquad R_1(x_0, x_1, x'_1)\big) \\
\qquad\quad \wedge \qquad R_2(x_0, x_1, x_2, x'_2)
\end{array}$$

- sequence of $\exists\wedge$ operations
- optimal order of processes (not variables this time):
  - early elimination of variables ($\exists$)
  - late introducing of variables

What else can be compute using OBDDs ?

- $L_\omega(\mathcal{A}) \neq \emptyset$ fair EG $\texttt{true}$
- LTL model checking
- $L_\omega(\mathcal{A}_1) \subseteq L_\omega(\mathcal{A}_2)$ $\mathcal{A}_1 \times \mathcal{A}_2 \models \mathsf{A}\,(\,\mathsf{G}\;\mathsf{F}\,q_1 \implies \mathsf{G}\;\mathsf{F}\,q_2)$
- μ-calculus model checking
- reachable states
- deadlocks
- (bi)simulation equivalence
- …

OBBDs are routinely used in hardware industry nowadays