Computer aided verification

Lecture 6: Symbolic verification I

EFp .... EXEXp EXp p

Symbolic model checking

model description

boolean encoding

QBF

implementation
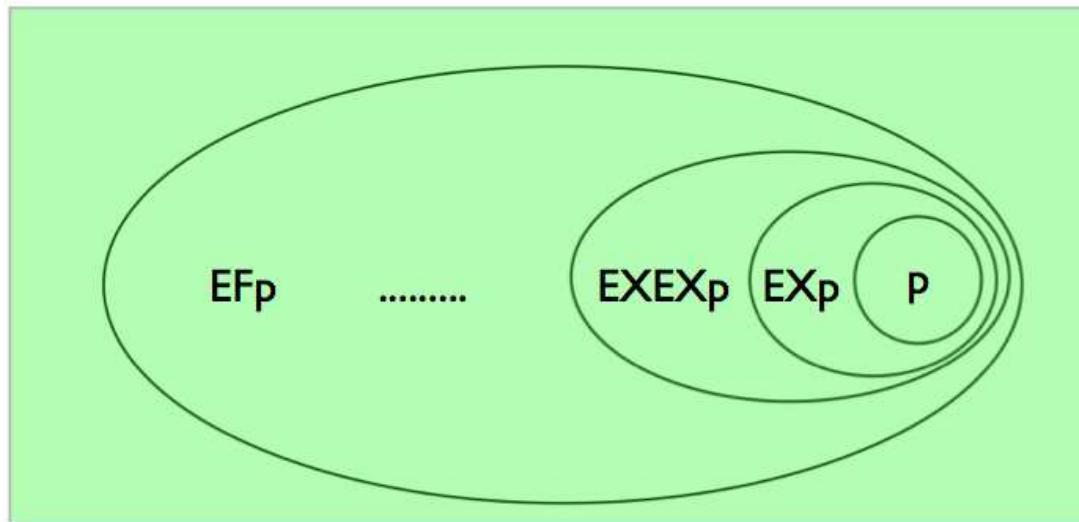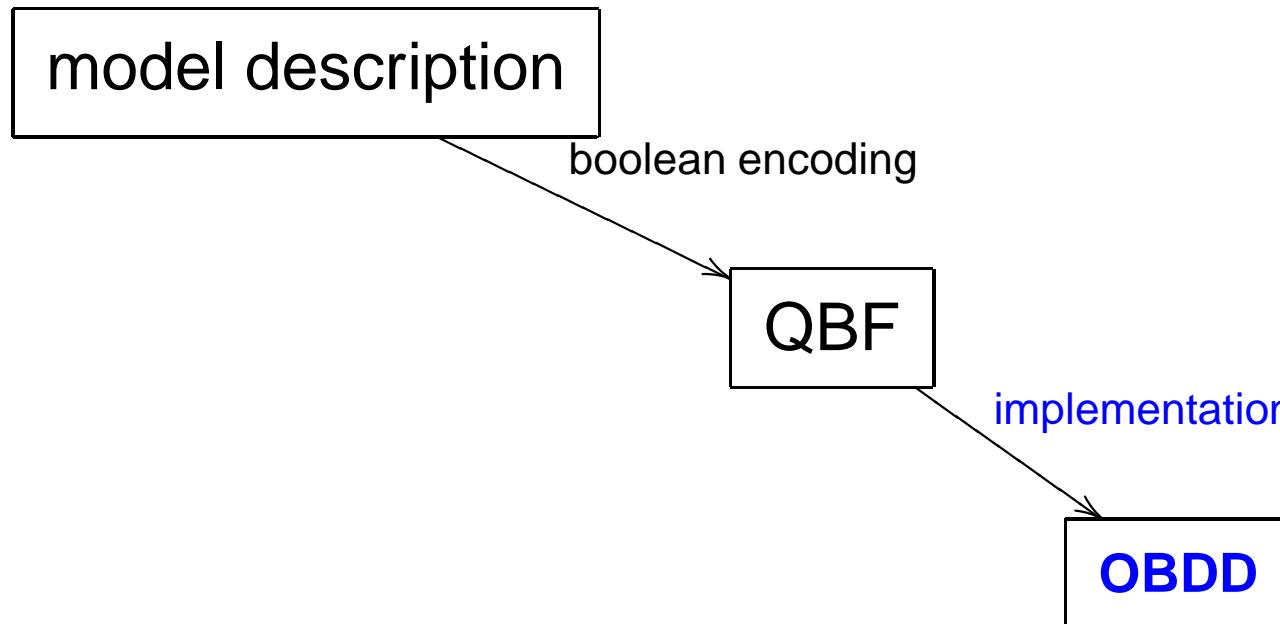
OBDD

model checking = operations on OBDDs

I. OBDD

Ordered Binary Decision Diagrams

x_1	x_2	x_3	f
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1
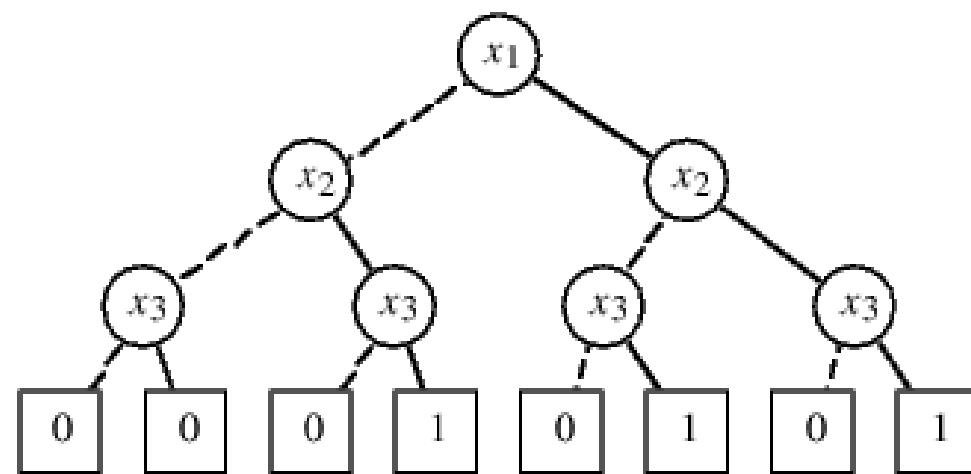
[Bryant 1992]

– $f : \{0,1\}^3 \rightarrow \{0,1\}$

– fixed order on variables: $x_1 < x_2 < x_3$

# OBDD = rooted acyclic graph

Attributes of a node v:

- when v is a leaf

    - $\mathrm{val}(v) \in \{0, 1\}$

- when v is not a leaf

    - $\mathrm{var}(v) \in \{x_1, x_2, \ldots\}$

    - $\mathrm{lo}(v), \mathrm{hi}(v)$ – 2 nodes

The order of variables must be obeyed on every path.

– remove redundant leaves

– remove redundant non-leaves

$OBDD \longmapsto ROBDD$

– remove redundant tests
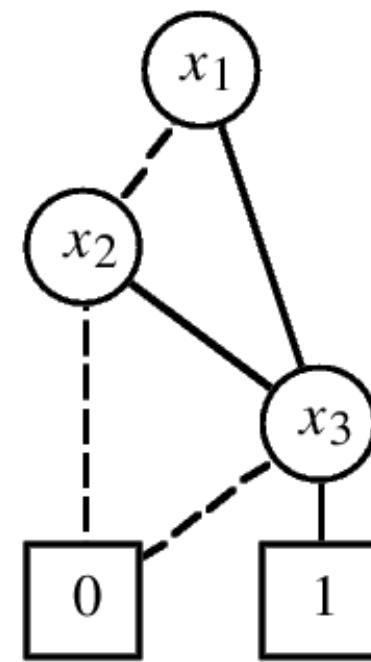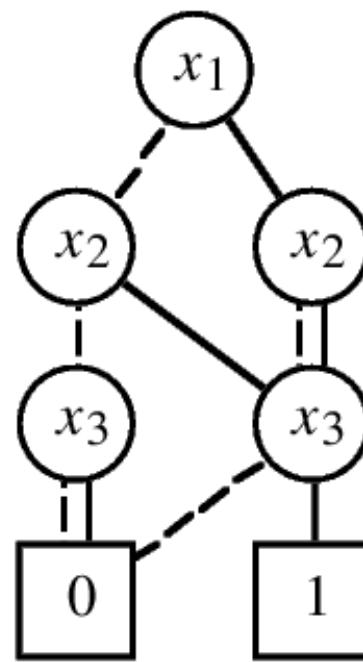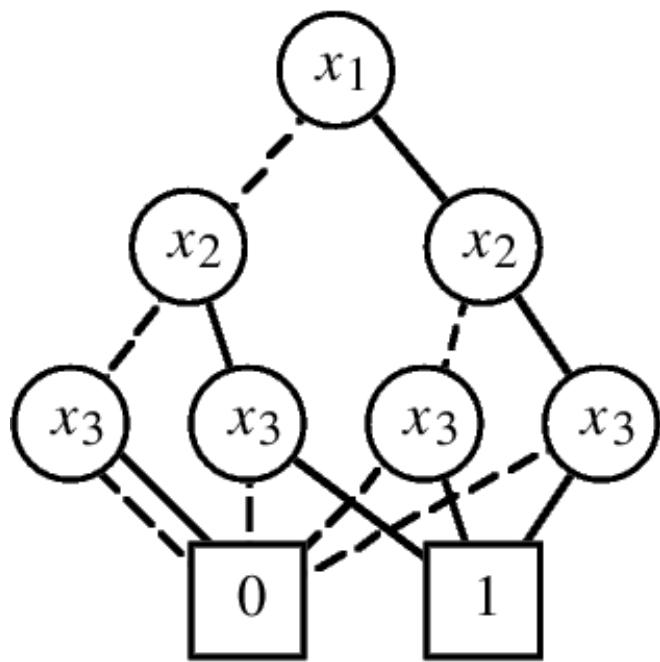
[Bryant 1992]

Canonical form: reduced OBDD

Canonical form for a boolean function:

- – independent from the initial OBDD

- – (strongly) dependent on the order of variables

Naive construction of an OBDD for a boolean formula ϕ:

$$\phi \quad \longmapsto \quad \text{decision tree} \quad \longmapsto \quad \text{canonical OBDD}$$

Finding an appropriate order of variables is crucial!

$$a_1 \wedge b_1 \quad \vee \quad a_2 \wedge b_2 \quad \vee \quad a_3 \wedge b_3$$
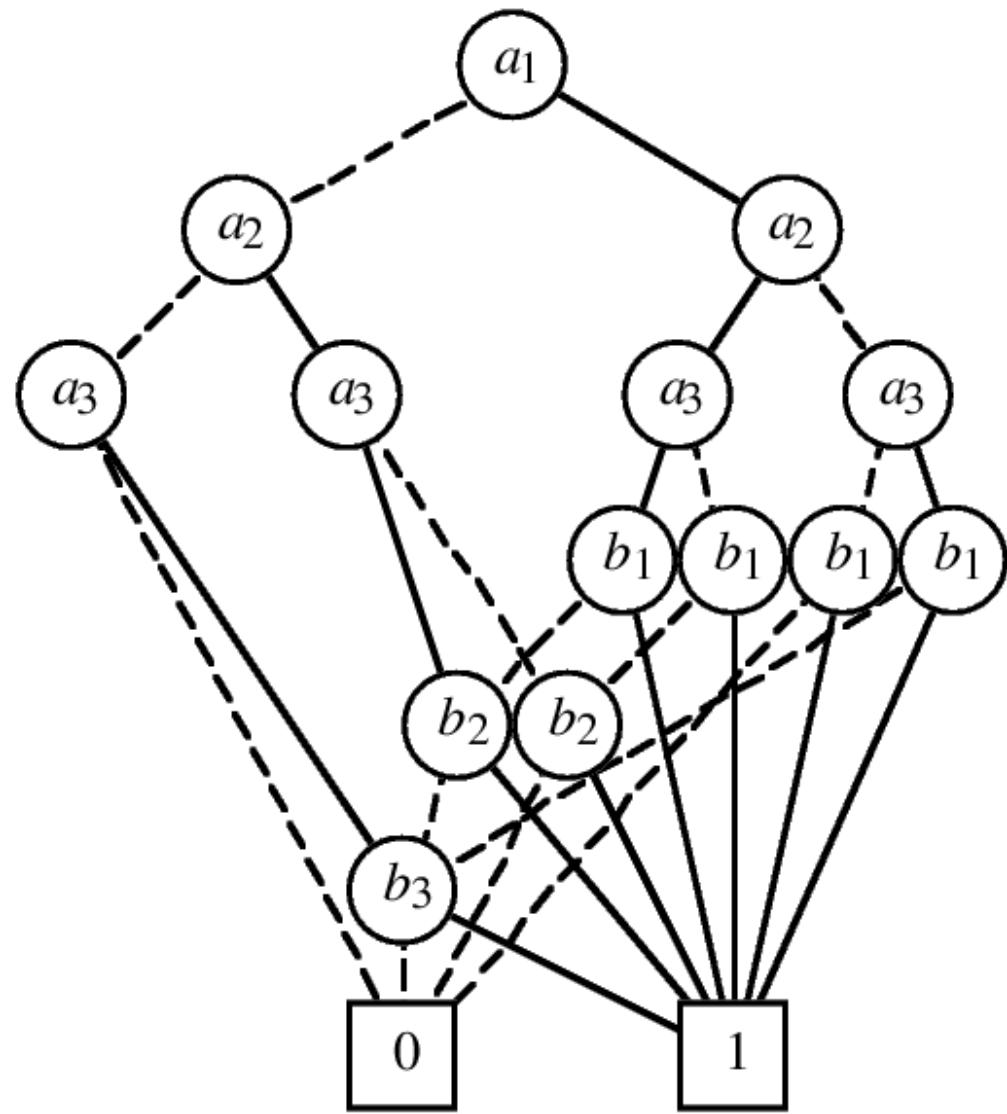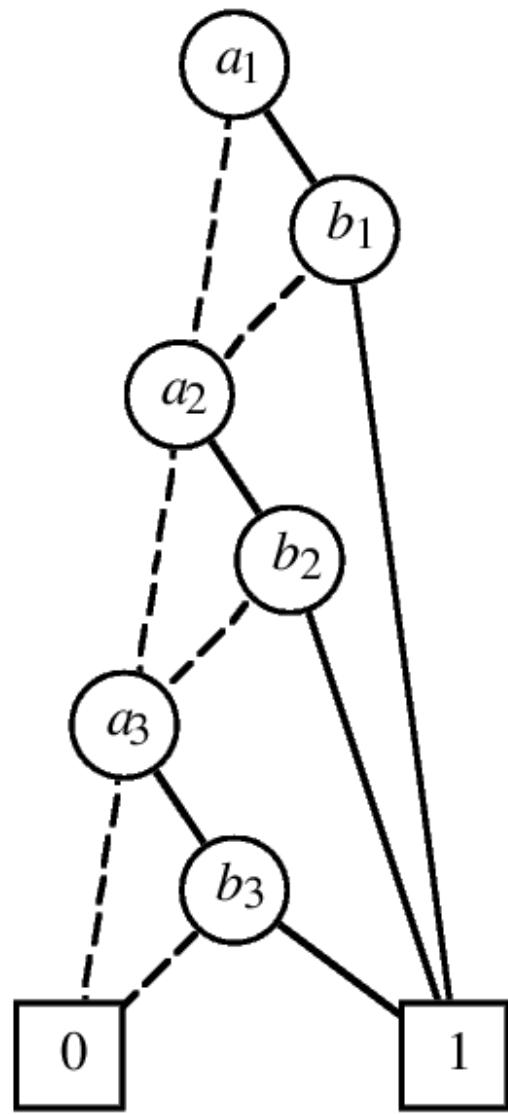
[Bryant 1992]

$$f(a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n) = a_1 \wedge b_1 \ \vee \ a_2 \wedge b_2 \ \vee \ \ldots \ \vee \ a_n \wedge b_n$$
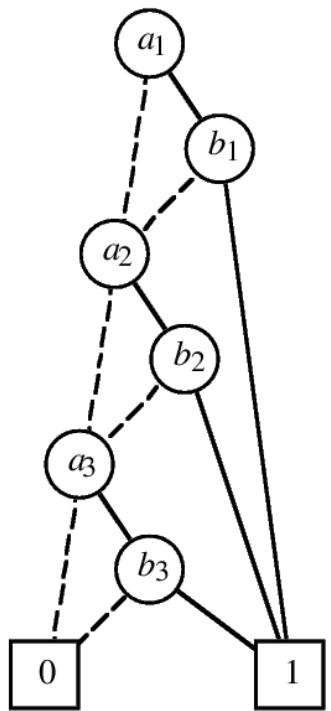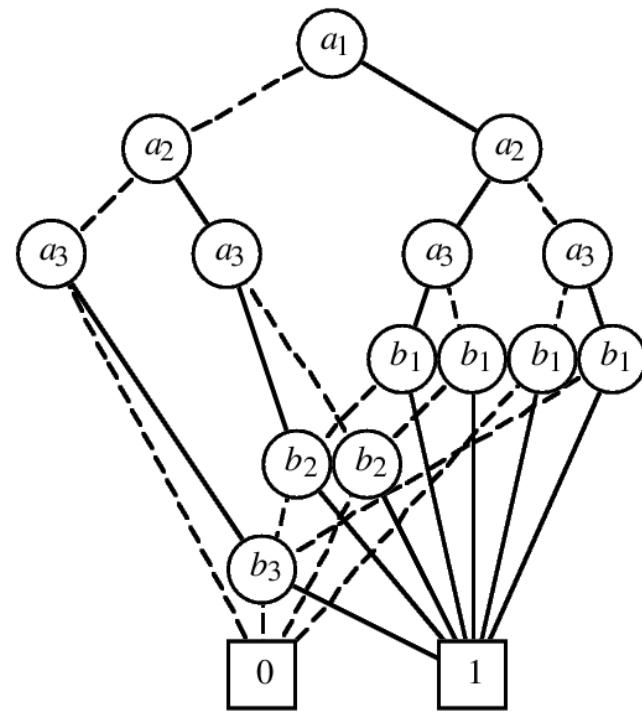
$$2 \cdot n \qquad\qquad\qquad 2 \cdot (2^n - 1)$$

Heuristic: closely related variables should be close in the order

example of a boolean function	lower bound	upper bound
symmetric functions	$\mathcal{O}(n)$	$\mathcal{O}(n^2)$
addition (oldest bits)	$\mathcal{O}(n)$	$\mathcal{O}(2^n)$
multiplication (middle bits)	$\mathcal{O}(2^n)$	$\mathcal{O}(2^n)$

$$f \;=\; \neg x \,\wedge\, f|_{x \leftarrow 0} \;\;\vee\;\; x \,\wedge\, f|_{x \leftarrow 1}$$

$$f|_{x_i \leftarrow b}(x_1, \ldots, x_n) \;=\; f(x_1, \ldots, x_{i-1}, b, x_{i+1}, \ldots, x_n)$$

$$f \;=\; \neg x \wedge f\big|_{x \leftarrow 0} \;\;\vee\;\; x \wedge f\big|_{x \leftarrow 1}$$

$$f\big|_{x_i \leftarrow b}(x_1, \ldots, x_n) \;=\; f(x_1, \ldots, x_{i-1}, b, x_{i+1}, \ldots, x_n)$$

$$v \;=\; \neg x \wedge \mathrm{lo}(v) \;\;\vee\;\; x \wedge \mathrm{hi}(v)$$

$$v \qquad\qquad x = \mathrm{var}(v)$$

$$\mathrm{lo}(v) \qquad\qquad \mathrm{hi}(v)$$
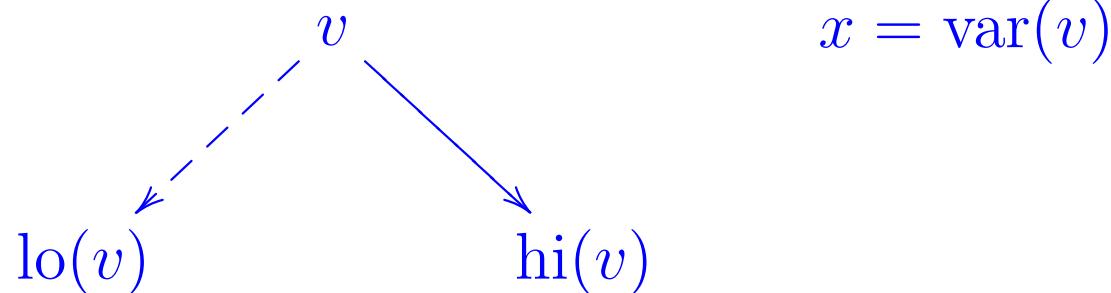
OBDDs as an abstract data type

the order of variables the same in all OBDDs

Operations:

$$f \vee g, \quad f \wedge g, \quad \neg f, \quad \texttt{false}, \quad \texttt{true} \qquad\qquad BF \mapsto OBDD$$

$$f|_{x \leftarrow 0}, \quad f|_{x \leftarrow 1}$$

$$\exists x.\, f, \quad \forall x.\, f \qquad\qquad QBF \mapsto OBDD$$

$$f = g$$

Note: operations on **functions**, not on values $\{0, 1\}$.

Implementation of unary operations

- $f|_{x \leftarrow b}$

  traverse nodes n of OBDD representing f:

    - if $x > \mathrm{var}(n)$ then recursively traverse $\mathrm{lo}(n)$ and $\mathrm{hi}(n)$;

    - if $x < \mathrm{var}(n)$ then stop;

    - otherwise replace n by: $\begin{cases} \mathrm{lo}(n) & \text{if } b = 0 \\ \mathrm{hi}(n) & \text{if } b = 1 \end{cases}$


[Bryant 1992]

– $\exists x.\, f \;=\; f|_{x\leftarrow 0} \vee f|_{x\leftarrow 1}$ the order of variables

remains the same!

– $\neg f$ **?**
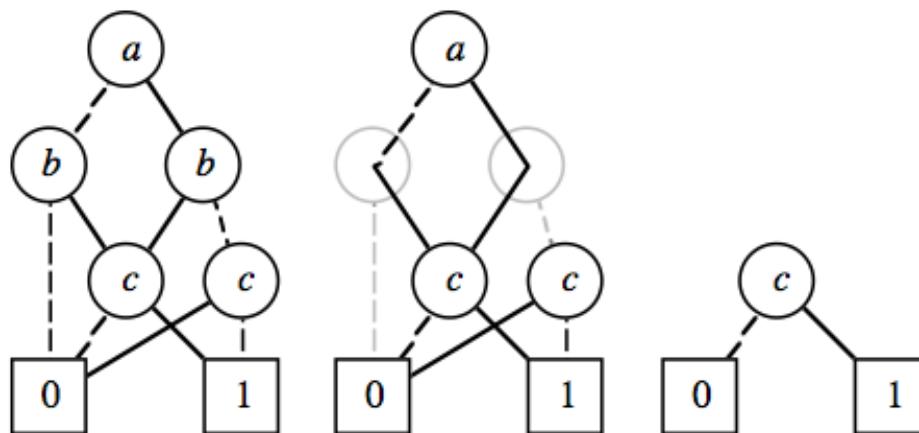
[Bryant 1992]

Implementation of binary operations

the order of variables the same in all OBDDs

• $\bullet \ : \{0,1\}^2 \rightarrow \{0,1\}$

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

$\mathrm{Apply}(\ f,\ g,\ \bullet\ )$ (think of f, g as roots of OBDDs)

- f, g leaves: $\mathrm{val}(f \bullet g) = \mathrm{val}(f) \bullet \mathrm{val}(g)$

- f leaf, g not: $f \bullet g = op(g)$

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

$$\mathrm{lo}(f \bullet g) = \mathrm{lo}(f) \bullet \mathrm{lo}(g) \qquad\qquad \mathrm{hi}(f \bullet g) = \mathrm{hi}(f) \bullet \mathrm{hi}(g)$$

- $\mathrm{var}(f) = x < y = \mathrm{var}(g)$:

$$\mathrm{lo}(f \bullet g) = \mathrm{lo}(f) \bullet g \qquad\qquad \mathrm{hi}(f \bullet g) = \mathrm{hi}(f) \bullet g$$

$$f \bullet g = \neg x \wedge (f \bullet g)|_{x \leftarrow 0} \quad \vee \quad x \wedge (f \bullet g)|_{x \leftarrow 1}$$
$$f \bullet g = \neg x \wedge (f|_{x \leftarrow 0} \bullet g|_{x \leftarrow 0}) \quad \vee \quad x \wedge (f|_{x \leftarrow 1} \bullet g|_{x \leftarrow 1})$$
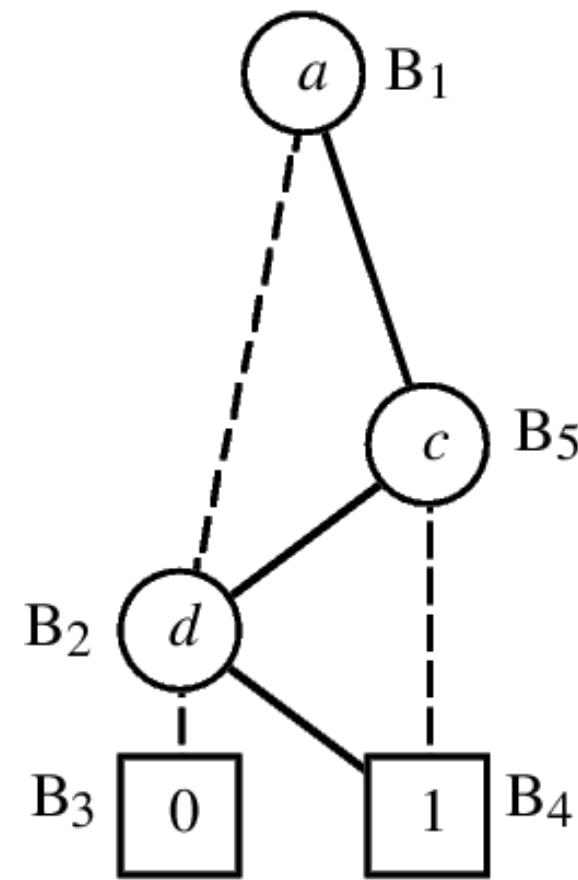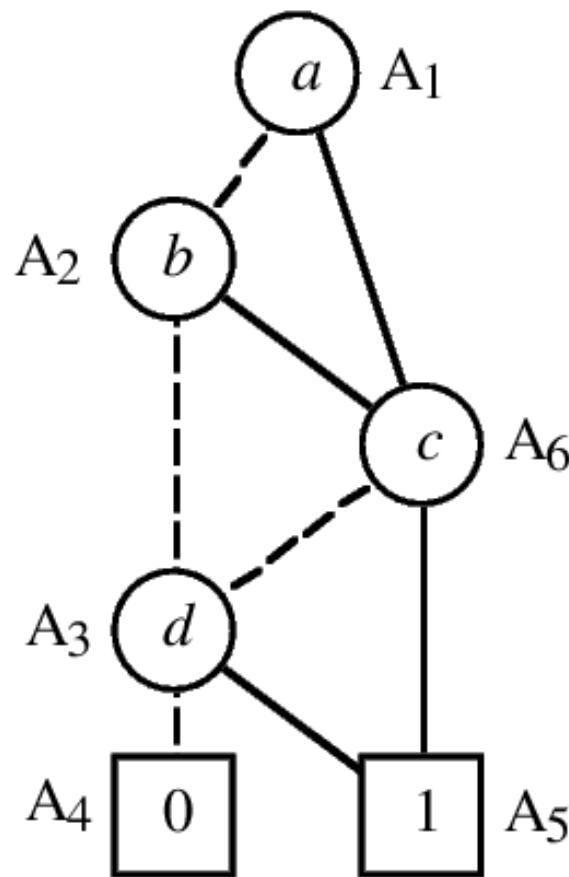
[Bryant 1992]

[Bryant 1992]

$(a \lor b) \land c \lor d$ $a \land \lnot c \lor d$

[Bryant 1992]

Example: reduced result = $a \lor b \land c \lor d$
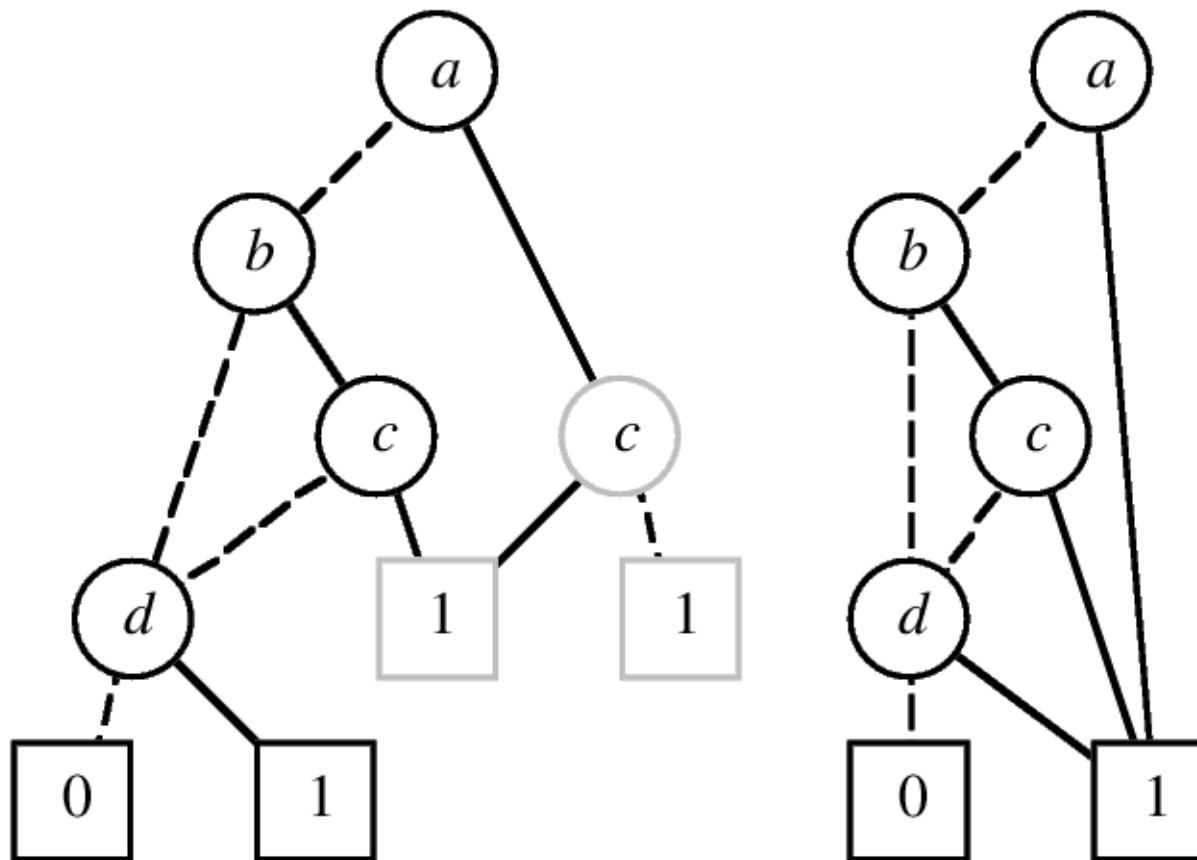
[Bryant 1992]

Implementation of binary operations

$\mathrm{Apply}(\ f,\ g,\ \bullet\ )$

- – running time: $\mathcal{O}(|f| \cdot |g|)$

- – result in the canonical form

Question: $\quad f \iff g$ **?** $\qquad\qquad f = g$ **?**

Variations

- one OBDD shared by all functions

    - $=$ in constant time

- edges representing $\neg$

- OZBDD

- ...

II. Boolean encoding

Boolean encoding
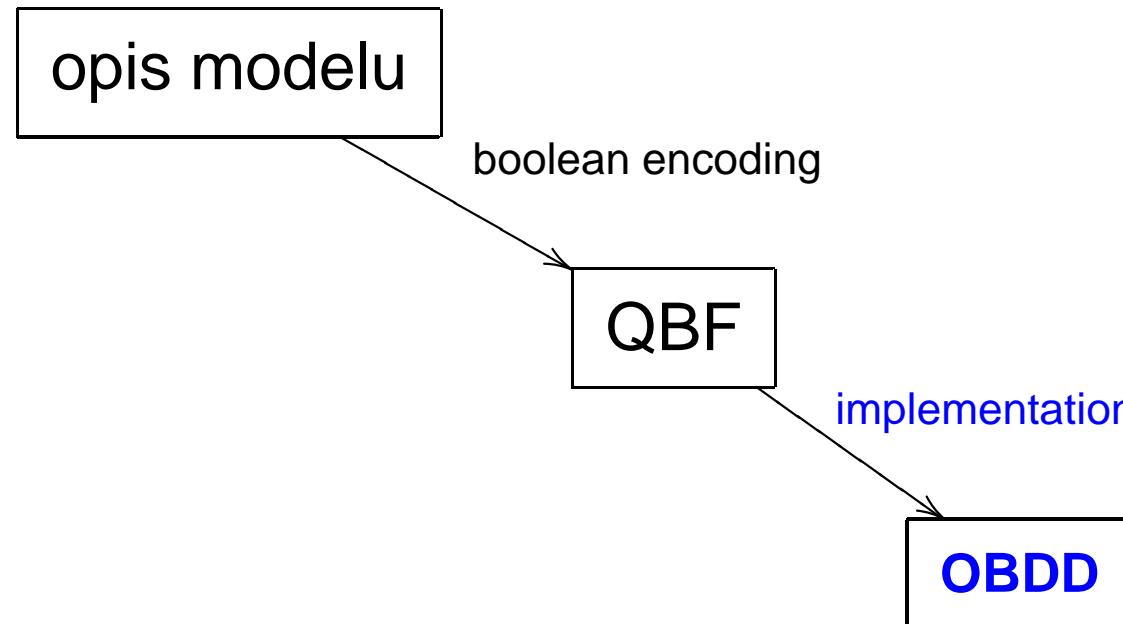
model checking   =   operations on OBDDs

– S described by m boolean variables: $S \equiv \{0,1\}^m$

– transition relation $R : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$

$$R(x_1, \ldots, x_m, x'_1, \ldots, x'_m) \in \{0,1\}$$

– initial states $S_0 : \{0,1\}^m \to \{0,1\}$

$$S_0(x_1, \ldots, x_m) \in \{0,1\}$$

– atomic properties $L_p = \{s \mid p \in L(s)\} : \{0,1\}^m \to \{0,1\}$

$$L_p(x_1, \ldots, x_m) \in \{0,1\}$$

(reachable states)
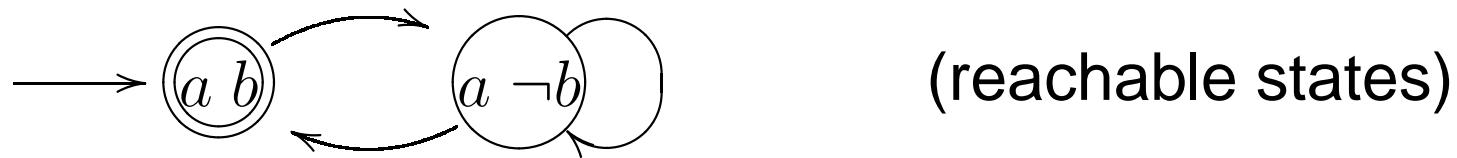
$$R \quad = \quad (x \wedge \neg x') \vee (\neg x \wedge \neg x') \vee (\neg x \wedge x')$$

$$S_0 \quad = \quad x$$

$$L_b \quad = \quad x$$

$$L_a \quad = \quad 1$$

description of a Kripke structure   **NO!**
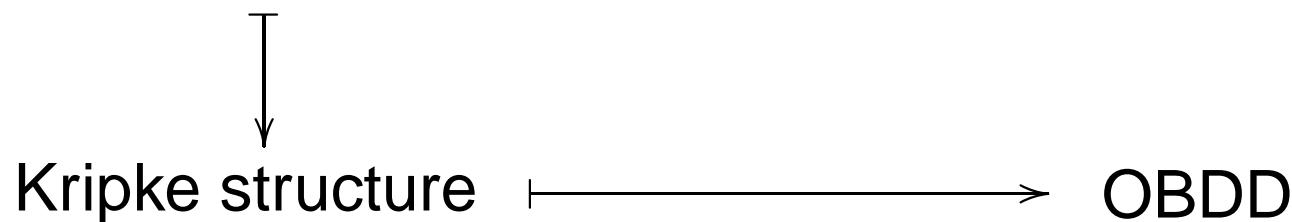
Kripke structure $\longmapsto$ OBDD

description of a Kripke structure   **NO!**

$$\text{Kripke structure} \longmapsto \text{OBDD}$$

description of a Kripke structure $\longmapsto$ OBDD   **YES!**
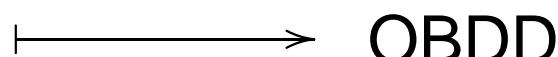
Compositional model desciption

Synchronous processes:

$$R \;=\; R_1 \;\wedge\; R_2 \wedge\; \ldots \;\wedge\; R_n$$

Asynchronous processes (interleaving):

$$R \;=\; R_1' \;\vee\; R_2' \vee\; \ldots \;\vee\; R_n'$$

$$R_i' \;=\; R_i \wedge \left(\bigwedge\nolimits_{j \neq i} \mathrm{Id}_j \right)$$

Asynchronous processes (simultaneous execution):

$$R \;=\; R_1' \;\wedge\; R_2' \wedge\; \ldots \;\wedge\; R_n'$$

$$R_i' \;=\; R_i \vee \mathrm{Id}_i$$

Restriction to reachable states

$$\widehat{R}(x_1, \ldots, x_m, x'_1, \ldots, x'_m) = 1$$

$$\Updownarrow$$

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

$$(x_1, \ldots, x_m), (x'_1, \ldots, x'_m) \text{ reachable}$$

$$\widehat{R}(x_1, \ldots, x_m, x'_1, \ldots, x'_m) = 1$$

$$\Updownarrow$$

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

$$(x_1, \ldots, x_m) \ \text{reachable}$$

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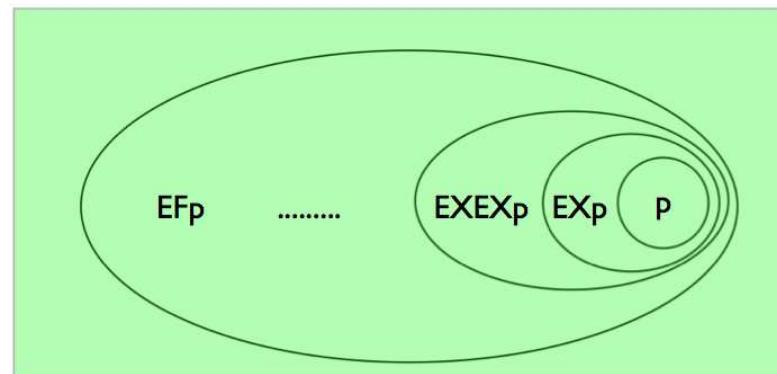
Fixed points in a complete lattice $\langle A, \leq \rangle$.

Let $f : A \to A$ monotonic.

- the least f.p.: $\perp \leq f(\perp) \leq f^2(\perp) \leq \ldots \rightsquigarrow \mu Z. f(Z)$

- 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.

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

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

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

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

`false`
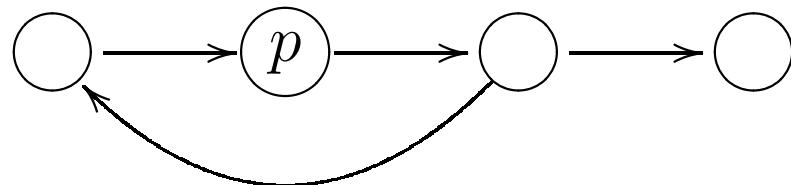
$p \vee \mathsf{EX}\, \texttt{false} \equiv p$
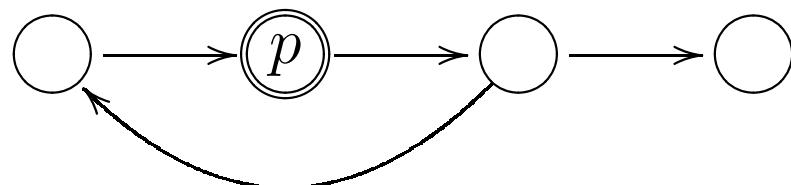
$p \vee \mathsf{EX}\, p$
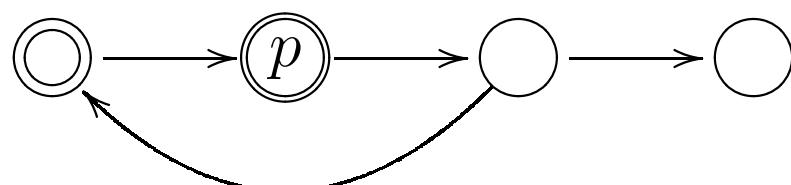
$p \vee \mathsf{EX}\, (p \vee \mathsf{EX}\, p)$
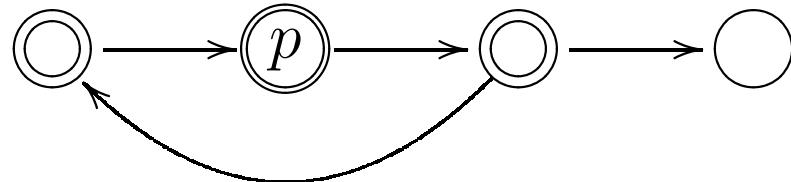
- $\mathsf{EF}\,\phi \;=\; \mu Z.\,\phi \vee \mathsf{EX}\,Z$ $\qquad\qquad\qquad\qquad\qquad Z \mapsto \phi \vee \mathsf{EX}\,Z$

- $\mathsf{AF}\,\phi \;=\; \mu Z.\,\phi \vee \mathsf{AX}\,Z$ $\qquad\qquad\qquad\qquad\qquad Z \mapsto \phi \vee \mathsf{AX}\,Z$

- $\mathsf{EG}\,\phi \;=\; \nu Z.\,\phi \wedge \mathsf{EX}\,Z$ $\qquad\qquad\qquad\qquad\qquad Z \mapsto \phi \wedge \mathsf{EX}\,Z$

- $\mathsf{AG}\,\phi \;=\; \nu Z.\,\phi \wedge \mathsf{AX}\,Z$ $\qquad\qquad\qquad\qquad\qquad Z \mapsto \phi \wedge \mathsf{AX}\,Z$

- $\mathsf{E}\,\phi\,\mathsf{U}\,\psi \;=\; \mu Z.\,\psi \vee (\phi \wedge \mathsf{EX}\,Z)$ $\qquad\qquad Z \mapsto \psi \vee (\phi \wedge \mathsf{EX}\,Z)$

- $\mathsf{A}\,\phi\,\mathsf{U}\,\psi \;=\; \mu Z.\,\psi \vee (\phi \wedge \mathsf{AX}\,Z)$ $\qquad\qquad Z \mapsto \psi \vee (\phi \wedge \mathsf{AX}\,Z)$

- …

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

`true`
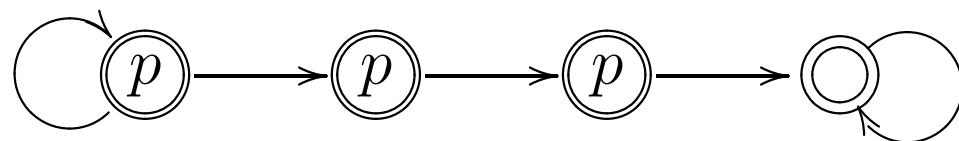
$$p \wedge \mathsf{EX}\,\texttt{true} \;\equiv\; p$$
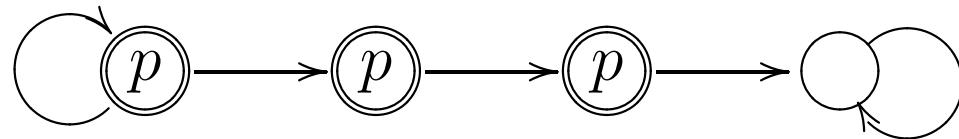
$$p \wedge \mathsf{EX}\,p$$
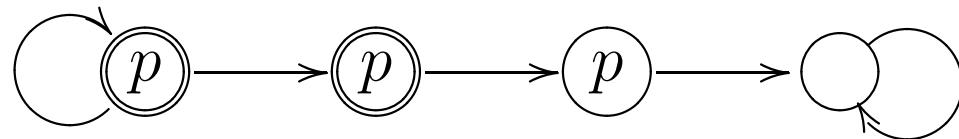
$$p \wedge \mathsf{EX}\,(p \wedge \mathsf{EX}\,p)$$
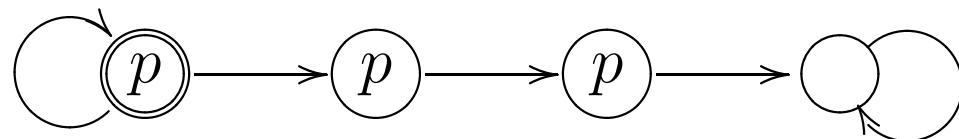
Symbolic model checking

CTL **(¬, ∧, EX, E_U_, EG)**   (these connectives are sufficient)

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

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

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

The order of variables is often crucial!

Symbolic model checking (EX _)

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

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

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

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

$$\boxed{\begin{array}{l} \mathsf{EX}\,\phi \\[2mm] \mathsf{EX}\,Z \\[2mm] \mathsf{EX}\,f \end{array}}$$

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

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

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

Symbolic model checking (E _ U _)

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

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

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

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

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

```
false
```
$$g \vee (f \wedge \mathsf{EX}\,\mathtt{false}) \qquad\qquad\qquad\ \equiv \ g$$
$$g \vee (f \wedge \mathsf{EX}\,(g \vee (f \wedge \mathsf{EX}\,\mathtt{false}))) \ \equiv \ g \vee (f \wedge \mathsf{EX}\, g)$$
$$\mathtt{...} \qquad\qquad\qquad\qquad\qquad\qquad \equiv \ g \vee (f \wedge \mathsf{EX}\,(g \vee (f \wedge \mathsf{EX}\, g$$

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

Symbolic model checking (EG _)

$\mathrm{Check} : \mathsf{CTL} \to \mathsf{OBDD}$ $\boxed{\mathrm{Check}(\phi) \ \text{represents} \ \{s \mid s \vDash \phi\}}$

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

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

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

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

$$\mathsf{EX}\,Z \qquad\qquad \mathsf{E}\,Z\,\mathsf{U}\,Z' \qquad\qquad \mathsf{EG}\,Z$$

$$\mathsf{EX}\,f \qquad\qquad \mathsf{E}\,f\,\mathsf{U}\,g \qquad\qquad \mathsf{EG}\,f$$