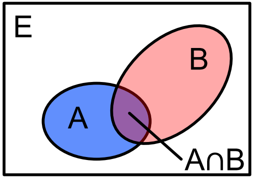
Crash course – Verification of Finite Automata
Binary Decision Diagrams

Exercise session 6
Xiaoxi He

Equivalence of representations



Sets

$\Leftrightarrow$

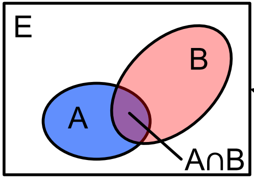
$$\psi_E = 1$$
$$\psi_A = f$$
$$\psi_B = g$$
$$\psi_{A \cap B} = f \cdot g$$

Boolean functions/
Characteristic functions

- Set algebra
- $\cup,\ \cap, \neg$

- Boole algebra
- $+,\ \cdot\ , \neg$

Equivalence of representations



Sets

- Set algebra
- $\cup,\ \cap, \neg$

$\Leftrightarrow$

$$\psi_E = 1$$
$$\psi_A = f$$
$$\psi_B = g$$
$$\psi_{A \cap B} = f \cdot g$$

Boolean functions/
Characteristic functions

- Boole algebra
- $+,\ \cdot, \neg$

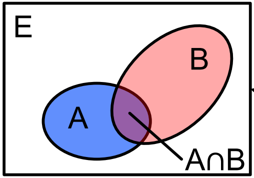
Binary encoding:

$$\sigma : X \rightarrow \Psi$$

→ Map a state to a binary expression

→ Bijective mapping!

Equivalence of representations



Sets

- Set algebra
- $\cup, \ \cap, \neg$

$\Leftrightarrow$

$$\psi_E = 1$$
$$\psi_A = f$$
$$\psi_B = g$$
$$\psi_{A \cap B} = f \cdot g$$

Boolean functions/
Characteristic functions

- Boole algebra
- $+, \ \cdot, \neg$

Binary encoding:

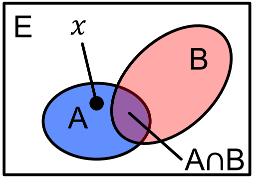
$$\sigma: X \rightarrow \Psi$$

States
Boolean functions

→ Map a state to a binary expression

→ Bijective mapping!

Equivalence of representations



Sets

$\Leftrightarrow$

$$\psi_E = 1$$
$$\psi_A = f$$
$$\psi_B = g$$
$$\psi_{A\cap B} = f \cdot g$$

Boolean functions/
Characteristic functions

- A
- $s \in A$ (proposition)

$\longleftrightarrow$ $\sigma(\cdot)$ $\longleftrightarrow$

- ψ_A
- $\psi_A(\sigma(s)) = 1$

  $\sigma(s) \vDash \psi_A$

  or just $s \vDash \psi_A$

Reads "s satisfies ψ_A"

Example:

$\sigma(s) = x_1\overline{x_0} = (1,0)$ and $\psi_A = x_1 + x_0$

$\rightarrow s \vDash \psi_A$?

Binary Decision Diagrams

Based on the Boole-Shannon decomposition:

$$\underline{f} = \overline{x} \cdot \underline{f\,|_{x=0}} + x \cdot \underline{f\,|_{x=1}}$$

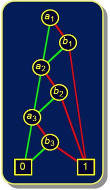
Boolean function of n and $(n-1)$ variables

→ For a given order of variable, **the decomposition is unique!**

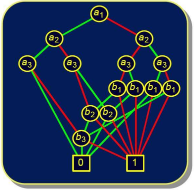
→ Hence the uniqueness of R(reduced)O(rdered)BDD.

Reminder:

In practice, simplicity of BDD depends strongly on the order.



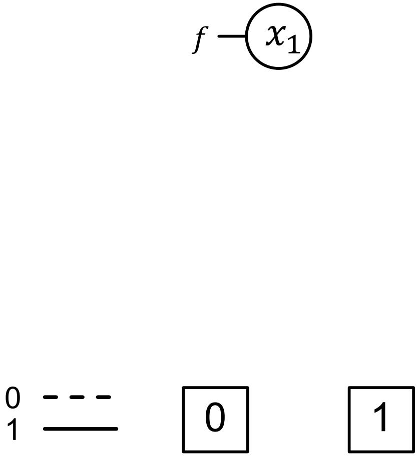
$(a_1 \wedge b_1) \vee$
$(a_2 \wedge b_2) \vee$
$(a_3 \wedge b_3)$



Good vs. Bad ordering

Binary Decision Diagrams: an example

$f: x_1 + \overline{x_1}\, x_2 + \overline{x_2}\, \overline{x_3}$

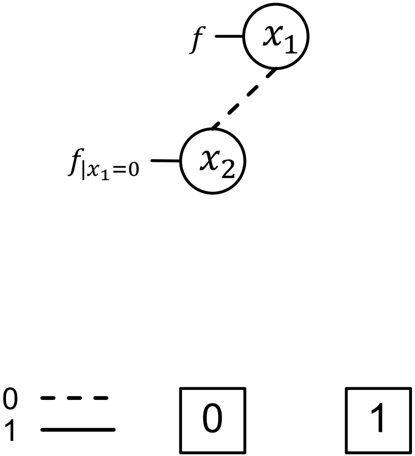


Binary Decision Diagrams: an example

$f: x_1 + \overline{x_1}\, x_2 + \overline{x_2}\, \overline{x_3}$

Fall $x_1 = 0$

$f_{|x_1=0}: x_2 + \overline{x_2}\, \overline{x_3}$



Binary Decision Diagrams: an example

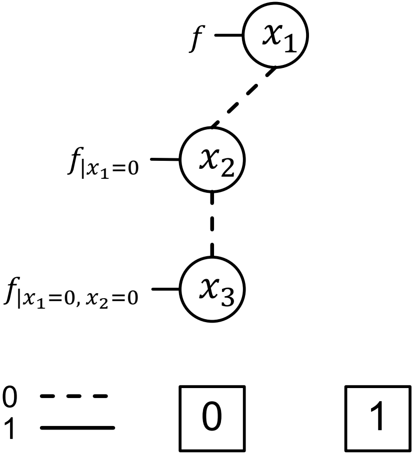
$f: x_1 + \overline{x_1}\, x_2 + \overline{x_2}\, \overline{x_3}$

Fall $x_1 = 0$

$f_{|x_1=0}: x_2 + \overline{x_2}\, \overline{x_3}$

Fall $x_2 = 0$

$f_{|x_1=0,\, x_2=0}: \overline{x_3}$



Binary Decision Diagrams: an example

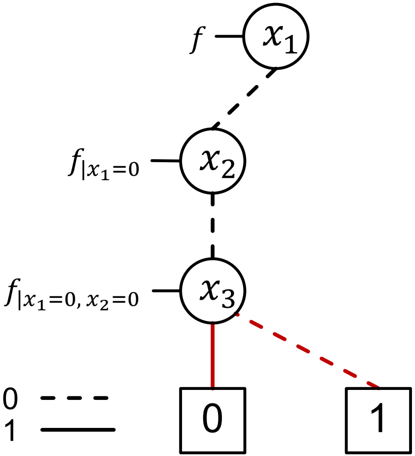
$f: x_1 + \overline{x_1}\, x_2 + \overline{x_2}\, \overline{x_3}$

Fall $x_1 = 0$

$f_{|x_1=0}: x_2 + \overline{x_2}\, \overline{x_3}$

Fall $x_2 = 0$

$f_{|x_1=0,\, x_2=0}: \overline{x_3}$



Binary Decision Diagrams: an example

$f: x_1 + \overline{x_1}\, x_2 + \overline{x_2}\, \overline{x_3}$

Fall $x_1 = 0$

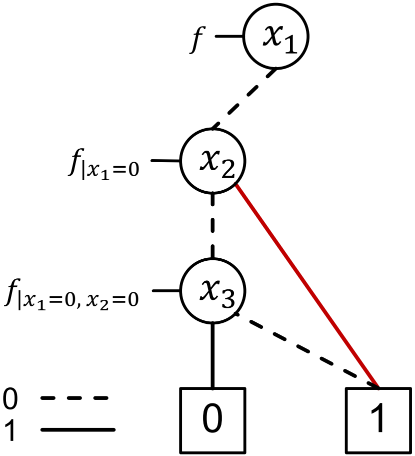
$f_{|x_1=0}: x_2 + \overline{x_2}\, \overline{x_3}$

Fall $x_2 = 0$

$f_{|x_1=0,\, x_2=0}: \overline{x_3}$

Fall $x_2 = 1$

$f_{|x_1=0,\, x_2=1}: 1$



Binary Decision Diagrams: an example

$f: x_1 + \overline{x_1}\, x_2 + \overline{x_2}\, \overline{x_3}$

Fall $x_1 = 0$

$f_{|x_1=0}: x_2 + \overline{x_2}\, \overline{x_3}$

Fall $x_2 = 0$

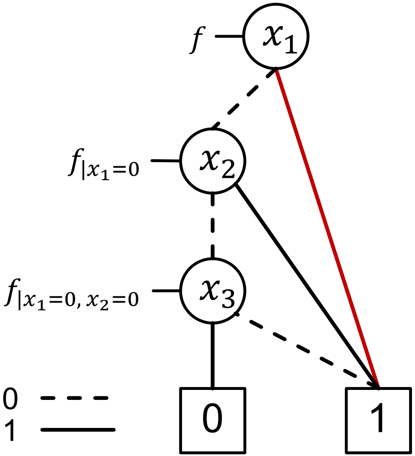
$f_{|x_1=0,\, x_2=0}: \overline{x_3}$

Fall $x_2 = 1$

$f_{|x_1=0,\, x_2=1}: 1$

Fall $x_1 = 1$

$f_{|x_1=1}: 1$



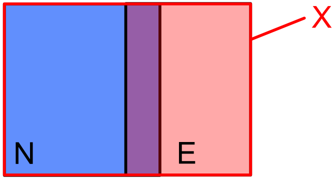
Crash course – Verification of Finite Automata

Binary Decision Diagrams

Your turn !

Ex1: Sets Representation

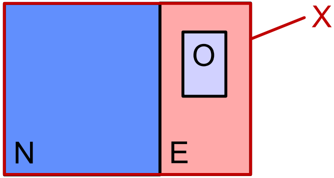
"Each state is either a nominal or an error state or both".



$\Rightarrow$ $$N \cup E = X \quad \Leftrightarrow \quad \psi_N + \psi_E = 1$$

Ex1: Sets Representation

“If a state is in the overflow set, it is not a nominal state".

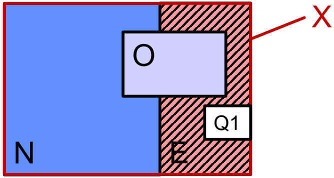


$\Rightarrow$ $$N \cap O = \emptyset \quad \Leftrightarrow \quad \psi_N \cdot \psi_O = 0$$

But note it is not necessarily true !!
Although you would like it to be…

Ex1: Sets Representation

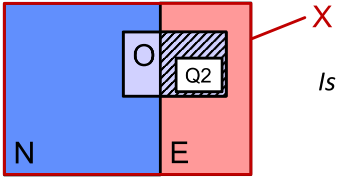
Describe Q1, the set of error states which are not an overflow, in term of sets and characteristic functions.



$\Rightarrow$ $$Q_1 = E \backslash O \quad \Leftrightarrow \quad \psi_{Q_1} = \psi_E \cdot \overline{\psi_O}$$

Ex1: Sets Representation

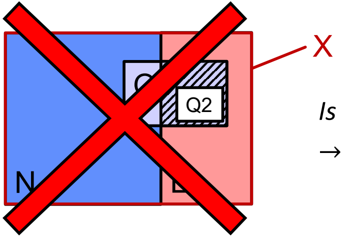
- Describe Q2, satisfying "O ⇒ E", i.e., the set of state for which this property holds, in term of sets and characteristic functions.



Is that correct ?

Ex1: Sets Representation

- Describe Q2, satisfying "O ⇒ E", i.e., the set of state for which this property holds, in term of sets and characteristic functions.



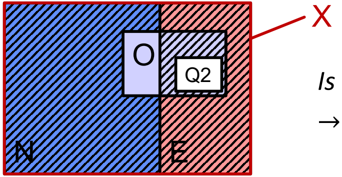
Is that correct? No!

→ *What if a state is not in O?*

Property is always true!

Ex1: Sets Representation

- Describe Q2, satisfying "O ⇒ E", i.e., the set of state for which this property holds, in term of sets and characteristic functions.



Is that correct? No!

→ *What if a state is not in O?*

Property is always true!

⇒

$$Q_2 = (O \cap E) \cup \overline{O} = (O \cup \overline{O}) \cap (E \cup \overline{O}) = X \cap (E \cup \overline{O}) = E \cup \overline{O} \quad \Leftrightarrow \quad \psi_{Q_2} = \psi_E + \overline{\psi_O}$$

Ex1.2: Specification Composition

C1: When one node in using the bus, the sink must be awake to receive data.

If at least one of the sensors is
active, the sink must be active too.

$$\psi_1 = (x_1 + x_2 + x_3) \cdot x_s$$

Ex1.2: Specification Composition

C1: When one node in using the bus, the sink must be awake to receive data.

If at least one of the sensors is active, the sink must be active too.

But when no node is using the bus, then the sink can be either awake or not.

$$\psi_1 = (x_1 + x_2 + x_3) \cdot x_s + \overline{x_1}\,\overline{x_2}\,\overline{x_3}$$

Ex1.2: Specification Composition

C1: When one node in using the bus, the sink must be awake to receive data.

If at least one of the sensors is active, the sink must be active too.

But when no node is using the bus, then the sink can be either awake or not.

$$\psi_1 = (x_1 + x_2 + x_3) \cdot x_s + \overline{x_1}\,\overline{x_2}\,\overline{x_3}$$

$$\psi_1 = \overline{x_1}\,\overline{x_2}\,\overline{x_3} + x_s$$

We can rewrite it into the following:
Either no sensor is active, or the sink is active.

Ex1.2: Specification Composition

C2: No more than one node can use the bus at the same time.

$$\psi_2 =$$

Ex1.2: Specification Composition

C2: No more than one node can use the bus at the same time.

Case: No sensor is active

$$\psi_2 = \overline{x_1}\,\overline{x_2}\,\overline{x_3} +$$

Ex1.2: Specification Composition

C2: No more than one node can use the bus at the same time.

Case: No sensor is active

$$\psi_2 = \overline{x_1}\,\overline{x_2}\,\overline{x_3} + x_1\,\overline{x_2}\,\overline{x_3} +$$

Case: Sensor 1 is active

Ex1.2: Specification Composition

C2: No more than one node can use the bus at the same time.

Case: No sensor is active

Case: Sensor 2 is active

$$\psi_2 = \overline{x}_1\overline{x}_2\overline{x}_3 + x_1\overline{x}_2\overline{x}_3 + \overline{x}_1 x_2 \overline{x}_3 +$$

Case: Sensor 1 is active

Ex1.2: Specification Composition

C2: No more than one node can use the bus at the same time.

Case: No sensor is active

Case: Sensor 2 is active

$$\psi_2 = \overline{x_1}\,\overline{x_2}\,\overline{x_3} + x_1\,\overline{x_2}\,\overline{x_3} + \overline{x_1}\,x_2\,\overline{x_3} + \overline{x_1}\,\overline{x_2}\,x_3$$

Case: Sensor 1 is active

Case: Sensor 3 is active

Ex1.2: Specification Composition

C3: In bootstrapping mode, the sink must be awake and the nodes cannot use the bus.

When we are in bootstrapping, ...

$$\psi_3 = x_b\, x_s\, \overline{x_1}\, \overline{x_2}\, \overline{x_3}$$

Ex1.2: Specification Composition

C3: In bootstrapping mode, the sink must be awake and the nodes cannot use the bus.

When we are in bootstrapping, ...

When not in bootstrapping, no constraints to the sink or the sensors.

$$\psi_3 = x_b x_s \overline{x_1}\,\overline{x_2}\,\overline{x_3} + \overline{x_b}$$

Ex1.2: Specification Composition

C3: In bootstrapping mode, the sink must be awake and the nodes cannot use the bus.

When we are in bootstrapping, ...

When not in bootstrapping, no constraints to the sink or the sensors.

$$\psi_3 = x_b x_s \overline{x_1}\,\overline{x_2}\,\overline{x_3} + \overline{x_b}$$

$$\psi_3 = x_s \overline{x_1}\,\overline{x_2}\,\overline{x_3} + \overline{x_b}$$

Simplification: Either we are not in bootstrapping, or the sink and no sensor is active.

Ex1.2: Specification Composition

What is the specification of the desired behavior?

$$\psi = \psi_1 \cdot \psi_2 \cdot \psi_3$$

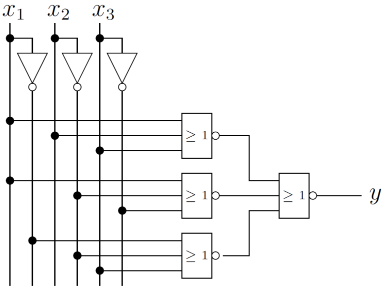
Ex1.2: Specification Composition

What is the specification of the desired behavior?

$$\psi = \psi_1 \cdot \psi_2 \cdot \psi_3$$

Remember: The union of sets corresponds to multiplication in Boolean Algebra

Ex2.1 Verication using BDDs



a) $f_2 : y = \overline{\overline{x_1 + x_2 + x_3} + \overline{x_1 + \overline{x_2} + \overline{x_3}} + \overline{\overline{x_1} + \overline{x_2} + x_3}}$

Ex2.1 Verication using BDDs

$$f_1 : (x_1\overline{x_2} + x_1x_3 + \overline{x_2}x_3 + \overline{x_1}x_2\overline{x_3})$$

Fall $x_1 = 0$

$y_{|x_1=0} = \overline{x_2}x_3 + x_2\overline{x_3}$

Fall $x_2 = 0$

$y_{|x_1=0,x_2=0} = x_3$

Fall $x_2 = 1$

$y_{|x_1=0,x_2=1} = \overline{x_3}$

Fall $x_1 = 1$

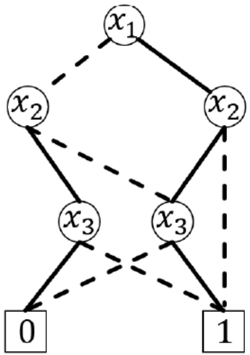
$y_{|x_1=1} = \overline{x_2} + x_3 + \overline{x_2}x_3$

Fall $x_2 = 0$

$y_{|x_1=1,x_2=0} = 1$

Fall $x_2 = 1$

$y_{|x_1=1,x_2=1} = x_3$



Ex2.1 Verication using BDDs

$$f_2 : y = \overline{\overline{x_1 + x_2 + x_3} + \overline{x_1 + \overline{x_2} + \overline{x_3}} + \overline{\overline{x_1} + \overline{x_2} + x_3}}$$

Fall $x_1 = 0$

$$y_{|x_1=0} = \overline{\overline{x_2 + x_3} + \overline{\overline{x_2} + \overline{x_3}}}$$

Fall $x_2 = 0$

$$y_{|x_1=0,x_2=0} = \overline{\overline{x_3} + \overline{1 + \overline{x_3}}} = x_3$$

Fall $x_2 = 1$

$$y_{|x_1=0,x_2=1} = \overline{\overline{1} + \overline{\overline{x_3}}} = \overline{x_3}$$

Fall $x_1 = 1$

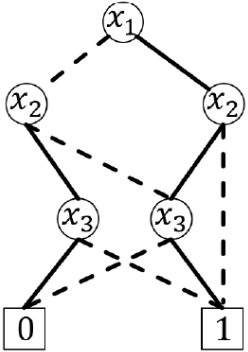
$$y_{|x_1=1} = \overline{\overline{1} + \overline{1} + \overline{\overline{x_2} + x_3}} = \overline{x_2} + x_3$$

Fall $x_2 = 0$

$$y_{|x_1=1,x_2=0} = 1$$

Fall $x_2 = 1$

$$y_{|x_1=1,x_2=1} = x_3$$

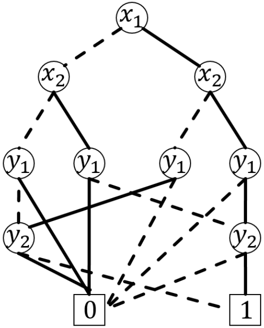


Ex2.2 BDDs with respect to different orderings

$$g(x_1, x_2, y_1, y_2) = (x_1 \equiv y_1) \cdot (x_2 \equiv y_2) \ , \quad \Pi : x_1 < x_2 < y_1 < y_2$$

a) $$g = x_1\{x_2[y_1(y_2) + \overline{y_1}(0)] + \overline{x_2}[y_1(\overline{y_2}) + \overline{y_1}(0)]\} + \overline{x_1}\{x_2[y_1(0) + \overline{y_1}(y_2)] + \overline{x_2}[y_1(0) + \overline{y_1}(\overline{y_2})]\}$$

b)



Ex2.2 BDDs with respect to different orderings

$$g(x_1, x_2, y_1, y_2) = (x_1 \equiv y_1) \cdot (x_2 \equiv y_2)\ ,\quad \Pi' : x_1 < y_1 < x_2 < y_2$$

c) $$g = x_1\{y_1[x_2(y_2) + \overline{x_2}(\overline{y_2})] + \overline{y_1}[0]\} + \overline{x_1}\{y_1[0] + \overline{y_1}[x_2(y_2) + \overline{x_2}(\overline{y_2})]\}$$

Better ordering:

6 vs. 9 nodes