Verification

Lecture 5

Bernd Finkbeiner

UNIVERSITÄT
DES
SAARLANDES

Plan for today

- Binary Decision Diagrams
- Symbolic model checking

Boolean functions

- Boolean functions $f : \mathbb{B}^n \to \mathbb{B}$ for $n \geq 0$ where $\mathbb{B} = \{0, 1\}$
  - examples: $f(x_1, x_2) = x_1 \wedge (x_2 \vee \neg x_1)$, and $f(x_1, x_2) = x_1 \leftrightarrow x_2$
- Finite sets are boolean functions
  - let $|S| = N$ and $2^{n-1} < N \leq 2^n$
  - encode any element $s \in S$ as boolean vector of length n: $[\![\ ]\!] : S \to \mathbb{B}^n$
  - $T \subseteq S$ is represented by f_T such that:

$$f_T([\![s]\!]) = 1 \quad \text{iff} \quad s \in T$$

  - this is the characteristic function of T
- Relations are boolean functions
  - $\mathcal{R} \subseteq S \times S$ is represented by $f_{\mathcal{R}}$ such that:

$$f_{\mathcal{R}}([\![s]\!], [\![t]\!]) = 1 \quad \text{iff} \quad (s, t) \in \mathcal{R}$$

Transition systems as boolean functions

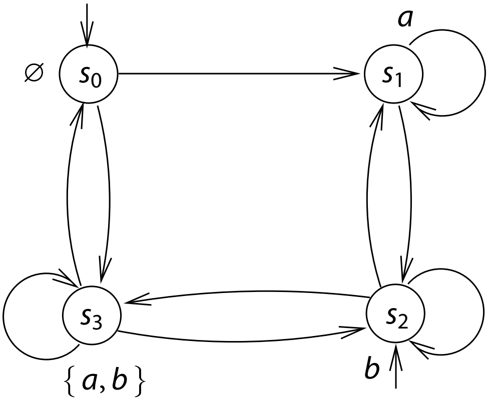
- Assume each state is uniquely labeled
  - $L(s) = L(s')$ implies $s = s'$
  - no restriction: if needed extend *AP* and label states uniquely
- Assume a fixed total order on propositions: $a_1 < a_2 < \ldots < a_K$
- Represent a state by a boolean function
  - over the boolean variables x_1 through x_K such that

$$[\![s]\!] = x_1^* \wedge x_2^* \wedge \ldots \wedge x_K^*$$

  - where the literal x_i^* equals x_i if $a_i \in L(s)$, and $\neg x_i$ otherwise

  $\Rightarrow$ no need to explicitly represent function *L*
- Represent *I* and $\rightarrow$ by their characteristic (boolean) functions
  - e.g., $f_{\rightarrow}([\![s]\!], [\![\alpha]\!], [\![t]\!]) = 1$ if and only if $s \xrightarrow{\alpha} t$

Example



state	bit-vector	boolean function
s_0	$\langle 0, 0 \rangle$	$\neg x_1 \wedge \neg x_2$
s_1	$\langle 0, 1 \rangle$	$\neg x_1 \wedge x_2$
s_2	$\langle 1, 0 \rangle$	$x_1 \wedge \neg x_2$
s_3	$\langle 1, 1 \rangle$	$x_1 \wedge x_2$

- States:
- Initial states:

$$f_I(x_1, x_2) = (\neg x_1 \wedge \neg x_2) \vee (x_1 \wedge \neg x_2)$$

Example (continued)

- Transition relation:

$f_\rightarrow$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$
$\langle 0,0\rangle$	0	1	0	1
$\langle 0,1\rangle$	0	1	1	0
$\langle 1,0\rangle$	0	1	1	1
$\langle 1,1\rangle$	1	0	1	1

- $f_\rightarrow(\underbrace{x_1, x_2}_{s}, \underbrace{x_1', x_2'}_{s'}) = 1$ if and only if $s \rightarrow s'$

$$
\begin{aligned}
f_\rightarrow(x_1, x_2, x_1', x_2') = \quad & (\neg x_1 \wedge \neg x_2 \wedge \neg x_1' \wedge x_2') \\
\vee \quad & (\neg x_1 \wedge \neg x_2 \wedge x_1' \wedge x_2') \\
\vee \quad & (\neg x_1 \wedge x_2 \wedge x_1' \wedge \neg x_2') \\
\vee \quad & \ldots \\
\vee \quad & (x_1 \wedge x_2 \wedge x_1' \wedge x_2')
\end{aligned}
$$

Representing boolean functions

representation	compact?	sat	$\wedge$	$\vee$	$\neg$
propositional formula	often	hard	easy	easy	easy
DNF	sometimes	easy	hard	easy	hard
CNF	sometimes	hard	easy	hard	hard
(ordered) truth table	never	hard	hard	hard	hard

Representing boolean functions

representation	compact?	sat	$\wedge$	$\vee$	$\neg$
propositional formula	often	hard	easy	easy	easy
DNF	sometimes	easy	hard	easy	hard
CNF	sometimes	hard	easy	hard	hard
(ordered) truth table	never	hard	hard	hard	hard
reduced ordered binary decision diagram	often	easy	medium	medium	easy

Binary decision trees

- Let X be a set of boolean variables and $<$ a total order on X
- Binary decision tree (BDT) is a complete binary tree over $\langle X, < \rangle$
  - each leaf v is labeled with a boolean value $val(v) \in \mathbb{B}$
  - non-leaf v is labeled by a boolean variable $Var(v) \in X$
  - such that for each non-leaf v and vertex w:

$$w \in \{ left(v), right(v) \} \Rightarrow (Var(v) < Var(w) \vee w \text{ is a leaf})$$

$\Rightarrow$ On each path from root to leaf, variables occur in the same order

Shannon expansion

- Each boolean function $f : \mathbb{B}^n \longrightarrow \mathbb{B}$ can be written as:

$$f(x_1, \ldots, x_n) = (x_i \ \wedge \ f[x_i := 1]) \ \vee \ (\neg x_i \ \wedge \ f[x_i := 0])$$

  - where $f[x_i := 1]$ stands for $f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$
  - and $f[x_i := 0]$ for $f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$
- The boolean function $f_B(v)$ represented by vertex v in BDT B is:
  - for v a leaf: $f_B(v) = val(v)$
  - otherwise:

$$f_B(v) = (Var(v) \ \wedge \ f_B(right(v))) \ \vee \ (\neg Var(v) \ \wedge \ f_B(left(v)))$$

- $f_B = f_B(v)$ where v is the root of B

Considerations on BDTs

- BDTs are not compact
  - a BDT for boolean function $f : \mathbb{B}^b \to \mathbb{B}$ has 2^n leafs
  - $\Rightarrow$ they are as space inefficient as truth tables!
- $\Rightarrow$ BDTs contain quite some redundancy
  - all leafs with value one (zero) could be collapsed into a single leaf
  - a similar scheme could be adopted for isomorphic subtrees
- The size of a BDT does not change if the variable order changes

Ordered Binary Decision Diagram

share equivalent expressions [Akers 76, Lee 59]

- Binary decision diagram (OBDD) is a directed graph over $\langle X, < \rangle$ with:
  - each leaf v is labeled with a boolean value $val(v) \in \{ 0, 1 \}$
  - non-leaf v is labeled by a boolean variable $Var(v) \in X$
  - such that for each non-leaf v and vertex w:

$$w \in \{ left(v), right(v) \} \;\Rightarrow\; (Var(v) < Var(w) \;\vee\; w \text{ is a leaf})$$

⇒ An OBDD is acyclic

  - f_B for OBDD B is obtained as for BDTs

Reduced OBDDs

OBDD B over $\langle X, < \rangle$ is called reduced iff:

1. for each leaf v, w: $(val(v) = val(w)) \;\Rightarrow\; v = w$

   $\Rightarrow$ identical terminal vertices are forbidden

2. for each non-leaf v: $left(v) \neq right(v)$

   $\Rightarrow$ non-leafs may not have identical children

3. for each non-leaf v, w:

$$(Var(v) = Var(w) \;\wedge\; right(v) \cong right(w) \;\wedge\; left(v) \cong left(w)) \;\Rightarrow\; v = w$$

   $\Rightarrow$ vertices may not have isomorphic sub-dags

this is what is mostly called BDD; in fact it is an ROBDD!

Dynamic generation of ROBDDs

Main idea:

- Construct directly an ROBDD from a boolean expression
- Create vertices in depth-first search order
- On-the-fly reduction by applying hashing
  - on encountering a new vertex v, check whether:
  - an equivalent vertex w has been created (same label and children)
  - $left(v) = right(v)$, i.e., vertex v is a "don't care" vertex

ROBDDs are canonical

[Fortune, Hopcroft & Schmidt, 1978]

For ROBDDs B and B′ over $\langle X, < \rangle$ we have:

$(f_B = f_{B'})$ implies B and B′ are isomorphic

$\Rightarrow$ for a fixed variable ordering, any boolean function
can be uniquely represented by an ROBDD (up to isomorphism)

The importance of canonicity

- Absence of redundant vertices
  - if f_B does not depend on x_i, ROBDD B does not contain an x_i vertex
- Test for equivalence: $f(x_1, \ldots, x_n) \equiv g(x_1, \ldots, x_n)$?
  - generate ROBDDs B_f and B_g, and check isomorphism
- Test for validity: $f(x_1, \ldots, x_n) = 1$?
  - generate ROBDD B_f and check whether it only consists of a 1-leaf
- Test for implication: $f(x_1, \ldots, x_n) \rightarrow g(x_1, \ldots, x_n)$?
  - generate ROBDD $B_f \wedge \neg B_g$ and check if it just consist of a 0-leaf
- Test for satisfiability
  - f is satisfiable if and only if B_f is not just the 0-leaf

Variable ordering

- Different ROBDDs are obtained for different variable orderings
- The size of the ROBDD depends on the variable ordering
- Some boolean functions have linear and exponential ROBDDs
- Some boolean functions only have polynomial ROBDDs
- Some boolean functions only have exponential ROBDDs

The even parity function

$f(x_1, \ldots, x_n) = 1$ iff the number of variables x_i with value 1 is even

truth table or propositional formula for f has exponential size

but an ROBDD of linear size is possible

Symmetric functions

$$f[x_1 := b_1, \ldots, x_n := b_n] = f[x_1 := b_{i_1}, \ldots, x_{i_n} := b_{i_n}]$$

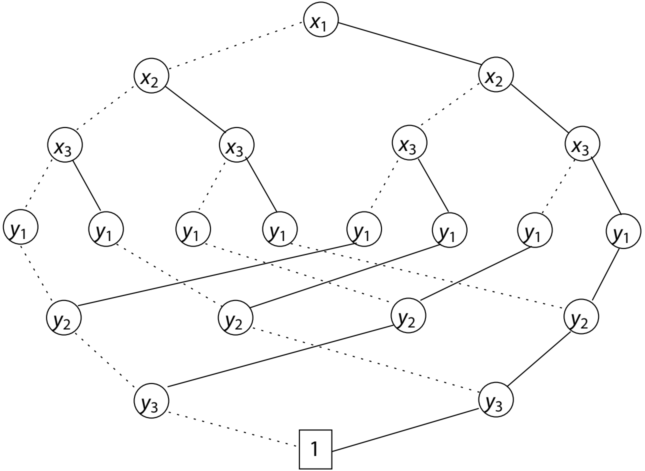
for each permutation $(i_1, \ldots, i_n)$ of $(1, \ldots, n)$

$\Rightarrow$ The value of f depends only on the number of ones!

Examples: $f(\ldots) = x_1 \oplus \ldots \oplus x_n$,
$f(\ldots) = 1$ iff $\geq k$ variables x_i are true

symmetric boolean functions have ROBDDs of size in $\mathcal{O}(n^2)$

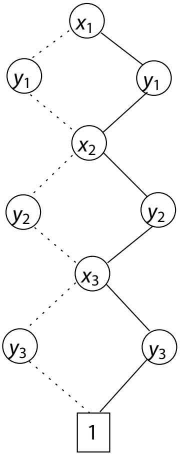
The function stable with exponential ROBDD



The ROBDD of $f(\overline{x}, \overline{y}) = (x_1 \leftrightarrow y_1) \wedge \ldots \wedge (x_n \leftrightarrow y_n)$

has $3 \cdot 2^n - 1$ vertices under ordering $x_1 < \ldots < x_n < y_1 < \ldots < y_n$

The function stable with linear ROBDD



The ROBDD of $f(\overline{x}, \overline{y}) = (x_1 \leftrightarrow y_1) \wedge \ldots \wedge (x_n \leftrightarrow y_n)$

has $3 \cdot n + 2$ vertices under ordering $x_1 < y_1 < \ldots < x_n < y_n$

Optimal variable ordering

- The size of ROBDDs is dependent on the variable ordering
- Is it possible to determine $<$ such that the ROBDD has minimal size?
  - the optimal variable ordering problem for ROBDDs is NP-complete (Bollig & Wegener, 1996)
- There are many boolean functions with large ROBDDs
- How to deal with this problem in practice?
  - guess a variable ordering in advance
  - rearrange the variable ordering during the manipulations of ROBDDs

Sifting algorithm

(Rudell, 1993)

Dynamic variable ordering using variable swapping:

1. Select a variable x_i
2. By successive swapping of x_i, determine $|B|$ at any position for x_i
3. Shift x_i to its optimal position
4. Go back to the first step until no improvement is made

- Characteristics:
  - a variable may change position several times during a single sifting iteration
  - often yields a local optimum, but works well in practice

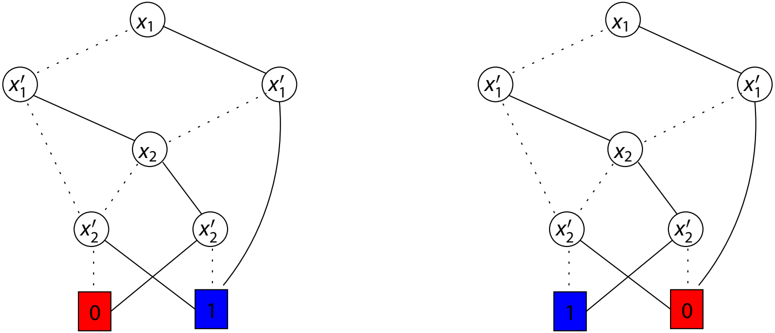
Interleaved variable ordering

- Which variable ordering to use for transition relations?
- The interleaved variable ordering:
  - for encodings $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ of state s and t respectively:

$$x_1 < y_1 < x_2 < y_2 < \ldots < x_n < y_n$$

- This variable ordering yields compact ROBDDs for binary relations

Negation



negation amounts to interchange the 0- and 1-leaf

Apply

- Shannon expansion for binary operations:

$$\begin{aligned} f \; op \; g \quad = \quad & (x_1 \land (f[x_1 := 1] \; op \; g[x_1 := 1])) \\ \lor \; & (\neg x_1 \land (f[x_1 := 0] \; op \; g[x_1 := 0])) \end{aligned}$$

- A top-down evaluation scheme using Shannon's expansion:
  - let v be the variable highest in the ordering occurring in B_f orB_g
  - split the problem into subproblems for $v := 0$ and $v := 1$, and solve recursively
  - at the leaves, apply the boolean operator *op* directly
  - reduce afterwards to turn the resulting OBDD into an ROBDD
- Efficiency gain is obtained by dynamic programming
  - the time complexity of constructing the ROBDD of $B_{f \; op \; g}$ is in $\mathcal{O}(|B_f| \cdot |B_g|)$

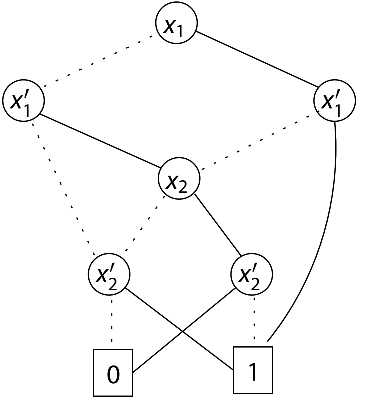
Algorithm Apply(op, B_f, B_g)

if $G(op, v_1, v_2) \neq$ empty **then return** $G(op, v_1, v_2)$ **fi**; {lookup in hashtable}
if (v_1 and v_2 are terminals) **then** res := $val(v_1)$ op $val(v_2)$ **fi**;
else if (v_1 is terminal and v_2 is nonterminal)
    then res := $MakeNode(Var(v_2)$, Apply$(op, v_1, left(v_2))$, Apply$(op, v_1, right(v_2)))$;
else if (v_1 is nonterminal and v_2 is terminal)
    then res := $MakeNode(Var(v_1)$, Apply$(op, left(v_1), v_2)$, Apply$(op, right(v_1), v_2))$;
else if ($Var(v_1) = Var(v_2)$)
    then res := $MakeNode(Var(v_1)$, Apply$(op, left(v_1), left(v_2))$,
        Apply$(op, right(v_1), right(v_2)))$;
else if ($Var(v_1) < Var(v_2)$)
    then res := $MakeNode(Var(v_1)$, Apply$(op, left(v_1), v_2)$, Apply$(op, right(v_1), v_2))$;
else {$Var(v_1) > Var(v_2)$}
    res := $MakeNode(Var(v_2)$, Apply$(op, v_1, left(v_2))$, Apply$(op, v_1, right(v_2)))$;
$G(op, v_1, v_2)$:= res; {memoize result}
return res

Algorithm Restrict(B, x, b)

- For each vertex v labeled with variable x:
  - if $b = 1$ then redirect incoming edges to $right(v)$
  - if $b = 0$ then redirect incoming edges to $left(v)$
  - remove vertex v, and all vertices only reachable through v
  - (if necessary) reduce (only above v)

Restrict



performing Restrict$(B, x_2, 1)$: replace x_2 by constant 1

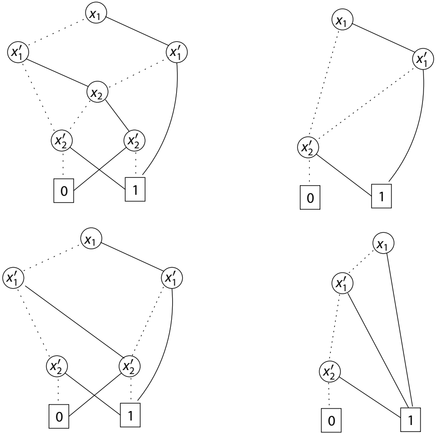
Abstract

- Existential quantification over x_i:

$$\exists x_i. f(x_1, \ldots, x_n) = f[x_i := 1] \;\vee\; f[x_i := 0]$$

- Naive realization: Apply$(\vee, \text{Restrict}(B_f, x_i, 1), \text{Restrict}(B_f, x_i, 0))$
- Efficiency gain:
    - observe that Restrict$(B_f, x_i, 1)$ and Restrict$(B_f, x_i, 0)$ are equal up to x_i
    - ... the resulting ROBDD also has the same structure up to x_i
    - replace each node labeled with x_i by the result of applying $\vee$ on its children
- This can easily be generalized to $\exists x_1. \ldots \exists x_k. f(x_1, \ldots x_n)$

Example



ROBBDs B_f (left up), $B_{f[x_2:=0]}$ (right up), $B_{f[x_2:=1]}$ (left down), and $B_{\exists x_2.\ f}$ (right down)

Operations on ROBDDs

Algorithm	Output	Time complexity	Space complexity
Not	$B_{\neg f}$	$\mathcal{O}(\|B_f\|)$	$\mathcal{O}(\|B_f\|)$
Apply	$B_{f\ op\ g}$	$\mathcal{O}(\|B_f\|\cdot\|B_g\|)$	$\mathcal{O}(\|B_f\|\cdot\|B_g\|)$
Restrict	$B_{f[x:=b]}$	$\mathcal{O}(\|B_f\|)$	$\mathcal{O}(\|B_f\|)$
Rename	$B_{f[x:=y]}$	$\mathcal{O}(\|B_f\|)$	$\mathcal{O}(\|B_f\|)$
Abstract	$B_{\exists x.\,f}$	$\mathcal{O}(\|B_f\|^2)$	$\mathcal{O}(\|B_f\|^2)$

operations are only efficient if f and g have compact ROBDD representations

Symbolic CTL model checking: Computing $Sat(\Phi)$

Require: CTL-formula Φ in ENF
Ensure: ROBDD $B_{Sat(\Phi)}$

---

switch(Φ):

true	:	**return** Const(1);
false	:	**return** Const(0);
x_i	:	**return** ROBDD B_f for $f(x_1, \ldots, x_n) = x_i$;
$\neg\Psi$	:	**return** Not($bddSat(\Psi)$)
$\Phi_1 \wedge \Phi_2$	:	**return** Apply($\wedge, bddSat(\Phi_1), bddSat(\Phi_2)$)
EX Ψ	:	**return** $bddEX(\Psi)$;
E (Φ_1 U Φ_2)	:	**return** $bddEU(\Phi_1, \Phi_2)$
EG Ψ	:	**return** $bddEG(\Psi)$

end switch

Symbolic CTL model checking: The next-step operator

$$Sat(\mathrm{X}\,\Phi) \;=\; \{\, q \in Q \mid \exists q'.\,(q,q') \in E \text{ and } q' \in Sat(\Phi) \,\}$$

Require: CTL-formula Φ in ENF
Ensure: ROBDD $\mathrm{B}_{Sat(\mathrm{X}\,\Phi)}$

B := $bddSat(\Phi)$; $\{Sat(\Phi)\}$
B := Rename$(\mathrm{B}, x_1, \ldots, x_n, x_1', \ldots, x_n')$;
B := Apply$(\wedge, \mathrm{B}_{\rightarrow}, \mathrm{B})$; $\{Pre(Sat(\Phi))\}$
return Abstract$(\mathrm{B}, x_1', \ldots, x_n')$

Symbolic CTL model checking: Existential until

Require: CTL-formulas Φ, Ψ in ENF
Ensure: ROBDD $B_{Sat(\mathsf{E}\,(\Phi\,\mathsf{U}\,\Psi))}$

---

var N, P, B : *ROBDD*;
N := *bddSat*(Ψ);
P := Const(0);
B := *bddSat*(Φ);
while (N ≠ P) **do**
  P := N; $\{T_i\}$
  N := Rename(N, $x_1, \ldots, x_n, x'_1, \ldots, x'_n$);
  N := Apply($\wedge$, $B_{\rightarrow}$, N); $\{Pre(T_i)\}$
  N := Abstract(N, $x'_1, \ldots, x'_n$);
  N := Apply($\wedge$, N, B); $\{Pre(T_i) \cap Sat(\Phi)\}$
  N := Apply($\vee$, P, N); $\{T_{i+1} = T_i \cup \ldots\ldots\}$
end while
return N

Symbolic CTL model checking: Possibly always

Require: CTL-formula Φ in ENF
Ensure: ROBDD $B_{Sat(\text{EG}\,\Phi)}$

---

var N, P, B : *ROBDD*;
B := $bddSat(\Phi)$;
N := B;
P := Const(0);
while (N $\neq$ P) **do**
  P := N; $\{T_i\}$
  N := Rename(N, $x_1, \ldots, x_n, x'_1, \ldots, x'_n$);
  N := Apply($\wedge$, $B_{\rightarrow}$, N); $\{Pre(T_i)\}$
  N := Abstract(N, $x'_1, \ldots, x'_n$);
  N := Apply($\wedge$, N, B); $\{Pre(T_i) \cap Sat(\Phi)\}$
  N := Apply($\wedge$, P, N); $\{T_{i+1} = T_i \cap \ldots\ldots\}$
end while
return N