ECE 510 OCE
BDDs and Their Applications

Lecture 8. Image Computation and Reachability Analysis

April 20, 2000
Alan Mishchenko

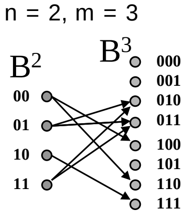
Overview

- Relations as the most fundamental(?) representation of discrete phenomena
- Image computation for relations
- Representing FSMs using relations
- Reachability analysis as an exploration of the state space of FSMs using the transition relation
- Applications of reachability analysis
  - Computing the transitive closure of relations
  - Equivalence checking of FSMs

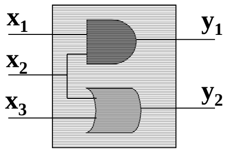
Boolean Functions and Relations

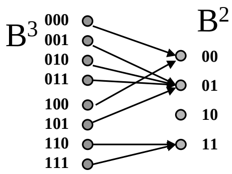
- Function is a mapping $B^n \to B$, $B = \{0,1\}$
- Function with DCs is a mapping $B^n \to \{0,1,-\}$
- Relation is a mapping $B^n \to B^m$, $n > 0$, $m > 0$.
- Example: $F(x_1,x_2, y_1,y_2,y_3)$, $n = 2$, $m = 3$

x_1	x_2	y_1	y_2	y_3
0	0	1	-	0
0	1	0	1	-
1	0	1	1	1
1	1	0	1	-



Example





x_1	x_2	x_3	y_1	y_2
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	0	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	1
1	1	1	1	1

Definition of Image

- Definitions. Given the relation R: $B^n \to B^m$, the set of all vertices in B^n is the input domain while the set of all vertices in B^m is the output domain. The domain of the relation is the subset of the input domain, for which the relation is defined. The range of the relation is the subset of the output domain which, under some inputs, may be the value of the relation
- Definition. Given subset X of the relation's domain ($X \in B^n$), the image of X w.r.t. the relation R is the subset Y of the range ($Y \in B^m$) composed of values the relation can take if its input values belong to X.

$$Y = Im_R(X)$$

Graphical Interpretation of Image

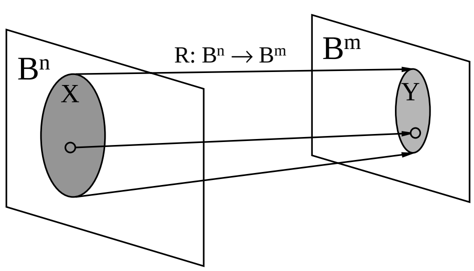


Image Computation

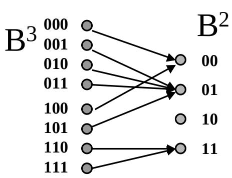
- Given the relation R(X, Y) and the set of input assignments A(X), it is possible to compute the set of assignments B(Y) such that X and Y satisfy relation R(X, Y).

  $B(Y) = \exists_x [\ R(X, Y)\ \&\ A(X)\ ]$
- B(Y) is the forward image of the set A(X) in the relation R(X, Y).
- Similarly, it is possible to compute the backward image A(X) of the set B(Y).

Example

Given the relation R and the set X = { (001), (110) },

the image is $Y = Im_R(X)$ = { (01), (11) }

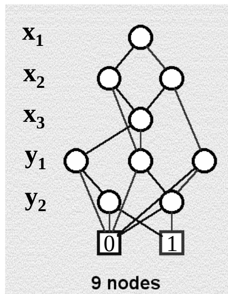


Reducing Relations to Functions

- Boolean relation over variables $(x_1,x_2,\ldots,x_n)$ and $(y_1,y_2,\ldots,y_m)$ can be represented as a boolean function, which is 1 for a given minterm iff this minterm represents *related* assignments of variables $(x_1,x_2,\ldots,x_n)$ and $(y_1,y_2,\ldots,y_m)$.

Example (continued)

x_1	x_2	x_3	y_1	y_2	F
0	0	0	0	0	1
0	0	1	0	1	1
0	1	0	0	1	1
0	1	1	0	1	1
1	0	0	0	0	1
1	0	1	0	1	1
1	1	0	1	1	1
1	1	1	1	1	1
other					0



FSM Transition Relation

- FSM is { I, O, S, δ, λ). Suppose r is the number of inputs I, m is the number of states S, and n is the number of outputs O; $\delta_k(i,s)$ and $\lambda_k(i,s)$ are vectors of next-state and output functions
- Transition relation is a boolean function
  $T: \{0,1\}^r \times \{0,1\}^m \times \{0,1\}^m \rightarrow \{0,1\}$
  such that T(i, s, n) = 1 iff state n can be reached in exactly one transition from state s when input i is applied

FSM Output Relation

- Output relation is a boolean function
  $O: \{0,1\}^r \times \{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}$
  such that O(i, x, o) = 1 iff output o can be produced when the FSM is in state x and input i is applied

Deriving Transition and Output Relations from NS/Output Functions

- If the FSM is given as { I, O, S, δ, λ), where $\delta_k(i,s)$ and $\lambda_k(i,s)$ are vectors of next-state and output functions, it is possible to compute the transition and output relations as follows:

  $T(i,s,n) = \Pi_k (n_k = \delta_k(i,s));$

  $O(i,s,o) = \Pi_k (o_k = \lambda_k(i,s))$
- Given the transition and output relations, it is possible to derive the next state and output functions

  $\delta_k(i,s) = \exists n_x (T(i,s,n) \,\&\, n_k), x \neq k$

Reachability Analysis for FSMs

- Reachability analysis is the use of image computation to derive the set of all reachable states by traversing the STG of the FSM, starting from the set of initial(reset) states
- The set of reachable states can be used:
  - to simplify the initial transition and output relations
  - to re-encode the FSM
  - to check whether a property is true for these states
    - in equivalence checking
    - in symbolic model checking

Computing Reachable State Set

```
Reached = ResetStates;
do {
        ReachedBefore = Reached;
        Reached += Image(Reached);
}
while (ReachedBefore != Reached);
```

(the state sets in this procedure are given by characteristic functions represented using BDDs)

Simplifying Transition and Output Relations Using Reachable State Set

- Suppose R(X) is the reachable state set, then the transition and output relations can be rewritten

T'(i,s,n) = T(i,s,n) & R(s) & R(n)
O'(i,s,o) = O(i,s,o) & R(s)

Definition of FSM Equivalence

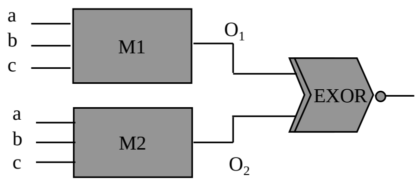
- Definition. State machines are equivalent, if starting from the reset states, for any sequence of input vectors, they respond by producing the same sequences of output vectors

Equivalence Checking

- Construct the transition relation of machines M_1 and M_2
- Find the product machine transition relation P
- Perform state traversal of the product machine, while checking its output
- If the output of the product machine is 1 for all reachable states, the machines M_1 and M_2 are equivalent
- It is possible to define equivalence relative to any *subset* of inputs and outputs of the FSM

Product Machine

- Given FSM { I, O, S, δ, λ},
  the product machine is { I, {0,1}, SxS, δ^2, λ^2}
  (r inputs, 2m states, 1 output)



Equivalence Checking Formulas

- Machines M1 and M2 are equivalent iff
  $\forall_{i,\,x,\,y}$ [A_R(x,y) => O(i,x,y)] = 1
  where A_R(x,y) is the characteristic function of the set of reachable states of product machine and O(i,x,y) is the output relation of product machine
- Alternatively, machines M1 and M2 are not equivalent iff
  $\exists_{i,\,x,\,y}$ [A_R(x,y) & O'(i,x,y)] = 0