Model checking with edge-valued decision diagrams

Pierre Roux[1] **Radu I. Siminiceanu**[2]

NASA Formal Methods Symposium

April 15, 2010

ÉNS Lyon, France (pierre.roux@ens-lyon.org)

NIA (radu@nianet.org)

1. Decision Diagrams
2. EVMDDs
3. Implementation

The State of Symbolic Model Checking

Evolution and Impact of Decision Diagrams

- Early 90s : the wow factor, BDDs are (re)discovered
- Late 90s - early 2000s : real progress
  - Extensions, generalizations (MTBDDs, BMDs, EVMDDs, etc)
  - New algorithms (saturation, bounded MC, CEGAR)
- Since then ...
  - Interest has shifted to other areas of verification
  - There are even rumors out there that symbolic MC has enetered a Brezhnev era ($\sim$ stagnation)
  - Fact or fiction ?

Purpose of this work

Stagnation: fact or fiction?

- A little bit of both
- New ideas exist, but are disparate
- Example of untapped resources:
  - Edge-valued decision diagrams (EVMDD)
  - Identity-reduced decision diagrams
  - Hashing, caching, garbage collection
  - Heuristics for SAT/SMT solving

Our goal

Represent in one formalism (some of) the best techniques available at the moment across a spectrum of existing tools

Encoding of functions

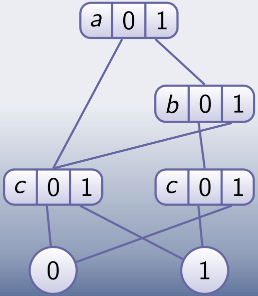
The advent of symbolic MC: **compact** representation of

- boolean functions $f : \{0,1\}^n \to \{0,1\}$
- sets $\left\{x \in \{0,1\}^n \mid f(x) = 1\right\}$

Evolution:

- Truth table: 2^n **entries**
- Binary Decision Diagram (BDD): merge common subtrees
  still exponential size in worst case, often better in practice

a	b	c	$f(a,b,c)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1



Integer/arithmetic functions

- $f : \{0,1\}^n \to \mathbb{Z}$
- Extend BDD to **Multi-Terminal BDD (MTBDD)**

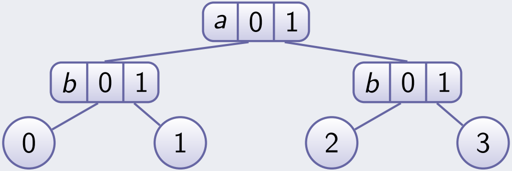


Figure: $f : (a,b) \mapsto 2a + b$

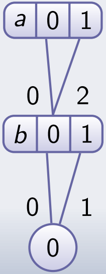
- Inefficient if $\mathrm{Img}(f)$ is large: less chances to share subtrees

Other forms of DDs:

- Multiway DDs (MDD): $f : \{0,\dots,k_1\} \times \cdots \times \{0,\dots,k_n\} \to \{0,1\}$
- Binary Moment Diagrams (BMD):
  $\to$ work well for multipliers, but not much else

Edge Valued MDDs (EVMDDs)

- EVBDDs introduced in 1992, but not sufficiently exploited
  ⇒ (*Reed-Müller spectrum !?!*)
- From MTBDDs to EVMDDs:
  merge all terminals (0) and assign (integer) values to edges



- Value of f: composition of edge-values (e.g. addition, $+$) along the path from root to terminal node

EVMDD characteristics

- EVMDD encoding cannot have more nodes than MTBDDs
  $\Rightarrow$ proved in this paper
- Size can be linear instead of exponential (e.g. linear functions)
- Composition $\Rightarrow$ a generic algorithm for all binary operators:
  for f, g encoded by EVMDDs of size $|f|$ and $|g|$
  $f * g$ computed in $\mathrm{O}\left(|f|\,|g|\,|\mathrm{Img}(f)|\,|\mathrm{Img}(g)|\right)$
- This algorithm has **exactly the same complexity**
  as its equivalent for MTBDDs, hence
  no gain in (worst-case) time complexity
- Is there room for improvement ?

EVMDD algorithms

Yes, for following operations:

- Addition:
  $f + g$ computed in $\mathrm{O}\left(|f| \cdot |g|\right)$
- Multiplication by constant:
  $f \times c$ computed in $\mathrm{O}(|f|)$
- Multiplication:
  $f \times g$ computed in $\mathrm{O}\left(|f|^2 \cdot |g|^2 \cdot |f \times g|\right)$
  - exponential in worst case
  - much better in many "practical" cases
- Remainder and Euclidean division by constant:
  f/c and $f\%c$ computed in $\mathrm{O}(c \cdot |f|)$

An EVMDD-based Model Checker

We have developed an EVMDD library featuring:

- EVMDDs for arithmetic expressions
- (Regular) MDDs for boolean expressions
- Identity-reduced encoding of transition relations
- Saturation-based state space construction
- Unsophisticated (i.e. fast) garbage collector (mark & sweep)

Some stats:

- 7 kLOC of ANSI C : library
- 4 kLOC : model checking front-end

Available at `http://research.nianet.org/~radu/evmdd/`

Results

Building state space vs CUDD (BFS) and SMART (saturation)

Model	Model size	Reachable states	CUDD (sec)	SMART (sec)	EVMDD (sec)
Dining philosophers	100	4×10^{62}	11.42	1.49	0.03
	200	2×10^{125}	3054.69	3.03	0.07
	15000	2×10^{9404}	—	—	195.29
Round robin mutual exclusion protocol	40	9×10^{13}	4.44	0.44	0.08
	100	2×10^{32}	—	2.84	1.17
	200	7×10^{62}	—	20.02	9.14
Slotted ring protocol	10	8×10^{9}	1.16	0.19	0.01
	20	2×10^{20}	—	0.71	0.04
	200	8×10^{211}	—	412.27	25.97

On Intel Core 2, 1.2GHz, 1.5GB mem ("—" means "$>$ 1h").

Results

Building state space vs CUDD (BFS) and SMART (saturation)

Model	Model size	Reachable states	CUDD (sec)	SMART (sec)	EVMDD (sec)
Kanban assembly line	15	4×10^{10}	80.43	3.41	0.01
	20	8×10^{11}	2071.58	8.23	0.02
	400	6×10^{25}	—	—	74.89
Knights problem	5	6×10^{7}	1024.42	5.29	0.27
	7	1×10^{15}	—	167.41	3.46
	9	8×10^{24}	—	—	32.20
Randomized leader election protocol	6	2×10^{6}	4.22	8.42	0.86
	9	5×10^{9}	—	954.81	18.89
	11	9×10^{11}	—	—	109.25

On Intel Core 2, 1.2GHz, 1.5GB mem ("—" means "$>$ 1h").

Questions

?