Extended Resolution Proofs for Symbolic SAT Solving

Toni Jussila, Carsten Sinz, and Armin Biere
Johannes Kepler University Linz, Austria

Why Propositional Logic Proofs?

- SAT-solvers and BDDs commercially employed
  - Hardware verification (Bounded Model Checking)
  - Product configuration

- Yes/No answer of solvers not sufficient
  - Counterexample or proof needed
  - Used for abstraction refinement, interpolant computation, proof checking, diagnosis, ...

Symbolic SAT-Solving

- Given: $F = C_1 \wedge \ldots \wedge C_n$, a formula in CNF
- Method: Build a BDD B for F by `BDD-and` and `BDD-exists` operations as follows:
  - take a variable ordering
  - put all clauses C_i to buckets (one bucket for each variable)
  - process buckets (variables) one by one
    - build conjunction of clauses (`BDD-and`)
    - eliminate variable by existential quantification (`BDD-exists`)
    - put resulting BDD to the right bucket

Symbolic SAT Solving (II)

- Fact: B=0 *iff* F unsatisfiable
- Question: How to build refutation proof for F if B=0?
- Solution: Use Extended Resolution as proof system.

Extended Resolution (ER)

- Resolution calculus: one inference rule

$$\frac{C \dot{\cup} \{l\} \quad \{\bar{l}\} \dot{\cup} D}{C \cup D}$$

C,*D*: clauses
l: literal occurring positively in *C* and negatively in *D*

- Extended Resolution: adds extension rule
  - Introduces new variable and clauses.
  - „Definitions“

$$\frac{}{\mathrm{CNF}(x \leftrightarrow F)}$$

x: new variable (neither occurring in *F* nor in current clause set)
F: arbitrary formula

- Goal: derive empty clause [Tseitin, 1970]

What Definitions?

- Add a new variable for *every* BDD node that occurs in the computation.
- *For BDD node f, definition is*
  - $f \leftrightarrow (x \,?\, f_1 : f_0)$
  - *where f_1 and f_0 are the children of f.*
  - as formula: $(x \rightarrow f_1) \wedge (\neg x \rightarrow f_0)$
  - *as clauses:* $(\neg f \;\; \neg x \;\; f_1)$, $(\neg f \;\; x \;\; f_0)$,
    $(f \;\; \neg x \;\; \neg f_1)$, $(f \;\; x \;\; \neg f_0)$

ER Proof Generation Outline (for unsatisfiable $F = C_1 \wedge \ldots \wedge C_n$)

1. Take first bucket U.
2. Compute BDDs B_i for all clauses C_i *in* U.
3. Add definitions for all BDD nodes occurring in any B_i.
   (convention: let b_i be ER variable of the top node of B_i)
4. Produce ER proofs $F \vdash b_i$ for all clauses in U.
5. Compute the BDD of the conjunction of the clauses of U. H_2=`BDD-and`(B_1, B_2) H_i=`BDD-and`(B_i, H_{i-1})
6. Produce ER proofs $F \vdash h_i$ for all h_i.

ER Proof Generation Outline (II)

7. Eliminate root variable, ie. compute BDD
   $H_i' = \texttt{BDD-exists}(H_i)$.
8. Produce ER proofs $F \vdash h_i'$ for all h_i'.
9. Let $U = next\_bucket()$ and go to 2.

ER Proofs from BDDs: Conjunctions (`BDD-and`)

- Build proof of $f \wedge g \rightarrow h$ recursively
  - from $f_0 \wedge g_0 \rightarrow h_0$ and $f_1 \wedge g_1 \rightarrow h_1$.

$$
\dfrac{
  \dfrac{(h x \bar{h}_0) \quad \dfrac{(\bar{g} x g_0) \quad \dfrac{(\bar{f} x f_0) \quad \dfrac{\vdots}{(\bar{f}_0 \bar{g}_0 h_0)}}{(\bar{f} x \bar{g}_0 h_0)}}{(\bar{f}\bar{g} x h_0)}}{(\bar{f}\bar{g} h x)}
  \qquad
  \dfrac{\dfrac{\dfrac{\dfrac{\vdots}{(\bar{f}_1 \bar{g}_1 h_1)} \quad (\bar{f} \bar{x} f_1)}{(\bar{f} \bar{x} \bar{g}_1 h_1)} \quad (\bar{g} \bar{x} g_1)}{(\bar{f}\bar{g}\bar{x} h_1)} \quad (h \bar{x} \bar{h}_1)}{(\bar{f}\bar{g} h \bar{x})}
}{(\bar{f}\bar{g}h)}
$$

Complexity: Requires 7 resolutions for each recursive step.

ER Proofs from BDDs: Quantification (`BDD-exists`)

- Given f (children f_0 and f_1), let $\exists f$ be the BDD where root variable of f existentially quantified.
- First prove $f_0 \vee f_1 \rightarrow \exists f$, *clauses* $(\neg f_0\ \exists f),(\neg f_1\ \exists f)$.
- *Then prove* $f \rightarrow \exists f$, *ie.* $(\neg f\ \exists f)$.

$$\dfrac{\dfrac{(\bar{f} x f_0) \quad (\bar{f}_0 \exists f)}{(\bar{f} x \exists f)} \qquad \dfrac{(\bar{f}_1 \exists f) \quad (\bar{f} \bar{x} f_1)}{(\bar{f} \bar{x} \exists f)}}{(\bar{f} \exists f)}$$

Implementation: `EBDDRES`

- Performs BDD computations.
- Generates extended resolution proofs fully automatically.
- Good performance on some SAT instances that are hard for DPLL/resolution-based provers (e.g. pigeon hole).
- Proof-checker for resolution-based solvers can easily be adapted for ER proofs.
  - Only non-cyclicity test for extension rule applications has to be added.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	MINISAT			EBDDRES							EBDDRES, quantification						
	solve resources		trace size	solve resources		trace				bdd nodes	solve resources		trace				bdd nodes
						gen	ASCII	bin	chk				gen	ASCII	bin	chk	
	sec	MB	MB	sec	MB	sec	MB	MB	sec	$\times 10^3$	sec	MB	sec	MB	MB	sec	$\times 10^3$
ph7	0	0	0	0	0	0	1	0	0	3	0	5	0	12	4	1	60
ph8	0	4	1	0	0	0	3	1	0	15	1	14	1	49	15	4	236
ph9	6	4	11	0	0	0	3	1	0	8	6	52	4	186	59	14	864
ph10	44	4	63	1	17	1	30	10	2	136	20	214	16	683	*	*	2974
ph11	884	6	929	1	13	1	21	8	2	35	-	*	-	-	-	-	-
ph12	*	-	-	2	22	1	33	12	3	31	-	*	-	-	-	-	-
ph13	*	-	-	10	126	7	260	92	20	850	-	*	-	-	-	-	-
ph14	*	-	-	9	111	7	204	74	18	166	-	*	-	-	-	-	-
mutcb8	0	0	0	0	0	0	2	1	0	10	0	0	0	3	1	0	16
mutcb9	0	4	0	0	5	0	5	2	0	27	0	4	0	6	2	0	35
mutcb10	0	4	1	0	8	0	11	4	1	58	0	5	0	11	4	1	59
mutcb11	1	4	4	1	17	1	31	10	2	153	1	8	1	23	7	2	123
mutcb12	8	4	22	2	32	2	69	22	5	320	1	13	1	38	12	3	198
mutcb13	112	5	244	7	126	5	181	61	13	817	2	24	2	70	22	5	347
mutcb14	488	8	972	14	250	10	393	132	27	1694	4	37	3	127	40	8	621
mutcb15	*	-	-	36	498	26	1009	*	*	4191	6	52	5	211	67	14	1012
mutcb16	*	-	-	-	*	-	-	-	-	-	12	104	9	391	126	26	1821
urq35	95	4	218	2	22	1	37	13	3	24	0	0	0	1	0	0	5
urq45	*	-	-	-	*	-	-	-	-	-	0	0	0	1	0	0	10
urq55	*	-	-	-	*	-	-	-	-	-	0	0	0	2	1	0	15
urq65	*	-	-	-	*	-	-	-	-	-	0	4	0	6	2	0	34
urq75	*	-	-	-	*	-	-	-	-	-	0	4	0	7	2	0	39
urq85	*	-	-	-	*	-	-	-	-	-	0	5	0	10	3	1	59
fpga108	0	2		6	47	4	135	47	11	186	8	92	6	239	77	18	1088
fpga109	0	0		3	44	2	70	24	6	83	10	114	8	323	105	9	1434
fpga1211	0	0		53	874	37	1214	*	*	1312	-	*	-	-	-	-	-
add16	0	0	0	0	4	0	6	2	0	30	0	3	0	4	2	0	26
add32	0	0	0	1	9	1	24	8	2	122	1	7	0	19	6	1	106
add64	0	0	0	12	146	9	338	112	23	1393	12	95	9	393	127	26	1839
add128	0	4	0	-	*	-	-	-	-	-	-	*	-	-	-	-	-

Summary

- Extends work of Biere & Sinz 2006 with existential quantification.
- Extended resolution proofs as generic proof format.
- Enabler for further applications of extended resolution.