SAT-Based Model Checking Without Unrolling

Aaron R. Bradley

Dept. of Electrical, Computer & Energy Engineering

University of Colorado, Boulder

Public History of Idea

- k-Step Relative Inductive Generalization (arXiv:1003.3649, March 2010)
- Competed in HWMCC'10:

	Solver	unsat	sat	solved
1	ABC (super)	412	320	732
2	PDTrav	423	308	731
3	IC3	405	308	713
4	ABC (d)	403	303	706
5 (uns)	tiplnd	373	281	654
5 (sol)	tipind	365	324	689

It is probably fair to say that IC3 is **better than any single engine** [based on sequential synthesis, induction, interpolation, BDD-based reachability, etc.] used within [ABC and PDTrav at HWMCC'10].

– Brayton, Een, and Mishchenko

"Continued Relevance of Bit-Level Verification Research"

November 2010

Multi-Engine?

Introducing IImc.

- Joint work with Fabio Somenzi and students:
  Arlen Cox, Dan Dunbar, Zyad Hassan, Yan Zhang
- So far, little communication among engines:

  IC3 + CUDD-based reachability + naive BMC
- Much to do, but **not difficult to surpass results of HWMCC'10**.

Induction

Foundation of verification for 40+ years (Floyd, Hoare)

To prove that $S : (I, T)$ has safety property P, prove:

- Base case:

$$I \Rightarrow P$$

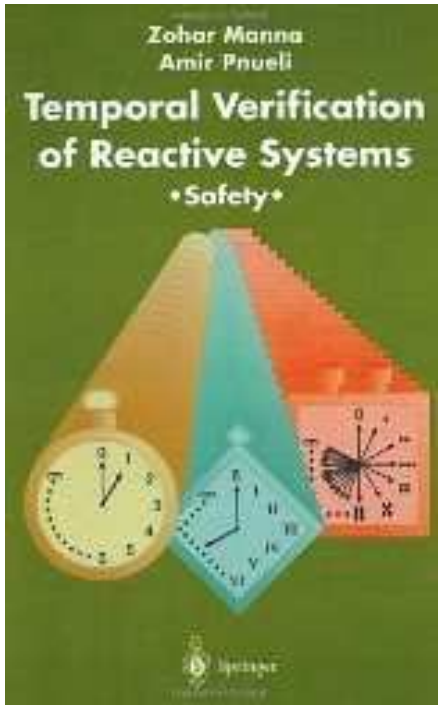
- Inductive case:

$$P \wedge T \Rightarrow P'$$

When Induction Fails

We present two solutions. . .

1. Use a stronger assertion, or
2. Construct an incremental proof, using previously established invariants.



– Manna and Pnueli

Temporal Verification of Reactive Systems: Safety

1995

Solution 1: Use a Stronger Assertion

Monolithic

- BDD/SAT-based reachability
  exact computation of strongest/weakest strengthening
- k-induction
  unroll to strengthen
- interpolation-based model checking
  property-focused abstract post-condition
- . . .

Solution 2: Incremental Proof

An alternate strategy is to identify an inductive assertion φ_1, such that φ_2 is inductive relative to φ_1 ...

We strongly recommend its use whenever applicable. Its main advantage is that of **modularity**.

– Manna and Pnueli

Temporal Verification of Reactive Systems: Safety

1995

Solution 2: Incremental Proof

An alternate strategy is to identify an inductive assertion φ_1, such that φ_2 is inductive relative to φ_1 ...

First prove φ_1:

- $I \Rightarrow \varphi_1$
- $\varphi_1 \wedge T \Rightarrow \varphi_1'$

Then prove φ_2 relative to φ_1:

- $I \Rightarrow \varphi_2$
- $\varphi_1 \wedge \varphi_2 \wedge T \Rightarrow \varphi_2'$

Good for humans. Good for computers?

Incremental Proof: Attempt #1

Incrementally construct $\varphi_1, \varphi_2, \ldots$ so that

- $I \Rightarrow \varphi_i$
- $\bigwedge_{j=1}^{i} \varphi_j \wedge P \wedge T \Rightarrow \varphi_i'$

until for some K

- $\bigwedge_{i=1}^{K} \varphi_i \wedge P \wedge T \Rightarrow P'$

Checking Safety by Inductive Generalization of Counterexamples to Induction
FMCAD, November 2007

Incremental Proof: Attempt #1

Counterexample to induction: State s for which

$$\bigwedge_{i=1}^{k} \varphi_i \wedge P \wedge T \Rightarrow P' \quad \text{fails.}$$

If possible (incremental proof)

- Find (small) relatively inductive subclause $c \subseteq \neg s$.
- $\varphi_{k+1} := c$

If none exists (fallback)

- Assume $\neg s$ and continue.
- $P := P \wedge \neg s$

Relatively Inductive Subclause

$c \subseteq \neg s$

- Base case:

$$I \Rightarrow c$$

- Inductive case:

$$\bigwedge_{i=1}^{k} \varphi_i \wedge P \wedge c \wedge T \Rightarrow c'$$

Problem

There are cases in which the conjunction $\varphi_1 \wedge \varphi_2$ is inductive, but it is not the case that φ_1 is inductive and φ_2 is inductive relative to φ_1.

– Manna and Pnueli

Temporal Verification of Reactive Systems: Safety

1995

New Approach

Stepwise-Relative
Incremental
Inductive
Strengthening

If I can't prove incrementally that s is unreachable, I can at least **prove that it is unreachable for some number of steps** and then **push forward from there**.

Main Idea

Given:

- Over-approximations of stepwise reachability:

$$I, F_1, F_2, \ldots, F_k$$

  Approximate "onion skins":

  - $F_i \Rightarrow F_{i+1}$
  - $F_i \wedge T \Rightarrow F'_{i+1}$

- Counterexample to stepwise-relative induction s:

$$F_i \wedge P \wedge T \Rightarrow P'$$

Main Idea

Find: weakest stepwise assumption (maximum i) s.t.

$$\exists c \subseteq \neg s \quad \text{s.t.} \quad F_i \wedge P \wedge c \wedge T \Rightarrow c'$$

- **Guaranteed to exist.**
- Prefer small (ideally minimal) clause c.
- Proof that s is unreachable for $i+1$ steps.

Main Idea

Push forward from there:

- Strengthens stepwise knowledge up to step $i+1$:

$$F_j := F_j \wedge c \quad \text{for} \quad j \in \{1, \ldots, i+1\}$$

- Now recur on the property $\neg s$ (at step $i+1$).

Completeness and performance are in the details.

Elements of “Monolithic” Approach

Approximate “onion skins”: interpolation-based MC.

Differences:

- Continual refinement at all steps.
- No unrolling.
- Abstraction (generalization) power from induction.
  - Discovers semantic similarities among states rather than similarities based on (transitive) adjacency.
  - “Strong” induction yields stronger clauses than “weak” induction (prime implicate finding).

Elements of Incremental Approach

Construct:

stepwise

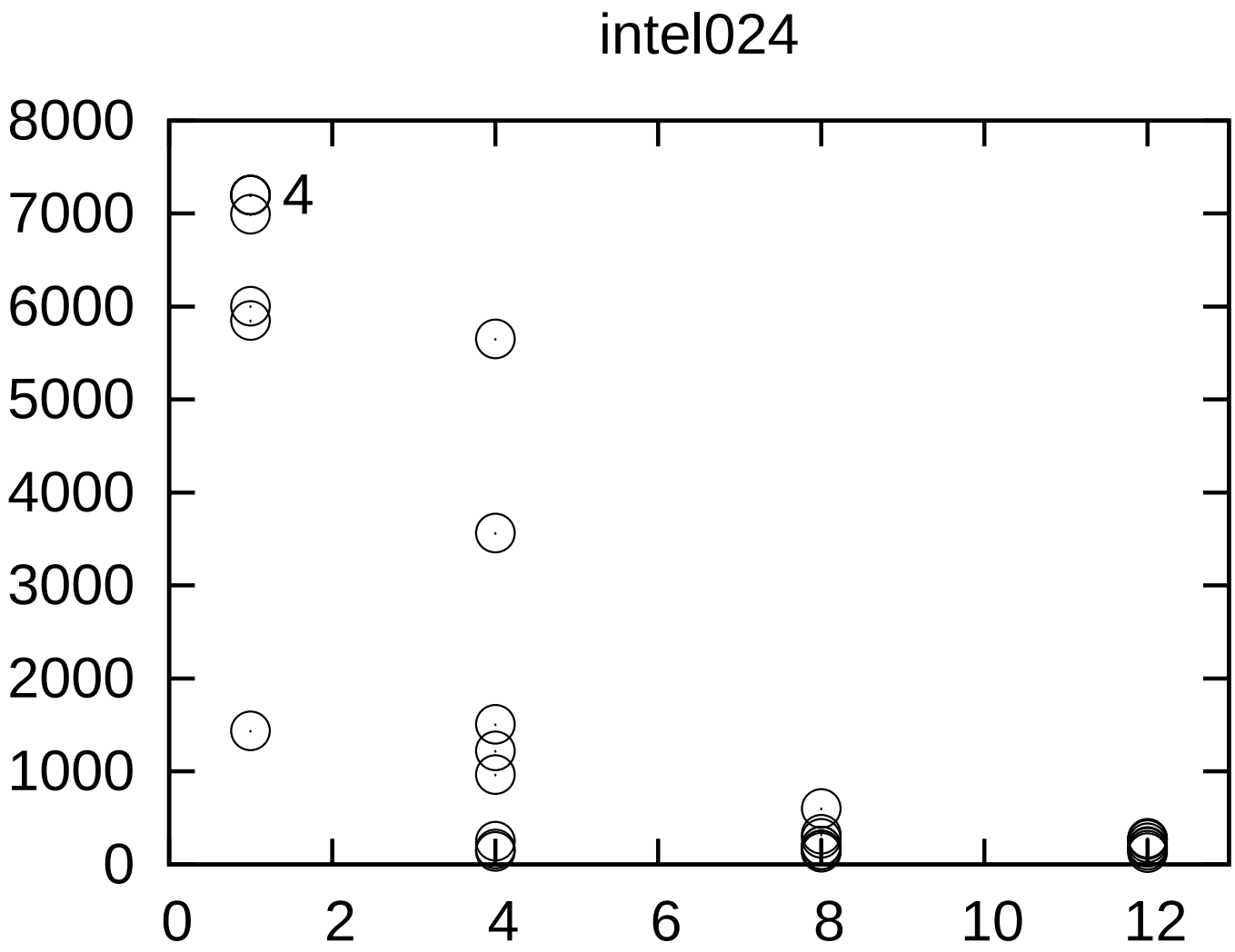
sequence of $\wedge$ relatively inductive assertions

Why is Incremental Good?

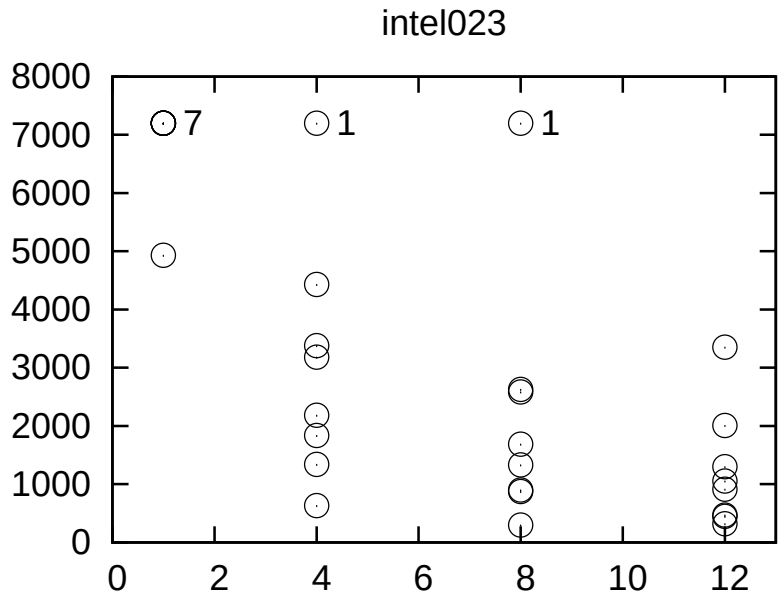
Modularity!

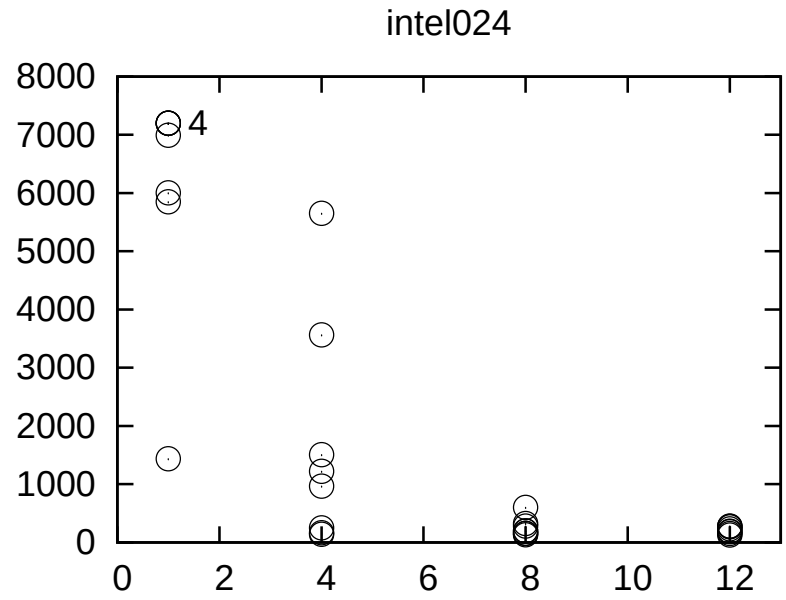
1. Low reasoning power.
   1000s of SAT problems solved per second.
2. On-the-fly abstraction.
3. Easy to implement for parallel computation.

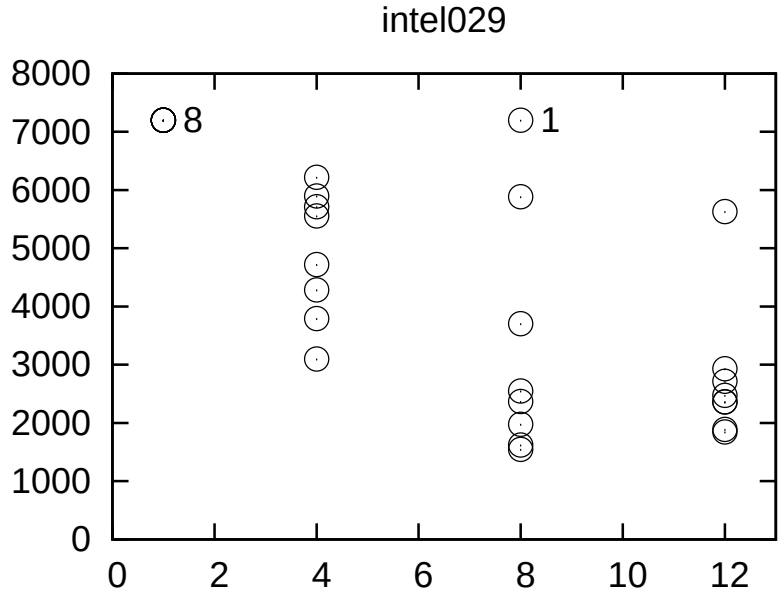
Parallel Implementation

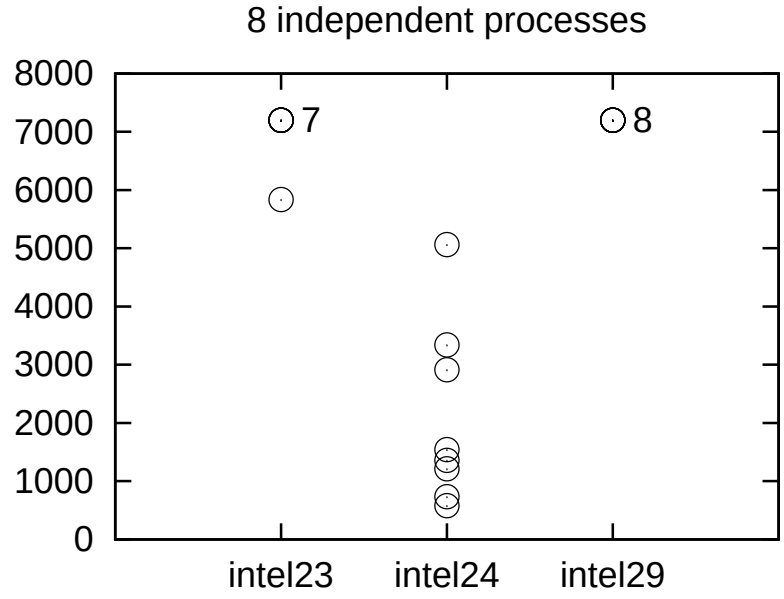


Parallel Implementation









Conclusion

Stepwise-relative
incremental
inductive
strengthening

A bridge between **monolithic** and **incremental** approaches.

Conclusion

Stepwise-relative
incremental
inductive
strengthening

. . . [a] paradigm for discovering new proof methods or improving the old ones.

– Brayton, Een, and Mishchenko
"Continued Relevance of Bit-Level Verification Research"
November 2010