Abstraction based Theorem Proving:

An Example from the Theory of Reals

Ashish Tiwari

Tiwari@csl.sri.com

Computer Science Laboratory

SRI International

Menlo Park CA 94025

`http://www.csl.sri.com/~tiwari`

Outline

1. Abstraction
2. A sound, but incomplete, decision procedure for the theory of reals
3. Experimental Results
4. Conclusion

Abstract Interpretation

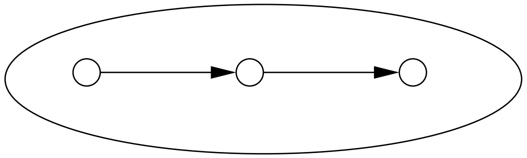
Problem:	Given a system S;
	Given a safety property ϕ;
	prove that ϕ is true in S
Insight:	Full, exact S may not be relevant for ϕ
Solution:	Construct an abstraction S_a of S;
	S_a has more behaviors than S;
	If $S_a \models \phi_a$, then $S \models \phi$
Observation:	There are many possible abstractions S_a of S
Issue:	finding the right abstraction

Theorem Proving

Problem:	Given a theory Th;
	Given a formula ϕ;
	decide if ϕ is valid in Th
Insight:	Full, exact Th may not be relevant
Solution:	Abstract the theory into a simpler theory Th_a
	Th_a has more satisfiable formulas than Th
	If $Th_a \models \phi_a$, then $Th \models \phi$
Observation:	There are many possible abstractions Th_a of Th
Issue:	finding the right abstraction

The correspondence

S_a



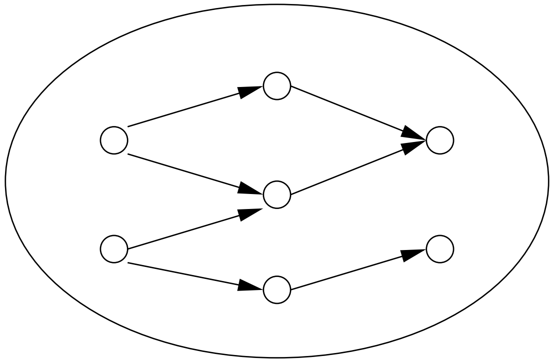
Th_a

DP for Th_a

beh(S_a) \supseteq beh(S)

Satis(T_a) \supseteq Satis(Th)

S



Th

DP for Th

sound, incomplete

Any set of sound and terminating inference rules for Th is a decision procedure for some abstraction theory Th_a

Current Trends

SAT + decision procedures: Abstract the theory to propositional logic

- CVC [Barrett, Stump, Dill: CAV 2002]
- Math-SAT [Audemard et. al. CADE 2002]
- ICS [deMoura, Ruess: SAT 2002]
- Touchstone prover [Necula: CADE 2000]
- UCLID [Bryant et. al.]

Constructing the abstraction mapping: Lazily or eagerly

More Examples...

Abstract the theory to a decidable fragment

- NO Combination Procedure [Nelson, Oppen: 1979]:
  Each component decision procedure deals with an abstraction of the union theory;
- Instantiation-based theorem proving [Ganzinger, Korovin: LICS 2003]:
  Abstract to a quantifier-free fragment
- Interactive theorem provers as PVS [Owre, Shankar: ??]:
  Create instantiations until formula decidable (grind)
- Others....

Constructing the abstraction mapping: variable abstraction, unification, or manual

This talk

Abstract even when the theory Th is decidable

Especially if

- the decision problem has a poor time and space complexity
- in practice, the decision procedure takes too much time, making it unsuitable for applications
- simpler efficiently decidable fragments exist

Argue by example: Sound, but incomplete, dec. proc. for the QF theory of reals

FO Theory of $\mathbb{R}$

Language	$\{0, 1, \mathbb{Q}, +, -, ., <, =\}$
Term	E.g. $2x + 3xy - 1$
Atomic Formula	$2x + 3xy - 1 < 0$
FO Formula	Application of boolean operators $\{\vee, \wedge, \neg\}$ and quantifiers $\{\exists, \forall\}$.

Formulas in the theory $\mathbb{R}$ containing free variables $x_1, \ldots, x_n$ denote a semialgebraic subset of $\mathbb{R}^n$.

Known Facts

- Full FO theory of $\mathbb{R}$ is decidable [Tarski48]
- Admits quantifier elimination
- "Efficient" algorithm based on cylindrical algebraic decomposition (CAD)
- The theory of linear real arithmetic is more efficiently decidable
- Quantifier-free linear formulas can be decided in polynomial time

QEPCAD Decision Procedure

- CAD: Decomposing the real space $\mathbb{R}^n$ into finite partitions which are sign-invariant for a set P of polynomials in $\mathbb{R}[x_1, \ldots, x_n]$
  Example: $x^2 - 4$ creates partitions $x < -2, x = -2, -2 \leq x < 2, x = 2$, and $2 < x$.
- QE: Get all polynomials in the formula ϕ, create the CAD decomposition, and evaluate formula on sample points.

The QEPCAD implementation is done over the SACLIB package.

Complexity: $n^{2^{O(n)}}$

Not a logical decision procedure, FAILs frequently, too slow for applications

Application

- HybridAbstraction: Constructing finite-state discrete abstractions of hybrid systems
- Uses the decision procedure for the reals in a “failure-tolerant” mode
- Require speed, soundness, but can compromise completeness
- Only for the quantifier-free theory of reals

Example: Is the following satisfiable

$$x2 = 0 \ \wedge \ -x1 * x2 - x1 * x3 > 0 \ \wedge \ x2 > 0$$

Terms

- Terms in this theory can be represented in a canonical form: polynomials
- Normalization can be described by a ground convergent (modulo AC) TRS
- Additionally, a polynomial $c_0 s_0 + c_1 s_1 + \cdots + c_k s_k$ is written s.t. $s_0 \succ s_1 \succ \cdots s_k$ in some "nice" ordering $\succ$ on power-products

Incomplete decision procedure for QF Theory of $\mathbb{R}$

Input: Conjunction of atomic formulas ϕ

Problem: Decide satisfiability of existential closure of ϕ

Approach:

- Separate atomic formulas into equations and (strict) inequalities: E, R, S
- Superposition on the equational part E: Gröbner basis
- Ordered chaining on the R, S components
- Interaction between E and R, S via paramodulation and additional ordered chaining
- Redundancy + Symbolic lower-upper bound computations

Superposition Inference Rules

$$\frac{(E' = E \cup \{c_0 s_0 + p = 0,\ d_0 t_0 + q = 0\}, R, S)}{(E' \cup \{c_0 t_0' q - d_0 s_0' p = 0\}, R, S)}$$

if $t_0' t_0 = s_0' s_0 = lcm(s_0, t_0) \neq s_0 t_0$

Example:

$$\frac{\frac{\frac{(E = \{x_1^2 x_2 = 0,\ x_1 x_2 = 1\}, R = \emptyset, S = \emptyset)}{(E' = E \cup \{x_1 = 0\}, \emptyset, \emptyset)}}{(E' \cup \{1 = 0\}, \emptyset, \emptyset)}}{\perp}$$

Preferentially simplify: Deduction $\Rightarrow$ Simplification

Ordered chaining

$$\frac{(E, R' = R \cup \{p > 0,\ q_1 > 0,\ \ldots,\ q_k > 0\}, S)}{(E, R' \cup \{p + |\frac{c}{d}| q_1 \cdots q_k > 0\}, S)}$$

if $LPP(p) = LPP(q_1) \cdots LPP(q_k)$, $LC(p) = c$, $d = LC(q_1) \cdots LC(q_k)$, and $cd < 0$.

Example.

$$\frac{\frac{\frac{\frac{(E = \emptyset, R = \{-x_1 x_2 + 5 > 0,\ x_1 - 2 > 0,\ x_2 - 4 > 0\}, S = \emptyset)}{(\emptyset, R' = R \cup \{-4x_1 - 2x_2 + 3 > 0\}, \emptyset)}}{(\emptyset, R'' = R' \cup \{-2x_2 + 5 > 0\}, \emptyset)}}{(\emptyset, R'' \cup \{-13 > 0\}, \emptyset)}}{\perp}$$

Ordered chaining: Notes

- k-chaining: Chaining using products of upto k polynomials
- Linear case: $k = 1$ sufficient for linear formulas;
  Mimics the Fourier-Motzkin decision procedure
- Nonlinear: Saturation for $k \leq 3$
  $k = 1$ tried preferentially over higher values
- Chaining inference result is a smaller polynomial
- Nonterminating

Iterative Root-Finding Numerical Algorithms

An example of nontermination:

$$\frac{\dfrac{\dfrac{\dfrac{(E = \emptyset, R = \{-x^2 + 4x - 4 > 0,\ x > 0\}, S = \emptyset)}{(\emptyset, R' = R \cup \{x - 1 > 0\}, \emptyset)}}{(\emptyset, R'' = R' \cup \{x - 3/2 > 0\}, \emptyset)}}{(\emptyset, R'' \cup \{x - 7/4 > 0\}, \emptyset)}}{\vdots}$$

Symbolic Lower- and Upper-Bounds

If numerical lower and upper bounds of certain variables are known, then symbolic lower and upper bounds of polynomial expressions can be computed, which would have a lower degree than the original polynomial.

$$\frac{(E, R \cup \{p + c\mu\nu > 0\}, S)}{(E, R \cup \{p + c\mu\nu > 0, p + cd\nu > 0\}, S)}$$

if $c > 0, (R \cup S) \models \nu > 0, \mu < d$

$(R \cup S) \models \mu < d$ is done using interval arithmetic

Inconsistency

$$\frac{(E \cup \{c_0 \approx 0\}, R, S)}{\bot} \quad \texttt{if}\, c_0 \neq 0$$

$$\frac{(E, R \cup \{c_0 > 0\}, S)}{\bot} \quad \texttt{if}\, c_0 \leq 0$$

$$\frac{(E, R, S \cup \{c_0 \geq 0\})}{\bot} \quad \texttt{if}\, c_0 < 0$$

Redundancy

Notion of redundancy for an incomplete algorithm is redundant!

A rule $q > 0$ is redundant in the state

$$
\begin{aligned}
(E &= \{p_i \approx 0 : i = 1, 2, \ldots\}, \\
R &= \{q_j > 0 : j = 1, 2, \ldots\}, \\
S &= \{r_k \geq 0 : k = 1, 2, \ldots\})
\end{aligned}
$$

if
(i) $q \rightarrow_E^* q'$ and
(ii) $q' = \Sigma_j c_j q_j + \Sigma_k d_k r_k + e$ for some nonnegative constants c_j's and d_k's, and positive constant e.

Restricted application: Consider upto 2 polynomials in summation

Experimental Results

	#variables	degree	status	QEPCAD	DP
Test1	4	2	satisfiable	30	1
Test2	7	3	inconsistent	20	1
Test3	6	3	inconsistent	4240	2
Test4	7	3	inconsistent	FAIL	5
Test5	7	3	inconsistent	FAIL	5

Table 1: Total running time averages (in milliseconds) for Tests1–5.

Conclusion

- Logical, incremental decision procedure for some abstraction of the theory of reals:
  sound, but incomplete for reals
- Decision procedure produces witnesses
- Completely motivated by the requirements of the HybridAbstractor
- "Abstract and Prove" – over undecidable and *decidable theories*