Combined Decision Techniques for the Existential Theory of the Reals

G. O. Passmore, P. B. Jackson

November 26, 2010

Last week...

quantifier elimination for $\mathbb{R}$ and $\mathbb{C}$

Now...

special case of deciding the quantifier-free fragment for reals

RAHD - Real Algebra in High Dimension(6)

basic idea:
use different techniques for different types of constraints
$\rightarrow$ exploit their "sweet spots"

Basic problem

Given implicitly existentially quantified formula ϕ,
which is a boolean combination of terms of the form

$$p \circ 0 \quad \circ \in \{<, \leq, =, \neq, \geq, >\}$$

where p is a polynomial,
determine whether ϕ is unsatisfiable.

Notation

- ϕ: formula to prove
- F: set of polynomials in ϕ
- $p, f, g, \ldots$: polynomials

Cylindrical Algebraic Decomposition

Idea: decompose $\mathbb{R}^n$ into cells where F is sign-invariant

Projection

recursively compute the sets $F_{n-1}, F_{n-2}, ..., F_1$ in $\mathbb{R}^{n-1}, \mathbb{R}^{n-2}, ..., \mathbb{R}^1$
such that
if a cell C in $\mathbb{R}^{k-1}$ is sign-invariant for F_{k-1},
then all polynomials in F_k over C have a fixed number of roots
$\rightarrow$ we can decompose the cylinder of C in $\mathbb{R}^k$

Construction

starting from F_1, for each F_i construct a partition in $\mathbb{R}^i$
at each step

- the polynomials $f \in F_i$ are univariate
- compute test points for each cell

CAD - for open sets

algorithm is dominated by a function doubly-exponential in n

Improvements

- not all cells are necessary for deciding the formula
  $\rightarrow$ reduces number of cells produced
- if ϕ contains only strict inequalities, cells are open sets
  $\rightarrow$ select only rational test points

References: original strict inequality paper (5), QEPCAD B tool (2), best explanation I could find (1)

Some algebra

Let $\mathbb{R}[x_1, ..., x_n]$ denote the set of all n-variate polynomials

Ideal

$I \subset \mathbb{R}[x_1, ..., x_n]$ such that

- $0 \in I$
- $f, g \in I$, then $f + g \in I$
- $f \in I$ and $h \in \mathbb{R}[x_1, ..., x_n]$, then $hf \in I$

$\rightarrow$ think of it as an analogue to a vector space, generated by some polynomials $I =< f_1, ..., f_s >$

analogous to vector spaces, different bases are possible

Groebner (standard) basis

special basis with some very nice properties

- every ideal has a finite unique (reduced) Groebner basis
- *Buchberger's algorithm* computes it for any set of polynomials
- provides necessary condition for the test $g \in I$

Reference: decent introduction (4)

Elimination property

Given

$$x^2 + y + z = 1$$
$$x + y^2 + z = 1$$
$$x + y + z^2 = 1$$

the ideal is $I =< x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 >$
then the Groebner basis is

$$g1 = x + y + z^2 - 1$$
$$g2 = y^2 - y - z^2 + z$$
$$g3 = 2yz^2 + z^4 - z^2$$
$$g4 = z^6 - 4z^4 + 4z^3 - z^2$$

There's a catch...

The back-substitution necessary for solving the system of equations only works for $\mathbb{C}$, but

- if ϕ unsatisfiable over $\mathbb{C}$, then also over $\mathbb{R}$
- rewriting of polynomials generating the ideal is still valid over $\mathbb{R}$

A note on complexity

- rational coefficients created can be very large
- degrees in the reduced basis can grow very large
- choosing the right monomial ordering can improve things

$\rightarrow$ the worst-case complexity not determined yet
$\rightarrow$ experimental results show useful for 'normal' problems

Virtual Term Substitution

Consider only formulas linear or quadratic in the quantified variable:

$$\exists x.[ax^2 + bx + c = 0] \wedge F$$

- replace x in F by the three possible solutions α_i for x
- add constraints for each case
- rewrite final expression so that it does not contain square roots

$\Rightarrow$ disjunction of formulas

- substitution may increase the degree of other variables
- resulting formulas may be unwieldy

$\Rightarrow$ if applicable (with degree-reduction heuristics) gives good performance for high-dimensional problems

References: original paper (7), improvements (3)

Stengle's Weak Positivstellensatz

$$\begin{aligned} F = \quad & p_1(\mathbf{x}) = 0 \wedge \dots \wedge p_k(\mathbf{x}) = 0 \\ & \wedge q_1(\mathbf{x}) \geq 0 \wedge \dots \wedge q_l(\mathbf{x}) \geq 0 \\ & \wedge s_1(\mathbf{x}) > 0 \wedge \dots \wedge s_m(\mathbf{x}) > 0 \end{aligned}$$

is unsatisfiable iff, if

$$\begin{aligned} \exists f &\in Ideal(p_1, \dots, p_k), \\ \exists g &\in Cone(q_1, \dots, q_l), \\ \exists h &\in Monomials(s_1, \dots s_m) \end{aligned}$$

such that

$$f + g + h^2 = -1$$

Simpler version

Given a constraint $p = 0$ or $p < 0$, then

$$\begin{aligned} & RC(p) > 0 \quad \text{(degree-zero coefficient)} \\ \wedge \quad & p \in \{\sum_{j=1}^{k} m^2 | m \text{ monomial with coeff. in } \mathbb{Q}\} \end{aligned}$$

is a witness certificate for unsatisfiability.

Sturm's theorem

Suppose we have an univariate constraint of the form $p = 0$. Given a Sturm chain $p, p_1, ..., p_m$

$$\begin{aligned}
p_0(x) &= p(x) \\
p_1(x) &= p'(x) \\
p_2(x) &= -rem(p_0, p_1) \quad &= p_1(x)q_0(x) - p_0(x) \\
p_3(x) &= -rem(p_1, p_2) \quad &= p_2(x)q_1(x) - p_1(x) \\
&\ldots \\
0 &= -rem(p_{m-1}, p_m)
\end{aligned}$$

denote by $\sigma(\xi)$ the number of sign changes in the sequence

$$p(\xi), p_1(\xi), p_2(\xi), ...p_m(\xi)$$

then for $a < b$, both real, the number of real roots in $(a, b]$ is $\sigma(a) - \sigma(b)$.

Application

For constraints of the form

$$[p > 0, \quad p \in \mathbb{Q}[x] \quad \wedge (x > q_1) \wedge (x < q_2)]$$

the following is a certificate for unsatisfiability

$$p(\frac{q_2 - q_1}{2}) \leq 0$$
$$SC(p, (q_1, q_2)) = 0$$
$$q_1 < q_2$$

Recap

- strict inequalities $\rightarrow$ CAD
- sum-of-squares $\rightarrow$ Positivstellensatz
- equalities $\rightarrow$ Groebner bases
- univariate constraints $\rightarrow$ Sturm's theorem

Dimension reduction

$$pq = 0 \iff (p = 0 \vee q = 0)$$

$$\sum_{i=1}^{k} p_i^2 = 0 \iff \bigwedge_{i=1}^{k} p_i = 0$$

- elimination ideals with Groebner bases
- (approximation of real radical ideals)

RAHD

Given a *goal* ϕ, show unsatisfiability.

1. put ϕ in DNF, giving a set of *cases*
2. normalize so that every case is a conjunction of equalities or strict inequalities over polynomials
3. use *case manipulation functions (CMF)* on each case in turn
   - report sat/unsat
   - return unchanged
   - make progress (e.g. by rewriting into equisatisfiable formula)
   - return boolean formula, but with reduced dimension

$\rightarrow$ ordering of CMF's is crucial

CMF ordering

- cheap functions first (Sturm chains before CAD)
- functions providing information to others first (Positivstellensatz search before Sturm)
- function is included several times, if it has a chance of making a more informed decision after certain steps have run (interval analysis before and after Groebner basis rewriting)

If all else fails, run the general CAD algorithm.

Comparison

Compared to

- QEPCAD-B
- Redlog/Rlqe (virtual term substitution, fallback on Rlcad)
- Redlog/Rlcad (partial CAD)

Results:

- RAHD can solve some (high-dimension, high-degree) problems, the others can not
- not the fastest on the other problems

References

V. Weispfennig A. Dolzmann, T. Strum.
Real quantifier elimination in practice.
Algorithmic Algebra and Number Theory, 1998.

Christopher W. Brown.
Qepcad b: A program for computing with semi-algebraic sets using cads.
SIGSAM BULLETIN, 37:97–108, 2003.

Christopher W. Brown.
On quantifier elimination by virtual term substitution.
Technical report, Naval Academy Annapolis, 2005.

David A. Cox, John Little, and Donal O'Shea.
Ideals, Varieties, and Algorithms An Introduction to Computational Algebraic Geometry and Commutative Algebra.
Springer, 2007.

S. McCallum.
Solving polynomial strict inequalities using cylindrical algebraic decomposition.
Technical report, Macquarie University, Australia, 1993.

Grant Olney Passmore and Paul B. Jackson.
Combined decision techniques for the existential theory of the reals.
In *CICM*, 2009.

V. Weispfenning.
Quantifier elimination for real algebra — the quadratic case and beyond.
Applicable Algebra in Engineering, Communication and Computing, 1997.