Unsatisfiability of Nonlinear Constra

An Algebraic Approach

Ashish Tiwari

Tiwari@csl.sri.com

Computer Science Laboratory

SRI International

Menlo Park CA 94025

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

Problem

Given a set of nonlinear equations and inequalities:

$$
\begin{aligned}
p &= 0, & p &\in P \\
q &> 0, & q &\in Q \\
r &\geq 0, & r &\in R
\end{aligned}
$$

where $P, Q, R \subset \mathbb{Q}[\vec{x}]$ are sets of polynomials over $\vec{x}$

Is the above set satisfiable over the reals?

Motivation

Model of bacterial resistance to antibiotic Tetracycline:

$$
\begin{aligned}
d[TetR]/dt &= f_1 - k_d[TetR] - k_+[Tc][TetR] + k_-[\\
d[TetRTc]/dt &= k_+[Tc][TetR] - k_-[TetRTc] - k_d[Te \\
d[Tc]/dt &= k_i([Tc]^0 - [Tc]) - \underline{k_p[Tc][TetA]} - \underline{k_+} \\
& \quad +k_-[TetRTc] - k_d[Tc] \\
d[TetA]/dt &= f_2 - k_d[TetA]
\end{aligned}
$$

If C denotes the constraint that $d\vec{x}/dt|_{\langle [TetR]_0, [TetRTc]_0, [Tc]_0, [T}$
proof obligation for model simplication is:

$$C \quad \Rightarrow \quad 10k_+[Tc]_0[TetR]_0 < k_p[Tc]_0[TetA]_0$$

Other Applications: control, robotics, solving games, static ana
systems, . . .

Known Results

- The full FO theory of reals is decidable [Tarski48]
  Nonelementary decision procedure, impractical
- Double-exponential time decision procedure [Collins74, Mon
- Exponential space lower bound
- Collin's algorithm based on " cylindrical algebraic decompos
  improved over the years and implemented in QEPCAD.
  In practice, could fail on $p > 0 \wedge p < 0$.

Need a practical method to decide nonlinear constraints

Not necessarily a decision procedure

Goal for this work

To develop a procedure for testing unsatisfiability of nonlinear

- detects inconsistency of "easy" instances efficiently
- admits a simple description using logical inference rules
- is incremental
- generates small unsatisfiable core

Example: consider

$$p > 0 \;\wedge\; q_1 > 0 \;\wedge\; q_2 > 0 \;\wedge\; \cdots \;\wedge\; q_n > 0 \;\wedge\; p$$

We present a sound and refutationally complete procedure
But we use its sound, terminating, and incomplete variant

Approach

- Introduce slack variables s.t. all inequality constraints are of
  $v > 0$, or $w \geq 0$

$$P = 0, \quad Q > 0, \quad R \geq 0 \quad \mapsto$$

$$\underline{P = 0}, \quad \underline{Q - \vec{v} = 0}, \quad \underline{R - \vec{w} = 0}, \quad \vec{v} > 0, \; \vec{w} \geq$$

- Search for a polynomial p s.t.

$$\underline{P = 0} \quad \Rightarrow \quad p = 0$$

$$\vec{v} > 0, \; \vec{w} \geq 0 \quad \Rightarrow \quad p > 0$$

- To search for p, compute the Gröbner basis for P using diffe
  orderings (pivot)

Note the parallel to Simplex

Example

Let $I = \{v_1 > 0, v_2 > 0, v_3 > 0\}$.

$$v_1 + v_2 - 1 = 0,\ v_1 v_3 + v_2 - v_3 - 2 = 0$$

$$v_1 + v_2 - 1 = 0,\ (1 - v_2)v_3 + v_2 - v_3 - 2 = 0$$

$$v_1 + v_2 - 1 = 0,\ v_2 v_3 - v_2 + 2 = 0$$

$$v_1 + v_2 - 1 = 0,\ v_2 v_3 - v_2 + 2 = 0,\ v_2 v_3 - v_4 =$$

$$v_1 + v_2 - 1 = 0,\ -v_2 + v_4 + 2 = 0,\ v_2 v_3 - v_4 =$$

$$v_1 + v_4 + 1 = 0,\ -v_2 + v_4 + 2 = 0,\ v_2 v_3 - v_4 =$$

$$\bot$$

The polynomial $v_1 + v_4 + 1$ is the required witness to the unsat
the constraints.

Positivstellensatz

What guarantees the existence of such a witness?

The constraint

$$\{p = 0 : p \in P\} \cup \{q \geq 0 : q \in Q\} \cup \{r \neq 0 : r \in$$

is unsatisfiable (over the reals) iff
there exist polynomials p, q, and r such that

$$p \in Ideal(P) \qquad \{\Sigma_i p_i q_i : p_i \in P\}$$

$$q \in Cone[Q] \qquad \{\Sigma_i c_i^+ q_1 q_2 \ldots q_k : q_i \in Q$$

$$r \in [R] \qquad \{r_1 r_2 \ldots r_k : r_i \in R\}$$

$$p + q + r^2 \equiv 0$$

Positivstellensatz Corollary

The constraint

$$\{p = 0 : p \in P\} \cup \{v > 0 : v \in \vec{v}\} \cup \{w \geq 0 : w \in$$

is unsatisfiable iff

$\exists p'$ such that

$$p' \in Ideal(P) \cap Cone[\vec{v}, \vec{w}]$$

and there is at least one monomial $c\mu$ in p' such that $c > 0$ and

How to find p'?

Finding p'

We know $p' \in Ideal(P)$.

If p' is "small-enough" in the ordering $\succ$, then p' will appear ex
Gröbner basis for P constructed using $\succ$.

Example: $P = \{w_1 - 2w_3 + 2,\ w_2 + 2w_3 - 1\}$ and $I = \{w_1$

If $w_1 \succ w_2 \succ w_3$, then $GB_{\succ}(P) = P$.

If we make $w_3 \succ w_1$ and $w_3 \succ w_2$ in the ordering, then

$$GB_{\succ}(P) = \{2w_3 - w_1 - 2,\ \underline{w_2 + w_1 + 1}\}.$$

For linear polynomials, this is pivoting, but what is its analogue
systems ?

Finding p': Nonlinear Issues

It is not always possible to change $\succ$ to get witness $p' \in GB_{\succ}($

- Problem 1:

$$P_1 = \{v + w_1 - 1,\ w_1 w_2 - w_1 + 1\}$$

  Need $w_1 \succ w_1 w_2$ to "get" $v + w_1 w_2$ in $GB(P_1)$.

- Problem 2:

$$P_2 = \{w_1^2 - 2w_1 w_2 + w_2^2 + 1\}$$

  Need $w_1, w_2 \succ (w_1 - w_2)^2$ to "get" the witness $(w_1 - w_2)^2$
  $GB(P_2)$.

Main Idea: Introduce new definitions and get flexibility in choo

Add $w_1 w_2 - w_3$ to P_1 and have $w_1 \succ w_3$.

Add $(w_1 - w_2)^2 - w_3$ to P_2 and have $w_1, w_2 \succ w_3$.

Example: Revisited

Let $I = \{v_1 > 0, v_2 > 0, v_3 > 0\}$.

$$v_1 + v_2 - 1 = 0,\ v_1 v_3 + v_2 - v_3 - 2 = 0$$

$$v_1 + v_2 - 1 = 0,\ (1 - v_2)v_3 + v_2 - v_3 - 2 = 0$$

$$v_1 + v_2 - 1 = 0,\ v_2 v_3 - v_2 + 2 = 0$$

$$v_1 + v_2 - 1 = 0,\ v_2 v_3 - v_2 + 2 = 0,\ v_2 v_3 - v_4 =$$

$$v_1 + v_2 - 1 = 0,\ -v_2 + v_4 + 2 = 0,\ v_2 v_3 - v_4 =$$

$$v_1 + v_4 + 1 = 0,\ -v_2 + v_4 + 2 = 0,\ v_2 v_3 - v_4 =$$

$$\perp$$

The polynomial $v_1 + v_4 + 1$ is the required witness to the unsat
the constraints.

Inference Rules

GB:

$$\frac{(V, P)}{(V, GB(P))}$$

Extend1:

$$\frac{(V, P' = P \cup \{\mu_0 + p\})}{(V \cup \{w'\}, P' \cup \{\mu_0 - w'\})}$$

if $\mu_0 \in [V_{\geq$

Extend2:

$$\frac{(V, P)}{(V \cup \{x'\}, P \cup \{\nu_0 + \alpha\nu_1 - x'\})}$$

if $\langle \nu_0, \nu_1 \rangle$ c
$x' \in V^{new}$

Detect:

$$\frac{(V, P' = P \cup \{c_0\mu_0 + p\})}{(V, P \cup \{c_0\mu_0, p\})}$$

if $c_0\mu_0 + p$
nomial over

Witness:

$$\frac{(V, P \cup \{c\mu\})}{\bot}$$

if $\mu \in [V_{>0}$

Refutational Completeness

If P_0 is unsatisfiable and $(V_0, P_0) \vdash^* (V, P)$ is a derivation usi
inference rules s.t. $P \neq \bot$, then
there exists a derivation from (V, P) to $\bot$.

Main idea of proof:

- consider the witness given by Positivstellensatz
- if it does not explicitly appear, then we can add a new definiti
- the witness in the new system is smaller in some well-founde

Inference rules yield a sound and refutationally complete proc
non-terminating

Implementation

- In our applications, termination and soundness are more imp
  refutational completeness.
  We have implemented a terminating and sound procedure ob
  restricting the number of new definitions.
- Projection onto the slack variables and testing satisfiability of
  is a powerful heuristic.
- Implementation is recursive: each new definition is introduce
  "incremental" way.
  Implementation is in Lisp.
- Experience is that it is much faster than, and about as good as
  formulas generated during the abstraction of polynomial hybr
  As fast as our earlier FM-based procedure, but gets more the

Conclusion

A simple sound and refutationally complete set of inference ru
unsatisfiability of nonlinear constraints. Features:

- Generalization of Simplex for linear constraints
- Simple: Gröbner basis computation + new definitions
- Refutationally complete: based on Positivstellensatz
- Degree bounds for Positivstellensatz is OPEN. If solved, our
  turns into a decision procedure.
- Can be combined with Simplex as well as unsound, comple
- A logical approach to practical decision procedures