Satisfiability Checking

Non-linear real arithmetic

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 14/15

Domain	$+$	$+ , \cdot$
Reals $\mathbb{R}$	linear real arithmetic decidable (Fourier-Motzkin, Simplex)	non-linear real arithmetic decidable
Integers $\mathbb{Z}$	linear integer arithmetic decidable (Branch-and-bound, Gomory cuts, Omega test)	non-linear integer arithmetic undecidable

Non-linear real arithmetic (NRA)

Real algebra is the first-order theory $(\mathbb{R}, +, \cdot, 0, 1, <)$ over the reals with addition and multiplication.

Syntax of real algebra

Terms:	t	$::=$	0	|	1	|	x	|	$t + t$	|	$t \cdot t$
Constraints:	c	$::=$	$t < t$								
Formulas:	φ	$::=$	c	|	$\neg\varphi$	|	$\varphi \wedge \varphi$	|	$\exists x.\ \varphi$		

where x is a variable.

- Syntactic sugar for constraints: $t_1 \leq t_2$, $t_1 = t_2$, $t_1 \neq t_2$.
- $\mathbb{Z}[x_1, \ldots, x_n]$ is the set of all polynomials over variables $x_1, \ldots, x_n$. What is the difference between $\mathbb{Z}[x_1, \ldots, x_n]$ and $\mathbb{Z}[x_1, \ldots, x_{n-1}][x_n]$?
- The semantics is standard.
- Real algebra is often called non-linear real arithmetic (NRA).
- We consider the satisfiability problem for the quantifier-free fragment QFNRA (equivalently, we consider the existential fragment, i.e., no negation of expressions containing quantifiers).

What is new?

- We can already check QFLRA (quantifier-free linear real arithmetic) formulas. Example:

$$\exists x.\ \exists y.\ x + 2y > 10 \land x \geq y \land (x < 0 \lor 2y > x)$$

- Now we might have also non-linear constraints in the formulas. Example:

$$\exists x.\ \exists y.\ (\ x^2 - 4x^3y^2 > 0 \land x - y = 1\ )$$

Some notions and notations

- Monomial: product of variables (the empty product represents the constant 1).
- Term: product of an integer coefficient and a monomial.
- Canonical form of polynomial constraints: $p \sim 0$, $\sim \in \{<, \leq, =, \geq, >\}$, p is a sum of terms (i.e., a linear combination of monomials).
- A polynomial in one variable is called univariate, polynomials in more than one variables are called multivariate.
- The degree of a polynomial is the highest degree of its monomials, when expressed in canonical form. The degree of a monomial is the sum of the exponents of the variables that appear in it. The word degree is now standard, but in some older books, the word order may be used instead.

Real algebra: On the border of decidability

Theorem (Alfred Tarski 1948)

The FO *theory of* $(\mathbb{R}, +, \cdot, 0, 1, <)$ *is decidable.*

- Tarski's proof was constructive, i.e., it defined a decision procedure.
- However, its time-complexity in the number of variables was non-elementary ("greater than all finite towers of powers of 2").

Real algebra: Some historic facts

1637 Descartes' rule of signs

1835 Jaques Charles François Sturm's theorem

1948 Alfred Tarski's "A decision method for elementary algebra and geometry"

1975 Cylindrical algebraic decomposition (CAD) method by George E. Collins

1979–80 First implementation of the CAD method by Dennis S. Arnon

1988 Virtual substitution by Volker Weispfenning

1990 First implementation of virtual substitution (Klaus-Dieter Burhenne)

1993 Gröbner bases approach by P. Pedersen, M.-F. Roy, A. Szpirglas, later extended by V. Weispfenning

1994 Implementation of the Gröbner bases approach (Andreas Dolzmann)

Real algebra: Implementations

Virtual substitution

- Computer logic system `Redlog` (package of `Reduce`)

Cylindrical algebraic decomposition

- `QEPCAD`, `Redlog`, ...

Gröbner bases

- `Maple`, `Mathematica`, `Singular`, `Maxima`, `CoCoA`, `Reduce`, ...

Other methods

- Interval arithmetic (`Ariadne` or `iSAT`)

The idea of quantifier elimination

Given: FO sentence φ over $(\mathbb{R}, +, \cdot, 0, 1, <)$ containing n quantifiers

1. Transform φ into prenex normal form:

$$\varphi \quad \equiv \quad Q_1 x_1 \ldots Q_n x_n \varphi_n(x_1, \ldots, x_n)$$

   where φ_n is a quantifier-free NRA formula with variables $x_1, \ldots, x_n$.

2. Eliminate iteratively the quantifiers $Q_n \ldots Q_1$ and thus the quantified variables:

$$\begin{aligned}
\varphi \quad &\equiv \quad Q_1 x_1 \ldots Q_{n-1} x_{n-1} \; Q_n x_n \quad \varphi_n(x_1, \ldots, x_n) \\
&\equiv \quad Q_1 x_1 \ldots Q_{n-1} x_{n-1} \quad \varphi_{n-1}(x_1, \ldots, x_{n-1}) \\
&\ldots \\
&\equiv \quad Q_1 x_1 \quad \varphi_1(x_1) \\
&\equiv \quad \varphi_0()
\end{aligned}$$

Removing universal quantification

Is it sufficient to eliminate existential quantifiers?

$$
\begin{array}{ll}
& \exists x_1.\, \exists x_2.\quad \forall x_3.\quad \exists x_4.\quad \forall x_5.\qquad \forall x_6.\quad \exists x_7.\, \exists x_8.\quad \varphi' \\
\equiv & \exists x_1.\, \exists x_2.\, \neg(\exists x_3.\, \neg(\exists x_4.\, \neg(\exists x_5.\, \neg(\neg(\exists x_6.\, \neg(\exists x_7.\, \exists x_8.\quad \varphi' \quad)))))) \\
\equiv & \exists x_1.\, \exists x_2.\, \neg(\exists x_3.\, \neg(\exists x_4.\, \neg(\exists x_5.\qquad \exists x_6.\, \neg(\exists x_7.\, \exists x_8.\quad \varphi' \quad))))
\end{array}
$$

But: increased complexity

Removing inequations

Is it sufficient to handle equations?

$$\begin{array}{lcl} p \geq 0 & \equiv & \exists \epsilon.\ p - \epsilon^2 = 0 \\ p \leq 0 & \equiv & \exists \epsilon.\ p + \epsilon^2 = 0 \\ p > 0 & \equiv & \exists \epsilon.\ 1 - p \cdot \epsilon^2 = 0 \\ p < 0 & \equiv & \exists \epsilon.\ 1 + p \cdot \epsilon^2 = 0 \\ p \neq 0 & \equiv & \not(p = 0) \end{array}$$

But: increased complexity

Existential quantifier elimination: Finite abstraction

- Given: $\varphi = \exists x_1. \ldots \exists x_n. \varphi_n$, where φ_n is a quantifier-free FO sentence over $(\mathbb{R}, +, \cdot, 0, 1, <)$
- Problem: $\mathbb{R}$ is uncountably infinite.
- Idea: Find a finite set $T \subset \mathbb{R}$ with

$$\exists x_1. \ldots \exists x_n. \varphi_n \quad \Leftrightarrow \quad \exists x_1. \ldots \exists x_{n-1}. \bigvee_{t \in T} \varphi_n[t/x_n]$$

- Each univariate polynomial $p(x)$ of degree d has at most d real roots (multivariate polynomials are seen as univariate ones with polynomial coefficients).
  The sign of p is invariant between each two successive real roots.
  This implies that $\mathbb{R}$ can be partitioned into at most $2d + 1$ sign invariant regions for p.
  T consists of a test (sample) point from each sign-invariant region.
- What remains: Determine the zeros of polynomials.

Some interesting decision procedues for NRA

We will have a look at the following satisfiability checking methods for (fragments of) NRA:

- Virtual substitution (VS)
- Cylindrical algebraic decomposition (CAD)
- Gröbner bases (GB)
- Interval constraint propagation (ICP)