Satisfiability Checking

21 The decomposition idea for solving real arithmetic problems

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 22/23

Real arithmetic: On the border of decidability

Theorem (Alfred Tarski 1948)

The problem to determine the truth of real-arithmetic sentences 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").

quantifier elimination method

① Resolution

$\underline{(x \vee C_1)} \wedge \underline{(\neg x \vee C_2)}$

$\Leftrightarrow C_1 \vee C_2$

$D_x \quad D_{\neg x} \quad R$

x不存在的clause

$\underbrace{\exists x. \bigwedge_{C_x \in D_x} D_x \wedge \bigwedge_{C_{\neg x} \in D_{\neg x}} C_{\neg x}}_{\text{Resolution 可消去}} \wedge \bigwedge_{C_R \in R} C_R$

② Fourier-M

$\exists x_i. \left.\begin{matrix} l_1 & < \\ \vdots & \\ l_k & \le \end{matrix}\right\} x_i \left\{\begin{matrix} < & u_1 \\ & \vdots \\ \le & u_j \end{matrix}\right.$

$\Leftrightarrow \bigwedge_{l=1}^{k} \bigwedge_{u=1}^{j} l_l \overset{\le}{<} u_u$

Real arithmetic: Some historical facts

- 1637 Descartes' rule of signs
- 1835 Sturm's theorem
- 1948 Tarski's "A decision method for elementary algebra and geometry"
- 1975 Cylindrical algebraic decomposition (CAD) method by Collins
- 1979–80 First implementation of the CAD method by Arnon
- 1988 Virtual substitution by Weispfenning
- 1990 First implementation of virtual substitution by Burhenne
- 1993 Gröbner bases approach by Pedersen, Roya and Szpirglas, later extended by Weispfenning
- 1994 Implementation of the Gröbner bases approach by Dolzmann
- 2017 Subtropical satisfiability by Fontaine, Ogawa, Sturm and Vu

The virtual substitution (VS) and the cylindrical algebraic decomposition (CAD) are quantifier elimination methods.

quantifier elimination methods本质上和
variable elimination methods一样

The idea of quantifier elimination

Given: FO sentence φ containing n quantifiers

1. Transform φ into prenex normal form:

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

Nonlinear Real Arithmetic

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, thereby maintaining semantical equivalence: 移除quantifier 的同时 移除对应的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?

$\forall x. R \Leftrightarrow \neg(\exists x. \neg R)$

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

But: increased complexity 因为 $\neg$

Equations are sufficient

It is sufficient to handle only equations on the cost of increased complexity.

$$
\begin{array}{lcl}
p \geq 0 & \equiv & \exists \epsilon.\ p - \epsilon^2 = 0 \\
p \leq 0 & \equiv & \exists \epsilon.\ p + \epsilon^2 = 0 \\
p > 0 & \equiv & \exists \epsilon.\ 1 - p \cdot \epsilon^2 = 0 \\
p < 0 & \equiv & \exists \epsilon.\ 1 + p \cdot \epsilon^2 = 0 \\
p \neq 0 & \equiv & \neg(p = 0)
\end{array}
$$

The idea of finite abstraction

- 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. term的degree为所有变量的幂指数求和, formula的degree为最大的term degree
  The word degree is now standard, but in some older books, the word order may be used instead.
- A real resp. complex root of a polynomial in n (ordered) variables is a value from $\mathbb{R}^n$ resp. $\mathbb{C}^n$ for which the polynomial evaluates to zero.
- Each univariate polynomial $p(x)$ of degree d has d complex roots.
  Each univariate polynomial $p(x)$ of degree d has at most d real roots.
  The sign of p is invariant between each two successive real roots.
  两个解之间多项式的正负是固定的(函数连续性)
  This implies that, if we know all roots, we can partition $\mathbb{R}$ into at most $2d+1$ sign invariant regions for p. 知道全部的解之后可以将数轴分成2d+1个区间
- Similar facts hold also for formulas: for each QFNRA formula there is a finite partitioning of the state space such that the formula's truth value is invariant in each partition. QFNRA的状态空间中也存在划分,使得在划分内公式的真值保持确定

Existential quantifier elimination: Finite abstraction

- Given: $\varphi = \exists x_1. \ldots \exists x_n. \varphi_n$, where φ_n is a quantifier-free real-arithmetic formula.
- Problem: $\mathbb{R}$ is uncountably infinite.
- Idea: Find a finite set $T \subset \mathbb{R}$ with

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

  T consists of one test (sample) point from each sign-invariant region that might contain solutions.
- Necessary: Determine the real roots of polynomials.

Real roots of univariate polynomials

What are the degrees and the real roots of these polynomials?

Polynomial	Degree	Values of real roots
x	1 1个解	0
$2x - 5$	1	2.5
x^2	2 2个解	0
$x^2 - 1$	2	$1, -1$
$x^2 + 1$	2	-
$x^2 - 2$	2	$\sqrt{2}, -\sqrt{2}$
$2x^6 - 5x^4 + 3x^2 - 6$	6	???

VS: Solution equations for polynomials up to degree 4

Real roots of univariate 一元 quadratic 二次 polynomials
$ax^2 + bx + c$ $(a, b, c \in \mathbb{Z})$:

$$\begin{array}{ll} \frac{-b \pm \sqrt{b^2-4ac}}{2a} & \text{if } a \neq 0 \text{ and } b^2 - 4ac \geq 0 \\ -\frac{c}{b} & \text{if } a = 0 \text{ and } b \neq 0 \\ \mathbb{R} & \text{if } a = 0 \text{ and } b = 0 \text{ and } c = 0 \\ \text{none} & \text{else.} \end{array}$$

Real roots of multivariate quadratic polynomials
$p_a x^2 + p_b x + p_c$ $(p_a, p_b, p_c \in \mathbb{Z}[\vec{y}])$:

$$\begin{array}{ll} \frac{-p_b \pm \sqrt{p_b^2-4p_a p_c}}{2p_a} & \text{if } p_a \neq 0 \text{ and } p_b^2 - 4p_a p_c \geq 0 \\ -\frac{p_c}{p_b} & \text{if } p_a = 0 \text{ and } p_b \neq 0 \\ \mathbb{R} & \text{if } p_a = 0 \text{ and } p_b = 0 \text{ and } p_c = 0 \\ \text{none} & \text{else.} \end{array}$$

Problem: expressions not in QFNRA. Solution: virtual substitution.

CAD: Real root isolation

- For polynomials of degree 5 or higher, no solution equations exist.
- Instead of computing the roots, we will isolate them: For each real root of a univariate polynomial, we define an interval in which this but no other root is included. 定义Interval, 其内部只有一个根
- This is the so-called interval representation of roots: (p, I) with univariate polynomial p and real interval I, such that p has exactly one real root in I.
- We need to be able to compute with this representation, e.g., substitute such a real root for a variable in a univariate polynomial constraint and check its truth.
- We will not go in detail, as we don't have sufficient time. We will stay at the level of intuition here.

Learning target

- Given an univariate polynomial, how many complex and real roots can it have?
- How can we compute real roots of quadratic polynomials with the solution equation?
- How can we represent roots of univariate polynomials in the interval representation?