Real Arithmetic

Max Haslbeck

Fakultät für Informatik
TU München

08 July 2016
Real Arithmetic

Is the theory $Th(\mathbb{R}, +, *, =, <)$ decidable?

Informally: Can we decide if a closed first order formula $F$ in $\mathbb{R}$ using $+, *, =$ and $<$ is true?

$$\exists xyz \forall abc$$

$$(12x^5y^4a^4 - 322x^4 + 78x^3y^2 - 1034 = 0) \land (2y^4 - 43z^2b^4 = 0) \land (38z^3y^2 - 322zc^{19} > 0) \land (123z^8 - 43x^3 + y^2 < 0)$$
Sturm Sequences  [Charles Sturm, 1803–1855]

Method to count number of real roots of a polynomial $P \in \mathbb{R}[X]$ in an interval
Sturm Sequences [Charles Sturm, 1803–1855]

Method to count number of real roots of a polynomial $P \in \mathbb{R}[X]$ in an interval

Build a sequence of polynomials with:

- $P_0 = P$
- $P_1 = P'$
- $P_{i+1} = -(P_{i-1} \mod P_i)$
Sturm Sequences [Charles Sturm, 1803–1855]

Method to count number of real roots of a polynomial \( P \in \mathbb{R}[X] \) in an interval

Build a sequence of polynomials with:

\[
\begin{align*}
P_0 &= P \\
P_1 &= P' \\
P_{i+1} &= -(P_{i-1} \mod P_i)
\end{align*}
\]

Let \( v_P(a) \) be the number of sign changes in the sequence \( P_0(a), P_1(a), \ldots, P_K(a) \)
Sturm Sequences Lemma

Let $a < b$ be real numbers which are not roots of $P$. 
Sturm Sequences Lemma

Let $a < b$ be real numbers which are not roots of $P$.

The difference $\nu_P(a) - \nu_P(b)$ is equal to the number of distinct roots of $P$ in the interval $(a, b)$. 
Sturm Sequences Lemma

Let $a < b$ be real numbers which are not roots of $P$.

The difference $v_P(a) - v_P(b)$ is equal to the number of distinct roots of $P$ in the interval $(a, b)$.

The difference $v_P(-\infty) - v_P(\infty)$ is equal to the number of distinct roots of $P$. 
Example

$P_0 = x^3 - 3x + 1$
Proof sketch

Assume $P$ has no multiple roots:

- If $c$ is a root of $P$:

<table>
<thead>
<tr>
<th>$x$</th>
<th>$c - \epsilon$</th>
<th>$c$</th>
<th>$c + \epsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_0$</td>
<td>-</td>
<td>0</td>
<td>+</td>
</tr>
<tr>
<td>$P_1$</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

or

<table>
<thead>
<tr>
<th>$x$</th>
<th>$c - \epsilon$</th>
<th>$c$</th>
<th>$c + \epsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_0$</td>
<td>+</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>$P_1$</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Proof sketch

Assume P has no multiple roots:

- If c is a root of P:

  \[
  \begin{array}{c|ccc}
  x & c - \epsilon & c & c + \epsilon \\
  \hline
  P_0 & - & 0 & + \\
  P_1 & + & + & +
  \end{array}
  \]

  or

  \[
  \begin{array}{c|ccc}
  x & c - \epsilon & c & c + \epsilon \\
  \hline
  P_0 & + & 0 & - \\
  P_1 & - & - & -
  \end{array}
  \]

- For \((1 < i < K)\) if c is a root of \(P_i\) and since
\[P_{i-1} = P_iQ - P_{i+1},\]
then \(P_{i+1}(c) = -P_{i-1}(c) \neq 0.\)
Proof sketch

Assume P has no multiple roots:

- If $c$ is a root of $P$:

<table>
<thead>
<tr>
<th>$x$</th>
<th>$c - \epsilon$</th>
<th>$c$</th>
<th>$c + \epsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_0$</td>
<td>-</td>
<td>0</td>
<td>+</td>
</tr>
<tr>
<td>$P_1$</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

or

<table>
<thead>
<tr>
<th>$x$</th>
<th>$c - \epsilon$</th>
<th>$c$</th>
<th>$c + \epsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_0$</td>
<td>+</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>$P_1$</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

- For $(1 < i < K)$ if $c$ is a root of $P_i$ and since $P_{i-1} = P_i Q - P_{i+1}$, then $P_{i+1}(c) = -P_{i-1}(c) \neq 0$.

Sturm sequences also work for $P$ with multiple roots.
Multiple Equations

\[ P_1 = 0, \ldots P_n = 0 \iff P_1^2 + \ldots + P_n^2 = 0 \]
One Equation + One Inequality

Let $Q$ be polynomial in $\mathbb{R}[X]$ and we want to count the number of real roots $c$ of $P$ such that $Q(c) > 0$.
One Equation + One Inequality

Let \( Q \) be polynomial in \( \mathbb{R}[X] \) and we want to count the number of real roots \( c \) of \( P \) such that \( Q(c) > 0 \)

Build a sequence of polynomials with:

- \( P_0 = P \)
- \( P_1 = P' Q \)
- \( P_{i+1} = -(P_{i-1} \mod P_i) \)

Let \( v(a) \) be the number of sign changes in the sequence \( P_0(a), P_1(a), \ldots, P_K(a) \)
Lemma

Let $a < b$ be real numbers which are not roots of $P$. The difference $\nu(a) - \nu(b)$ is equal to the number of distinct roots of $P$ in the interval $(a, b)$ such that $Q(c) > 0$ minus the number such that $Q(c) < 0$. 
One Equation + Multiple Inequalities

- \( P = 0, Q_1 > 0, \ldots, Q_k > 0 \)  
  \((P\ is\ relatively\ prime\ with\ all\ Q_i)\)
- \( \epsilon = (\epsilon_1, \ldots, \epsilon_k) \in \{0, 1\}^k \)
- \( \varphi = (\varphi_1, \ldots, \varphi_k) \in \{0, 1\}^k \)
- \( Q_\epsilon = Q_{\epsilon_1}^{\epsilon_1} \cdots Q_{\epsilon_k}^{\epsilon_k} \)
- \( s_\epsilon = \nu_{P, Q_\epsilon}(-\infty) - \nu_{P, Q_\epsilon}(\infty) \)
- \( c_\varphi = \# \) of distinct real roots \( c \) of \( P \) such that the sign of \( Q_i(c) \) is \((-1)^{\varphi_i}\)

- Let \( s \) (resp. \( c \)) be the vector whose coordinates are all \( s_\epsilon \) (resp. \( c_\varphi \))

Lemma
There is an invertible \( 2^k \times 2^k \) matrix \( A_k \), depending only on \( k \), such that \( s = A_{\ell} \cdot c \).
Multiple inequalities

\[ Q_1 > 0, \ldots, Q_n > 0 \]

- The system is satisfied on an unbounded interval iff the leading coefficients of \( Q_1, \ldots, Q_n \) or \( Q_1(-X), \ldots, Q_n(-X) \) are all positive.

- Let \( Q = \prod_{i=1}^{n} Q_i \). The system is satisfied iff the system \( Q' = 0, Q_1 > 0, \ldots, Q_n > 0 \) has a real solution.
Example

\( f(x) = -x^2 + 1 \)

\( g(x) = x^3 - 3x + 1 \)

\( (g*f)(x) \)

\( (g*f)'(x) \)
Quantifier elimination
[A. Tarski 1951, A. Seidenberg 1952]

Let $S(T, X)$ be system of polynomial equations/inequalities in the variables $T = (T_1, \ldots, T_n)$ and $X$.

There exists a disjunction $C$ of polynomial equations/equalities $C_1(T) \lor \ldots \lor C_n(T)$ which is equivalent to $\exists X \ S(T, X)$. $C$ is computable.
Tarski’s algorithm has NONELEMENTARY complexity
(excision time not bound by a tower of $2^{2^n}$)
Cylindrical algebraic decomposition (George Collins, 1975)
Worst case runtime is doubly exponential
Thank you.
Michel Coste.
An introduction to semialgebraic geometry.