Non-linear Arithmetic
SAT/SMT Summer School 2014

Leonardo de Moura
Microsoft Research
Slides at: http://leodemoura.github.io/
IMO

[2001] For all $a, b, c > 0$, prove that

$$\frac{a}{\sqrt{a^2 + 8bc}} + \frac{b}{\sqrt{b^2 + 8ca}} + \frac{c}{\sqrt{c^2 + 8ab}} \geq 1$$

[2005] For all $x, y, z > 0$, $xyz \geq 1$, prove that

$$\frac{x^5 - x^2}{x^5 + y^2 + z^2} + \frac{y^5 - y^2}{x^2 + y^5 + z^2} + \frac{z^5 - z^2}{x^2 + y^2 + z^5} \geq 0.$$
Polynomial Constraints

AKA
Existential Theory of the Reals

\[ x^2 - 4x + y^2 - y + 8 < 1 \]
\[ xy - 2x - 2y + 4 > 1 \]
How hard is $\exists R$?

PSPACE

$\exists R$

NP

PSPACE membership
Canny – 1988,
Grigor’ev – 1988

NP-hardness

$x$ is “Boolean” $\rightarrow x(x-1) = 0$

$x$ or $y$ or $z$ $\rightarrow x + y + z > 0$
Example

\[ x_1 \geq 2, \quad x_1 = 2 \]
\[ x_2 \geq x_1^2, \quad x_2 = 4 \]
\[ x_3 \geq x_2^2, \quad x_3 = 16 \]
\[ \ldots \]
\[ x_n \geq x_{n-1}^2, \quad x_n = 2^{2^n} \]
Main Techniques

High-School Level Procedures - Cohen, Muchnick, Hormander 60’s

Wu’s method for Geometry Theorem Proving - Wu 1983

Solving equations in $\mathbb{C}$ via Gröbner Basis - Buchberger 1985

CAD: Cylindrical Algebraic Decomposition 70’s

Ben-Or, Kozen, Reif’s doubly exponential procedure 80’s

VTS: Virtual Term Substitution (Weispfenning 1988)

Special cases (e.g., quadratic, cubic) for QE

ICP: Interval Constraint Propagation
Polynomials

Univariate
\[ x^3 - x + 1 \]

Multivariate
\[ xy^5 - x^2z^2 + 1 \]
Reduction to a single equation

\[ p \neq 0 \]
\[ p \geq 0 \]
\[ p > 0 \]
\[ p = 0 \land q = 0 \]
\[ p = 0 \lor q = 0 \]

\[ \exists k, p \cdot k - 1 = 0 \]
\[ \exists k, p - k^2 = 0 \]
\[ \exists k, p \cdot k^2 - 1 = 0 \]
\[ p^2 + q^2 = 0 \]
\[ p \cdot q = 0 \]
Example

\[ xy \geq 1 \land x < 0 \]

\[ xy - 1 \geq 0 \land -x > 0 \]

\[ xy - 1 - k_1^2 = 0 \land -x > 0 \]

\[ xy - 1 - k_1^2 = 0 \land -xk_2^2 - 1 = 0 \]

\[ (xy - 1 - k_1^2)^2 + (-xk_2^2 - 1)^2 = 0 \]

\[ x^2y^2 - 2xy + k_1^4 - 2k_1^2xy + 2k_1^2 + k_2^4x^2 + 2k_2^2x + 2 = 0 \]
Polynomial division (univariate)

\[
polydiv(f, g)
\]
\[
q := 0
\]
\[
r := f
\]
\[
while \text{deg}(r) \geq \text{deg}(g)
\]
\[
\text{invariant } f = q \cdot g + r
\]
\[
d := \text{deg}(r) - \text{deg}(g)
\]
\[
q := q + \frac{\text{lc}(r)}{\text{lc}(g)} \cdot x^d
\]
\[
r := r - \frac{\text{lc}(r)}{\text{lc}(g)} \cdot x^d \cdot g
\]
Example

\( f: 3x^3 + x^2 + 1, \quad g: x^2 + 1 \)

\( q := 0, \quad r := 3x^3 + x^2 + 1, \)

\( \text{lc}(r) = 3, \quad \text{lc}(g) = 1, \quad \text{deg}(r) - \text{deg}(g) = 1 \)

\( q := 3x, \quad r := 3x^3 + x^2 + 1 - 3x(x^2 + 1) = x^2 - 3x + 1 \)

\( \text{lc}(r) = 1, \quad \text{deg}(r) - \text{deg}(g) = 0 \)

\( q := 3x + 1, \quad r := x^2 - 3x + 1 - 1(x^2 + 1) = -3x \)

\[
\begin{align*}
\textbf{f} &= \quad \textcolor{green}{q} \quad \cdot \quad \textcolor{blue}{g} \quad + \quad \textcolor{red}{r} \\
3x^3 + x^2 + 1 &= (3x + 1)(x^2 + 1) - 3x
\end{align*}
\]
Important

\[ f = q \cdot g + r \]

If \[ g(a) = 0 \]

Then \[ f(a) = r(a) \]

The **sign** of \( f \) at a root (aka zero) \( a \) of \( g \) is equal to the sign of \( r \) at \( a \)
Polynomial Sequence

\[ S = \langle p_0, p_1, \ldots, p_m \rangle \]

\( \text{Var}(S, a) \): number of sign variations at \( a \)

Example
\[ S = \langle 3x^4 - 3x^2 - 2, 12x^3 - 6x, x^2 + 1, x - 1, -1 \rangle \]

at 1
\[ \langle -2, 6, 2, 0, -1 \rangle \]

\( \text{Var}(S, 1) = 2 \)
Sturm Sequence for \((f, g)\)

\[
\begin{align*}
    h_0 &= f \\
    h_1 &= g \\
    h_0 &= q_1 h_1 - h_2 \\
    h_1 &= q_1 h_2 - h_3 \\
    \quad \vdots \\
    h_{i-1} &= q_i h_i - h_{i+1} \\
    \quad \vdots \\
    h_{n-1} &= q_n h_n
\end{align*}
\]

\[
\begin{align*}
    h_0 &= f \\
    h_1 &= g \\
    h_2 &= -\text{rem}(h_0, h_1) \\
    h_3 &= -\text{rem}(h_1, h_2) \\
    \quad \vdots \\
    h_{i+1} &= -\text{rem}(h_{i-1}, h_i) \\
    \quad \vdots \\
    h_n &= -\text{rem}(h_{n-2}, h_{n-1}) \\
    \text{rem}(h_{n-1}, h_n) &= 0
\end{align*}
\]
Sturm Sequence for \((f, g)\)

\[
\begin{align*}
h_0 &= f \\
h_1 &= g \\
h_0 &= q_1 h_1 - h_2 \\
h_1 &= q_1 h_2 - h_3 \\
&\quad\vdots \\
h_{i-1} &= q_i h_i - h_{i+1} \\
&\quad\vdots \\
h_{n-1} &= q_n h_n \\
\text{forall } 0 \leq i \leq n, \\
h_0(a) &= h_1(a) = 0 \\
&\quad\Rightarrow h_i(a) = 0 \\
h_n(a) &= 0 \\
&\quad\Rightarrow h_i(a) = 0 \\
h_j(a) &= 0, h_{j+1}(a) = 0 \\
&\quad\Rightarrow h_i(a) = 0
\end{align*}
\]
Sturm Theorem

\[ S = Sturm(f, f'), a < b, f(a) \neq 0, f(b) \neq 0 \]

\[ f' \text{ is the derivative of } f \]

\[ \Rightarrow \]

\[ Var(S, a) - Var(S, b) = \#\{c \mid a < c < b, f(c) = 0\} \]

Number of zeros in \((a, b)\)
Example

\[ h_0 = f = x^4 - 10x^3 + 32x^2 - 38x + 15 \]
\[ h_1 = f' = 4x^3 - 30x^2 + 64x - 38 \]
\[ h_2 = -\text{rem}(h_0, h_1) = \frac{11}{4} x^2 - \frac{23}{2} x + \frac{35}{4} \]
\[ h_3 = -\text{rem}(h_1, h_2) = \frac{512}{121} x - \frac{512}{121} \]
Example

\[ h_0 = f = x^4 - 10x^3 + 32x^2 - 38x + 15 \]
\[ h_1 = f' = 4x^3 - 30x^2 + 64x - 38 \]
\[ h_2 = -\text{rem}(h_0, h_1) \sim 11x^2 - 46x + 35 \]
\[ h_3 = -\text{rem}(h_1, h_2) \sim x - 1 \]
Example

\[ f = (x - 1)^2(x - 3)(x - 5) \]

\[ h_0 = f = x^4 - 10x^3 + 32x^2 - 38x + 15 \]

\[ h_1 = f' = 4x^3 - 30x^2 + 64x - 38 \]

\[ h_2 = -\text{rem}(h_0, h_1) \sim 11x^2 - 46x + 35 \]

\[ h_3 = -\text{rem}(h_1, h_2) \sim x - 1 \]

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>2</th>
<th>4</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>( h_0 )</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>( h_1 )</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>( h_2 )</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>( h_3 )</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
Simple procedure

We can already decide formulas such as

\[ p = 0, \quad p > 0, \quad p < 0 \]

Example: \( x^2 + 1 < 0 \)

<table>
<thead>
<tr>
<th></th>
<th>-∞</th>
<th>∞</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x^2 + 1 )</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>( 2x )</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>(-1)</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Only the signs of the leading coefficients matter at \(-\infty\) and \(\infty\)
Sturm-Tarski Theorem

\[ S = Sturm(f, f'g), a < b, f(a) \neq 0, f(b) \neq 0 \]

\( f' \) is the derivative of \( f \)

\[ \Rightarrow \]

\[ \Var(S, a) - \Var(S, b) = \]

\[ \#\{c \mid a < c < b, f(c) = 0, g(c) > 0\} \]

\[ - \]

\[ \#\{c \mid a < c < b, f(c) = 0, g(c) < 0\} \]

\[ TaQ(g, f; (a, b)) \]

\[ TaQ(g, f) = TaQ(g, f; (-\infty, \infty)) \]
Sturm-Tarski Theorem

\[ TaQ(g, f) = \#\{c \mid f(c) = 0, g(c) > 0\} - \#\{c \mid f(c) = 0, g(c) < 0\} \]

\[ TaQ(1, f) = \text{Numbers of zeros (roots) of } f \]

\[ TaQ(g, f) = \#(g > 0) - \#(g < 0) \]

\[ TaQ(g^2, f) = \#(g > 0) + \#(g < 0) \]

\[ TaQ(1, f) = \#(g = 0) + \#(g > 0) + \#(g < 0) \]
System of equations

<table>
<thead>
<tr>
<th>(#(g = 0))</th>
<th>(#(g &gt; 0))</th>
<th>(#(g &lt; 0))</th>
<th>(TaQ(1, f))</th>
<th>(TaQ(g, f))</th>
<th>(TaQ(g^2, f))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>-1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
New procedure

Now, we can decide formulas such as

\[ f = 0 \land g < 0, \quad f = 0 \land g = 0, \]
\[ f = 0 \land g > 0 \]
New procedure

Now, we can decide formulas such as

\[ f = 0 \land g > 0 \]

Example: \( x^2 - 1 = 0 \land x + 1 > 0 \)

\[
\begin{array}{|c|c|c|c|}
\hline
#(g = 0) & #(g > 0) & #(g < 0) & \\
\hline
1 & 1 & 1 & TaQ(1, f) = 2 \\
0 & 1 & -1 & TaQ(g, f) = 1 \\
0 & 1 & 1 & TaQ(g^2, f) = 2 \\
\hline
\end{array}
\]
New procedure

Now, we can decide formulas such as

\[ f = 0 \land g > 0 \]

Example: \( x^2 - 1 = 0 \land x + 1 > 0 \)

\[
\begin{array}{|c|c|c|c|}
\hline
(g = 0) & (g > 0) & (g < 0) & \text{TaQ}(g, f) \\
\hline
1 & 1 & 1 & 2 \\
0 & 1 & -1 & 1 \\
0 & 1 & 1 & 2 \\
\hline
\end{array}
\]

\[#(g = 0) = 1, #(g > 0) = 1, #(g < 0) = 0\]
New procedure

Now, we can decide formulas such as

\[ f = 0 \land g > 0 \]

What about \( x^2 - 1 = 0 \land x + 1 < 0 \)?

<table>
<thead>
<tr>
<th>((g = 0))</th>
<th>((g &gt; 0))</th>
<th>((g &lt; 0))</th>
<th>(TaQ(g, f))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

\[ \#(g = 0) = 1, \#(g > 0) = 1, \#(g < 0) = 0 \]
Sturm-Tarski Theorem

\[ \text{TaQ}(g_1g_2, f) = \# \{ c \mid f(c) = 0, g_1(c)g_2(c) > 0 \} \]
\[- \# \{ c \mid f(c) = 0, g_1(c)g_2(c) < 0 \} \]
\[= \#(g_1 > 0, g_2 > 0) + \#(g_1 < 0, \#g_2 < 0) \]
\[- \#(g_1 > 0, g_2 < 0) - \#(g_1 < 0, \#g_2 > 0) \]
Sturm-Tarski Theorem

\[ TaQ(g_1^2 g_2, f) = \#\{c \mid f(c) = 0, g_1^2(c)g_2(x) > 0\} \]
\[-\#\{c \mid f(c) = 0, g_1^2(c)g_2(x) < 0\} \]
\[= \#(g_1 > 0, g_2 > 0) + \#(g_1 < 0, g_2 > 0)\]
\[-\#(g_1 > 0, g_2 < 0) - \#(g_1 < 0, g_2 < 0)\]
New procedure

Now, we can decide formulas such as

\[ f = 0 \land g_1 < 0 \land g_2 < 0, \]
\[ f = 0 \land g_1 > 0 \land g_2 < 0, \ldots \]

We can generalize to \( \{f, g_1, g_2, \ldots, g_k\} \)

\( 3^k \) equations!
We can do better than $3^k$

Ben-Or, Kozen, Reif Optimization

Number of zeros (roots) of $f \ll 3^k$

Each “unknown” is an integer $\geq 0$

Solve the system incrementally!

$f, \{g_1\}$

Suppose $\#(g_1 > 0) = 0 \rightarrow \#(g_1 > 0,*) = 0$

Found $3^{k-1}$ zeros!

$f, \{g_1, g_2\}$

...
Missing case

What about formulas such as

\[ g_1 < 0 \land g_2 > 0 \]

?
Given \( \{g_1, \ldots, g_k\} \), take \( f = g_1 \cdots g_k \)

1) \( TaQ(1, f) = 0 \)

\( g_i \)'s have constant sign, use sign of leading coefficients.

2) \( TaQ(1, f) = 1 \)

\( g_i \)'s have at most one zero, use leading coefficients to compute sign at \(-\infty\) and \(\infty\).

3) \( TaQ(1, f) > 1 \)

\(-\infty, \infty, \) and \( f' = 0 \) contains all realizable sign conditions.
Multivariate case

\[ y^2z^2 + z^2 + xyz + z + x^3 + y^2 \]

\[ \Rightarrow \]

\[ (y^2 + 1)z^2 + (xy + 1)z + (x^3 + y^2) \]

\( TaQ(g, f) \) only uses the sign of the leading coefficients.
Pseudo Polynomial Division

\[(y^2 + 1)z^2 + (xy + 1)z + (x^3 + y^2)\]
is a polynomial in \(\mathbb{Q}[x, y](z)\)

The previous decision algorithm does not work. \(\mathbb{Q}[x, y]\) does not have multiplicative inverse!

Trick (clean denominators)
\[lc(g)^k f = q g + r\]
Pseudo Polynomial Division

polydiv(f, g)
q := 0
r := f
l := 1
while \( \deg(r) \geq \deg(g) \)
  invariant l.f = q.g + r
  l := lc(g).l
  q := lc(g).q
  r := lc(g).r
  d := \deg(r) - \deg(g)
  q := q + lc(r)/lc(g).x^d
  r := r - lc(r)/lc(g).x^d.g
Pseudo Polynomial Division

polydiv(f, g)

\[ q := 0 \]
\[ r := f \]
\[ l := 1 \]

while \( \deg(r) \geq \deg(g) \)

\[ \text{invariant } l.f = q.g + r \]
\[ l := lc(g).l \]
\[ d := \deg(r) - \deg(g) \]
\[ q := lc(g).q + lc(r).x^d \]
\[ r := lc(g).r - lc(r).x^d.g \]
Example

\[ f : z^2 + 1 \quad g : xz + 1 \]

\[ q = 0, \]
\[ r = z^2 + 1 \]
\[ l = 1 \]
\[ q = z \]
\[ r = x(z^2 + 1) - z(xz + 1) = -z + x \]
\[ l = x \]
\[ q = xz - 1 \]
\[ r = x(-z + x) - (-1)(xz + 1) = x^2 + 1 \]
\[ l = x^2 \]

We “want” \( \frac{lc(r)}{lc(g)} = \frac{1}{x} \)
Example

\[ f: z^2 + 1 \quad g: xz + 1 \]

\[ q = xz - 1 \]
\[ r = x^2 + 1 \]
\[ l = x^2 \]

\[ x^2(z^2 + 1) = (xz - 1)(xz + 1) + x^2 + 1 \]
Sturm “Tree” for multivariate poly

Branch on sign of the leading coefficient

\[ ax^2 + bx + c \]

- \( a \neq 0 \):
  - \( a < 0 \):
    - \( \delta < 0 \):
      - \( \delta = 0 \):
        - \( \delta > 0 \):
          - \( a < 0 \):
            - \( \delta < 0 \):
              - \( \delta = 0 \):
                - \( \delta > 0 \):
      - \( \delta > 0 \):
    - \( a > 0 \):
      - \( \delta > 0 \):

- \( a = 0 \):
  - \( b \neq 0 \):
    - \( b > 0 \):
      - \( \delta = 0 \):
        - \( \delta > 0 \):
      - \( \delta < 0 \):
        - \( \delta = 0 \):
          - \( \delta > 0 \):
    - \( b = 0 \):
      - \( \delta < 0 \):
        - \( \delta = 0 \):
          - \( \delta > 0 \):
      - \( \delta = 0 \):
      - \( \delta > 0 \):

- \( \delta : b^2 - 4ac \)

- \( bx + c \):
  - \( b \neq 0 \):
    - \( b > 0 \):
      - \( \delta > 0 \):
    - \( \delta < 0 \):
      - \( \delta = 0 \):
        - \( \delta > 0 \):
  - \( b = 0 \):
    - \( \delta < 0 \):
      - \( \delta = 0 \):
        - \( \delta > 0 \):

- \( c \)
Sturm “Tree” for multivariate poly

Branch on sign of the leading coefficient

\[ ax^2 + bx + c \]

- \( a \neq 0 \)
- \( a = 0 \)

- \( ax^2 + bx + c \)
- \( 2ax + b \)
- \( \delta: b^2 - 4ac \)

- \( a < 0 \)
- \( a > 0 \)

- \( \delta < 0 \)
- \( \delta = 0 \)
- \( \delta > 0 \)
\[ ax^2 + bx + c \]

Assumptions
\[ a > 0 \]
\[ b^2 - 4ac < 0 \]

\[ \begin{array}{cc}
-\infty & \infty \\
ax^2 + bx + c & + & + \\
2ax + b & - & + \\
b^2 - 4ac & - & - \\
\end{array} \]

No zero
\[ ax^2 + bx + c \]

Assumptions
\[ a > 0 \]
\[ b^2 - 4ac = 0 \]

| \[ ax^2 + bx + c \] | \(-\infty\) | \(\infty\) |
| \[ 2ax + b \] | + | + |
| \[ b^2 - 4ac \] | 0 | 0 |

1 zero
\[ ax^2 + bx + c \]

Assumptions
\[ a > 0 \]
\[ b^2 - 4ac > 0 \]

<table>
<thead>
<tr>
<th>( ax^2 + bx + c )</th>
<th>(-\infty)</th>
<th>(\infty)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2ax + b )</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>( b^2 - 4ac )</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

2 zeros
Model-guided procedure

Build model incrementally (like a SAT solver)
Given polynomials \( \{g_1, \ldots, g_k\} \) in \( \mathbb{Q}[\hat{y}](x) \)
An assignment for \( \hat{y} \)
We have to consider only one branch of the tree!
Example: \( a := 1, b := 2, c := 1 \)

\[ ax^2 + bx + c \quad a > 0 \]
\[ 2ax + b \quad b^2 - 4ac = 0 \]
\[ b^2 - 4ac \]
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$

$3x^4 + 2x^2 + 1 < 0$

No solutions
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$

$3x^4 + 2x^2 + 1 < 0$

No solutions

Idea: Generalize the inconsistency using the corresponding branch of the Sturm tree

$(y + 2)x^4 + (y^2 + 1)x^2 + 1 \quad y + 2 > 0$
$4(y + 2)x^3 + 2(y^2 + 1)x$
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$

$3x^4 + 2x^2 + 1 < 0$

Idea: Generalize the inconsistency using the corresponding branch of the Sturm tree

$(y + 2)x^4 + (y^2 + 1)x^2 + 1 \quad y + 2 > 0$
$4(y + 2)x^3 + 2(y^2 + 1)x \quad y^2 + 1 > 0$
$-(y^2 + 1)x^2 - 1$
Example: \( y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0 \)

Assign: \( y := 1 \)

\( 3x^4 + 2x^2 + 1 < 0 \)

No solutions

Idea: Generalize the inconsistency using the corresponding branch of the Sturm tree

\[
(y + 2)x^4 + (y^2 + 1)x^2 + 1 \quad y + 2 > 0 \\
4(y + 2)x^3 + 2(y^2 + 1)x \quad y^2 + 1 > 0 \\
-(y^2 + 1)x^2 - 1 \\
(-y^4 - 2y^2 + 2y + 3)x \quad -y^4 - 2y^2 + 2y + 3 > 0
\]
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$

$3x^4 + 2x^2 + 1 < 0$

No solutions

Idea: Generalize the inconsistency using the corresponding branch of the Sturm tree

$$(y + 2)x^4 + (y^2 + 1)x^2 + 1 \quad y + 2 > 0$$

$$4(y + 2)x^3 + 2(y^2 + 1)x \quad y^2 + 1 > 0$$

$$-(y^2 + 1)x^2 - 1$$

$$-y^4 - 2y^2 + 2y + 3 \quad -y^4 - 2y^2 + 2y + 3 > 0$$

1
Example: \( y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0 \)

Assign: \( y := 1 \)

\[
\begin{align*}
(y + 2)x^4 + (y^2 + 1)x^2 + 1 &> 0 \\
4(y + 2)x^3 + 2(y^2 + 1)x &> 0 \\
-(y^2 + 1)x^2 - 1 &< 0 \\
(-y^4 - 2y^2 + 2y + 3)x &< 0 \\
1 &> 0
\end{align*}
\]
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$

$y + 2 > 0$

$y^2 + 1 > 0$

$-y^4 - 2y^2 + 2y + 3 > 0$

$-(y^2 + 1)x^2 - 1$  
$(-y^4 - 2y^2 + 2y + 3)x$  
$1$

$(y + 2)x^4 + (y^2 + 1)x^2 + 1 > 0$
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y \equiv 1$

\[
\begin{align*}
(y + 2)x^4 + (y^2 + 1)x^2 + 1 &> 0 \\
4(y + 2)x^3 + 2(y^2 + 1)x &> 0 \\
-(y^2 + 1)x^2 - 1 &> 0 \\
(-y^4 - 2y^2 + 2y + 3)x &> 0 \\
1 &> 0
\end{align*}
\]


tables

(y + 2)x^4 + (y^2 + 1)x^2 + 1 > 0
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$

$y + 2 > 0$

REDUNDANT $-y^4 - 2y^2 + 2y + 3 > 0$

$$
\begin{array}{c|cc}
& -\infty & \infty \\
\hline
(y + 2)x^4 + (y^2 + 1)x^2 + 1 & + & + \\
4(y + 2)x^3 + 2(y^2 + 1)x & - & + \\
-(y^2 + 1)x^2 - 1 & - & - \\
(-y^4 - 2y^2 + 2y + 3)x & - & + \\
1 & + & + \\
\end{array}
$$

$(y + 2)x^4 + (y^2 + 1)x^2 + 1 > 0$
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$

\[ y + 2 > 0 \]

\[ (y + 2)x^4 + (y^2 + 1)x^2 + 1 > 0 \]
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$

\[ \neg (y + 2 > 0) \lor (y + 2)x^4 + (y^2 + 1)x^2 + 1 > 0 \]

\[ \neg (y + 2 > 0) \lor (y + 2)x^4 + (y^2 + 1)x^2 + 1 \geq 0 \]

\[ \neg (y + 2 > 0) \lor \neg((y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0) \]
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$

$\neg (y + 2 > 0) \lor \neg((y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0)$

Resolvent: $\neg(y + 2 > 0)$

The resolvent "blocks" $y := 1$, and many other values.
Example: $y > 0 \land (y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0$

Assign: $y := 1$

$$\neg (y + 2 > 0) \lor \neg ((y + 2)x^4 + (y^2 + 1)x^2 + 1 < 0)$$

Resolvent: $\neg (y + 2 > 0)$

The resolvent "blocks" $y := 1$, and many other values.

The problem is unsat
$$y > 0 \land \neg (y + 2 > 0) \equiv y \leq -2$$
How do we represent an assignment?

Real algebraic numbers

$$\sqrt{2} + \sqrt{3}$$

$$\sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}}$$

First zero of $$x^5 - x + 1$$
Tower of algebraic extensions

\( \mathbb{Q}(\alpha_1) \ldots (\alpha_k) \)
Tower of extensions

(Computable) ordered field $K$

Operations: $+$, $-$, $\times$, $\text{inv}$, $\text{sign}$

$$a < b \iff \text{sign}(a - b) = -1$$

Approximation: $\text{approx}(a) \in B_\infty$-interval

$$B_\infty = B \cup \{-\infty, \infty\}$$

$$a \neq 0 \Rightarrow 0 \not\in \text{approx}(a)$$

Refine approximation
Algebraic Extensions

\[ K(\alpha) \]
\[ \alpha \text{ is a root of a polynomial with coefficients in } K \]

Encoding \( \alpha \) as polynomial + interval
Algebraic Extensions

The elements of $K(\alpha)$ are polynomials $q(\alpha)$.

Implement $+,-,\times$ using polynomial arithmetic.

Compute sign (when possible) using interval arithmetic.
Algebraic Extensions

\[ \alpha = (-2 + x^2, (1,2), \{\}) \]

Let \( \alpha \) be \( q(\alpha) = 1 + \alpha^3 \)

We can normalize \( \alpha \) by computing the polynomial remainder.

\[
1 + x^3 = x(-2 + x^2) + (1 + 2x)
\]

\[
1 + \alpha^3 = \alpha(-2 + \alpha^2) + (1 + 2\alpha) = 1 + 2\alpha
\]

\[
a = rem(1 + x^3, -2 + x^2)(\alpha)
\]
Algebraic Extensions: non-minimal Polynomials

Computing the inverse of $q(\alpha)$, where $\alpha = (p, (a, b), S)$

Find $h(\alpha)$ s.t. $q(\alpha) \cdot h(\alpha) = 1$

Compute the extended GCD of $p$ and $q$.

$$r(x) p(x) + h(x) q(x) = 1$$

$$r(\alpha) p(\alpha) + h(\alpha) q(\alpha) = 1$$

0
Algebraic Extensions: non-minimal Polynomials

We only use square-free polynomials $p$ in $\alpha = (p, (a, b), S)$

They are not necessarily minimal in our implementation.

$p(x) = q(x)s(x)$

$K[x]/\langle p \rangle \cong K(\alpha)$

Solution: Dynamically refine $p$, when computing inverses.
1. **Project/Saturate** set of polynomials

2. **Lift/Search**: Incrementally build assignment \( \nu: x_k \rightarrow \alpha_k \)
   - Isolate roots of polynomials \( f_i(\alpha, x) \)
   - Select a feasible cell \( C \), and assign \( x_k \) some \( \alpha_k \in C \)
   - If there is no feasible cell, then backtrack
### CAD “Big Picture”

\[
x^2 + y^2 - 1 < 0 \\
x y - 1 > 0
\]

1. Saturate

\[
x^4 - x^2 + 1 \\
x^2 - 1 \\
x
\]

2. Search

<table>
<thead>
<tr>
<th></th>
<th>((-\infty, -1))</th>
<th>(-1)</th>
<th>((-1, 0))</th>
<th>(0)</th>
<th>((0, 1))</th>
<th>(1)</th>
<th>((1, \infty))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x^4 - x^2 + 1)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>(x^2 - 1)</td>
<td>+</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>+</td>
</tr>
<tr>
<td>(x)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
CAD “Big Picture”

\[ x^2 + y^2 - 1 < 0 \quad \text{and} \quad xy - 1 > 0 \]

1. Saturate

\[ x^4 - x^2 + 1 \quad \text{and} \quad x^2 - 1 \]

\[ x \]

<table>
<thead>
<tr>
<th>((-\infty, -\frac{1}{2}))</th>
<th>(-\frac{1}{2})</th>
<th>((-\frac{1}{2}, \infty))</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 + y^2 - 1</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>-2y - 1</td>
<td>+</td>
<td>0</td>
</tr>
</tbody>
</table>

2. Search

<table>
<thead>
<tr>
<th>((-\infty, -1))</th>
<th>-1</th>
<th>((-1, 0))</th>
<th>0</th>
<th>((0, 1))</th>
<th>1</th>
<th>((1, \infty))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x^4 - x^2 + 1)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>(x^2 - 1)</td>
<td>+</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>(x)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
CAD “Big Picture”

$x^2 + y^2 - 1 < 0$

$x y - 1 > 0$

$1. \text{ Saturate} \quad x^4 - x^2 + 1$

$x^2 - 1$

$x$

$x \rightarrow - 2$

$\text{2. Search}$

\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
& (-\infty, -\frac{1}{2}) & -\frac{1}{2} & (-\frac{1}{2},\infty) & 4 + y^2 - 1 & + & + & + \\
\hline
-2y - 1 & + & 0 & - & CONFLICT & - \\
\hline
\end{array}

\begin{array}{|c|c|c|c|c|c|c|c|c|}
\hline
& (-\infty, -1) & -1 & (-1, 0) & 0 & (0, 1) & 1 & (1, \infty) \\
\hline
x^4 - x^2 + 1 & + & + & + & + & + & + & + \\
\hline
x^2 - 1 & + & 0 & - & - & - & 0 & + \\
\hline
x & - & - & - & 0 & + & + & + \\
\hline
\end{array}
Delineability

\[ x^2 + y^2 + z^2 = 1 \]
Resources

http://tinyurl.com/ksb32xw