Non-linear Arithmetic

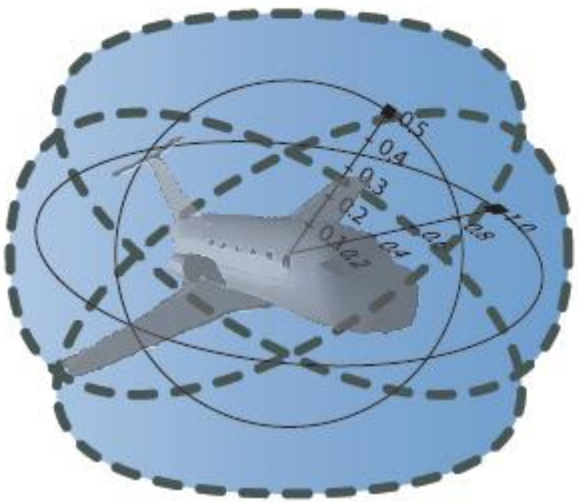
SAT/SMT Summer School 2014

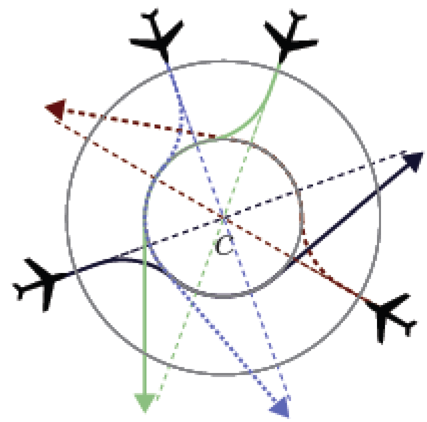
Leonardo de Moura

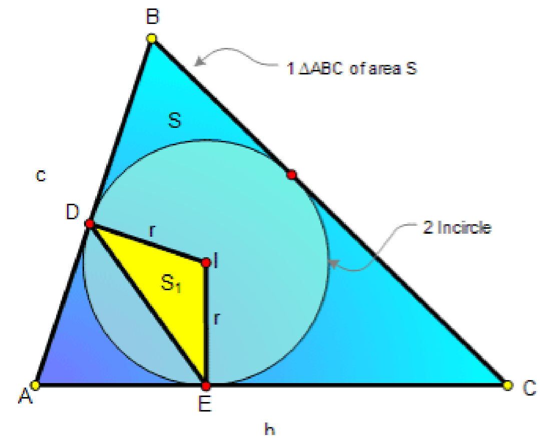
Microsoft Research

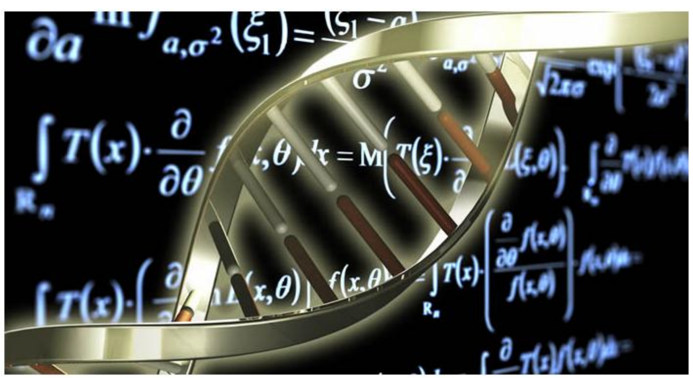
Slides at: http://leodemoura.github.io/

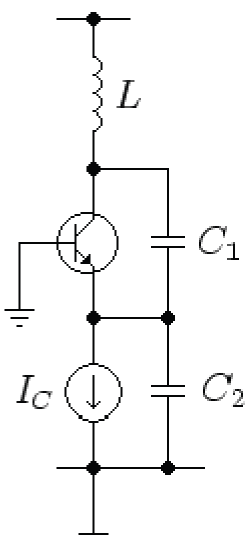
Applications











IMO

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

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

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

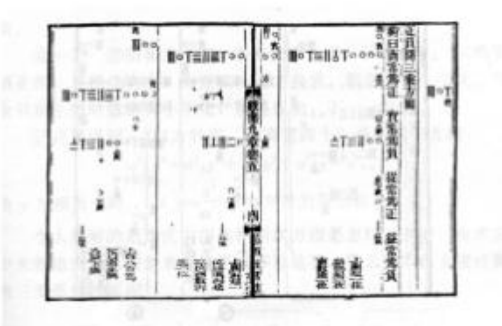
$$\frac{x^5 - x^2}{x^5 + y^2 + z^2} + \frac{y^5 - y^2}{x^2 + y^5 + z^2} + \frac{z^5 - z^2}{x^2 + y^2 + z^5} \geq 0.$$

Polynomial Constraints

AKA
Existential Theory of the Reals
∃R

$$x^2 - 4x + y^2 - y + 8 < 1$$
$$xy - 2x - 2y + 4 > 1$$

Milestones

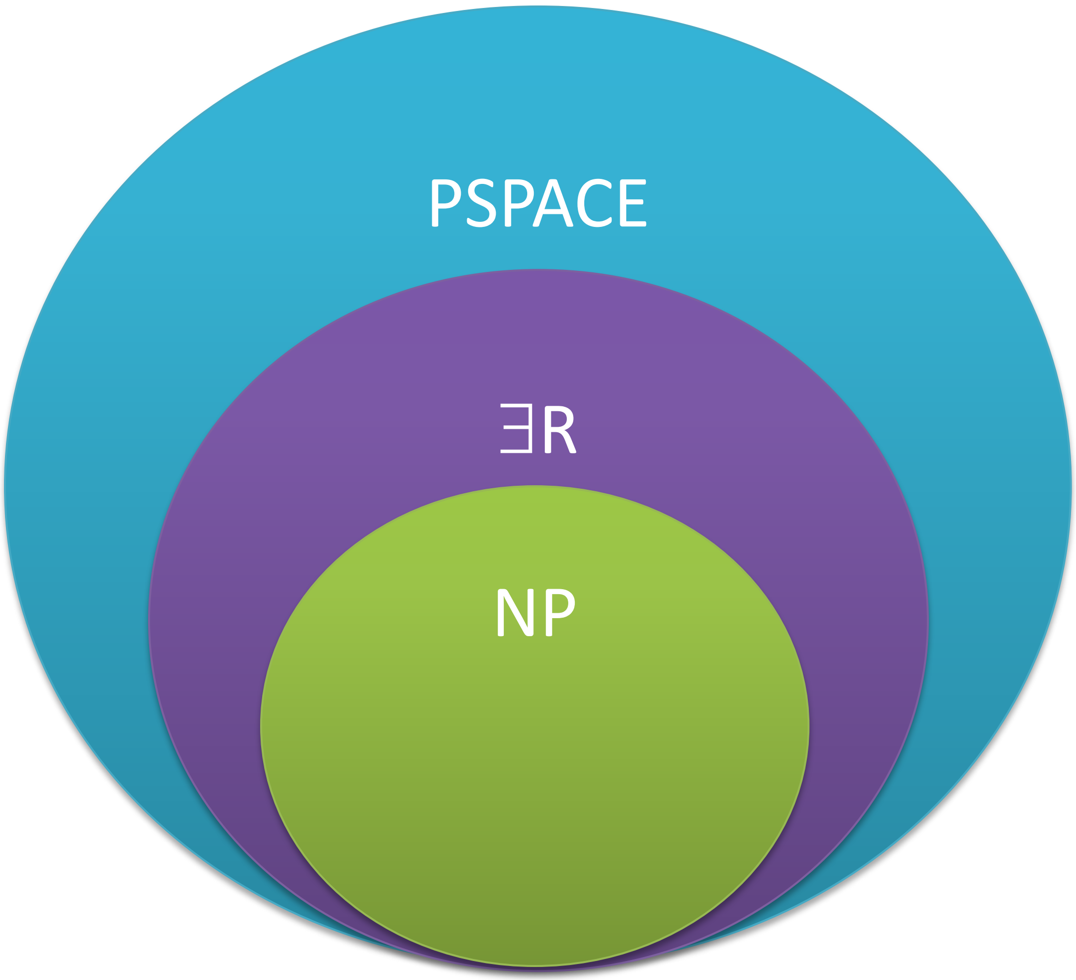


RCF admits QE
non elementary complexity

820 1247 1637 1732 1830 1835 1876 1930 1975

QE by CAD
Doubly exponential

How hard is ∃R?



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

$$x_1 \geq 2, \qquad x_1 = 2$$

$$x_2 \geq x_1^2, \qquad x_2 = 4$$

$$x_3 \geq x_2^2, \qquad x_3 = 16$$

$$\dots$$

$$x_n \geq x_{n-1}^2, \qquad x_n = 2^{2^n}$$

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

$p \neq 0$	$\exists\, k, p.k - 1 = 0$
$p \geq 0$	$\exists k, p - k^2 = 0$
$p > 0$	$\exists k, p.k^2 - 1 = 0$
$p = 0 \wedge q = 0$	$p^2 + q^2 = 0$
$p = 0 \vee q = 0$	$p.q = 0$

Example

$$xy \geq 1 \wedge x < 0$$

$$xy - 1 \geq 0 \wedge -x > 0$$

$$xy - 1 - k_1^2 = 0 \wedge -x > 0$$

$$xy - 1 - k_1^2 = 0 \wedge -xk_2^2 - 1 = 0$$

$$(xy - 1 - k_1^2)^2 + (-xk_2^2 - 1)^2 = 0$$

$$x^2y^2 - 2xy + k_1^4 - 2k_1^2xy + 2k_1^2 + k_2^4x^2 + 2k_2^2x + 2 = 0$$

Polynomial division (univariate)

lc : leading coefficient

```
polydiv(f, g)
    q := 0
    r := f
    while deg(r)>= deg(g)
        invariant f = q.g + r
        d := deg(r)-deg(g)
        q := q + lc(r)/lc(g).x^d
        r := r - lc(r)/lc(g).x^d.g
```

Example

f: $3x^3 + x^2 + 1$,   g: $x^2 + 1$

q := 0   r := $3x^3 + x^2 + 1$,

lc(r) = 3, lc(g)=1, deg(r)-deg(g) = 1

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

lc(r)=1, deg(r)-deg(g) = 0

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

f = **q** . **g** + **r**

$$3x^3 + x^2 + 1 = (3x + 1)(x^2 + 1) - 3x$$

Important

$$f = q.g + r$$

If $\quad g(a) = 0$

Then $\quad f(a) = r(a)$

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

Polynomial Sequence

$$S = \langle p_0, p_1, \ldots, p_m \rangle$$

$Var(S,a)$: 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

$$\langle -2, \quad 6, \quad 2, \quad 0, \quad -1 \rangle$$

$Var(S,1) = 2$

Sturm Sequence for (f, g)

$$h_0 = f$$
$$h_1 = g$$
$$h_0 = q_1 h_1 - h_2$$
$$h_1 = q_1 h_2 - h_3$$
$$\ldots$$
$$h_{i-1} = q_i h_i - h_{i+1}$$
$$\ldots$$
$$h_{n-1} = q_n h_n$$

$$h_0 = f$$
$$h_1 = g$$
$$h_2 = -rem(h_0, h_1)$$
$$h_3 = -rem(h_1, h_2)$$
$$\ldots$$
$$h_{i+1} = -rem(h_{i-1}, h_i)$$
$$\ldots$$
$$h_n = -rem(h_{n-2}, h_{n-1})$$
$$rem(h_{n-1}, h_n) = 0$$

Sturm Sequence for (f, g)

$$h_0 = f$$
$$h_1 = g$$
$$h_0 = q_1 h_1 - h_2$$
$$h_1 = q_1 h_2 - h_3$$
$$\dots$$
$$h_{i-1} = q_i h_i - h_{i+1}$$
$$\dots$$
$$h_{n-1} = q_n h_n$$

forall $0 \le i \le n$,

$$h_0(a) = h_1(a) = 0$$
$$\Rightarrow h_i(a) = 0$$

$$h_n(a) = 0$$
$$\Rightarrow h_i(a) = 0$$

$$h_j(a) = 0, h_{j+1}(a) = 0$$
$$\Rightarrow h_i(a) = 0$$

Sturm Theorem

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

f' is the derivative of f

$\Rightarrow$

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

Number of zeros in (a, b)

Example

$$h_0 = f = x^4 - 10x^3 + 32x^2 - 38x + 15$$

$$h_1 = f' = 4x^3 - 30x^2 + 64x - 38$$

$$h_2 = -rem(h_0, h_1) = \frac{11}{4}x^2 - \frac{23}{2}x + \frac{35}{4}$$

$$h_3 = -rem(h_1, h_2) = \frac{512}{121}x - \frac{512}{121}$$

Example

$$h_0 = f = x^4 - 10x^3 + 32x^2 - 38x + 15$$

$$h_1 = f' = 4x^3 - 30x^2 + 64x - 38$$

$$h_2 = -rem(h_0, h_1) \sim 11x^2 - 46x + 35$$

$$h_3 = -rem(h_1, h_2) \sim x - 1$$

Example

$$f = (x-1)^2(x-3)(x-5)$$

$$h_0 = f = x^4 - 10x^3 + 32x^2 - 38x + 15$$

$$h_1 = f' = 4x^3 - 30x^2 + 64x - 38$$

$$h_2 = -rem(h_0, h_1) \sim 11x^2 - 46x + 35$$

$$h_3 = -rem(h_1, h_2) \sim x - 1$$

	0	2	4	6
h_0	+	+	-	+
h_1	-	+	-	+
h_2	+	-	+	+
h_3	-	+	+	+

Simple procedure

We can already decide formulas such as

$$p = 0, \qquad p > 0, \qquad p < 0$$

Example: $x^2 + 1 < 0$

	-∞	∞
$x^2 + 1$	+	+
$2x$	-	+
-1	-	-

Only the signs of the leading coefficients matter at $-\infty$ and ∞

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

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

$TaQ(1, f)$ = 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

$\#(g = 0)$	$\#(g > 0)$	$\#(g < 0)$	
1	1	1	$TaQ(1, f)$
0	1	-1	$TaQ(g, f)$
0	1	1	$TaQ(g^2, f)$

New procedure

Now, we can decide formulas such as

$$f = 0 \land g < 0,\ f = 0 \land g = 0,$$

$$f = 0 \land g > 0$$

New procedure

Now, we can decide formulas such as

$$f = 0 \wedge g > 0$$

Example: $x^2 - 1 = 0 \wedge x + 1 > 0$

$\#(g = 0)$	$\#(g > 0)$	$\#(g < 0)$	
1	1	1	$TaQ(1, f)$ = 2
0	1	-1	$TaQ(g, f) = 1$
0	1	1	$TaQ(g^2, f)$= 2

New procedure

Now, we can decide formulas such as

$$f = 0 \wedge g > 0$$

Example: $x^2 - 1 = 0 \wedge x + 1 > 0$

$\#(g = 0)$	$\#(g > 0)$	$\#(g < 0)$	
1	1	1	$TaQ(1, f)$ = 2
0	1	-1	$TaQ(g, f) = 1$
0	1	1	$TaQ(g^2, f)$= 2

$$\#(g = 0) = 1, \#(g > 0) = 1, \#(g < 0) = 0$$

New procedure

Now, we can decide formulas such as

$$f = 0 \wedge g > 0$$

What about $x^2 - 1 = 0 \wedge x + 1 < 0$?

$\#(g = 0)$	$\#(g > 0)$	$\#(g < 0)$	
1	1	1	$TaQ(1, f)$ = 2
0	1	-1	$TaQ(g, f) = 1$
0	1	1	$TaQ(g^2, f)$= 2

$$\#(g = 0) = 1, \#(g > 0) = 1, \#(g < 0) = 0$$

Sturm-Tarski Theorem

$$TaQ(g_1g_2, f) = \#\{c \mid f(c) = 0, g_1(c)g_2(c) > 0\}$$
$$- \#\{c \mid f(c) = 0, g_1(c)g_2(c) < 0\}$$

$$= \#(g_1 > 0, g_2 > 0) + \#(g_1 < 0, \#g_2 < 0)$$
$$- \#(g_1 > 0, g_2 < 0) - \#(g_1 < 0, \#g_2 > 0)$$

Sturm-Tarski Theorem

$$TaQ(g_1^2 g_2, f) = \#\{c\ | f(c) = 0, g_1^2(c) g_2(x) > 0\}$$
$$- \#\{c\ | f(c) = 0, g_1^2(c) g_2(x) < 0\}$$

$$= \#(g_1 > 0, g_2 > 0) + \#(g_1 < 0, \#g_2 > 0)$$
$$- \#(g_1 > 0, g_2 < 0) - \#(g_1 < 0, \#g_2 < 0)$$

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 ≥ 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

$$g_1 < 0 \wedge g_2 > 0$$

?

Given $\{g_1, \ldots, g_k\}$, take $f = g_1 \ldots g_k$

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 ∞.

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

$-\infty$, ∞, 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)>= 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)>= deg(g)
            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

$f: z^2 + 1 \quad g: xz + 1$

$q = 0,$

$r = z^2 + 1$

$l = 1$

We "want" $\frac{lc(r)}{lc(g)} = \frac{1}{x}$

$q = z$

$r = x(z^2 + 1) - z(xz + 1) = -z + x$

$l = x$

$q = xz - 1$

$r = x(-z + x) - (-1)(xz + 1) = x^2 + 1$

$l = x^2$

Example

$f: z^2 + 1 \quad g: xz + 1$

$q = xz - 1$

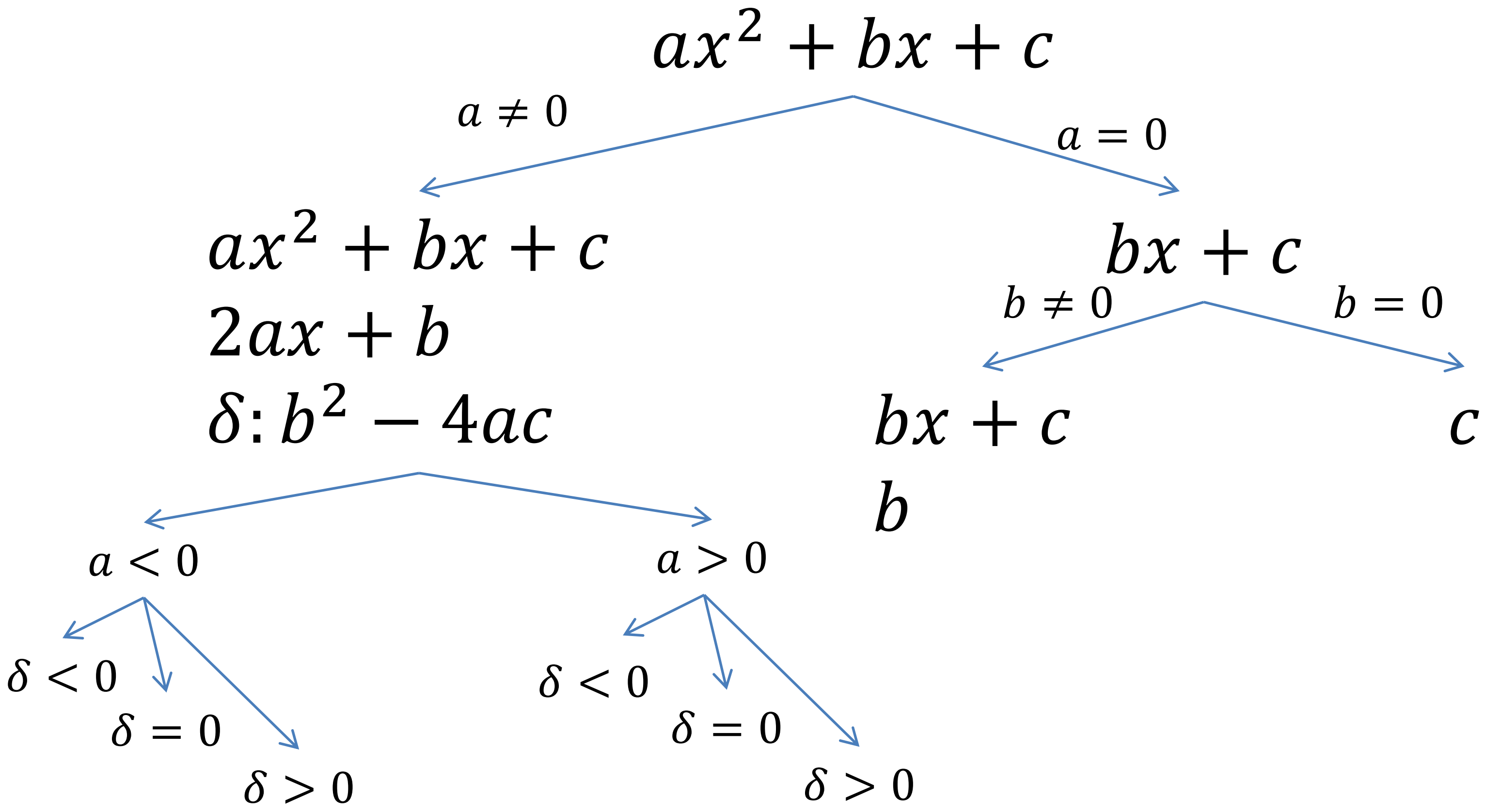
$r = x^2 + 1$

$l = x^2$

$x^2(z^2 + 1) = (xz - 1)(xz + 1) + x^2 + 1$

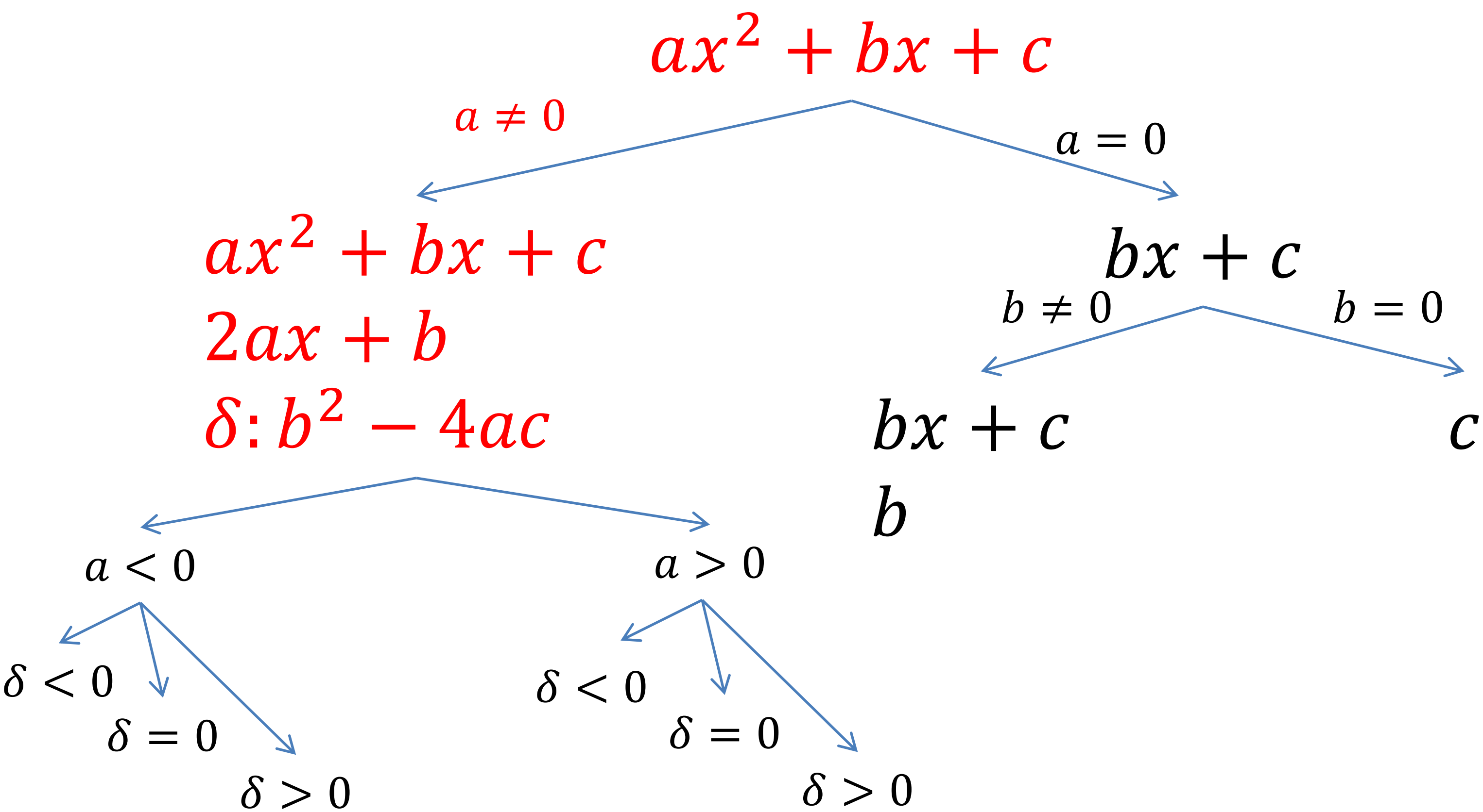
Sturm “Tree” for multivariate poly

Branch on sign of the leading coefficient



Sturm "Tree" for multivariate poly

Branch on sign of the leading coefficient



$$ax^2 + bx + c$$

Assumptions

$a > 0$

$b^2 - 4ac < 0$

	$-\infty$	∞
$ax^2 + bx + c$	+	+
$2ax + b$	-	+
$b^2 - 4ac$	-	-

No zero

$$ax^2 + bx + c$$

Assumptions

$a > 0$

$b^2 - 4ac = 0$

	$-\infty$	∞
$ax^2 + bx + c$	+	+
$2ax + b$	-	+
$b^2 - 4ac$	0	0

1 zero

$$ax^2 + bx + c$$

Assumptions

$a > 0$

$b^2 - 4ac > 0$

	$-\infty$	∞
$ax^2 + bx + c$	+	+
$2ax + b$	-	+
$b^2 - 4ac$	+	+

2 zeros

Model-guided procedure

Build model incrementally (like a SAT solver)

Given polynomials $\{g_1, \dots, g_k\}$ in $\mathbb{Q}[\vec{y}](x)$

An assignment for $\vec{y}$

We have to consider only one branch of the tree!

Example: $a \coloneqq 1, b \coloneqq 2, c \coloneqq 1$

$$ax^2 + bx + c \qquad a > 0$$
$$2ax + b \qquad b^2 - 4ac = 0$$
$$b^2 - 4ac$$

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

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

Assign: $y \coloneqq 1$

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

Assign: $y := 1$

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

No solutions

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

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

Assign: $y := 1$

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

No solutions

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

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

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

$-(y^2+1)x^2 - 1$ $\qquad y^2 + 1 > 0$

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

Assign: $y := 1$

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

No solutions

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

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

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

Assign: $y := 1$

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

No solutions

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

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

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

Assign: $y := 1$

$$y + 2 > 0$$

$$y^2 + 1 > 0$$

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

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

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

Assign: $y \coloneqq 1$

$y + 2 > 0$

$y^2 + 1 > 0$

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

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

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

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

Assign: $y \coloneqq 1$

$$y + 2 > 0$$

REDUNDANT $y^2 + 1 > 0$

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

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

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

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

Assign: $y \coloneqq 1$

$$y + 2 > 0$$

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

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

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

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

Assign: $y := 1$

$$y + 2 > 0$$

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

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

Assign: $y \coloneqq 1$

$$\neg\,(y+2>0) \vee (y+2)x^4 + (y^2+1)x^2 + 1 > 0$$

$$\Downarrow$$

$$\neg\,(y+2>0) \vee (y+2)x^4 + (y^2+1)x^2 + 1 \geq 0$$

$$\Updownarrow$$

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

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

Assign: $y \coloneqq 1$

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

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

The resolvent “blocks” $y \coloneqq 1$, and many other values.

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

Assign: $y := 1$

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

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

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

The problem is unsat

$$y > 0 \wedge \neg(y+2>0) \equiv y \le -2$$

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: $+,\ -,\ \times,\ inv,\ sign$

$$a < b \Leftrightarrow sign(a-b) = -1$$

Binary Rational
$$\frac{a}{2^k}$$

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

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

$$a \neq 0 \Rightarrow 0 \notin approx(a)$$

Refine approximation

Algebraic Extensions

$K(\alpha)$
α is a root of a polynomial with coefficients in K

Encoding α 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 a be $q(\alpha)$ = $1 + \ \alpha^3$

We can normalize a by computing the polynomial remainder.

Polynomial Remainder

$1 + \mathrm{x}^3 = x\,(-2 + x^2) + (1 + 2x)$

$1 + \ \alpha^3 = \alpha(-2 + \alpha^2) + (1 + 2\alpha) = 1 + 2\alpha$

$a = rem(1 + x^3, -2 + x^2)(\alpha)$

Algebraic Extensions: non-minimal Polynomials

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

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

Compute the extended GCD of p and q.

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

$$\underbrace{r(\alpha)p(\alpha)}_{0} + h(\alpha)q(\alpha) = 1$$

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

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

Only is p is minimal

Solution: Dynamically refine p, when computing inverses.

CAD "Big Picture"

1. Project/Saturate set of polynomials
2. Lift/Search: Incrementally build assignment v: $x_k \rightarrow \alpha_k$

    Isolate roots of polynomials $f_i(\boldsymbol{\alpha}, x)$

    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

	$(-\infty, -1)$	-1	$(-1, 0)$	0	$(0, 1)$	1	$(1, \infty)$
$x^4 - x^2 + 1$	+	+	+	+	+	+	+
$x^2 - 1$	+	0	-	-	-	0	+
x	-	-	-	0	+	+	+

CAD "Big Picture"

$\boldsymbol{x^2 + y^2 - 1} < 0$
$\boldsymbol{x\, y - 1} > 0$

1. Saturate

$x^4 - x^2 + 1$

$x^2 - 1$

x

	$(-\infty, -\frac{\mathbf{1}}{\mathbf{2}})$	$-\frac{\mathbf{1}}{\mathbf{2}}$	$(-\frac{\mathbf{1}}{\mathbf{2}}, \infty)$
$4 + y^2 - 1$	+	+	+
$-2\mathrm{y} - 1$	+	0	-

$\boldsymbol{x \to -2}$

2. Search

	$(\mathbf{-\infty, -1})$	$\mathbf{-1}$	$(\mathbf{-1, 0})$	$\mathbf{0}$	$(\mathbf{0, 1})$	$\mathbf{1}$	$(\mathbf{1, \infty})$
$x^4 - x^2 + 1$	+	+	+	+	+	+	+
$x^2 - 1$	+	0	-	-	-	0	+
x	-	-	-	0	+	+	+

CAD "Big Picture"

$\boldsymbol{x^2 + y^2 - 1 < 0}$

$x\,y - 1 > 0$

1. Saturate

$x^4 - x^2 + 1$

$x^2 - 1$

x

	$(-\infty, -\frac{1}{2})$	$-\frac{1}{2}$	$(-\frac{1}{2}, \infty)$
$\boldsymbol{4 + y^2 - 1}$	**+**	**+**	**+**
$-2y - 1$	+	0	-

CONFLICT

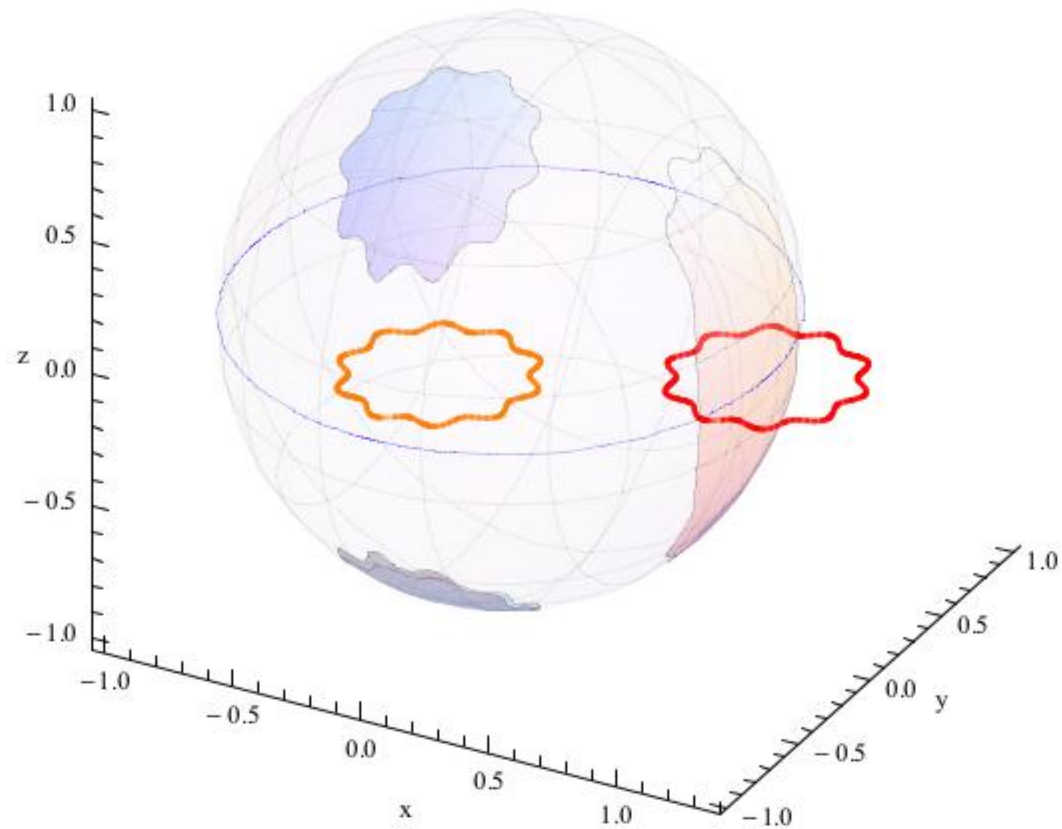
$\boldsymbol{x \to -2}$

2. Search

	$(-\infty, -1)$	-1	$(-1, 0)$	0	$(0, 1)$	1	$(1, \infty)$
$x^4 - x^2 + 1$	+	+	+	+	+	+	+
$x^2 - 1$	+	0	-	-	-	0	+
x	-	-	-	0	+	+	+

Delineability

$$x^2 + y^2 + z^2 = 1$$



Resources

http://tinyurl.com/ksb32xw