Solving Nonlinear Arithmetic

IJCAR 2012

Dejan Jovanović
NYU

Leonardo de Moura
Microsoft Research

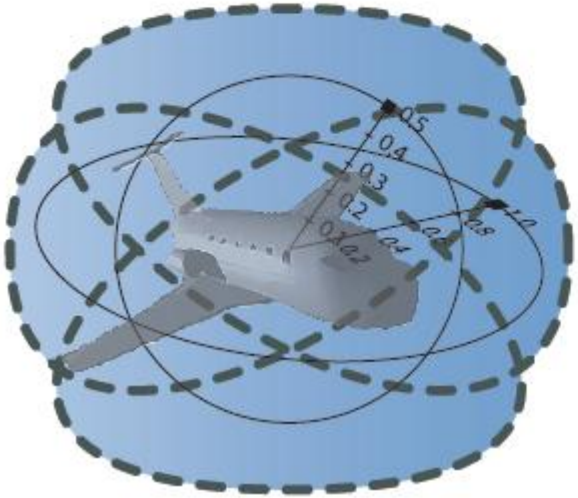
Polynomial Constraints

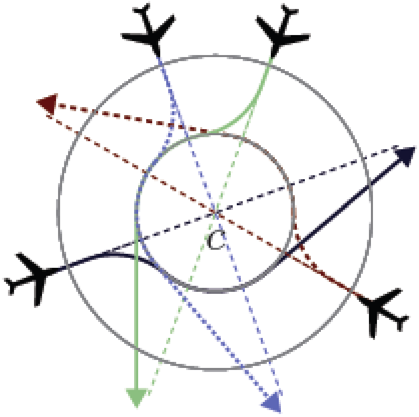
AKA
Existential Theory of the Reals
∃R

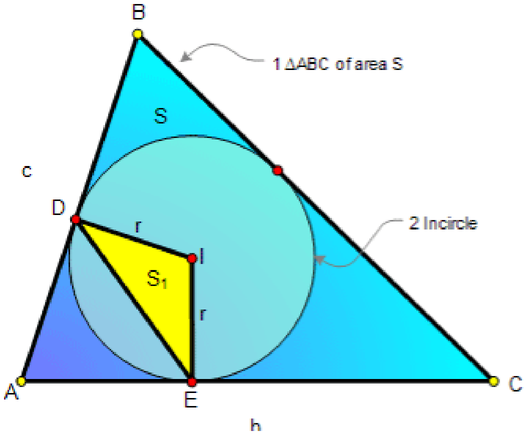
$$x^2 - 4x + y^2 - y + 8 < 1$$

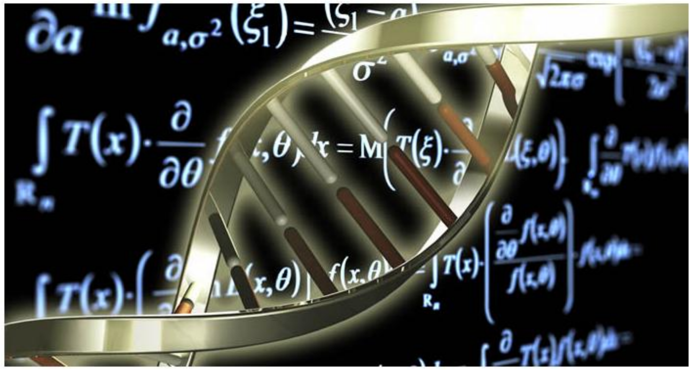
$$xy - 2x - 2y + 4 > 1$$

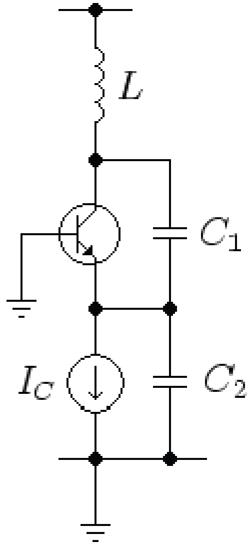
Applications



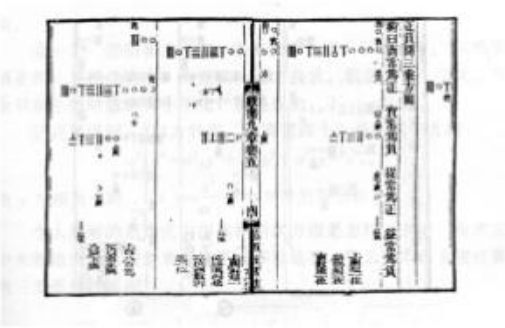








Milestones



RCF admits QE
non elementary complexity

820 1247 1637 1732 1830 1835 1876 1930 1975

QE by CAD
Doubly exponential

Other Relevant Work

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

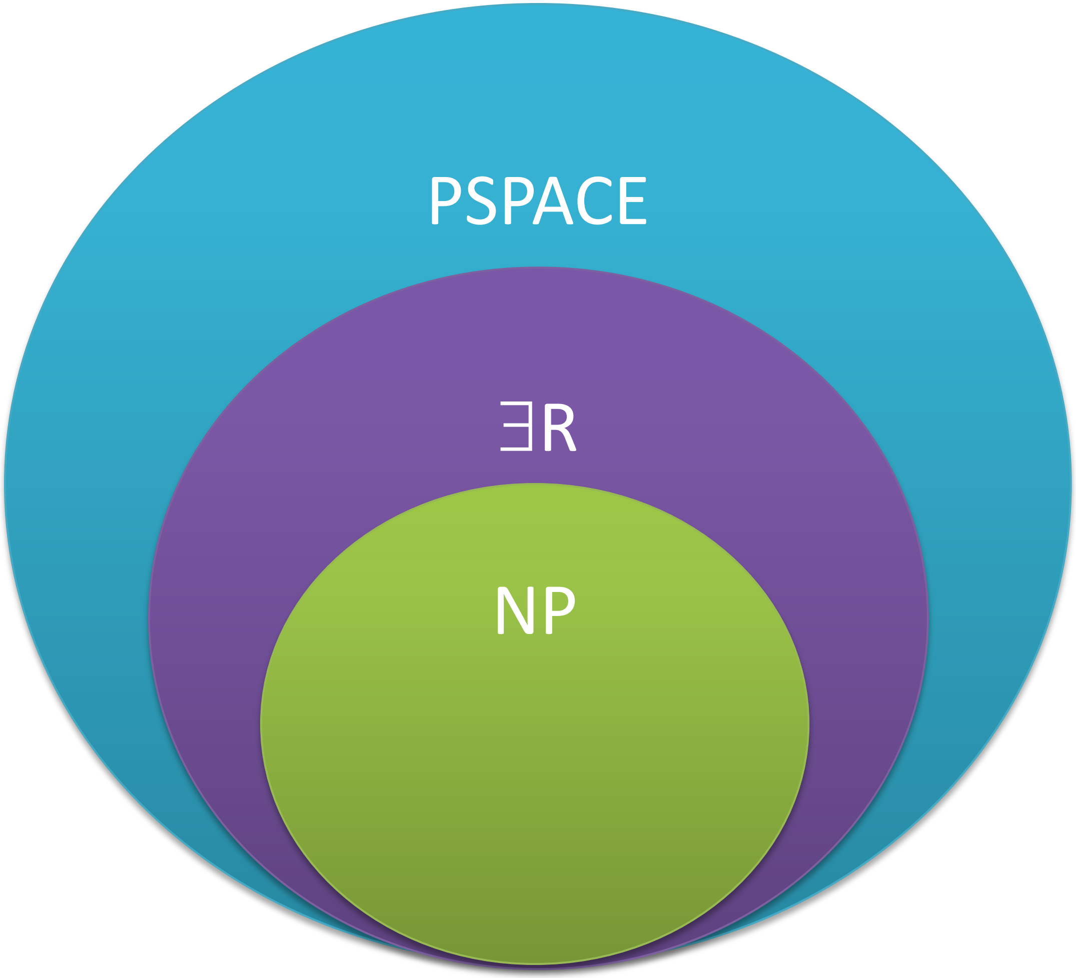
∃R in exponential time - Grigor'ev 1988, Canny 1988, Renegar 1989

In practice CAD based methods are far superior

VTS: Virtual Term Substitution (Weispfenning 1988)

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

How hard is ∃R?



PSPACE membership

Canny – 1988,

Grigor’ev – 1988

NP-hardness

x is “Boolean”→ $x(x-1) = 0$

x or y or z → $x + y + z > 0$

Multivariate Polynomials

$f \in \mathbb{Z}[\boldsymbol{y}, x]$ is of the form

$$f(\boldsymbol{y}, x) = a_m \cdot x^{d_m} + a_{m-1} \cdot x^{d_{m-1}} + \cdots + a_1 \cdot x^{d_1} + a_0$$

a_i are in $\mathbb{Z}[\boldsymbol{y}]$

$$x^3y^2 + y^2 + xy + x^2y + y + x + 1 = (x^3+1)y^2 + (x + x^2 + 1)y + (x + 1)$$

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”

$$\begin{array}{l} x^2 + y^2 - 1 < 0 \\ x\,y - 1 > 0 \end{array} \xrightarrow[\text{1. Saturate}]{} \begin{array}{l} x^4 - x^2 + 1 \\ x^2 - 1 \\ x \end{array}$$

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”

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

$\boldsymbol{x\,y} \; \boldsymbol{- 1} > 0$

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	-

$\boldsymbol{x \!\rightarrow\! -2}$

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

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

Our Procedure

Static x Dynamic

Optimistic approach

Key ideas

NEW Calculus / Abstract Procedure

- Start the Search before Saturate/Project
- We saturate on demand

Our Procedure (1)

Two kinds of decision

1. case-analysis (Boolean)

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

2. model construction (CAD lifting)

$$\boldsymbol{x \to -2}$$

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

Our Procedure (1)

Two kinds of decision

1. case-analysis (Boolean)
2. model construction (CAD lifting)

Parametric calculus: $explain(F, M)$

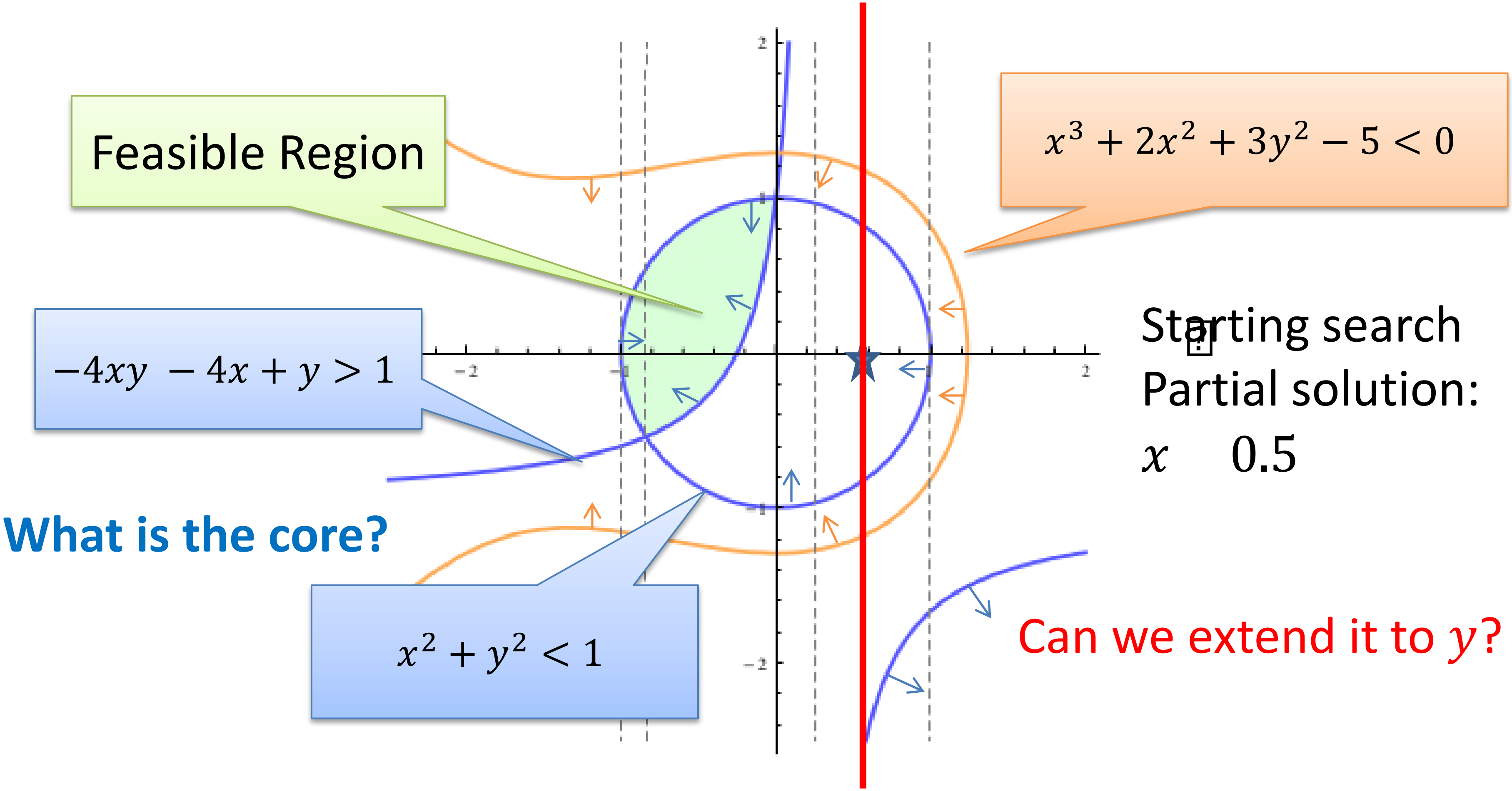
Finite basis explanation function

Explanations may contain new literals

They evaluate to false in the current state

Our Procedure (2)

Key ideas: Use partial solution to guide the search



Feasible Region

$x^3 + 2x^2 + 3y^2 - 5 < 0$

$-4xy - 4x + y > 1$

$x^2 + y^2 < 1$

Starting search

Partial solution:

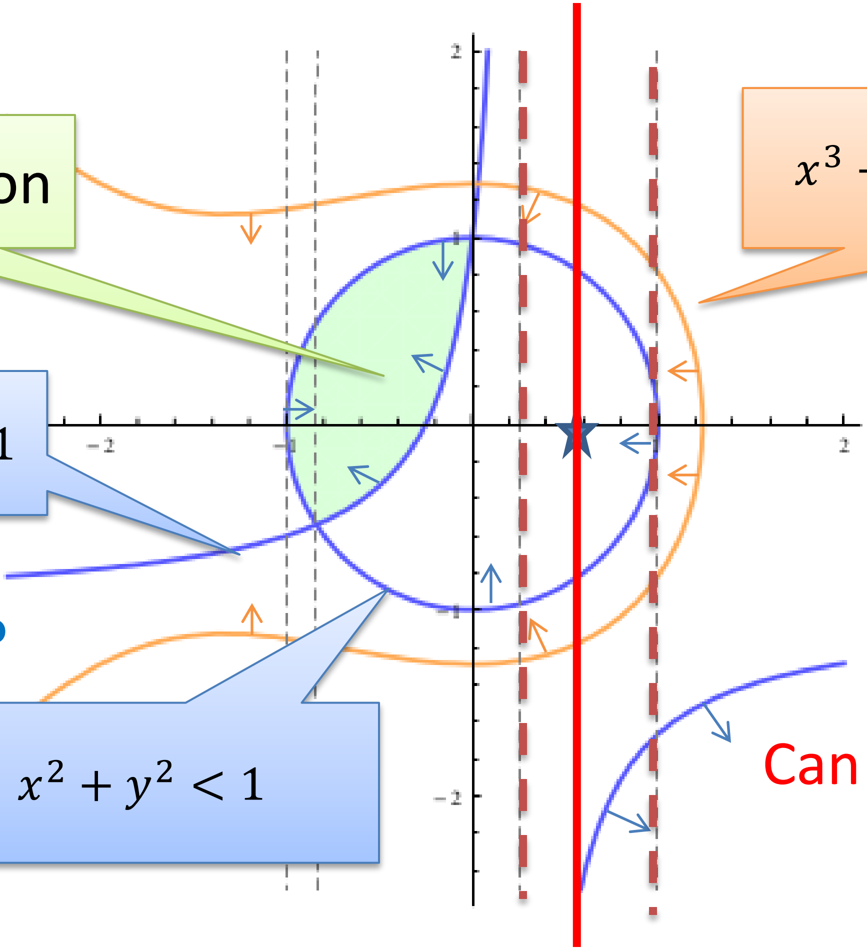
$x \quad 0.5$

What is the core?

Can we extend it to y?

Our Procedure (2)

Key ideas: Use partial solution to guide the search



Feasible Region

$-4xy - 4x + y > 1$

$x^3 + 2x^2 + 3y^2 - 5 < 0$

$x^2 + y^2 < 1$

Starting search

Partial solution:

$x \quad 0.5$

What is the core?

Can we extend it to y?

Our Procedure (3)

Key ideas: Solution based Project/Saturate

$$\mathsf{P}_c(A, x) = \bigcup_{f \in A} \mathsf{coeff}(f, x) \cup \bigcup_{\substack{f \in A \\ g \in \mathsf{R}(f, x)}} \mathsf{psc}(g, g'_x, x) \cup \bigcup_{\substack{i < j \\ g_i \in \mathsf{R}(f_i, x) \\ g_j \in \mathsf{R}(f_j, x)}} \mathsf{psc}(g_i, g_j, x)$$

Standard project operators are pessimistic.
Coefficients can vanish!

Our Procedure (4)

Key ideas: Lemma Learning

Prevent a **Conflict** from happening again.

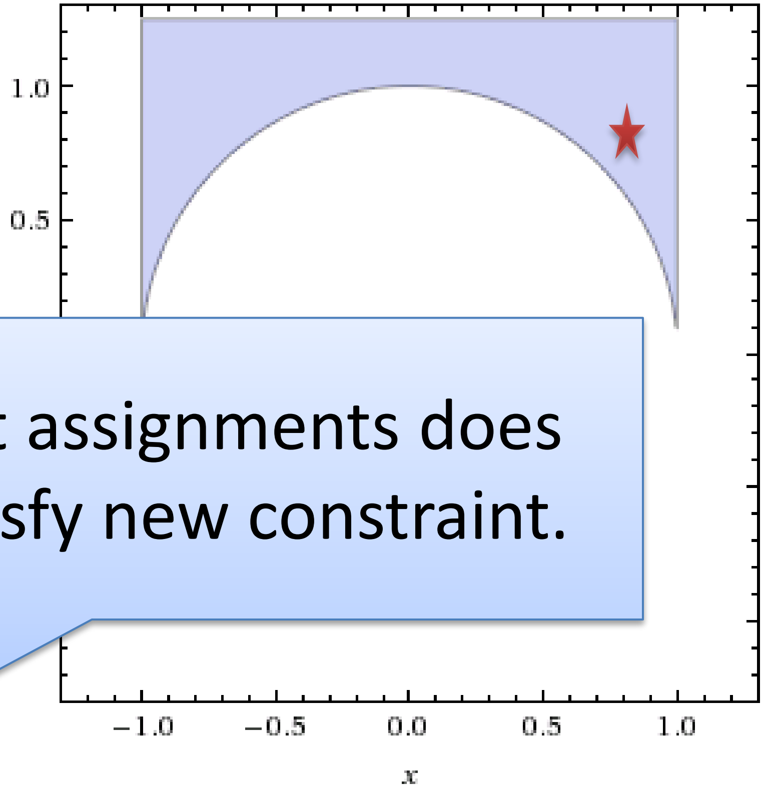
Current assignment

$x \to 0.75$

$y \to 0.75$

Conflict

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



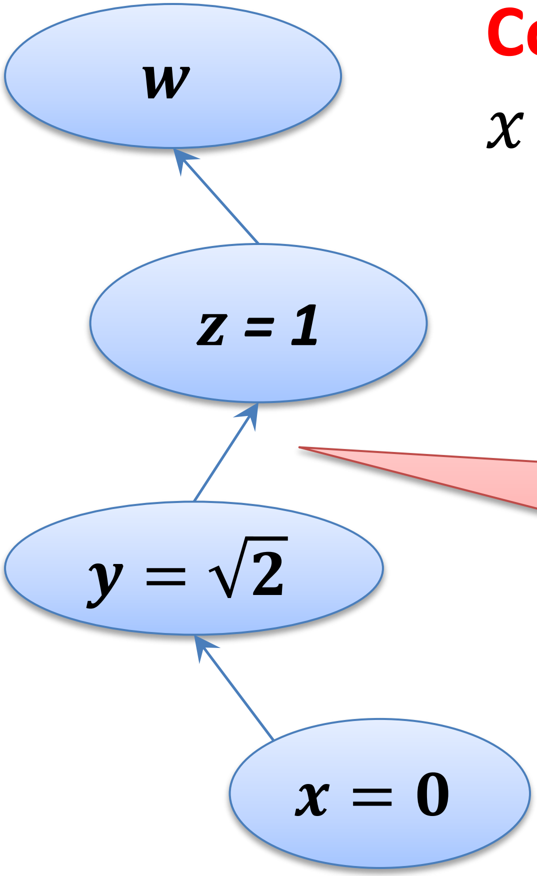
Current assignments does not satisfy new constraint.

Lemma

$$-1 < x < 1 \ \wedge\ y > root_2(1 - \tilde{y}^2 - x^2) \Rightarrow \bot$$

Our Procedure (5)

Key ideas: Nonchronological Backtracking



Conflict

$x\,w = 1$

The values chosen for z and y are **irrelevant**.

Machinery

Multivariate & univariate Polynomials

- Basic operations, Pseudo-division,
- GCD, Resultant, PSC, Factorization,
- Root isolation algorithms, Sturm sequences

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

Real Algebraic Numbers

Real Algebraic Numbers

Polynomial + Isolating Interval

$x^2 - 2, (1, 2)$

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

$$x^9 + 3x^6 + 3x^3 - 1, (0,1)$$

Complexity Trap: P ≠ Efficient

"Real algebraic numbers are efficient"

"CAD is polynomial for a fixed number of variables"

$$(2n)^{3^{r+1}} m^{2^r} d^2$$

Every detail matters

GCD of two polynomials

Our procedure "dies" in polynomial time steps

Real algebraic number computations

Computing PSCs

Root isolation of polynomials with irrational coefficients

Example

```
17775151118729246135103863388881244617666660995187997666751969361497959600261429526762965024955216280099712289835808749268353553329553408 x^532 +
14473361351917674942786915532863722010517729893029084002260132795724226061515042219666395922056072037155588196471401681986578474461376811173412864 x^528 +
722926499831393949975528590233592651930705659755165138114675351164604773814690541506747739888886171123037369344999237989374743845932980662659815833 6 x^524 +
15878482744622230892197972763581705423599198084235302253839649254815362649956536420885372278601947898596949668258188411414058700707614097818551897 2928 x^520 -
441056316892715495930778728080914837301015415664983397825606403637643700154268742903457693363893181553410527582696941674756975078517960210327134 2211072 x^516 +
2759816048096581254889263811999858551935527755151446322230233394005727041010304866236302653112594658205142494857875295213851675572471796341032045762 31424 x^512 +
600549611385170923215918938715543212918612426238702234537406210779953603570017956680791982312522261480140160267542183558518647461235243782062563242541 0560 x^508 +
986851623576407033251667128425075053871774092470521079882014728025896492535101475346629442538978949089841828419532025253587833424875817887721509965791 2320 x^504 -
37802815947438723742578392456237020646480154189917313873828344821455250631048120772292593335477190067155566022331743171410770501741115073710230504517455052 8 x^500 -
17808730106231073191878658236761328920282399007852768768460960004984306031572442483001419105190712931575531169183096099485281417843325729694855759690884710 40 x^496 +
499056042846765486019660459745332484355908796327648169789986321972544655976949236752298964078854322021966157875411405519439979849191085710760772381062044057 6 x^492 +
59251181672059584077424535291209687078232953829881306760118723543670560648034779432845164225459730400245051751104340753741284859922353854611675214692701175808 x^488 +
1092017519208785541520696785247822870462979710359943329303051621626835897822456431263911868073955738503583944530203686322073460825004038623204773151992509 89056 x^484 -
543635472379893925360505124247110498770961588622964318091251368183582212798004391152930087582383621190153681363319204281535655046706194540731277164848615522304 x^480 -
319467095685650703817078280486926680272540264528410267903714550137435243679311740648068119877675673103847778472072103116271080164575723290534999481202286316748 8 x^476 -
438954299961664863117689686214048249602518057020416060686860405285195203838325232722440215369487649947139126138438597879486746848593176449879699729721718 5251328 x^472 +
155244636404779293426230126890684432389069219173184149010156675706512101578825430510082705071220593632438219134709813772709069671327568113496009937103912 90757120 x^468 +
802304300188341860540966721892330963082372283785151440561292803608349097943365594348033594664116921125418823658961662101728781789222367734861999948661958 13629952 x^464 +
1307832834300115929925259376882712917479508640330118234991220976233111393118710554687813577764682644005497865325272169324076254180753523763498530190681194721443 84 x^460 -
603515363531880305347629272973673999840254885950960752636592855387320876645135969143917415265782142463399153489049891827712485940804469109934359753723649479 14752 x^456 -
673737188260475498982932420729791402429356609686364569053248570809232723474624874495372845950372093438174034642659688327168552160083094705613444283604882272 813056 x^452 -
131811750992779350616238022522802399028774191247872006680924599227171242149100913345996920654348978565223176619487767156004802154839890648633944230129061138 0060160 x^448 -
120577290229662435352506446822973129415995240282650240796695724371247404487175686397722086733944561995888270953554211662426899494709509900060140179454389155 7384192 x^444 -
498147540139927868371121123193544793997390792351584158209270507443166229317102963234758051076664986272012629263789383825333809441919597343891557884342482707152896 x^440 -
425183160356878150295004373290497531448531707780745037228573567097834830394339645980206627893938113569840552964828888053504977660681317926480110529303629 53957376 x^436 +
216799680499315816300118199578322679363512359867175466272738511237447749437563641630160944211130355312981999689785679524795667581500369918330859566054969131086643 2 x^432 +
924012106926705129504541700085160869321670714510686588822211807393607838481261709510334075318556181864640033346946429887901663831983250663946949994965022155818926 08 x^428 +
1414267487396571444108636929326335108159895348343497845222094625163440549057003916534164788048618203094794185311232037363935192511774826046464811661680716051958988 8 x^424
+ 4804392316217169298797299552280517149141556371101110118079706175749819893456084330834213192017152592033652756465196002644939544131707849914986554956068418796650496 x^420
- 6134328651047789328297594265911322867983176776828417042204526328352800710210496869027446316063433853708134399584229350095830205627581054793407103214275303368032256 x^416
+ 3667090053094090945313756073105630333582362976190542753984041052543074833064572525231477454196982964134256021905924763753701259287857721495779112184940262523404288 x^412
- 4781820198104808767769065630992852415507493062829305852058164950978621797100893773428877424282581150957974441863892727553275078361312064250261404560053284183736 32 x^408 -
501869018552131548554553226731641856960269716175435981415999194603017043489940477695539196666994884695057609251003594264592927299386026917322338047138829450 39892480 x^404 -
4978319291936067294196583692279610225583133967603674973571919327069960414411761549915139996360383851501430786663336942672133777211398736701796223078193928056340480 0 x^400
```

....

```
138938572627213982760039178751645714640405758108415962812938795986790444153337888273265668102438185532244 8 x^24 +
62062881776151490581128269961882121775983963464033372796514247786621932457485753479461152094854262 65049 x^20 +
3674270746104540700564697951655801960500001941136725305589283646358260904060306369054292574969226365 44 x^16 +
70332887417991884658952663143921054160262580168445685617174831300163538633716580995934281038561 2800 x^12 -
68999097046917627889169552420353798555453476109616123008816364722270432052018874285536216875008 x^8 -
140432623903101758790898107887718053467061472637614549187228994429864721538224739784429911670784 x^4 +
27265487456553904947773592051322041224875999574237205760221637206308453667976670187041587 2000
```

Systems

Mathematica: Wolfram's Research (CAD, FD CAD, …)

Redlog (VTS, CAD, Simplifications, …)

QEPCAD (Collins students)

MiniSMT ($\mathbb{Q}(\sqrt{2})$ model finder)

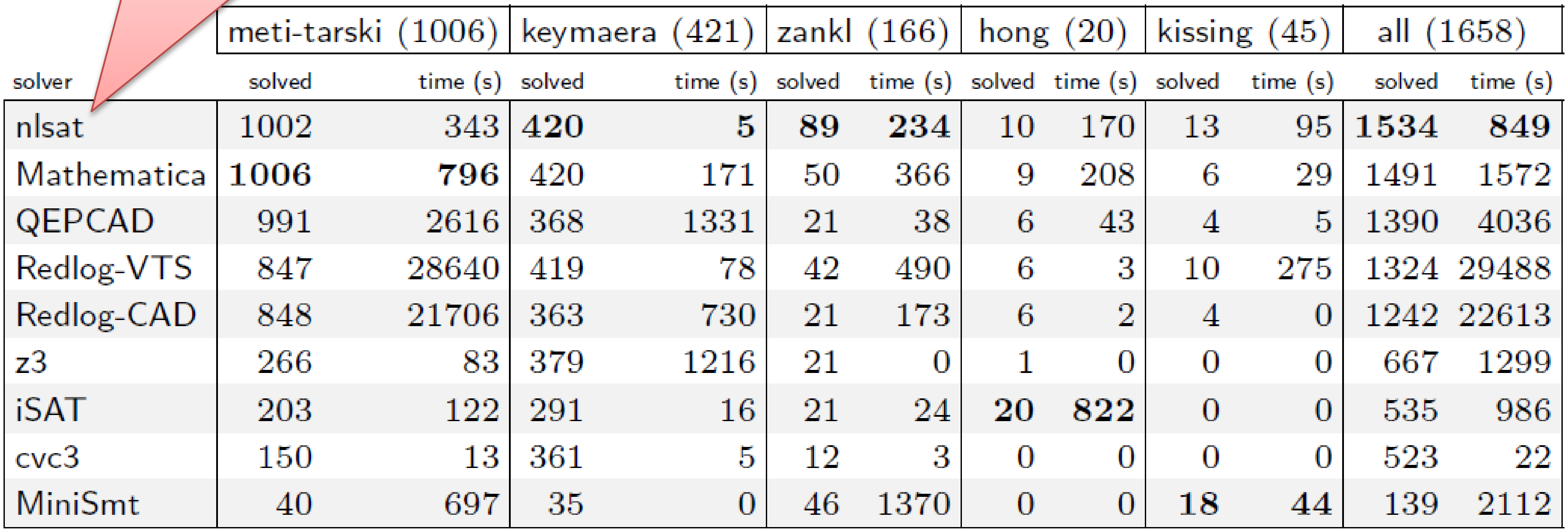
iSAT (interval based)

CVC3

Z3 3.x (GB, Simplex, interval analysis, VTS, $\mathbb{Q}(\sqrt{2})$ model finder)

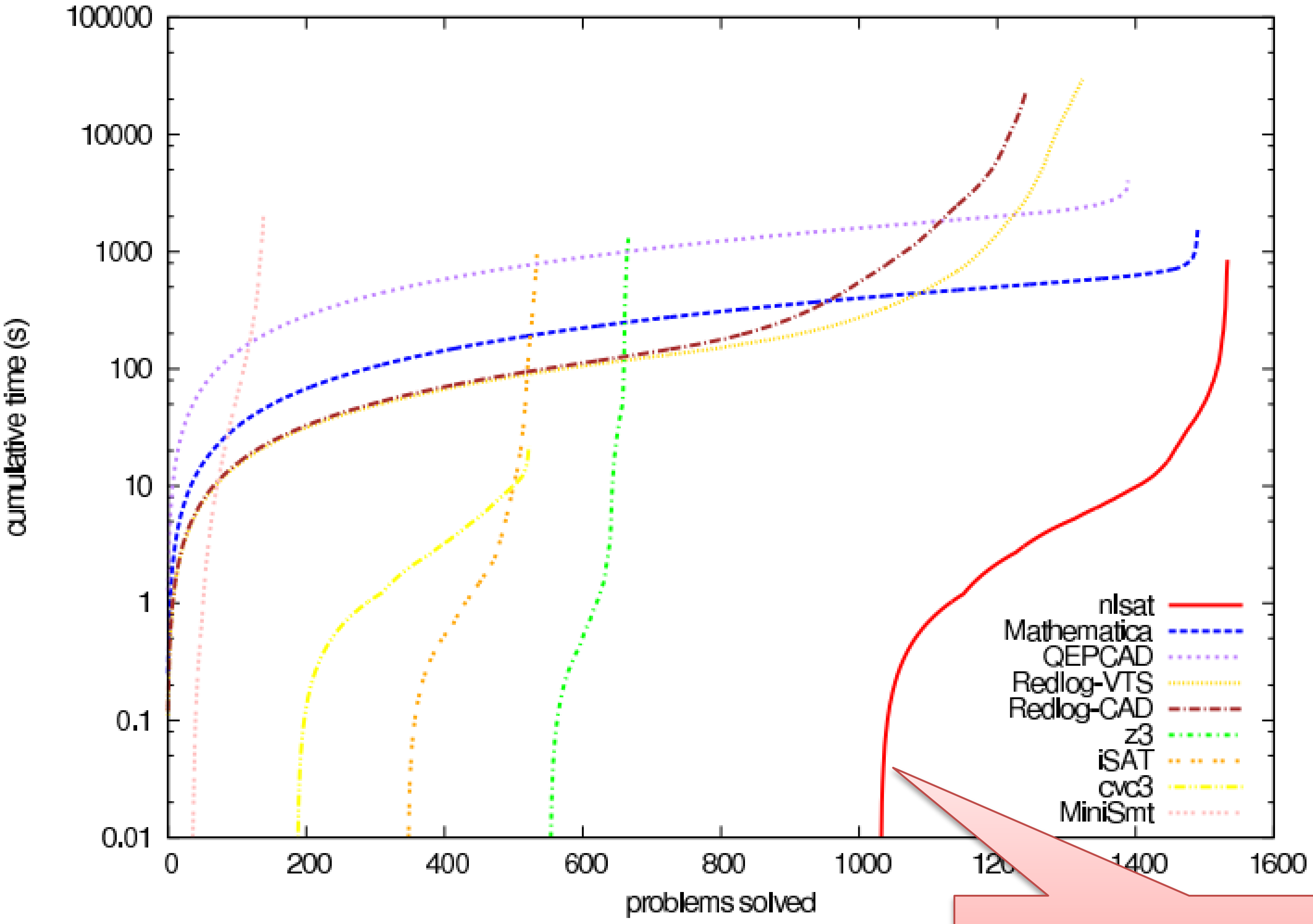
Experimental Results (1)

OUR NEW ENGINE



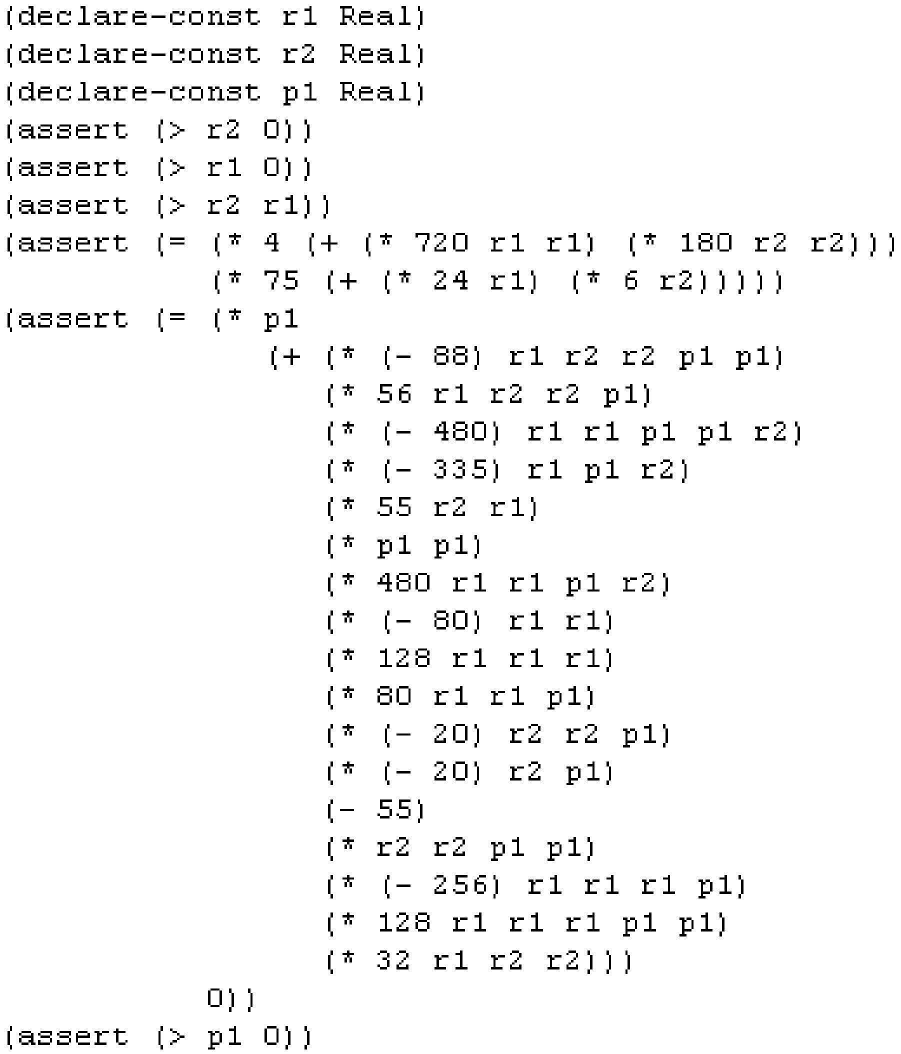
	meti-tarski (1006)		keymaera (421)		zankl (166)		hong (20)		kissing (45)		all (1658)	
solver	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)
nlsat	1002	343	**420**	**5**	**89**	**234**	10	170	13	95	**1534**	**849**
Mathematica	**1006**	**796**	420	171	50	366	9	208	6	29	1491	1572
QEPCAD	991	2616	368	1331	21	38	6	43	4	5	1390	4036
Redlog-VTS	847	28640	419	78	42	490	6	3	10	275	1324	29488
Redlog-CAD	848	21706	363	730	21	173	6	2	4	0	1242	22613
z3	266	83	379	1216	21	0	1	0	0	0	667	1299
iSAT	203	122	291	16	21	24	**20**	**822**	0	0	535	986
cvc3	150	13	361	5	12	3	0	0	0	0	523	22
MiniSmt	40	697	35	0	46	1370	0	0	**18**	**44**	139	2112

Experimental Results (2)

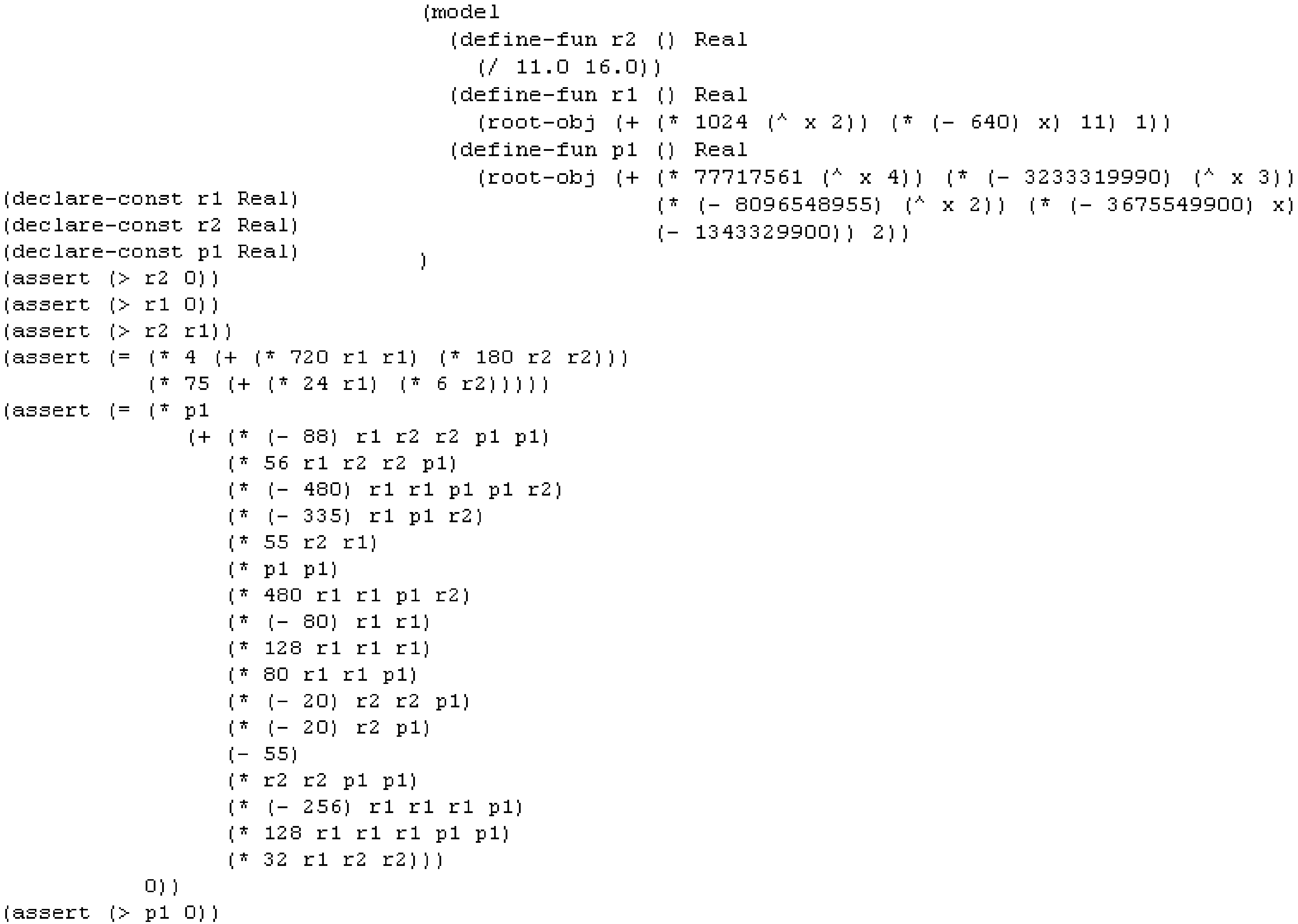


OUR NEW ENGINE

Example

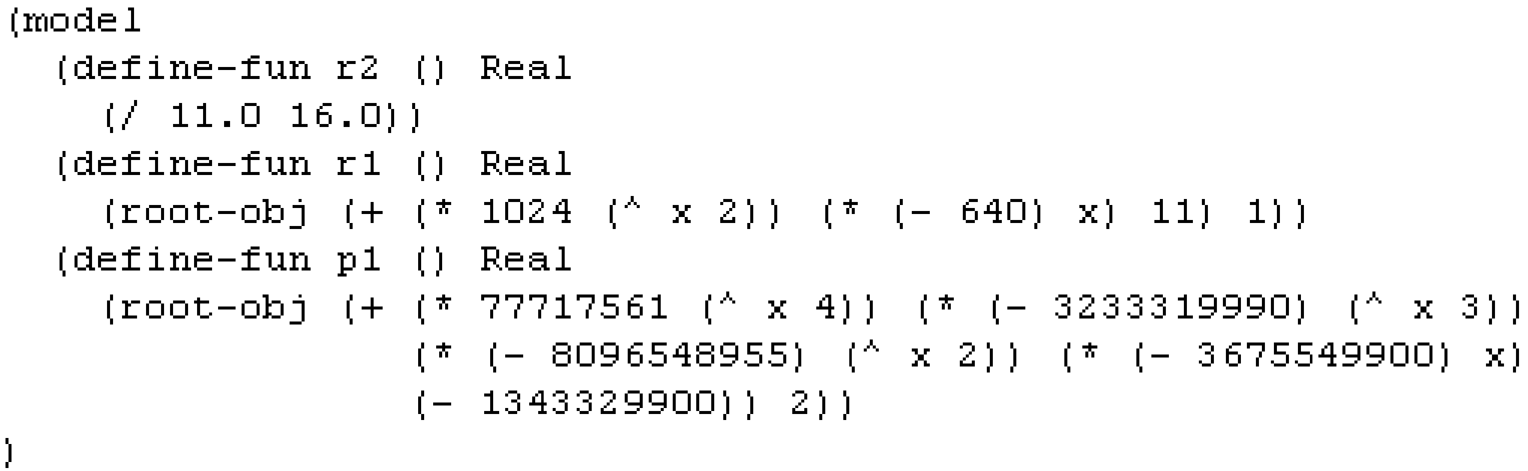


```
(declare-const r1 Real)
(declare-const r2 Real)
(declare-const p1 Real)
(assert (> r2 0))
(assert (> r1 0))
(assert (> r2 r1))
(assert (= (* 4 (+ (* 720 r1 r1) (* 180 r2 r2)))
           (* 75 (+ (* 24 r1) (* 6 r2)))))
(assert (= (* p1
              (+ (* (- 88) r1 r2 r2 p1 p1)
                 (* 56 r1 r2 r2 p1)
                 (* (- 480) r1 r1 p1 p1 r2)
                 (* (- 335) r1 p1 r2)
                 (* 55 r2 r1)
                 (* p1 p1)
                 (* 480 r1 r1 p1 r2)
                 (* (- 80) r1 r1)
                 (* 128 r1 r1 r1)
                 (* 80 r1 r1 p1)
                 (* (- 20) r2 r2 p1)
                 (* (- 20) r2 p1)
                 (- 55)
                 (* r2 r2 p1 p1)
                 (* (- 256) r1 r1 r1 p1)
                 (* 128 r1 r1 r1 p1 p1)
                 (* 32 r1 r2 r2)))
           0))
(assert (> p1 0))
```

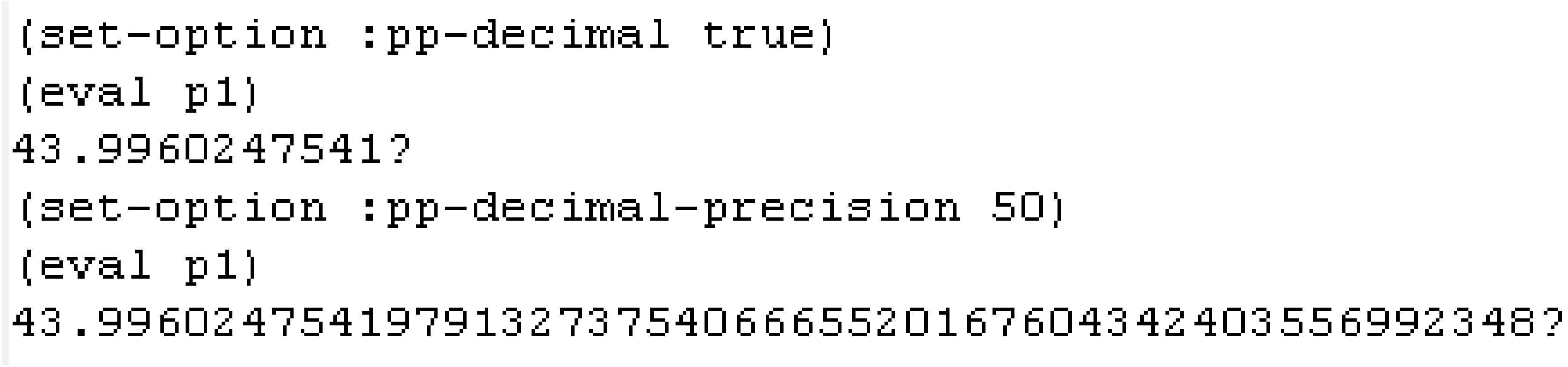


```
(model
  (define-fun r2 () Real
    (/ 11.0 16.0))
  (define-fun r1 () Real
    (root-obj (+ (* 1024 (^ x 2)) (* (- 640) x) 11) 1))
  (define-fun p1 () Real
    (root-obj (+ (* 77717561 (^ x 4)) (* (- 3233319990) (^ x 3))
                 (* (- 8096548955) (^ x 2)) (* (- 3675549900) x)
                 (- 1343329900)) 2))
)
```

```
(declare-const r1 Real)
(declare-const r2 Real)
(declare-const p1 Real)
(assert (> r2 0))
(assert (> r1 0))
(assert (> r2 r1))
(assert (= (* 4 (+ (* 720 r1 r1) (* 180 r2 r2)))
           (* 75 (+ (* 24 r1) (* 6 r2)))))
(assert (= (* p1
              (+ (* (- 88) r1 r2 r2 p1 p1)
                 (* 56 r1 r2 r2 p1)
                 (* (- 480) r1 r1 p1 p1 r2)
                 (* (- 335) r1 p1 r2)
                 (* 55 r2 r1)
                 (* p1 p1)
                 (* 480 r1 r1 p1 r2)
                 (* (- 80) r1 r1)
                 (* 128 r1 r1 r1)
                 (* 80 r1 r1 p1)
                 (* (- 20) r2 r2 p1)
                 (* (- 20) r2 p1)
                 (- 55)
                 (* r2 r2 p1 p1)
                 (* (- 256) r1 r1 r1 p1)
                 (* 128 r1 r1 r1 p1 p1)
                 (* 32 r1 r2 r2)))
           0))
(assert (> p1 0))
```



```
(model
  (define-fun r2 () Real
    (/ 11.0 16.0))
  (define-fun r1 () Real
    (root-obj (+ (* 1024 (^ x 2)) (* (- 640) x) 11) 1))
  (define-fun p1 () Real
    (root-obj (+ (* 77717561 (^ x 4)) (* (- 3233319990) (^ x 3))
                 (* (- 8096548955) (^ x 2)) (* (- 3675549900) x)
                 (- 1343329900)) 2))
)
```



```
(set-option :pp-decimal true)
(eval p1)
43.9960247541?
(set-option :pp-decimal-precision 50)
(eval p1)
43.99602475419791327375406665520167604342403556992348?
```

Generating Proofs

The “skeleton” is a resolution proof.

Our current $explain(F, M)$ is based on CAD.

Lemmas are hard to check.

Alternative: $explain(F, M)$ based on

Cohen, Muchnick, Hormander

Easy to Check.

Nonelementary complexity.

Future Work

Other $explain$ procedures and refinements

New real algebraic number package

Heuristics: variable reordering, lemma GC, etc.

Simplex integration for pruning state space

Algorithmic improvements

QE based on our procedure

Nonlinear integer arithmetic

Transcendental functions