SMT Nonlinear Real Arithmetic and Computer Algebra: a Dialogue of the Deaf?

James Davenport[1]
University of Bath
J.H.Davenport@bath.ac.uk

23 July 2017

[1]Thanks to EU H2020-FETOPEN-2016-2017-CSA project $\mathcal{SC}^2$ (712689) and the many partners on that project: www.sc-square.org

Thesis

At a deep level, the problems which SMT's Nonlinear Real Arithmetic (NRA) and Computer Algebra's Cylindrical Algebraic Decomposition (CAD) wish to solve are the same: nevertheless the approaches are completely different, and are described in different languages. We give an NRA/CAD dictionary, explain the CAD process as it is traditionally presented (and some variants), then ask how NRA and CAD might have a more fruitful dialogue.

(partial) Dictionary

Concept	SMT's NRA	CA and CAD
	Arithmetic	Algebra
	Unquantified	$\exists$quantified
	Quantified	Alternation of quantifiers
Goal	A model	Set of all models
	or UNSAT	Quantifier elimination etc.
Starting point	Boolean structure	Polynomials
Order	frequent change	absolutely fixed
	(of boolean variables)	(of theory variables)
Measure	Performance	complexity

Logical/Polynomial Systems over $(\mathbf{R})$

Let p_i be the Boolean $f_i \sigma_i 0$ where $f_i \in \mathbf{Z}[x_1, \ldots, x_n]$ and $\sigma_i \in \{=, \neq, <, \leq, >, \geq\}$.
Let the problem be $\Psi := \mathcal{Q}_1 x_1 \mathcal{Q}_2 x_2 \ldots \mathcal{Q}_n x_n \Phi(p_1, \ldots, p_m)$, where Φ is a Boolean combination (typically in CNF for SAT), and $\mathcal{Q} \in \{\exists, \forall, \text{free}\}$. SMT typically has all $\mathcal{Q}_i$ as $\exists$, QE insists the free occur first (say $x_1, \ldots, x_k$).
Then the goals are:

- **NRA** SAT and a model, or UNSAT (?+proof);
- **CAD** A decomposition of $\mathbf{R}^n$ into D_j such that every f_i is sign-invariant (> 0, $= 0$ or < 0) on each D_j
- **cylindrical** $\forall i, j, k : \pi_k(D_i)$ and $\pi_k(D_j)$ are disjoinnt or equal
- **QE** $\widehat{\Phi}(q_i, \ldots, q_{m'})$, where $q_i := g_i \tau_i 0$, $g_i \in \mathbf{Z}[x_1, \ldots, x_k]$ and $\tau_i \in \{=, \neq, <, \leq, >, \geq\}$.

Approaches (very simplified)

NRA1 Ignore the f_i.

NRA2 Find a Φ-satisfying assigment to p_i.

NRA3 Check this against the theory $p_i = f_i \sigma_i 0$, and SAT

NRA4 or try again (maybe learning a lemma).

QE1 Ignore Φ and the p_i.

QE2 Decompose $\mathbf{R}^n$ into regions (with a sample point) where the f_i are sign-invariant on each region.

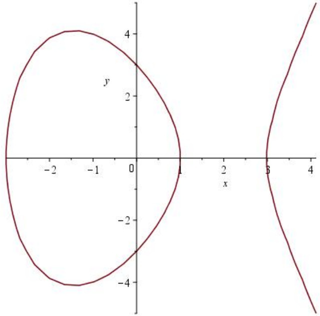
QE3 Evaluate Φ at each sample point.

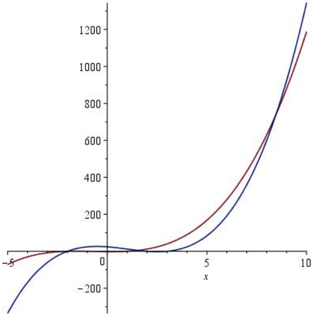
QE4 By cylindricity, evaluate Ψ at sample points of $\mathbf{R}^k$.

$$\forall x_l \Rightarrow \bigwedge_{x_l \text{ sample points}} ; \exists x_l \Rightarrow \bigvee_{x_l \text{ sample points}}$$

QE5 $\widehat{\Phi} := \bigvee$description of Ψ-true cells.

Why might Φ have different values? Geometry($x_2 = y$)





$$\mathrm{disc}_y(y^2 - x^3 + x^2 + 9x - 9)$$

$$4x^3 - 4x^2 - 36x + 36$$

$$\{-3, 1, 3\}$$

$$\mathrm{res}_y(\; y - x^3 - 2x^2 + x + 2,\; y - 2x^3 + 6x^2 + 8x - 24)$$

$$-x^3 + 8x^2 + 7x - 26$$

$$\{-2., 1.535898384, 8.464101616\}$$

So just compute resultants and discriminants?

Not quite: more can go wrong, especially in higher dimensions
We certainly need to worry about contents if non-trivial

- [Col75] Also all coefficients, and subresultants
- [McC84] Not the subresultants
- But a resultant might vanish identically on a set: CAD fails "not well-oriented"
- [Hon90] Unconditional slight improvement on [Col75].
- [Laz94] Conjectures (false proof) we only need leading & trailing coefficients
- [MPP16] Proves Lazard projection (better than McCallum)

So what's the complexity?

Suppose $\Xi_n = \{$ polynomials in $\Phi\}$ has m polynomials of degree $\leq d$ (in each variable).

Then after Geometry(x_n), Ξ_{n-1} has $O(m^2)$ polynomials of degree $O(d^2)$.

Then after Geometry(x_{n-1}), Ξ_{n-2} has $O(m^4)$ polynomials of degree $O(d^4)$.

After Geometry(x_2), Ξ_1 has $m^{2^{O(n)}}$ polynomials of degree $d^{2^{O(n)}}$.

The analysis is significantly messier than this, but qualitatively these results are right.

This doubly-exponential behaviour is inherent in CAD and QE [DH88, BD07], even for the description of a single sample point.

However, for QE these assume $O(n)$ alternations of quantifiers, and there are theoretical results showing $m^{n2^{O(a)}}$, $d^{n2^{O(a)}}$.

But we can do better (by looking at the logic)

SMT It's silly to ignore Φ and p_i.

[Col98] True, if $\Phi = (f_1 = 0) \wedge \Phi'$, we're not interested in Φ' except when $f_1 = 0$.

[McC99] Implemented this: replaces n by $n - 1$ in double exponent of m (therefore $C \to \sqrt{C}$).

- $\Phi := (f_1 = 0 \wedge \Phi_1) \vee (f_2 = 0 \wedge \Phi_2)$ can be written as $f_1 f_2 = 0 \wedge \Phi$ and benefit (but $d \to 2d$)

[BDE+13] address this structure directly

[BDE+16] the case $(f_1 = 0 \wedge \Phi_1) \vee \Phi_2$ etc.

[ED16, DE16] the case $(f_1 = 0) \wedge \cdots \wedge (f_s = 0) \wedge \Phi'$ replaces n by $n - s$ in double exponents of m and d

provided the iterated resultants are primitive: alas not a technicality

Two alternative methods for computing CAD

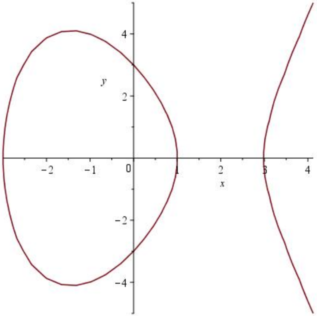
- Regular Chains [CM16]
  1. Decompose $\mathbf{C}^n$ cylindrically by regular chains ($\mathbf{C}^1$ is "special cases" + "the rest")
  2. `MakeSemiAlgebraic` to decompose $\mathbf{R}^i \subset \mathbf{C}^i$ — "the rest" is generally not connected in $\mathbf{R}^i$ and needs to be split up
  3. Read off a CAD
  - Less theory but often better computation in practice
- Comprehensive Gröbner Bases [Wei92]
  1. Build a CGB, i.e. the generic solution *and* all the special cases.
  2. Use this to build CAD [FIS15]
  - Bath have been unable to get this to work

Or Just produce a single cell of the CAD [Bro15]: start from a sample point and see what the obstacles to extending it are

- Inspired by NLSAT [JdM13]

QE Needn't be by CAD: Virtual Term Substitution [Wei98, KS15], very effective for linear/ quadratic problems

There are algebraic deductions: consider



The discriminant is $4x^3 - 4x^2 - 36x + 36$, so $y^2 < x^3 - x^2 - 9x + 9 \Rightarrow (x > -3 \wedge x < 1) \vee (x > 3)$; however $y^2 > x^3 - x^2 - 9x + 9$ gives no deductions.

Does it make sense to partition the logic variables by the theory variables they relate to, and to ask the theory to produce deductions with fewer variables?

More information

- **SC²** Symbolic Computation and Satisfiability Checking. Project description [ABB+16] and www.sc-square.org. Workshop in Kaiserslautern next Saturday and at FLoC 2018.
- **CAD/QE** [CJ98], probably best analysis in [BDE+16].
- **Computer Algebra** [vzGG13] is probably the best text; I am writing one at http://staff.bath.ac.uk/masjhd/JHD-CA.pdf.

Questions?

Bibliography

I

E. Ábrahám, B. Becker, A. Bigatti, B. Buchberger, C. Cimatti, J.H. Davenport, M. England, P. Fontaine, S. Forrest, D. Kroening, W. Seiler, and T. Sturm.
SC^2: Satisfiability Checking meets Symbolic Computation (Project Paper).
In *Proceedings CICM 2016*, pages 28–43, 2016.

C.W. Brown and J.H. Davenport.
The Complexity of Quantifier Elimination and Cylindrical Algebraic Decomposition.
In C.W. Brown, editor, *Proceedings ISSAC 2007*, pages 54–60, 2007.

Bibliography

II

R.J. Bradford, J.H. Davenport, M. England, S. McCallum, and D.J. Wilson.
Cylindrical Algebraic Decompositions for Boolean Combinations.
In *Proceedings ISSAC 2013*, pages 125–132, 2013.

R.J. Bradford, J.H. Davenport, M. England, S. McCallum, and D.J. Wilson.
Truth table invariant cylindrical algebraic decomposition.
J. Symbolic Computation, 76:1–35, 2016.

C.W. Brown.
Open Non-uniform Cylindrical Algebraic Decompositions.
In *Proceedings ISSAC 2015*, pages 85–92, 2015.

Bibliography III

B.F. Caviness and J.R. (eds.) Johnson.
Quantifier Elimination and Cylindrical Algebraic Decomposition.
Springer-Verlag, 1998.

C. Chen and M. Moreno Maza.
Quantifier elimination by cylindrical algebraic decomposition based on regular chains.
J. Symbolic Comp., 75:74–93, 2016.

G.E. Collins.
Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition.
In *Proceedings 2nd. GI Conference Automata Theory & Formal Languages*, pages 134–183, 1975.

Bibliography IV

G.E. Collins.
Quantifier elimination by cylindrical algebraic decomposition — twenty years of progess.
In B.F. Caviness and J.R. Johnson, editors, *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 8–23. Springer Verlag, Wien, 1998.

J.H. Davenport and M. England.
Need Polynomial Systems be Doubly-exponential?
In *Proceedings ICMS 2016*, pages 157–164, 2016.

J.H. Davenport and J. Heintz.
Real Quantifier Elimination is Doubly Exponential.
J. Symbolic Comp., 5:29–35, 1988.

Bibliography

M. England and J.H. Davenport.
The complexity of cylindrical algebraic decomposition with respect to polynomial degree.
In *Proceedings CASC 2016*, pages 172–192, 2016.

R. Fukasaku, H. Iwane, and Y. Sato.
Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems.
In D. Robertz, editor, *Proceedings ISSAC 2015*, pages 173–180, 2015.

H. Hong.
An Improvement of the Projection Operator in Cylindrical Algebraic Decomposition.
In S. Watanabe and M. Nagata, editors, *Proceedings ISSAC '90*, pages 261–264, 1990.

D. Jovanović and L. de Moura.
Solving non-linear arithmetic.
ACM Communications in Computer Algebra, 46(3/4):104–105, 2013.

M. Košta and T. Sturm.
A Generalized Framework for Virtual Substitution.
http://arxiv.org/abs/1501.05826, 2015.

D. Lazard.
An Improved Projection Operator for Cylindrical Algebraic Decomposition.
In *Proceedings Algebraic Geometry and its Applications*, 1994.

S. McCallum.
An Improved Projection Operation for Cylindrical Algebraic Decomposition.
PhD thesis, University of Wisconsin-Madison Computer Science, 1984.

S. McCallum.
On Projection in CAD-Based Quantifier Elimination with Equational Constraints.
In S. Dooley, editor, *Proceedings ISSAC '99*, pages 145–149, 1999.

S. McCallum, A. Parusinski, and L. Paunescu.
Validity proof of Lazard's method for CAD construction.
https://arxiv.org/abs/1607.00264, 2016.

J. von zur Gathen and J. Gerhard.
Modern Computer Algebra (3rd edition).
Cambridge University Press New York, 2013.

V. Weispfenning.
Comprehensive Gröbner Bases.
J. Symbolic Comp., 14:1–29, 1992.

V. Weispfenning.
A New Approach to Quantifier Elimination for Real Algebra.
Quantifier Elimination and Cylindrical Algebraic Decomposition, pages 376–392, 1998.