New Opportunities for the Formal Proof of Computational Real Geometry?

Professor James Davenport
(joint work with Erika Ábrahám, Matthew England, Gereon Kremer, Zak Tonks)

University of Bath

5 July 2020

Provable Solutions?

- **SAT** A satisfying assignment is a proof,
- **UNSAT** we ask for an UNSAT core,
- **+** and ask a verified SAT solver to demonstrate UNSAT here
- **SMT** Depends on the 'T'
- **QF_NRA** $\exists x_1 \ldots \exists x_n \Phi(x_1, \ldots, x_n)$
- **often** There is no non-trivial UNSAT core, but the space partitions into regions with local UNSAT cores, which may be quite simple.
- **+?** There is no practicable verified QF_NRA solver.

QF_NRA Algorithms?

Tarski Complexity infeasible [Tar51], slightly better version due to Hörmander [Hö05]

Cylindrical Algebraic Decomposition (CAD) [Col75, many improvements], also solves $\exists x_1 \forall x_2 \cdots$ etc., therefore doubly exponential in n [DH88, BD07].

Virtual Term Substitution [Wei88, Kos16]: limited to degree ≤ 3 *including recursively*.

NLSAT Essentially a refutation-based method [JdM12].

NuCAD Non-Uniform CAD [Bro15].

Cylindrical Algebraic Coverings [ADEK20].

verified QF_NRA solver

Not for want of trying (mostly around Coq).

[Mah07] Implemented CAD in Coq, but didn't have a proof of correctness.

Topology enters, particularly in the improvements.

[CM12] Proved correct an implementation of Hörmander [Hö05].

So the feasible is unproven, and the proven is infeasible.

Also There is no fully-described theory of handling "local UNSAT cores", or even a method of finding them.

Sketch of Cylindrical Algebraic Coverings [ADEK20]

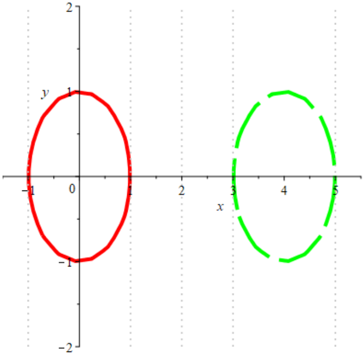
1. Guess a sample point ($x_1 := s_1$) then ($x_2 := s_2$) until ($\mathrm{x} = \mathrm{s}, x_i = s_i^{(1)}$) is infeasible
2. Generalise the contradiction at $s_i^{(1)}$ to rule out all $x_i \in (l_i^{(1)}, u_i^{(1)})$

NB $l_i^{(1)}, u_i^{(1)}$ will be roots of resultants/discriminants/lc

3. Choose a sample ($\mathrm{x} = \mathrm{s}, x_i = s_i^{(2)}$), and exclude all $x_i \in (l_i^{(2)}, u_i^{(2)})$
4. Continue until the whole line (s, x_i) is ruled out by $-\infty < l_i^{(2)} < u_i^{(1)} < l_i^{(3)} < u_i^{(2)} < \cdots < \infty$
5. Looking at the resultants $l_i^{(j+1)}, u_i^{(j)}$ and discriminants, extend $s_{i-1}^{(1)}$ to an interval $l_{i-1}^{(1)}, u_{i-1}^{(1)}$
6. Choose a different sample point $s_{i-1}^{(2)}$, and extend that, ...

Until R^n is covered by cells of infeasibility.

Example 1



$c_1 := (x^2 + y^2 < 1) \wedge$

$c_2 := ((x-4)^2 + y^2 < 1)$

$x = -1$: c_1 is (just) infeasible

$x = -2$: c_1 rules out $(-\infty, -1)$

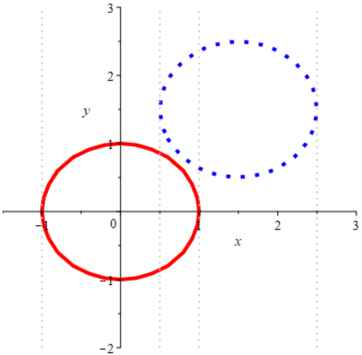
$x = 0$ c_2 rules out $(-\infty, 3)$

$x = 4$ c_1 rules out $(1, \infty)$

Hence $\mathrm{R} = (-\infty, 3) \cup (1, \infty)$ is infeasible

Very like the human proof.

Example 2



$x = 0$	c_2 rules out $(-\infty, \frac{1}{2})$
$x = 4$	c_1 rules out $(1, \infty)$
$x = \frac{3}{4}$	No y satisfies both, and this extends to $(\frac{1}{2}, 1)$
$x = \frac{1}{2}$	c_2 rules out
$x = 1$	c_1 rules out
Hence	R is unfeasible

Perhaps not the human proof, but at least understandable.

Current state

- + We have an implementation of CAC, described in [ADEK20], and a talk at ICMS on 14 July.
- – We don't have a proper output of the informal reasoning as above
- – – We don't have a translation of this into tactics for a theorem-prover
- ! Collaborators welcome

Bath is recruiting!

Post-doctoral researcher for three years, ideally starting 1 October 2020 (but can be flexible).

Typical starting salary £39,000.

To work on a joint project with Matthew England on "Pushing Back the Doubly-Exponential Wall of Cylindrical Algebraic Decomposition".

Covid-19 has got in the way of formal advertising, but express interest to `J.H.Davenport@bath.ac.uk`

Bibliography I

E. Ábrahám, J.H. Davenport, M. England, and G. Kremer.
Deciding the Consistency of Non-Linear Real Arithmetic Constraints with a Conflict Driven Search Using Cylindrical Algebraic Coverings.
http://arxiv.org/abs/2003.05633, 2020.

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.

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

Bibliography II

C. Cohen and A. Mahboubi.
Formal Proofs in Real Algebraic Geometry: From Ordered Fields to Quantifier Elimination.
Logical Methods in Computer Science, 8:1–40, 2012.

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.

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

Bibliography III

L. Hörmander.
The analysis of linear partial differential operators. II. Differential operators with constant coefficients, volume 257 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*.
Springer-Verlag, Berlin, 1983; republished 2005.

D. Jovanović and L. de Moura.
Solving Non-Linear Arithmetic.
In *Proceedings IJCAR 2012*, pages 339–354, 2012.

M. Košta.
New concepts for real quantifier elimination by virtual substitution.
PhD thesis, Universität des Saarlandes, 2016.

Bibliography IV

A. Mahboubi.
Implementing the cylindrical algebraic decomposition within the Coq system.
Math. Struct. in Comp. Science, 17:99–127, 2007.

A. Tarski.
A Decision Method for Elementary Algebra and Geometry.
2nd ed., Univ. Cal. Press. Reprinted in *Quantifier Elimination and Cylindrical Algebraic Decomposition* (ed. B.F. Caviness & J.R. Johnson), Springer-Verlag, Wein-New York, 1998, pp. 24–84., 1951.

V. Weispfenning.
The Complexity of Linear Problems in Fields.
J. Symbolic Comp., 5:3–27, 1988.