# The doubly-exponential problem in equation/inequality solving

James Davenport[1]
University of Bath
Fulbright Scholar at NYU
J.H.Davenport@bath.ac.uk

30 April 2017

[1]Thanks to Matthew England (Coventry), EPSRC EP/J003247/1, EU H2020-FETOPEN-2016-2017-CSA project $\mathcal{SC}^2$ (712689)

# But first, a word from our sponsors

EU Coordinating and Support Action 712689
Satisfiability Checking and Symbolic Computation
`http://www.sc-square.org/CSA/welcome.html`

| | |
|---|---|
| University of Bath | James Davenport; Russell Bradford |
| RWTH Aachen | Erika Ábrahám |
| Fondazione Bruno Kessler | Alberto Griggio; Alessandro Cimatt |
| Università degli Studi di Genova | Anna Bigatti |
| Maplesoft Europe Ltd | Jürgen Gerhard; Stephen Forrest |
| Université de Lorraine (LORIA) | Pascal Fontaine |
| Coventry University | Matthew England |
| University of Oxford | Daniel Kroening; Martin Brain |
| Universität Kassel | Werner Seiler; John Abbott |
| Max Planck Institut für Informatik | Thomas Sturm |
| Universität Linz | Tudur Jebelean; Bruno Buchberger |
| | Wolfgang Windsteiger; Roxana-Maria Holom |

# Aims

Symbolic Computation and Satisfiability Checking tackle similar problems but with different algorithmic and technological solutions. Though both communities have made remarkable progress in the last decades, they still need to be strengthened to tackle practical problems of rapidly increasing size and complexity. Currently the two communities are largely disjoint and unaware of the achievements of each other: researchers from these two communities rarely interact, and also their tools lack common, mutual interfaces for unifiying their strengths. Bridges between the communities in the form of common platforms and roadmaps are necessary to initiate an exchange, and to support and to direct their interaction.

# Activities

1. $SC^2$ special session at ACA 2016, CASC 2016
2. First $SC^2$ workshop September 24 2016 (Timișoara)
3. Second $SC^2$ workshop July 29 2017 (Kaiserslautern)
4. $SC^2$ summer school July 31-August 4 2017 (Saarbrücken)
5. Third $SC^2$ workshop August 2018 (Oxford)

# Theoretical versus Practical Complexity

**Notation** $n$ variables, $m$ polynomials of degree $d$ (in each variable separately; $\mathfrak{d}$ total degree: $d \leq \mathfrak{d} \leq nd$), coefficients length $l$

**Theoretical** doubly exponential, whether via Gröbner bases [MM82, Yap91, lower], [Dub90, upper] or Cylindrical Algebraic Decomposition [DH88, BD07, lower], [Col75, BDE$^+$16, upper]

**But** this is doubly exponential in $n$, polynomial in everything else.

**In practice** we see very bad dependence on $m, d, l$, and $n$ is often fixed

**Anyway** The Bézout bound says there are $\mathfrak{d}^n$ solutions to such polynomial systems: singly exponential if the system is zero-dimensional

# Gröbner bases: [MR13] versus [MM82]

Let $r$ be the dimension of the variety of solutions. Focus on the degrees of the polynomials (more intrinsic than actual times) [MR13] modified both lower and upper bounds to show $\mathfrak{d}^{n^{\Theta(1)}2^{\Theta(r)}}$

lower Essentially, use the $r$-variable [Yap91] ideal

which encodes an EXPSPACE-complete rewriting problem into a system of binomials

note that these ideals are definitely not radical (square-free)

upper A very significant improvement to [Dub90], again using $r$ rather than $n$ where possible

# What we would like to do (but can't)

| | |
|---|---|
| Show | radical ideal problems are only singly-exponential in $n$ |
| This | ought to follow from [Kol88] |
| Show | non-radical ideals are rare (non-square-free polynomials occur with density 0) |
| However | there seems to be no theory of distribution of ideals |
| Deduce | weak worst-case complexity (i.e. apart from an exponentially-rare subset: [AL15]) of Gröbner bases is singly exponential |

# There's a catch [Chi09]

**Theorem**

*$\forall n \geq n_0, d \geq d_0$ there are homogeneous $f_1, \ldots, f_\nu \in k[x_1, \ldots, x_n]$ ($\nu \leq n$, $\deg f_i \leq d$) and a prime ideal $\mathfrak{p}$ such that*

1. *the zeros $\mathcal{Z}(\mathfrak{p})$ coincides with a component, defined over $k$, of $\mathcal{Z}(f_1, \ldots, f_\nu)$, and furthermore $\mathcal{Z}(f_1, \ldots, f_\nu)$ has exactly two components irreducible over $\overline{k}$: $\mathcal{Z}(\mathfrak{p})$ and linear space;*
2. *the Hilbert function of $\mathfrak{p}$ only stabilised after $d^{2^{\Omega(n)}}$;*
3. *the maximum degree of any system of generators of $\mathfrak{p}$ is $d^{2^{\Omega(n)}}$.*

I don't fully understand the construction: it starts with [Yap91], as [MR13], but somehow builds a prime ideal inside this

# A technical complication, and solution

Making sets of polynomials square-free, or even irreducible,

- is computationally nearly always advantageous
- is sometimes required by the theory

**but** might leave the degree alone, or might replace one polynomial by $O(\sqrt{d})$ polynomials

**hard** to control from the point of view of complexity theory.

**Solution** [McC84] Say that a set of polynomials has the $(M, D)$ property if it can be partitioned into $M$ sets, each with combined degree at most $D$ (in each variable)

**This** is preserved by taking square-free decompositions etc.

**Can** Define $(M, \mathfrak{D})$ analogously

# Cylindrical Algebraic Decomposition for polynomials

Assume All CADs we encounter are well-oriented [McC84], i.e. no relevant polynomial vanishes identically on a cell

However there is no theory of distribution of CADs

And Bath has a family of examples which aren't well-oriented

And rescuing from failure is doable, but not well-studied

Note [MPP16] says this is no longer relevant

Then if $A_n$ is the polynomials in $n$ variables, with primitive irreducible basis $B_n$, the projection is

$$A_{n-1} := \mathrm{cont}(A_n) \cup [\mathcal{P}(B_n) := \mathrm{coeff}(B_n) \cup \mathrm{disc}(B_n) \cup \mathrm{res}(B_n)]$$

If $A_n$ has $(M, D)$ then $A_{n-1}$ has $\left((M+1)^2/2, 2D^2\right)$
Hence doubly-exponential growth in $n$
The induction (on $n$) hypothesis is order-invariant decompositions

# Cylindrical Algebraic Decomposition for propositions (1)

Suppose we are tryimg to understand (e.g. quantifier elimination) a proposition $\Phi$ (or set of propositions), and $f(\mathbf{x}) = 0$ is a consequence of $\Phi$ (either explicit or implicit), an equational constraint, and $f$ involves $x_n$ and is primitive
Then [Col98] we are only interested in $\mathbf{R}^n | f(\mathbf{x}) = 0$, not $\mathbf{R}^n$
So [McC99] let $F$ be an irreducible basis for $f$, and use
$\mathcal{P}_F(B) := \mathcal{P}(F) \cup \{\mathrm{res}(f, b) | f \in F, b \in B \setminus F\}$
This has $(2M, 2D^2)$ rather than $(O(M^2), 2D^2)$, but only produces a sign-invariant decomposition

# Cylindrical Algebraic Decomposition for propositions (2)

Generalised to $\mathcal{P}_F^*(B) := \mathcal{P}_F(B) \cup \mathrm{disc}(B \setminus F)$ [McC01], which produces an order-invariant decomposition, and has $(3M, 2D^2)$

If $f(\mathbf{x}) = 0$ and $g(\mathbf{x}) = 0$ are both equational constraints, then $\mathrm{res}_{x_n}(f, g)$ is also an equational constraint

Suppose we have $s$ equational constraints

And (after resultants) we have a constraint in each of the last $s$ variables

And these constraints are all primitive

Then [EBD15] we get $O\left(m^{s2^{n-s}} d^{2^n}\right)$ behaviour

# Recent Developments

CASC 2016[ED16] Under the same assumptions,
$O\left(m^{s2^{n-s}} d^{s2^{n-s}}\right)$ behaviour

using Gröbner bases rather than resultants for the elimination, but multivariate resultants [BM09] for the bounds

ICMS 2016[DE16] The primitivity restriction is inherent: we can write [DH88] in this format, with $n-1$ non-primitive equational constraints

ISSAC2017 (lots) Can do Cylindrical Algebraic Decomposition in 12 variables with 11 equational constraints

# it's not $\mathbf{R}/\mathbf{C}$: it's quantifiers (and alternations)

[DH88, BD07] Are really about the combinatorial complexity of

Let $S_k(x_k, y_k)$ be the statement $x_k = f(y_k)$ and then define recursively $S_{k-1}(x_{k-1}, y_{k-1}) := x_{k-1} = f(f(y_{k-1})) :=$

$$\underbrace{\exists z_k \forall x_k \forall y_k}_{Q_k} \underbrace{((y_{k-1} = y_k \wedge x_k = z_k) \vee (y_k = z_k \wedge x_{k-1} = x_k))}_{L_k} \Rightarrow S_k(x_k, y_k$$

We can transpose this to the complexes, and get zero-dimensional QE examples in $\mathbf{C}^n$ with $2^{2^{O(n)}}$ isolated point solutions, even though the equations are all linear and the solution set is zero-dimensional.

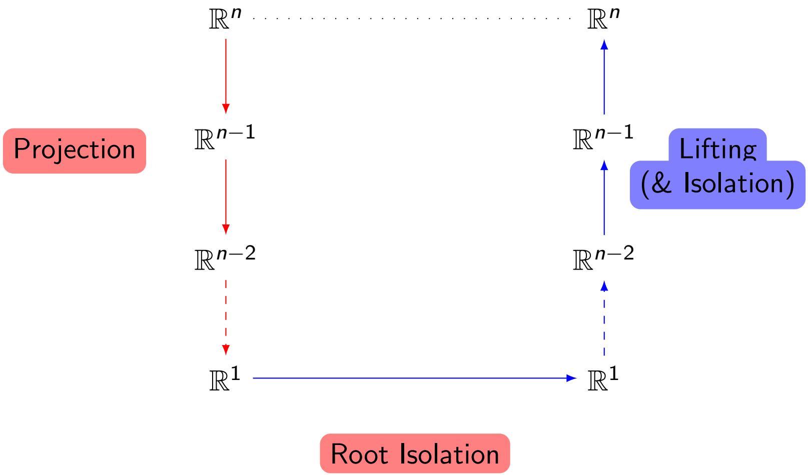
# So let's not be mesmerised by the QE problem

Consider (as we, TS and others have been doing) a single semi-algebraic set defined by

$$f_1(x_1,\ldots,x_{n-1},k_1)=0 \land f_2(x_1,\ldots,x_{n-1},k_1)=0 \land \cdots$$
$$f_{n-1}(x_1,\ldots,x_{n-1},k_1)=0 \land x_1>0 \land \cdots \land x_{n-1}>0$$

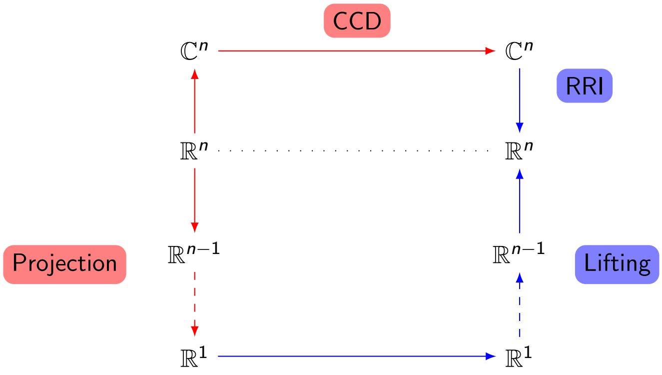
and ask the question "How does the number of solutions vary with $k_1$?" The $f_i$ are multilinear ($d=1$) and primitive, and are pretty "generic".
Of course, this doesn't guarantee that all the iterated resultants in [EBD15], or the Gröbner polynomials in [ED16], are primitive, but in practice they are.

# The basic idea for CAD [Col75]



# An alternative approach [CMXY09]

Proceed via the complex numbers,




Do a complex cylindrical decomposition via Regular Chains, then use Real Root Isolation

# Regular Chain Decompositions

Fix an ordering of variables. The initial of $f$, $\mathrm{init}(f)$, is the leading coefficient of $f$ with respect to its main variable.

## Definition

A list, or chain, of polynomials $f_1, \ldots, f_k$ is a *regular chain* if:

1. whenever $i < j$, $\mathrm{mvar}(f_i) \prec \mathrm{mvar}(f_j)$ (therefore the chain is triangular);
2. $\mathrm{init}(f_i)$ is invertible modulo the ideal $(f_j : j < i)$.

The set of *regular zeros* $W(S)$ of a set $S$ of polynomials is $V(S) \setminus V(\mathrm{init}(S))$.
A (Complex) Regular Chain Decomposition of $I$ is a set of regular chains $T_i$ such that $V(I) = \bigcup W(T_i)$.

Normally (and I wish I knew what that meant) there is one RC of maximal (complex) dimension, and many of lower dimension.

# RealTriangularize (assuming a pure conjunction)

1. Do a CCD of all the equations
2. Make the result SemiAlgebraic over the reals
3. Add all the inequalities, splitting chains as we need to

`LazyRealTriangularize` [CDM+13] doesn't bother with the lower (complex) dimensional components, but wraps then up as unevaluated calls to itself: "Here's the generic answers(s), and how to ask me for the special cases".

In the examples with TS, `LazyRealTriangularize` seems to produce the same answer as the [ED16] version of Projection CAD. This is good news, as what we want should be a geometric invariant.

# Questions?

D. Amelunxen and M. Lotz.
Average-case complexity without the black swans.
http://arxiv.org/abs/1512.09290, 2015.

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.

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.

# Bibliography II

L. Busé and B. Mourrain.
Explicit factors of some iterated resultants and discriminants.
*Math. Comp.*, 78:345–386, 2009.

C. Chen, J.H. Davenport, J.P. May, M. Moreno Maza, B. Xia, and R. Xiao.
Triangular decomposition of semi-algebraic systems.
*J. Symbolic Comp.*, 49:3–26, 2013.

A.L. Chistov.
Double-exponential lower bound for the degree of any system of generators of a polynomial prime ideal.
*St. Petersburg Math. J.*, 20:983–1001, 2009.

# Bibliography III


C. Chen, M. Moreno Maza, B. Xia, and L. Yang.
Computing Cylindrical Algebraic Decomposition via Triangular Decomposition.
In J. May, editor, *Proceedings ISSAC 2009*, pages 95–102, 2009.

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

V


T.W. Dubé.
The structure of polynomial ideals and Gröbner Bases.
*SIAM J. Comp.*, 19:750–753, 1990.

M. England, R. Bradford, and J.H. Davenport.
Improving the Use of Equational Constraints in Cylindrical Algebraic Decomposition.
In D. Robertz, editor, *Proceedings ISSAC 2015*, pages 165–172, 2015.

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.

J. Kollár.
Sharp effective nullstellensatz.
*J.A.M.S.*, 1:963–975, 1988.

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.
On Propagation of Equational Constraints in CAD-Based Quantifier Elimination.
In B. Mourrain, editor, *Proceedings ISSAC 2001*, pages 223–230, 2001.

E. Mayr and A. Meyer.
The Complexity of the Word Problem for Commutative Semi-groups and Polynomial Ideals.
*Adv. in Math.*, 46:305–329, 1982.

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

E.W. Mayr and S. Ritscher.
Dimension-dependent bounds for Gröbner bases of polynomial ideals.
*J. Symbolic Comp.*, 49:78–94, 2013.

C.K. Yap.
A new lower bound construction for commutative Thue systems with applications.
*J. Symbolic Comp.*, 12:1–27, 1991.