Complexity of Equation Solving

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

29 April 2016

[1]Thanks to Matthew England (Coventry), EPSRC EP/J003247/1,

Theoretical versus Practical Complexity

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

Theoretical doubly exponential, whether via Gröbner bases [MM82, Yap91, lower], [Dub90, upper] or Cylindrical Algebraic Decomposition [DH88, BD07]

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 polynomials: singly exponential

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]

What we would like to do

- 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

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.

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

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 Φ (or set of propositions), and $f(\mathbf{x}) = 0$ is a consequence of Φ (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

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

[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 $S_{k-1}(x_{k-1}, y_{k-1}) := x_{k-1} = f(f(y_{k-1})) :=$

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

Questions?

Bibliography

I

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.

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

Bibliography II

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

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.

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.

Bibliography

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.