Varieties of Doubly-Exponential Behaviour in Cylindrical Algebraic Decomposition

James H. Davenport[1]

University of Bath, Bath BA2 7AY, United Kingdom
J.H.Davenport@bath.ac.uk

16 August 2021 at SIAM AG21

[1] Support of EPSRC (Grant EP/T015713/1) is gratefully acknowledged.

Plan of Talk

1. Introduction
2. The Heintz Construction and Examples
3. Graphs and Chordality
4. Equational Constraints
5. Challenges
6. Q&A

Notation

- a The number of *alternations* of quantifiers: $\exists\forall\forall\exists$ has $a = 2$.
- c The number of equational constraints.
- d The maximum degree of the polynomials (in any specific x_i, not total degree)
- l Maximum bit-length of coefficients
- m Number of polynomials.
- n Number of variables $x_1, \ldots, x_n$.
- s Number of iterations of the Heintz construction [Hei83].

McCallum's Notation [McC84]

Relatively prime square-free decompositions of sets of polynomials are an important requirement in many of these algorithms.
But this may increase the number of polynomials, and isn't guaranteed to reduce the degree, so is a nuisance for complexity theory.

Notation (McCallum)

We say that a set $S \subset K[x_1, \ldots, x_n]$ *has the* (M, D) *property if it can be partitioned into* $\leq M$ *sets, and the product of the polynomials in each set has degree* $\leq D$.

Proposition

The set of discriminants of an (M, D) *set is an* $(M, 2D^2)$ *set.*

Proposition

The set of resultants of an (M, D) *set is an* $(\frac{1}{2}M(M-1), 2D^2)$ *set*

1951 [Tar51] shows that quantifier elimination in $\mathbb{Q}[x_1, \ldots, x_n]$ is decidable.

1975 [Col75] produces "cylindrical algebraic decomposition" with doubly exponential complexity $(2n + O(1))$. See also [Wüt76].

* Every time we eliminate a variable, we square both d and m (at least).

1984 [McC84] if the problem is "well-oriented" (certain polynomials don't vanish on certain varieties), then doubly exponential complexity $(\cancel{2}n + O(1))$.

1986 JHD sits down with Joos Heintz and drafts [DH88] showing that real quantifier elimination has doubly exponential lower complexity $(\frac{1}{5}n + O(1))$.

2019 [MPP19] justified the Lazard projection/lifting [Laz94]: $\cancel{2}n + O(1)$ without a well-oriented requirement.

The Heintz Construction [Hei83]

$$\begin{aligned} f_2(z_1,z_2) := \quad & \exists y \forall x_1 \forall x_2 \quad (((x_1 = z_1) \wedge (x_2 = y)) \vee \\ & \qquad ((x_1 = y) \wedge (x_2 = z_2)) \Rightarrow f_1(x_1,x_2)) \end{aligned}$$

simplifies to

$$f_2(z_1,z_2) := \exists y \; f_1(z_1,y) \wedge f_1(y,z_2)$$

If $f_1(x_1,x_2)$ is of the form $x_1 = g(x_2)$, then f_2 is $z_1 = g(g(z_2))$, f_3 is $x_1 = \underbrace{g(\cdots g(}_{\times 4} x_2)\cdots)$, f_4 is $z_1 = \underbrace{g(\cdots g(}_{\times 16} z_2)\cdots)$, etc.

Davenport–Heintz Application [DH88]

We used $z_{1,R}, z_{1,I}$ rather than just z_1 (also z_2, x_1, x_2, y), and $f_1(x_{1,R}, x_{1,I}, x_{2,R}, x_{2,I})$ is the $\wedge$ of the real and imaginary parts of $(x_{1,R} + ix_{1,I})^4 = x_{2,R} + ix_{2,I}$.
f_2 is then $\exists y : z_1^4 = y \wedge y^4 = z_2$ (in complexes) so $z_1^{16} = z_2$. In reals this is $\wedge$ of the real and imaginary parts of $(z_{1,R} + iz_{1,I})^{16} = z_{2,R} + iz_{2,I}$, at the cost of six quantifiers (and two alternations), and the construction can be repeated (swapping x and z).
We set the last z_2 to be 1, and have constructed the 4^{2^s} complex roots of unity with s iterations.
In fact it can be brought down to five quantifiers, giving a lower bound double exponent of $\frac{1}{5}n + O(1)$.

“Doubly Exponential” versus Bézout [Béz79]

But the Bézout bound is singly exponential!
Suppose f, g, h have degree d in each variable (x, y, z).
Then $\mathrm{res}_x(f, g)$ has degree $2d^2$ and is zero at $\{(y, z) | \exists x : f(x, y, z) = g(x, y, z) = 0\}$.
Then $\mathrm{res}_y(\mathrm{res}_x(f, g), \mathrm{res}_x(f, h))$ has degree $8d^4$ and is zero at $\{z | \exists y (\exists x_1 : f(x_1, y, z) = g(x_1, y, z) = 0) \wedge (\exists x_2 : f(x_2, y, z) = h(x_2, y, z) = 0)\}$: both the genuine “triple zeros” $(x_1 = x_2)$ and spurious zeros.
The Boolean structure of the Heintz construction allows us to leverage the spurious zeros, and hence we get the double exponential behaviour.
However, if we have a simple situations and equational constraints, Gröbner bases can be very useful [EBD20].

A note on satisfiability

What if one solution is enough? Although we have constructed $z_1^{4^{2^s}} = z_2$ in s iterations of the Heintz construction, or the 4^{2^s} roots of unity, it can be objected that 1 is still a solution.
If we add that $0 < z_{1,R} < 1$, this rules that (and $-1, \pm i$ out, but still allows the relatively simple $\frac{1+i}{\sqrt{2}}$. To rule this out, we need tighter bounds, and it would seem that a difficult example (rather than all examples) requires high-complexity inequalities.
There is another solution: at the cost of a constant overhead, we can ask for $z_1^{4^{2^s}} = z_2 \wedge z_1^{4^{2^{s-1}}} \neq z_2$, which means we have solutions all of which are defined by truly high-degree polynomials.

Problem

Find a neat formulation of this construction, in particular the growth in l.

Instead we let

$$f_1(x_1, x_2) = (x_1 \leq \frac{1}{2} \wedge x_2 = 2x_1) \vee (x_1 > \frac{1}{2} \wedge x_2 = 2 - 2x_1)$$

(a $\bigwedge$ shape). Then $x_2 = \frac{1}{2}$ has two solutions ($x_1 = \frac{1}{4}, \frac{3}{4}$) and as we iterate, we get 2^{2^s} solutions, at $\frac{\text{odd}}{2^{2^s+1}} \in [0, 1]$.
Note that $l = 2^s + 1$ is only singly exponential, and satisfiability is relatively simple.

Brown–Davenport example [BD07, Theorem 7]

The ordering among the x_i can be crucial.

[BD07] This exhibits a polynomial p in $3n+4$ variables such that *any* CAD, w.r.t. one order, of R^{3n+4} sign-invariant for p has $O\left(2^{2^n}\right)$ cells, but w.r.t. another order has 3 cells.

Hence numerous heuristics to choose the order [DSS04, Bro04, and many more]

And an interest in machine learning for orders [HEW+19].

The Polynomial

$$
\begin{aligned}
p := x^{n+1} &\left(\left(y_{n-1}-\tfrac{1}{2}\right)^2+\left(x_{n-1}-z_n\right)^2\right)\left(\left(y_{n-1}-z_n\right)^2+\left(x_{n-1}-x_n\right)^2\right. \\
+\textstyle\sum_{i=1}^{n-1} x^{i+1} &\left(\left(y_{i-1}-y_i\right)^2+\left(x_{i-1}-z_i\right)^2\right)\left(\left(y_{i-1}-z_i\right)^2+\left(x_{i-1}-x_i\right)^2\right. \\
&+x\left(\left(y_0-2x_0\right)^2+\left(\alpha^2+\left(x_0-\tfrac{1}{2}\right)\right)^2\right)\times \\
&\left(\left(y_0-2+2x_0\right)^2+\left(\alpha^2+\left(x_0-\tfrac{1}{2}\right)\right)^2\right)+a.
\end{aligned}
$$

- The bad order (eliminating x, then $y_0, \alpha, x_0, z_1, y_1, z_1, \ldots,$ x_n, a) needs $O\left(2^{2^n}\right)$ (Maple: 141 when $n = 0$) cells.
- Any order eliminating a first says that R^{3n+3} is undecomposed, and the only question is $p = 0$, which is linear in a, and we get three cells: $p < 0$, $p = 0$ and $p > 0$.
- However, if we replace a by a^3, the topology is essentially the same, but the discriminant is no longer trivial, and the "good" order now takes 213 cells in Maple.

More application of Heintz?

- D–Heintz: Used a complex polynomial (real and imaginary parts), hence $\frac{1}{5}n + O(1)$.
- $+$ Doubly exponential degree for a single solution.
- Brown–D: Used a simple sawtooth over the reals, hence $\frac{1}{3}n + O(1)$ (the natural limit of Heintz).
- – Each solution is only singly exponential.
- ? Are there examples with both properties?

  Probably so, but requires understanding $\underbrace{f(f(\cdots f(}_{\times 2^{2^s}}x)\cdots)$ for suitable f:
- ?? can we force this irreducible, very close roots etc.

Graph Theory to the rescue?

Instead of considering degrees of the polynomials in F, consider the graph $\mathcal{G}(F)$ on $\{x_1, \ldots, x_n\}$ with an edge betwen (x_i, x_j) iff there is a polynomial in F contaning both x_i and x_j.

Connectedness?

Gröbner
: If $\mathcal{G}(F)$ is not connected, the problems are independent, and [Buc79, Criterion 1] will treat them as such.

CAD
: Essentially independent, but this is hard to describe: we have "the outer product" of the two (or more) CADs. We definitely need to project one component at a time.

Problem

Recognise, and treat effectively, this case, also "nearly disconnected" (see next)

Graph Theory to the rescue continued

A graph $\mathcal{G}$ is *chordal* if every >3-cycle has a chord. Equivalently, every induced cycle has length 3. Every graph $\mathcal{G}$ has a chordal completion $\overline{\mathcal{G}}$.

Minimum chordal completion is NP-complete [Yan81], but that doesn't really worry me.

If this is the complete graph, then graph theory doesn't seem to help us: the exciting case is when $\overline{\mathcal{G}}$ is smaller.

An ordering $\succ$ on the vertices $x_1, \ldots, x_n$ is a *perfect elimination ordering* if $\forall i$ x_i and its neighbours $x_j : x_j \prec x_i$ form a clique. This, and chordality, can be found efficiently [RTL76].

Let n' be the maximal length of a path from x_1 to x_n in $\mathcal{G}$ following $\succ$.

Graph Theory to the rescue continued

Non-trivial chordality has been exploited.

Regular Chains [Che20] shows how it can be exploited efficiently.

Gröbner Bases [CP16] consider "chordal elimination". The challenge here is that an S-polynomial can introduce new edges in $\mathcal{G}$.

CAD [LXZZ21] consider chordality, ordering x_i in a perfect elimination ordering, then essentially use the same algorithm.

Double exponent is now n' rather than n (polynomials "drop through" layers!).

The quantifier structure may be incompatible with the perfect elimination ordering.

What we currently lack is any view of how common in practice these non-trivial chordal structures are, but they are related to "nearly disconnected" $\mathcal{G}$.

Equational Constraints

[Col98] What if our formula Φ is $f = 0 \wedge \hat{\Phi}$, where $\hat{\Phi}$ involves $m-1$ polynomials g_i?

[McC99] Answers this: we only need $O(m)$ $\mathrm{res}_x(f, g_i)$, not $O(m^2)$ $\mathrm{res}_x(g_i, g_j)$, since

$$\mathrm{res}_x(g_i, g_j)|_{f=0} \propto \mathrm{res}_y(\mathrm{res}_x(f, g_i), \mathrm{res}_x(f, g_j)). \tag{1}$$

Means that, after the x projection, we only have $O(m)$ polynomials not $O(m^2)$.

[McC01] Generalises to $f_1 = 0 \wedge \cdots \wedge f_c = 0 \wedge \hat{\Phi}$.

$+$ Reduces the double exponent of m from n to $n-c$.

[BDE+16] Generalises to where only part of the formula has equational constraints: "truth-table invariant CAD"

[EBD20] Can use Gröbner bases, rather than just iterated resultants, to reduce degree growth, ideally the double exponent of d becomes $n-c$.

But All this is for the McCallum projection, i.e. well-oriented.

Doesn't Lazard projection/lifting eliminate "well-oriented"?

+ Yes, for straight cylindrical algebraic decomposition

But if $f(x, y, z, \ldots)$ vanishes identically on some surface $S(y, z, \ldots)$, the constant of proportionality in (1) is 0, and we learn nothing about $\mathrm{res}_x(g_i, g_j)$ from $\mathrm{res}_x(f, x_i)$.

"Nullification" has come back to bite us, but only nullification of f, not the g_i.

Call S the *foot* of the curtain $f = 0$ [NDS20].

dim(S) The case $\dim(S) = 0$ is tractable [Nai21] — see that thesis for more details of $\dim(S) > 0$.

Challenges

1. More applications of Heintz construction.
2. The argument in [EBD20], that Gröbner bases reduced degree growth, depended on genericity: what if one has doubly exponential growth in Gröbner degree [MR13]? Being radical doesn't necessarily help [Chi09].
3. Curtains with $\dim(S) > 0$.
4. What are "typical" problems for QE/CAD — note many verification examples are purely existential, *but* want a proof of non-satisfiability [ADEK21].

Hope Quantifier Elimination has weak singly exponential complexity in the sense of [AL15], i.e. the doubly exponential examples are exponentially rare.

Q&A

? Any questions?

Bibliography I

- E. Ábrahám, J.H. Davenport, M. England, and G. Kremer.
  Proving UNSAT in SMT: The Case of Quantifier Free Non-Linear Real Arithmetic.
  https://www.researchgate.net/publication/353838748_Proving_UNSAT_in_SMT_The_Case_of_Quantifier_Free_Non-Linear_Real_Arithmetic/references, 2021.

- 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.

Bibliography II

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.

E. Bézout.
Théorie générale des équations algébriques.
Ph.-D. Pierres, 1779.

C.W. Brown.
Tutorial handout.
`http://www.cs.usna.edu/~wcbrown/research/ISSAC04/handout.pdf`, 2004.

B. Buchberger.
A Criterion for Detecting Unnecessary Reductions in the Construction of Groebner Bases.
In *Proceedings EUROSAM 79*, pages 3–21, 1979.

Changbo Chen.
Chordality Preserving Incremental Triangular Decomposition and Its Implementation.
volume 12097 of *Springer Lecture Notes in Computer Science*, pages 27–38. 2020.
URL: https://www.researchgate.net/publication/342758264_Chordality_Preserving_Incremental_Triangular_Decomposition_and_Its_Implementation, doi:10.1007/978-3-030-52200-1_3.

Bibliography IV

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.

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.

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.

D. Cifuentes and P. Parrilo.
Exploiting chordal structure in polynomial ideals: A Grobner bases approach.
SIAM Journal on Discrete Mathematics, 30:1534–1570, 2016.

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

A. Dolzmann, A. Seidl, and Th. Sturm.
Efficient Projection Orders for CAD.
In J. Gutierrez, editor, *Proceedings ISSAC 2004*, pages 111–118, 2004.

M. England, R.J. Bradford, and J.H. Davenport.
Cylindrical Algebraic Decomposition with Equational Constraints.
In J.H. Davenport, M. England, A. Griggio, T. Sturm, and C. Tinelli, editors, *Symbolic Computation and Satisfiability Checking: special issue of Journal of Symbolic Computation*, volume 100, pages 38–71. 2020.

J. Heintz.
Definability and Fast Quantifier Elimination in Algebraically Closed Fields.
Theor. Comp. Sci., 24:239–277, 1983.

Z. Huang, M. England, D. Wilson, J.H. Davenport, and L.C. Paulson.
Using Machine Learning to Improve Cylindrical Algebraic Decomposition.
Mathematics in Computer Science, 11:461–488, 2019.

D. Lazard.
An Improved Projection Operator for Cylindrical Algebraic Decomposition.
In C.L. Bajaj, editor, *Proceedings Algebraic Geometry and its Applications: Collections of Papers from Shreeram S. Abhyankar's 60th Birthday Conference*, pages 467–476, 1994.

H. Li, B. Xia, H. Zhang, and T. Zheng.
Choosing the Variable Ordering for Cylindrical Algebraic Decomposition via Exploiting Chordal Structure.
ISSAC '21: Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation, pages 281–288, 2021.

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.

S. McCallum, A. Parusiński, and L. Paunescu.
Validity proof of Lazard's method for CAD construction.
J. Symbolic Comp., 92:52–69, 2019.

Bibliography X

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

A.S. Nair.
Exploiting Equational Constraints to Improve the Algorithms for Computing Cylindrical Algebraic Decompositions.
PhD thesis, University of Bath, 2021.

A.S. Nair, J.H. Davenport, and G.K. Sankaran.
Curtains in CAD: Why Are They a Problem and How Do We Fix Them?
In *Proceedings ICMS 2020*, volume 12097 of *Springer Lecture Notes in Computer Science*, pages 17–26. Springer, 2020.

Donald J Rose, R Endre Tarjan, and George S Lueker.
Algorithmic aspects of vertex elimination on graphs.
SIAM Journal on computing, 5(2):266–283, 1976.

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.

H.T. Wüthrich.
Ein Entscheidungsverfahren für die Theorie der reell-abgeschlossenen Körper.
In E. Specker and V. Strassen, editors, *Proceedings Komplexität von Entschiedungsproblemen*, pages 138–162, 1976.

Bibliography XII

Mihalis Yannakakis.
Computing the minimum fill-in is NP-complete.
SIAM Journal on Algebraic Discrete Methods, 2(1):77–79, 1981.