Cylindrical Algebraic Decomposition with Logical Structure

James Davenport (Bath

Thanks to Russell Bradford (Bath), Matthew England (Coventry), David Wilson (Bath/Silicon Valley), Marc Moreno Maza (U.W.O.), Changbo Chen (Chongqing), Scott McCallum (Macquarie); and EPSRC grant: EP/J003247/1

14 December 2015

Overview

History of Quantifier Elimination

- In 1930, Tarski discovered [Tar51] that the (semi-)algebraic theory of $\mathbf{R}^n$ admitted quantifier elimination

  $\exists x_{k+1} \forall x_{k+2} \ldots \Phi(x_1, \ldots, x_n) \equiv \Psi(x_1, \ldots, x_k)$
- "Semi" = "allowing $>$, $\leq$ and $\neq$ as well as $=$"
- Needed as $\exists y : x = y^2 \Leftrightarrow x \geq 0$
- The complexity of this was indescribable
- In the sense of not being elementary recursive!
- In 1973, Collins [Col75] discovered a much better way:
- Complexity (m polynomials, degree d, n variables, coefficient length l)

$$(2d)^{2^{2n+8}} m^{2^{n+6}} l^3 \qquad (1)$$

- Construct a cylindrical algebraic decomposition of $\mathbf{R}^n$, sign invariant for every polynomial
- Then read off the answer

What is a CAD?

A Cylindrical Algebraic Decomposition (CAD) is a mathematical object. Defined by Collins who also gave the first algorithm to compute one. A CAD is:

- a decomposition meaning a partition of $\mathbf{R}^n$ into connected subsets called cells;
- (semi-)algebraic meaning that each cell can be defined by a sequence of polynomial equations and inequalities;
- cylindrical meaning the cells are arranged in a useful manner — their projections are either equal or disjoint.

In addition, there is (usually) a sample point in each cell, and an index locating it in the decomposition

“Read off the answer”

- Each cell is sign invariant, so the the truth of a formula throughout the cell is the truth at the sample point.
- $\forall x F(x) \Leftrightarrow$ “$F(x)$ is true at all sample points”
- $\exists x F(x) \Leftrightarrow$ “$F(x)$ is true at some sample point”
- $\forall x \exists y F(x,y) \Leftrightarrow$ “take a CAD of $\mathbf{R}^2$, cylindrical for y projected onto x-space, then check

$$\forall \text{ sample } x \ \exists \text{ sample } (x,y) : F(x,y) \text{ is true''}: \text{ finite check}$$

NB The order of the quantifiers defines the order of projection

So all we need is a CAD!

The basic idea for CAD [Col75]

$$
\begin{tikzcd}
\mathbb{R}^n \arrow[d] \arrow[r, dotted, no head] & \mathbb{R}^n \\
\mathbb{R}^{n-1} \arrow[d] & \mathbb{R}^{n-1} \arrow[u] \\
\mathbb{R}^{n-2} \arrow[d, dashed] & \mathbb{R}^{n-2} \arrow[u] \\
\mathbb{R}^1 \arrow[r] & \mathbb{R}^1 \arrow[u, dashed]
\end{tikzcd}
$$

Projection

Lifting
(& Isolation)

Root Isolation

So how do we project? (Lifting is in fact relatively straight-forward)

Given polynomials $\mathcal{P}_n = \{p_i\}$ in $x_1, \ldots, x_n$, what should $\mathcal{P}_{n-1}$ be?

- **Naïve** (Doesn't work!) Every $\mathrm{Disc}_{x_n}(p_i)$, every $\mathrm{Res}_{x_n}(p_i, p_j)$
- **i.e.** where the polynomials fold, or cross: misses lots of "special" cases
- **[Col75]** First enlarge $\mathcal{P}_n$ with all its reducta, then naïve plus the coefficients of $\mathcal{P}_n$ (with respect to x_n) the principal subresultant coefficients from the Disc_{x_n} and Res_{x_n} calculations
- **[Hon90]** a tidied version of [Col75].
- **[McC88]** Let $\mathcal{B}_n$ be a squarefree basis for the primitive parts of $\mathcal{P}_n$. Then $\mathcal{P}_{n-1}$ is the contents of $\mathcal{P}_n$, the coefficients of $\mathcal{B}_n$ and every $\mathrm{Disc}_{x_n}(b_i)$, $\mathrm{Res}_{x_n}(b_i, b_j)$ from $\mathcal{B}_n$
- **[Bro01]** Naïve plus leading coefficients (not squarefree!)

Setting

Cylindrical Algebraic Decomposition in $\mathbf{R}[x_1, \ldots, x_n]$, with x_n the first variable to be eliminated.
General method via Projection/Lifting in the style of [Col75, Ẅ76].

Open Problem

Extend part 2 of this to the Regular Chains approach [CMXY09]

- [Col75] A cylindrical decomposition of $\mathbf{R}^n$ *sign-invariant* for each polynomial
- [McC84] A cylindrical decomposition of $\mathbf{R}^{n-1}$ *order-invariant* for each polynomial at this stage, and a cylindrical decomposition of $\mathbf{R}^n$ *sign-invariant* for each polynomial
  - or failure if the polynomials were not well-oriented which occurs with probability 0 in theory, but quite often in practice.
- EC An *equational constraint* is $f(\mathbf{x}) = 0 \land \cdots$

Are these projections correct?

[Col75] Yes, and it's relatively straightforward to prove that, over a cell in $\mathbf{R}^{n-1}$ sign-invariant for $\mathcal{P}_{n-1}$, the polynomials of $\mathcal{P}_n$ do not cross, and define cells sign-invariant for the polynomials of $\mathcal{P}_n$

[McC88] 52 pages (based on [Zar75]) prove the equivalent statement, but for order-invariance, not sign-invariance, provided the polynomials are well-oriented, a test that has to be applied during lifting.

But if they're not known to be well-oriented?

[McC88] suggests adding all partial derivatives

In practice hope for well-oriented, and if it fails use Hong's projection.

[Bro01] Needs well-orientedness and additional checks

Motivations for cylindrical algebraic decomposition

1. Quantifier elimination — the original one
   * May have local or global equational constraints
2. Robot Motion Planning — [SS83]
   * Normally has local and global equational constraints
3. Branch Cut analysis [BBDP07]
   * Normally has local equational constraints

Note that we can sometimes transform local ECs into global:

$$(f_1 = 0 \land \phi_1) \lor (f_2 = 0 \land \phi_2)$$

is equivalent to

$$f_1 f_2 = 0 \land [(f_1 = 0 \land \phi_1) \lor (f_2 = 0 \land \phi_2)]$$

Mostly applicable to Quantifier Elimination

Complexity Analysis for [McC84]

Assume m polynomials of degree (in each variable) $\leq d$.
Measure the *number of cells* in the output.
Upper bounds

[McC85, Theorem 6.1.5] $m^{2^n}(2d)^{n2^n}$

[BDE+14, (12)] $2^{2^{n-1}}m(m+1)^{2^n-2}d^{2^n-1}$

* (Same algorithm, better analysis)

Lower bounds (actually of cells in $\mathbf{R}^1$)

[DH88]; $d=4$ $2^{2^{(n-1)/5}}$, and these are the roots of a polynomial of this degree

[BD07]; $d=1$ $2^{2^{(n-1)/3}}$, and in $\mathbf{R}^1$ these are rationals with a succint description.

The original EC observation [Col98, McC99b]

If we have a global equational constraint $f = 0 \wedge \phi$, then all we need is a decomposition that is

1. Sign (or order) invariant for f
2. Sign (or order) invariant for the polynomials g_i of ϕ *when* $f = 0$

Intuitively, we can do this by considering f and $\mathrm{Res}_{x_n}(f, g_i)$ rather than f and g_i for the first projection level, build the order-invariant decomposition of $\mathbf{R}^{n-1}$ for these polynomials (as before), then lift to a sign-invariant decomposition of $\mathbf{R}^n$

Number of cells bounded by [BDE⁺14, (14)]

$$2^{2^{n-1}} d^{2^n-1} m(3m+1)^{2^{n-1}-1},$$

which is "intuitively reasonable" — we can do nothing about degree growth, but combinatorial growth is as for one fewer variable

The theorem that justifies this [McC99b]

Theorem (McCallum1999)

Let f and g be integral polynomials with mvar x_n, and $r(x_1,\ldots,x_{n-1})\neq 0$ be their resultant. Let S be a connected subset of $\mathbf{R}^{n-1}$ on which f is delineable and r order-invariant. Then g is sign-invariant in every section of f over S.

So we can use the McCallum projection

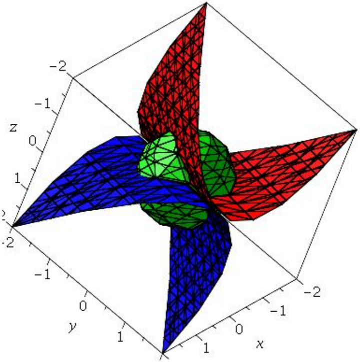
$$P(B) := \mathrm{coeff}(B)\cup \mathrm{Disc}(B)\cup \mathrm{Res}(B)$$

after x_n, where B is the square-free basis of the polynomials, and

$$P_F(B) := P(F)\cup\{\mathrm{Res}(f,g) | f\in F; g\in B\setminus F\}$$

at x_n, where F is the square-free basis of the equational constraint. Note that this theorem does not compose nicely with itself.

Example



$f_1 = x + y^2 + z$
$f_2 = x - y^2 + z$
$g = x^2 + y^2 + z^2 - 1$
$f_1 = 0 \wedge f_2 = 0 \wedge g \geq 0$

Solutions: $y = 0$, $|x| \geq \frac{1}{2}\sqrt{2}$, $z = -x$ (4 cells)
Sign-invariant c.a.d. for $\{f_1, f_2., g\}$ has 1487 cells
Declaring either equational constraint gives 289 cells, but the solution is 8 cells since we have $x = \frac{1}{2}(1 \pm \sqrt{6})$ as additional points from $\mathrm{Disc}_y(\mathrm{Res}_z(f_1, g))$

Part 1: local equational constraints [BDE+13]

Suppose we are doing quantifier elimination on $\phi_1 \vee \phi_2 \vee \cdots$, where each ϕ_i is $f_i = 0 \wedge g_i > 0$ (for simplicity).
There is an implicit equation constraint $F := \prod f_i = 0$, and using [McC99a] our first projection is (ignoring coefficients) $\mathrm{Disc}(F) \cup \{\mathrm{Res}(F, g_i)\}$, which is

$$\{\mathrm{Disc}(f_i)\} \cup \{\mathrm{Res}(f_i, f_j)\} \cup \{\mathrm{Res}(f_i, g_{\color{red}j})\}$$

But this includes $\mathrm{Res}(f_i, g_j)$ $(i \neq j)$, which is logically unnecessary, but is needed to give us a decomposition sign-invariant for each f_i, g_j when $F = 0$.
Relax to demanding a decomposition that's truth-invariant for each ϕ_i:

$$\{\mathrm{Disc}(f_i)\} \cup \{\mathrm{Res}(f_i, f_j)\} \cup \{\mathrm{Res}(f_i, g_{\color{red}i})\}$$

Very useful for the branch cut problem

Local equational constraints continued [BDE+14]

But suppose only *some* ϕ_i have equational constraints, so there isn't a global implicit equational constraint.
Then for those ϕ_i that *do* have an equational constraint $f_i = 0$, the corresponding g_i (possibly many) need only feature in $\mathrm{Res}(f_i, g_i)$: for those ϕ_i with no equational constraint, the g_i feature as usual.

Part 2: A better theorem [McC01]

Theorem (McCallum2001)

Let f and g be integral polynomials with mvar x_n, and $r(x_1,\ldots,x_{n-1})\neq 0$ be their resultant, $d(x_1,\ldots,x_{n-1})\neq 0$ be the discriminant of g. Let S be a connected subset of $\mathbf{R}^{n-1}$ on which f is analytic delineable, g not nullified and r,d order-invariant. Then g is order-invariant in every section of f over S.

This justifies using

$$P_F^*(B) := P_F(B)\cup \mathrm{Disc}(B\setminus F)$$

at levels below x_n where there is an equational constraint, however we need to assume the constraints are primitive.
If we have $f_1=f_2=0$ at x_n, we use $f_1=0$ here, and $\mathrm{Res}(f_1,f_2)$ at level x_{n-1}, etc.
The double exponent of m is reduced by the number of equational constraints.

Better Projection, yes but . . .

Everyone knows that the main cost of c.a.d. is in the lifting. We can also get better lifting, providing we abandon two key principles:

1. That the projection polynomials are a fixed set.
2. That the invariance structure of the final CAD can be expressed in terms of sign-invariance of polynomials.

Idea 1: forget polynomials

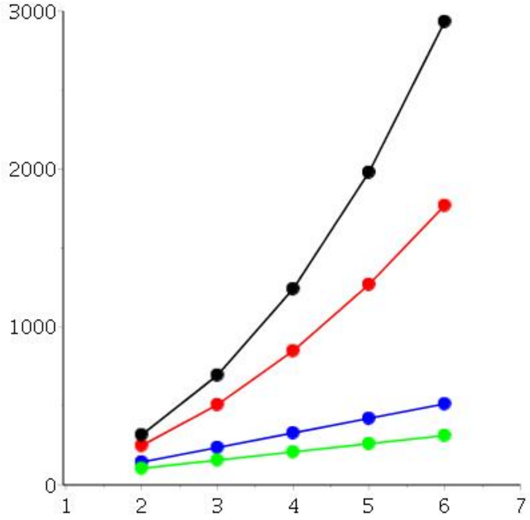
The 1999 theorem states "g is sign-invariant in every section of f over S."

Hence g is unnecessary at the final lift.

Follows from [McC99a], but only noticed in [BDE$^+$13]

Pragmatically very important, but we don't have a theoretical analysis

Idea 1 — Graph of #cells ($n = 2$; $d = 2$; $m = 2 \times x$-axis)



Full CAD
QEPCAD with EC
Our EC with Idea 1
TTICAD

Idea 2: forget sign-invariance

If a cell in $\mathbf{R}^k$ is already known to be false, there is no point doing any (non-trivial) lifting over it.
If we have $f_1 = 0 \wedge f_2 = 0 \wedge \ldots$, then in R^{n-2} we will be looking at the zeros of $\mathrm{Res}_{x_n}(f_1, f_2)$. Away from the zeros of this, $f_1 = 0 \wedge f_2 = 0$ is trivially false, so we needn't do any lifting.
Also, no lifting over C means no nullification worries over C, since this is a *local* concern.

Open Problem

Extend the Phase 2 ideas to merge with Phase 1 (done for some of the lifting reduction)

This seems needed for

Open Problem

Handle non-primitive equational constraints:
$f = 0 \Leftrightarrow \mathrm{pp}_{x_n}(f) = 0 \vee \mathrm{cont}_{x_n}(f) = 0$

Open Problem

Combine this with [BM09] on iterated resultants.

Bibliography

J.C. Beaumont, R.J. Bradford, J.H. Davenport, and N. Phisanbut.
Testing Elementary Function Identities Using CAD.
AAECC, 18:513–543, 2007.

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.
Cylindrical Algebraic Decompositions for Boolean Combinations.
In *Proceedings ISSAC 2013*, pages 125–132, 2013.

Bibliography II

R.J. Bradford, J.H. Davenport, M. England, S. McCallum, and D.J. Wilson.
Truth Table Invariant Cylindrical Algebraic Decomposition.
To appear in J. Symbolic Computation, 2014.

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

C.W. Brown.
Improved Projection for Cylindrical Algebraic Decomposition.
J. Symbolic Comp., 32:447–465, 2001.

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

Bibliography

V

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.

H. Hong.
Improvements in CAD-Based Quantifier Elimination.
PhD thesis, OSU-CISRC-10/90-TR29 Ohio State University, 1990.

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

S. McCallum.
An Improved Projection Operation for Cylindrical Algebraic Decomposition.
Technical Report 548 Computer Science University Wisconsin at Madison, 1985.

S. McCallum.
An Improved Projection Operation for Cylindrical Algebraic Decomposition of Three-dimensional Space.
J. Symbolic Comp., 5:141–161, 1988.

S. McCallum.
Factors of iterated resultants and discriminants.
J. Symbolic. Comp., 27:367–385, 1999.

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.

J.T. Schwartz and M. Sharir.
On the "Piano-Movers" Problem: II. General Techniques for Computing Topological Properties of Real Algebraic Manifolds.

Adv. Appl. Math., 4:298–351, 1983.

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.

O. Zariski.
On equimultiple subvarieties of algebroid hypersurfaces.
Proc. Nat. Acad. Sci., 72:1425–1426, 3260, 1975.