More than one equation constraint in Cylindrical Algebraic Decomposition

James Davenport [1]
University of Bath, U.K.
Supported by EPSRC EP/J003247/1

SIAM AAG 15/ 3–7 August 2015

[1] Thanks to: Russell Bradford, Matthew England, David Wilson (Bath), Changbo Chen (Chinese Academy of Sciences, Chongqing), Scott McCallum (Macquarie), Marc Moreno Maza (Western Ontario)

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 any tower of exponentials!
- In 1973, Collins [Col75] discovered a much better way:
- Complexity (m polynomials, degree d, n variables, coefficient length l)
$$(2d)^{2^{2n+8}} m^{2^{n+6}} l^3 \tag{1}$$
- 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 inequations;
- 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"

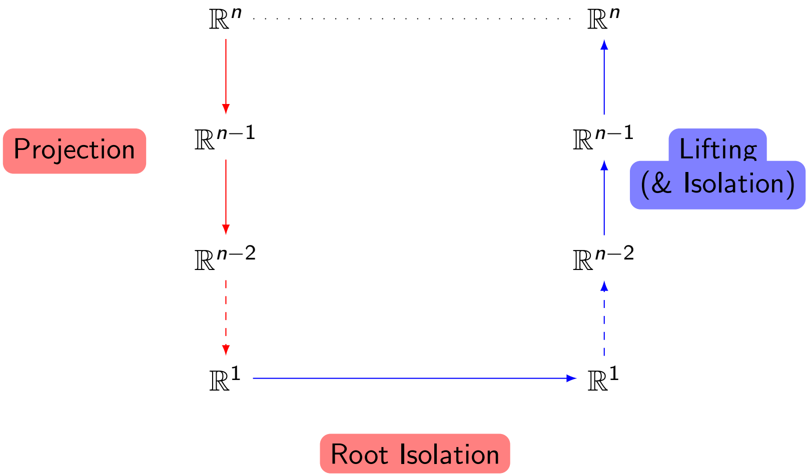
- Each cell is sign invariant, so the the truth of a formula throughout the cell is the truth at the sample point.
- $\forall x F(x) \Leftrightarrow$ "$F(x)$ is true at all sample points"
- $\exists x F(x) \Leftrightarrow$ "$F(x)$ is true at some sample point"
- $\forall x \exists y F(x, y) \Leftrightarrow$ "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]



So how do we project? (Lifting has in fact been 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!)

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

What about the complexity?

n variables, m polynomials, d degree (in each variable), coefficient length l

If the McCallum projection is well-oriented, the complexity is

$$\underbrace{(2d)^{n2^{n+7}}}_{\text{algebraic}} \times \underbrace{m^{2^{n+4}}}_{\text{combinatorial}} \times \underbrace{l^3}_{\text{arithmetic}} \qquad (2)$$

versus the original

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

and in practice the gains in running time can be factors of a thousand, or, more often, the difference between feasibility and infeasibility

"Randomly", well-orientedness ought to occur with probability 1, but we have a family of "real-world" examples where it often fails

Massive Overkill?

From this CAD, you can "read off" the truth of every

$$Q_{k+1}x_{k+1}\dots Q_n x_n \Phi(x_1,\dots,x_n)$$

for any k, any $Q_i \in \{\exists,\forall\}$ and any Boolean Φ.

[Col98] observed that we can do better if we restrict Φ to be $f(x_1,\dots,x_n)=0\land\Phi'$, because we don't care about Φ' when $f\ne 0$

Such a single "equational constraint" was implemented by [McC99]

[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 $\mathcal{B}_n$

[McC99] Suppose $\mathcal{F}\subset\mathcal{B}_n$. Then $\mathcal{P}_{n-1}^{\mathcal{F}}$ is the contents of $\mathcal{P}_n$, $\mathcal{P}_n(\mathcal{F})$, and every $\mathrm{res}_{x_n}(f_i,b_j)$ from $\mathcal{F}\times(\mathcal{B}_n\setminus\mathcal{F})$

Then let $\mathcal{F}$ be the square-free basis of f, use $\mathcal{P}_n^{\mathcal{F}}$ and then $\mathcal{P}_i$ for $i<n$, to get an order-invariant CAD of $\mathbf{R}^{n-1}$ and then a sign-invariant CAD of $\mathbf{R}^n$: needs new theorem!

Essentially reduces n by 1 in combinatorial complexity

But order/sign means this doesn't compose!

Multiple Equational Constraints [McC01, EBD15]

[McC01] Let $\mathcal{B}_n$ be a squarefree basis for the primitive parts of $\mathcal{P}_n$, and $\mathcal{F} \subset \mathcal{B}_n$. Then $\mathcal{P}_{n-1}^{\mathcal{F}^*}$ is the contents of $\mathcal{P}_n$, $\mathcal{P}_n^{\mathcal{F}}(\mathcal{B})$, and every $\mathrm{disc}\, x_n(b_i)$ from $\mathcal{B}_n \setminus \mathcal{F}$

Then [McC01] use of $\mathcal{P}_i^{\mathcal{F}^*}(\mathcal{B})$ lifts a well-oriented order-invariant CAD to an order-invariant CAD, so does compose

$f = 0 \wedge g = 0 \wedge \Phi'$ is equivalent to $f = 0 \wedge \mathrm{res}_{x_n}(f, g) = 0 \wedge \Phi'$

Hence use $\mathcal{P}_n^{\mathcal{F}}$ for the first equational constraint, $\mathcal{P}_n^{\mathcal{F}^*}$ for subsequent equational constraints, or their resultants, until we run out, then use $\mathcal{P}_i$, always assuming well-orientedness

A snag is that, while $\mathcal{P}_n^{\mathcal{F}}$ is much smaller than $\mathcal{P}_n$, $\mathcal{P}_n^{\mathcal{F}^*}$ is not (at the level of $O(\ldots)$ — it is still usefully smaller)

More ideas 1: originally [BDE+13]

The key principles of Projection/Lifting CAD

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

Let's abandon these: more precisely

- for x_i where there is a primitive equational constraint $f(x_i, \ldots) = 0$, lift only with respect to this polynomial

But doesn't this lose information about the signs of the other polynomials etc.? Yes, but not when $f = 0$

More ideas 2: [EBD15]

- If we had a primitive equational constraint $g = 0$ at the previous level, then only the sections (even index at that level) have $g = 0$, while the sectors between them have $g \neq 0$. Hence the sectors S_i can be lifted trivially to $S_i \times \mathbf{R}$.

But doesn't this lose information about the signs of the other polynomials etc.?
Yes, but in terms of the validity of $g = 0 \wedge \ldots$ we don't care
The combined effect of these is that the n in the double exponent of the combinatorial complexity is effectively reduced by the number of equational constraints

Example ($z > y > x > u > v$)

$$x - y + z^2 = 0 \wedge z^2 - u^2 + v^2 - 1 = 0 \wedge x + y + z^2 = 0 \wedge$$
$$z^2 + u^2 - v^2 - 1 = 0 \wedge x^2 - 1 \geq 0 \wedge z \geq 0$$

60 different choices of equational constraints, but in fact only 3 different answers, with 93, 103 or 113 cells. This compares with

[McC99]+1 3023, 10935 or 48299 $\times$ 2 cells

[McC99] 11961, 30233, 158475 or 158451 cells

QEPCAD all ECs (i.e. no improvements to lifting) 21097 cells

* We can make QEPCAD do 5633 cells

sign-invariant 1118205 cells

But we said primitive

Currently this is a genuine restriction. $f = 0 \Leftrightarrow (f_p = 0) \vee (f_c = 0)$ so lifting only $f_p = 0$ would ignore the case $f_c = 0, f_p \neq 0$ and *vice versa*

At AG'13 Matthew England presented our theory of *Truth-Table Invariant CADs* [BDE+13, BDE+14], which deals with

$$(f_1 = 0 \wedge \Phi_1) \vee (f_2 = 0 \wedge \Phi_2) \vee \cdots ,$$

but this doesn't deal with multiple equations.

Future work: unify the two developments

Also, idea 2 would need rethinking, as the sectors of the primitive part living over sections of the content need to be lifted properly

Bibliography

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.

R.J. Bradford, J.H. Davenport, M. England, S. McCallum, and D.J. Wilson.
Truth Table Invariant Cylindrical Algebraic Decomposition.
http://arxiv.org/abs/1401.0645, 2014.

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

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.

Bibliography III

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 of Three-dimensional Space.
J. Symbolic Comp., 5:141–161, 1988.

Bibliography IV

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.

Bibliography

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.

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