The CAD Conundrum: Lex-Least vs Order

Scott McCallum
Dept. of Computing
Macquarie University
Sydney, Australia
0000-0002-5682-7993

Akshar Nair
Dept. of Computer Science
University of Bath
Bath, United Kingdom
0000-0001-7379-1868

James Davenport
Dept. of Computer Science
University of Bath
Bath, United Kingdom
0000-0002-3982-7545

Gregory Sankaran
Dept. of Mathematics
University of Bath
Bath, United Kingdom
0000-0002-5846-6490

***Abstract*—This paper is part of our ongoing research and collaboration on understanding the relations between CAD algorithms, equational constraints and curtains. Our previous work manages to circumvent the curtain problem in the single equational constraint by taking advantage of the Lex-least valuation (even in the presence of curtains). That method however fails to take full advantage of multiple equational constraints. In this paper we provide further clarification of McCallum's work to validate the use of restricted projection operator at 2 levels. We also discuss the close relationship between order invariant and lex-least invariant CAD's.**

***Index Terms*—Cylindrical Algebraic Decomposition, Equational Constraints, Lex-Least Invariance, Order Invariance**

I. Introduction

A Cylindrical Algebraic Decomposition (CAD) is a decomposition of a semi-algebraic subset of $\mathbb{R}^n$ (for any n) into semi-algebraic sets (also known as cells) homeomorphic to $\mathbb{R}^m$, where $0 \leq m \leq n$, such that the projection of any two cells onto the first k coordinates is either the same or disjoint. We generally want the cells to have some property relative to some given set of input polynomials, often used to form constraints using sign conditions. Within the context of this paper we will primarily speak about order and lex-least invariance.

Definition 1: A Quantifier Free Tarski Formula (QFF) is made up of atoms connected by the standard boolean operators $\wedge, \vee$ and $\neg$. The atoms are statements about signs of polynomials $f \in \mathbb{R}[x_1, \ldots, x_n]$, of the form $f * 0$ where $* \in \{=, <, >\}$ (and by combination also $\{\geq, \leq, \neq\}$).

Strictly speaking we need only the relation $<$, but this form is more convenient because of the next definition.

Definition 2: [4] An Equational Constraint (EC) is a polynomial equation logically implied by a QFF. If it is an atom of the formula, it is said to be *explicit*; if not, then it is *implicit*. If the constraint is visibly an equality constraint one from the formula, i.e. the formula Φ is $f = 0 \wedge \Phi'$, we say the constraint is *syntactically explicit*.

In order to understand lex-least valuation, let us recall *lexicographic order* $\geq_{\text{lex}}$ on $\mathbb{N}^n$, where $n \geq 1$.

Definition 3: We say that $v = (v_1, \ldots, v_n) \geq_{\text{lex}} (w_1, \ldots, w_n) = w$ if and only if either $v = w$ or there exists an $i \leq n$ such that $v_i > w_i$ and $v_k = w_k$ for all k in the range $1 \leq k < i$.

Definition 4: [9, Definition 2.4] Let $n \geq 1$ and suppose that $f \in \mathbb{R}[x_1, \ldots, x_n]$ is non-zero and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$. The lex-least valuation $\nu_\alpha(f)$ at α is the least (with respect to $\geq_{\text{lex}}$) element $v = (v_1, \ldots, v_n) \in \mathbb{N}^n$ such that f expanded about α has the term

$$c(x_1 - \alpha_1)^{v_1} \cdots (x_n - \alpha_n)^{v_n},$$

where $c \neq 0$.

Note that $\nu_\alpha(f) = (0, \ldots, 0)$ if and only if $f(\alpha) \neq 0$.

[10] proposed some geometric terminology to describe the conditions under which a polynomial is nullified in the terminology of [7].

Definition 5: A variety $C \subseteq \mathbb{R}^n$ is called a curtain if, whenever $(\alpha_1, \ldots, \alpha_n) \in C$, then $(\alpha_1, \ldots, \alpha_{n-1}, \beta) \in C$ for all $\beta \in \mathbb{R}$.

Definition 6: Suppose $f \in \mathbb{R}[x_1, \ldots, x_n]$ and $S \subseteq \mathbb{R}^{n-1}$. We say that f has a curtain over S if for all $(\alpha_1, \ldots, \alpha_{n-1}) \in S$ and $\beta \in \mathbb{R}$ we have $f(\alpha_1, \ldots, \alpha_{n-1}, \beta) = 0$.

Remark 1: Lazard delineability differs from delineability as in [2] and [7] in two important ways. First, we require lex-least invariance on the sections. Second, delineability is not defined on curtains, but Lazard delineability is.
For background information on lex-least valuation, Lazard's original algorithm and curtains, see [11].

We focus on exploiting syntactically explicit equational constraints. For further details we refer to [10].

Section II discusses some steps towards producing an algorithm that exploits equational constraints, as in [8], but using lex-least invariance instead of order invariance.

Section III examines the relationship between order invariance and lex-least invariance with reference to [9]. Section IV states a strengthened version of Theorem 4.1 in [8] and outlines its proof.

II. Developments in Lex-least Valuation

In this section we discuss the stages of development of the relationship between equality constraints and lex-least invariant CADs.

Our first result (see Theorem 1 and Theorem 2 below) allowed us to exploit an equational constraint to produce a sign-invariant CAD. We begin with some notation and definitions.

We fix an order $x_1 \prec x_2 \cdots \prec x_n$ on the variables in $\mathbb{R}[x_1, \ldots, x_n]$ and we write $x = (x_1, \ldots, x_{n-1})$. For

The second author's PhD is supported by the University of Bath and EPSRC.

$f, g \in \mathbb{R}[x_1, \ldots, x_n]$ we define $l_f(x)$, $t_f(x)$, $D_f(x)$ to be, respectively, the leading coefficient, trailing coefficient and discriminant of f, and $R_{f,g}(x)$ to be the resultant $\mathrm{res}_{x_n}(f, g)$. These are all elements of $\mathbb{R}[x]$.

If X and Y are subsets of $\mathbb{R}[x_1, \ldots, x_n]$ we define $\mathrm{ldcf}(X) = \{\mathrm{ldcf}_x(f) \mid f \in X\}$ to be the set of leading coefficients from X, and $\mathrm{trcf}(X)$ and $\mathrm{disc}(X)$ similarly. We also define $\mathrm{res}(X, Y) = \{R_{f,g}(x) \mid f \in X, g \in Y\}$.

Definition 7: [11] Let $A \subset \mathbb{R}[x_1, \ldots, x_n]$ be a set of polynomials. Let $E \subseteq A$, and define the projection operator $\mathrm{PL}_E(A)$ as

$$\mathrm{PL}_E(A) = \mathrm{ldcf}(E) \cup \mathrm{trcf}(E) \cup \mathrm{disc}(E) \cup \mathrm{res}(E, E) \cup \mathrm{res}(E, A \setminus E).$$

We will be comparing this to Lazard's projection operator $\mathrm{PL}(A)$ defined in [9]. In the practical use of the operator, the set E corresponds to equational constraints.

Theorem 1: [9] Suppose that $f(x, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ is of positive degree in x_n, and that $D_f(x)$ is not identically zero. Let S be a connected subset of $\mathbb{R}^{n-1}$ in which $D_f(x)$, $l_f(x)$ and $t_f(x)$ are all lex-least invariant. Then f is Lazard delineable on S, and hence f is lex-least invariant in every Lazard section and sector over S.

Theorem 2: [11] Let $n \geq 2$ and let $f, g \in \mathbb{R}[x_1, \ldots, x_n]$ be of positive degrees in the main variable x_n. Suppose that f is Lazard delineable on a connected subset $S \subset \mathbb{R}^{n-1}$, in which $R_{f,g}$ is lex-least invariant, and f does not have a curtain over S. Then g is sign-invariant in each section of f over S.

Theorem 1 improves the result in [7] because it uses Lazard's algorithm, which does not have any problem with curtains. Unfortunately the problem reappears when lifting from lex-least to sign invariance as in Theorem 2, if the equational constraint has a curtain. The improvement comes from not being concerned about non-equality constraints having curtains.

We further proceeded, in [12], by modifying Lazard's algorithm to deal with curtains on equational constraints.

Our current work looks at producing a new projection operator and clarifying the relationship between order invariant CAD and lex-least invariant CAD.

Theorem 3: Suppose $f, g \in \mathbb{R}[x_1, \ldots, x_n]$ both have positive degree in x_n, and that D_g is not identically zero. Let $S \subset \mathbb{R}^{n-1}$ be a connected subset such that f does not have a curtain over S. If $D_g(x)$, $l_g(x)$, $t_g(x)$ and $R_{f,g}(x)$ are all lex-least invariant over S, then g is lex-least invariant on every section of f over S.

Proof: This is a direct consequence of [9, Theorem 5.1]. □

Remark 2: In Theorem 3 we are only concerned with the sections of f and not the sectors. This is because when we are exploiting equational constraints, we are only interested in when they are zero, i.e. their sections.

Definition 8: Let $A \subset \mathbb{R}[x_1, \ldots, x_n]$ be a set of polynomials. Let $E \subseteq A$, and define the projection operator $\mathrm{PL}^*_E(A)$ as

$$\mathrm{PL}^*_E(A) = \mathrm{ldcf}(A) \cup \mathrm{trcf}(A) \cup \mathrm{disc}(A) \cup \mathrm{res}(E, E) \cup \mathrm{res}(E, A \setminus E).$$

Theorem 4: Let $A \subset \mathbb{R}[x_1, \ldots, x_n]$ be a set of irreducible polynomials and let $E \subset A$. Let S be a connected submanifold of $\mathbb{R}^{n-1}$ such that every element of $\mathrm{PL}^*_E(A)$ is lex-least invariant in S. Then each element of E either vanishes identically on S or is Lazard delineable on S. The sections of any $f \in E$ that does not vanish identically over S are pairwise disjoint, and each element of $A \setminus E$ is lex-least invariant in every such section.

Proof: The resultants are only needed to split cells with respect to sectors of $f \in E$ and the curtains of $f \in E$. From Theorem 3 we know that every element of $A \setminus E$ is independently lex-least invariant on every section of $f \in E$. Since every element of $\mathrm{res}(E, A \setminus E)$ is invariant on S, every element of $A \setminus E$ is simultaneously lex-least invariant on every section of $f \in E$. □

Remark 3: The difference between this result and Theorem 2.2 [8] is that in Theorem 4 the inequality constraints may vanish identically over S. This is because we are looking at lex-least invariance and Lazard's algorithm allows one to decompose curtains. Unfortunately, this refers only to the curtains in non-equational constraints. If the equational constraint contained a curtain, this method would fail to decompose it.

Remark 4: Note that in practice set E in Definitions 7 and 8 is a singleton set.

III. Order versus Lex-least

This section looks at the relation between order invariant and lex-least invariant CADs. Let us recall the relation established from [9].

Theorem 5: Let $f \in \mathbb{R}[x_1, x_2]$ be a non-zero element and $S \subset \mathbb{R}^2$ be connected. If f is lex-least invariant in S then f is order invariant in S.

Proof: Since a polynomial is (order or lex-least) invariant if and only if its irreducible factors are invariant, we may assume that f is irreducible.

If S is a singleton then we are done, so assume otherwise. Suppose first that f has positive degree in x_2. We know that the valuation of f in S is $(0, 1)$ for all but finitely many points. Since S is infinite and f is valuation invariant in S, the valuation must be $(0, 1)$. Hence, f is order invariant in S with order 1.

If f has zero degree in x_2 it has no multiple roots (because it is irreducible), so hence it has valuation $(0, 1)$ in S and again f is order invariant in S with order 1. □

Remark 5: [9] This is not true for $n > 2$. For example, consider $f = x_3^2 + x_1 x_2 \in \mathbb{R}[x_1, x_2, x_3]$ and take $S = \{(t, 0, 0) \mid t \in \mathbb{R}\}$. Then f is lex-least invariant in S, with valuation $(0, 0, 2)$, but the order of f is 2 at the origin and 1 at all other points of S.

Note that although this example shows that lex-least invariance does not imply order invariance for functions, it says nothing about the relation between order invariance and lex-least invariance for CADs.

Theorem 6: Let A be a set of polynomials and D the corresponding order invariant CAD computed through McCallum's projection $P(A)$. Then D is also lex-least invariant on cells that do not have curtains.

Proof: In Lazard's algorithm, the lifting phase consists of finding the roots of residues of polynomials computed at sample points. In McCallum's algorithm, however, the polynomials' roots are found after substituting the sample points. This returns zero on curtains, so McCallum's algorithm fails in that case. Away from curtains, we know that $\mathrm{PL}(A) \subset P(A)$, so the roots obtained from Lazard's algorithm form a subset of the roots obtained from McCallum's algorithm. This implies that the cells of D are obtained by subdivision from cells computed by Lazard's algorithm, but these are already lex-least invariant. □

This gives rise to an open question: is it possible to have a CAD that is order-invariant for a set of polynomial but is not lex-least invariant for them? We note that it is possible to have fairly perverse CADs, that no known algorithm would construct but which actually obey the definition [3].

IV. Clarification on Order Invariance and Equational Constraints

In this section we present a delineability condition subject to equational constraints. We use intersection multiplicities, which we define following the procedure in [1]. For this purpose, we temporarily pass to complex coefficients.

Let f, $g \in \mathbb{C}[x_1, \ldots, x_n]$ be coprime and nonconstant, and and let $p \in \mathbb{C}^n$. By an affine change of coordinates we may assume that p is the origin and that $f(0, x_n)$ is not identically zero so it vanishes at $x_n = 0$ to some finite order m. Then by Hensel's lemma (see [1, Lecture 12]) there exist unique elements $q(x, x_n)$ and $h(x, x_n)$ of $\mathbb{C}[[x]][x_n]$, with h monic of degree m, such that $f(x, x_n) = q(x, x_n)h(x, x_n)$, $h(0, x_n) = x_n^m$ and $q(0, 0) \neq 0$. We define the *intersection order* of f and g at p to be the order of the resultant $\mathrm{res}_{x_n}(h, g)$ of h and g with respect to x_n.

Geometrically, this is the same as taking a general plane section Π through p and asking for the intersection mutiplicity at p of the plane curves $(f = 0) \cap \Pi$ and $(g = 0) \cap \Pi$.

Remark 6: With the help of this new concept, we can observe a slight strengthening of an existing result from the literature. Namely, consider Theorem 2.2 of [7], which is the main "lemma" of that work. We can right away strengthen the conclusion of that theorem to be: "Then f and g are intersection order invariant in each section of f over S." No change to the hypotheses is needed. Nor is anything more required in the existing proof, since the last paragraph of the proof already deduces that the analytic function P, the resultant of h and g, is order invariant in S near the origin. By definition, this immediately implies that f and g are intersection order invariant in σ near the origin.

We could similarly define the concept of intersection lex-least valuation of f and g at p, which is the lex-least valuation of the resultant $\mathrm{res}_{x_n}(h, g)$ of h and g with respect to x_n.

Theorem 7: Let e, $f \in \mathbb{R}[x_1, \ldots, x_n]$ be real polynomials of positive degree in x_n. Put $d = D_f$ and suppose that $\mathrm{res}_{x_{n-1}}(e, d)$ is not identically zero. Let T be a connected submanifold of $\mathbb{R}^{n-2}$ on which e is analytic delineable, and let σ be a section of e over T which contains no singular point of the hypersurface $e = 0$. Suppose that f is degree invariant and does not vanish identically on σ, and that d and e are intersection order invariant in σ. Then f is analytic delineable on σ.

Proof: By the invariance, d vanishes on σ either everywhere or nowhere: in the latter case f is analytic delineability on σ by [6, Theorem 2]. So we assume that d vanishes identically on σ.

Since T, and hence σ, is connected, it suffices to show that f is analytic delineable on σ near an arbitrary point of σ, which we may assume to be the origin. Since $e = 0$ is nonsingular there, we may also assume that $\partial e/\partial x_{n-1} \neq 0$ at the origin, by making a linear change of coordinates in $\mathbb{R}^{n-1}$. For σ is assumed to contain no singular point of the hypersurface in $\mathbb{R}^{n-1}$ defined by $e = 0$, so $\partial e/\partial x_i \neq 0$ at the origin, for some i. Let $\pi_i \colon \mathbb{R}^{n-1} \to \mathbb{R}^{n-2}$ be the projection $\pi_i(x_1, \ldots, x_{n-1}) = (x_1, \ldots, \hat{x}_i, \ldots, x_{n-1})$. It is not difficult to show (with the help of the implicit function theorem) that $T_i := \pi_i(\sigma)$ is a connected submanifold of $\mathbb{R}^{n-2}$ near the origin, on which e is analytic delineable near the origin. Hence we may simply interchange the x_i and x_{n-1} coordinates, and adjust the submanifold T as needed, to obtain $\partial e/\partial x_{n-1} \neq 0$ at the origin (in particular, e is of positive degree), with all the other assumptions still valid.

We denote the $(n-2)$-tuple $(x_1, \ldots, x_{n-2})$ by ξ. Let

$$e(\xi, x_{n-1}) = a_0(\xi)x_{n-1}^k + a_1(\xi)x_{n-1}^{k-1} + \cdots + a_k(\xi).$$

Now the order of $e(0, x_{n-1})$ is 1 since $\partial e/\partial x_{n-1} \neq 0$ at the origin. Therefore, by an extension of Hensel's lemma (exercise on page 95 of [1], or [7, Theorem 3.1] for the 3 variable case), there is an open box B about the origin in $\mathbb{R}^{n-2}$ and elements $q(\xi, x_{n-1}) = b_0(\xi)x_{n-1}^{k-1} + \cdots + b_{k-1}(\xi)$ and $h(\xi, x_{n-1}) = x_{n-1} - c(\xi)$ of $\mathbb{R}[[\xi]][x_{n-1}]$, whose coefficients b_i and c are real power series in ξ, absolutely convergent in B, such that $e(\xi, x_{n-1}) = q(\xi, x_{n-1})h(\xi, x_{n-1})$, $h(0, x_{n-1}) = x_{n-1}$, and $q(0, 0) \neq 0$. Since a function defined as the sum of a convergent power series is analytic the coefficients b_i of q and c of h are analytic in B. Since $q(0, 0) \neq 0$ at the origin and q is analytic – hence continuous – near the origin, there exists $\epsilon > 0$ and an open box $B' \subset B$ about the origin such that $q \neq 0$ throughout all of $B' \times (-\epsilon, \epsilon)$. In the open box $B' \times (-\epsilon, \epsilon)$, therefore, the real variety of e is identical with the graph of the real analytic function $x_{n-1} = c(\xi)$.

For $\xi \in B'$, put

$$f_1(\xi, x_n) = f(\xi, c(\xi), x_n).$$

Then f_1 is a polynomial in x_n whose coefficients are real analytic functions defined in B': put $d_1 = D_{f_1}$. Then $d_1(\xi) = d(\xi, c(\xi))$ for all $x \in B'$. Indeed, we have $d_1(\xi) = \mathrm{res}_{x_{n-1}}(h, d)$ for all $\xi \in B'$, by [5, Theorem 1]. Furthermore,

$$\mathrm{res}_{x_{n-1}}(e, d) = \mathrm{res}_{x_{n-1}}(q, d)\,\mathrm{res}_{x_{n-1}}(h, d)$$

for all $\xi \in B'$, by [5, Theorem 3]. Since $\mathrm{res}_{x_{n-1}}(e, d)$ is a nonzero polynomial by assumption, it follows that

$\operatorname{res}_{x_{n-1}}(h,d) = d_1$ is also a nonzero polynomial. Moreover, the assumptions directly imply that f_1 is degree invariant and not identically vanishing on $T \cap B'$, and that d_1 is order invariant in $T \cap B'$. Hence, by [8, Theorem 7.1] applied to f_1, f_1 is analytic delineable on $T \cap B'$. Therefore, f is analytic delineable on σ, near the origin. □

Remark 7: The example presented in Section 6 of [8] provides a contradiction to the strengthening of the result presented there and its analogous version with respect to lex-least valuation. This generalization hopes to solidify the results stated in [8] in order to provide a base for further research concerning equational constraints and lex-least valuation.

Remark 8: Our generalization is presented here with the hope and expectation that it may be applicable for the first and second projections for quantifier elimination involving arbitrarily many variables.

V. Conclusion and Further Research

Theorem 6 provides a clear relation between order invariant and lex-least invariant CADs as we construct them (because of [3]). A polynomial that is order invariant on some set does not have to be lex-least invariant there, as an example in [9] shows, nor conversely, as Example 3 shows. However, one important CAD algorithm in fact produces a CAD that is simultaneously order invariant and lex-least invariant. We are currently extending this approach and combining it with the machinery of Theorem 7 with the aim of finding a better projection operator than the one in Definition 8, able to deal with curtains present in equational constraints.

References

[1] S.S. Abhyankar. *Algebraic geometry for scientists and engineers*. Mathematical surveys and monographs; no. 35. American Mathematical Society, Providence, Rhode Island, 1990.

[2] 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.

[3] J.H. Davenport, A.F. Locatelli, and G.K. Sankaran. Regular cylindrical algebraic decomposition. *J. LMS.*, 101:43–59, 2020.

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

[5] R. Loos. Computing in Algebraic Extensions. *Symbolic and Algebraic Computation (Computing Supplementum 4) Springer-Verlag*, pages 173–187, 1982.

[6] S. McCallum. An Improved Projection Operation for Cylindrical Algebraic Decomposition. In B.F. Caviness and J.R. Johnson, editors, *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 242–268. Springer-Verlag Vienna, 1998.

[7] S. McCallum. On Projection in CAD-Based Quantifier Elimination with Equational Constraints. In S. Dooley, editor, *Proceedings ISSAC '99*, pages 145–149, 1999.

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

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

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

[11] A.S. Nair, J.H. Davenport, and G.K. Sankaran. On Benefits of Equality Constraints in Lex-Least Invariant CAD (Extended Abstract). In *SC-Square 2019: Satisfiability Checking and Symbolic Computation*, volume 2460 of *CEUR WS Proceedings*, pages 6:1–6:9, 2019. URL: http://ceur-ws.org/Vol-2460/paper6.pdf.

[12] 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.