*J. Symbolic Computation* (2001) **32**, 447–465
doi:10.1006/jsco.2001.0463
Available online at http://www.idealibrary.com on IDEAL®

# Improved Projection for Cylindrical Algebraic Decomposition

CHRISTOPHER W. BROWN†

*Department of Computer Science, United States Naval Academy, U.S.A.*

McCallum's projection operator for cylindrical algebraic decomposition (CAD) represented a huge step forward for the practical utility of the CAD algorithm. This paper presents a simple theorem showing that the mathematics in McCallum's paper actually point to a better projection operator than he proposes—a *reduced* McCallum projection. The reduced projection has the potential to not simply speed up CAD computation for problems that are currently solvable in practice, but actually increase the scope of problems that can realistically be attacked via CADs. Additionally, the same methods are used to show that McCallum's projection can be reduced still further when CAD is applied to certain types of commonly occurring quantifier elimination problems.



## 1. Introduction

Cylindrical algebraic decomposition (CAD) is an important tool for the investigation of real algebraic and semi-algebraic sets. Introduced by Collins in the early 1970s (Collins, 1975) as the basis of his quantifier elimination method, the algorithm for CAD construction has been steadily improved, and has found application in many areas including stability analysis (Hong *et al.*, 1997) and numerical integration (Strzebonski, 2000).

Given a set $A \subset \mathbb{R}[x_1, \ldots, x_k]$, the CAD algorithm constructs a decomposition of $\mathbb{R}^k$ into cylindrically arranged cells such that the signs of the elements of $A$ are constant inside any given cell. This cylindrical arrangement means that the projections onto $\mathbb{R}^{k-1}$ of any two cells are either identical or disjoint. CAD construction proceeds in two phases, *projection* and *lifting*. The projection phase, which is the focus of this paper, computes a set of polynomials called the *projection factor set*. The projection factor set contains the irreducible factors of the set $A$, and, in general, other polynomials as well. The maximal connected regions in which the projection factors have invariant signs are the cells of the CAD that is to be constructed. Thus, the projection factor set provides an implicit representation of the CAD. The lifting phase then constructs an explicit representation of this CAD. General descriptions of CAD construction may be found in Collins and Hong (1991), Arnon *et al.* (1984), and Collins (1975).

The projection phase is typically determined by a *projection operator* which, from the set $A$, defines a set $A' \subset \mathbb{R}[x_1, \ldots, x_{k-1}]$ such that if $c \subseteq \mathbb{R}^{k-1}$ is a cell in a CAD produced from $A'$, then the maximal connected regions in $c \times \mathbb{R}$ in which the elements of $A$ have invariant sign are cylindrically arranged. Thus, after applying the projection operator to $A$ to produce $A'$, we are left with the problem of producing a CAD in whose cells

†E-mail: wcbrown@usna.edu

0747–7171/01/110447 + 19 $35.00/0 

the elements of $A'$ have invariant sign, i.e. the same problem as we originally faced, but with fewer variables. To produce this CAD we start by applying the projection operator to $A'$ to produce $A'' \subset \mathbb{R}[x_1, \ldots, x_{k-2}]$, and so on. Thus, the projection phase consists of repeatedly applying the projection operator until we are left with a set of univariate polynomials in $x_1$. The projection factor set consists of all irreducible factors of elements of $A$ and of any polynomial produced by any of the applications of the projection operator.

It is crucially important for the efficiency of CAD construction that the projection operator produce as small a set of polynomials as possible, while still ensuring the cylindrical arrangement of cells in the resulting decomposition. For most problems, the current best projection operator is due to McCallum (McCallum, 1984, 1988, 1998). In this paper it is shown that certain polynomials included in McCallum's projection are in fact unnecessary, and thus the paper provides a reduced projection factor set. The main result is Theorem 3.1 in Section 3, which is essentially a corollary of a theorem due to McCallum (Theorem 2 of McCallum, 1998).

Additionally, it is shown that in certain situations arising in the CAD-based quantifier elimination method, still more polynomials may be eliminated from McCallum's projection. This is based on Theorem 5.1 from Section 5, which builds on Theorem 3.1.

This paper is firmly rooted in McCallum's papers (McCallum, 1988, 1998), and the reader is referred to those articles for many definitions and results. McCallum (1988) provides a more intuitive presentation of McCallum's projection operator, but is restricted to the three-variable case. None the less, it provides most of the concepts and terminology required for this paper. Section 2 of this paper provides a brief review of McCallum's projection and the role of projection in CAD construction. The main result of the paper, a *reduced* McCallum projection operator, is described in Section 3, and the specialized projection for certain types of quantifier elimination problems is introduced in Section 5.

McCallum's projection operator and the reduced McCallum projection operator proposed in this paper require that the lifting method described in Collins' original paper be modified. The differences between Collins' original lifting method, the lifting method required with McCallum's projection, and the lifting method proposed in conjunction with this paper's improved McCallum projection are discussed in Section 4.

## 2. McCallum's Projection Operator

This section gives a brief description of McCallum's projection operator and the main theorem on which it is based. The reader is referred to McCallum (1988, 1998) for a complete presentation.

Crucial to projection and the theory of CADs as introduced in Collins (1975) is the concept of the *delineability* of a polynomial. A polynomial $f \in \mathbb{R}[x_1, \ldots, x_k]$ is delineable over a region $S \subseteq \mathbb{R}^{k-1}$ provided the real zeros of $f$ over $S$ define continuous real-valued functions $\theta_1, \ldots, \theta_s$ such that, for all $p \in S$, $\theta_1(p) < \cdots < \theta_s(p)$, and for each $\theta_i$ there is an integer $m_i$ such that $m_i$ is the multiplicity of the root $\theta_i(p)$ of $f(p, x_k)$. (The $\theta_i$s are referred to as *sections*, or as *$f$-sections*.) Delineability is important because if $f$ is delineable over $S$, the maximal connected regions over $S$ in which $f$ is sign-invariant are cylindrically arranged.

McCallum uses the notion of *analytic delineability*, which has essentially the same definition, requiring additionally that $S$ is an algebraic submanifold and that the $\theta_i$ are analytic functions. Definitions of the terms *analytic*, *submanifold*, and *order-invariant* used in this paper may all be found in McCallum (1988, 1998).

McCallum's projection operator is based on the following theorem (Theorem 2 in McCallum, 1998):

THEOREM 2.1. (MCCALLUM) *Let $k \geq 2$. Let $f(\overline{x}, x_k)$ be a polynomial in $\mathbb{R}[\overline{x}, x_k]$ of positive degree. Let $D(\overline{x})$ be the discriminant of $f(\overline{x}, x_k)$ and suppose that $D(\overline{x})$ is a non-zero polynomial. Let $S$ be a connected submanifold of $\mathbb{R}^{k-1}$ on which $f$ is degree-invariant and does not vanish identically, and in which $D$ is order-invariant. Then $f$ is analytic delineable on $S$ and is order-invariant in each $f$-section over $S$.*

McCallum's use of order-invariance rather than sign-invariance is crucial to his improvement of projection, though it might also seem to be incompatible with the definition of CADs based on maximal *sign*-invariant regions. However, part of what this theorem shows is that the maximal connected regions of $S \times \mathbb{R}$ in which $f$ is *sign*-invariant are also regions in which $f$ is *order*-invariant.

Based on this theorem, McCallum proposes the projection operator ProjMC, such that ProjMC($f$) consists of the discriminant of $f$ and all coefficients of $f$ (as a polynomial in $x_k$). If we recursively construct a CAD for ProjMC($f$), then $f$ will be degree-invariant in any cell of the CAD, since the degree of $f$ is determined by the signs of its coefficients, and $D$ will be order-invariant, by repeated application of the above theorem.

ProjMC is defined for sets of polynomials as the union of ProjMC for each polynomial individually, and the resultant of each pair of polynomials in the set. (McCallum actually reduces the case of a set of polynomials to that of a single polynomial by considering the product of all elements of the set as a single polynomial to be projected.) The following definition of ProjMC is from McCallum (1998):

DEFINITION. Let $A$ be a squarefree basis in $\mathbb{Z}[x_1, \ldots, x_k]$, where $k \geq 2$. We define the projection ProjMC($A$) of $A$ to be the union of the set of all non-zero coefficients of the elements of $A$, the set of all discriminants of elements $f$ of $A$, and the set of all resultants of pairs $f, g$ of distinct elements of $A$.

The lifting methods described in Collins and Hong (1991), Arnon *et al.* (1984), and Collins (1975) may be used with McCallum's projection to produce a CAD that is order-invariant for the initial set of polynomials as long as no projection factor vanishes identically over any region. McCallum describes how to augment the usual lifting algorithm so that it produces order-invariant decompositions for $f$ when $f$ vanishes identically over a zero-dimensional cell. Thus, McCallum's projection (along with his augmentation of the lifting algorithm) produces an order-invariant CAD from an initial set of polynomials provided that no projection factor vanishes over a region of dimension greater than zero.

## 3. A Refinement of McCallum's Projection

The main result of this paper is that the degree-invariance required by Theorem 2.1 is actually implied by the order-invariance of the discriminant and the sign-invariance of the leading coefficient, so that including other coefficients in the projection is unnecessary.

THEOREM 3.1. *Let $f \in \mathbb{R}[\overline{x}, z]$ be a $(k+1)$-variate polynomial of positive degree $n$ in the variable $z$ with discriminant $D(\overline{x}) \neq 0$. Let $S$ be a connected analytic submanifold of $\mathbb{R}^k$ in which $D$ is order-invariant, the leading coefficient of $f$ is sign-invariant, and such that $f$ vanishes identically at no point in $S$. $f$ is degree-invariant on $S$.*

PROOF. We assume $S$ has positive dimension—the dimension zero case is trivial—and we assume the leading coefficient of $f$ is zero in $S$—the case in which it is non-zero is trivial. By the connectedness of $S$, it suffices to show that f is degree-invariant on $S$ near an arbitrary point $p \in S$. That is, it is enough to show that for every point $p \in S$, there exists a neighborhood $N$ of $p$ such that $f$ is degree-invariant on $S \cap N$. Let $p$ be a point of $S$.

Let $\overline{f} = f(\overline{x}, z + \gamma)$, where $\gamma$ is not a root of $f(p, z)$, and let $N$ be a neighborhood of $p$ such that $\gamma$ is not a root of $f(q, z)$ for any $q \in N$. Note that the roots of $f$ are exactly the roots of $\overline{f}$ shifted by $\gamma$. Moreover, $\text{disc}_z(f) = \text{disc}_z(\overline{f})$. Also note that the constant coefficient (in $z$) of $\overline{f}$ is non-vanishing in $N$.

Let $f^* = z^n \overline{f}(\overline{x}, 1/z)$. Since the leading coefficient of $f^*$ is the trailing coefficient of $\overline{f}$, $f^*$ has constant degree $n$ on $N$. Note the one-to-one correspondence in $N$ between the non-zero roots of $f^*$ and the roots of $f$ via the mapping that takes a non-zero root $\zeta$ of $f^*$ and maps it to the root $\gamma + 1/\zeta$ of $f$. Moreover, note that $\text{disc}_z(f^*) = \text{disc}_z(f)$ by Lemma 8.1 (see Section 8), which implies the order-invariance of $\text{disc}_z(f^*)$ in $S$.

By Lemma 8.2 (see Section 8), $N$ can be refined to a neighborhood of $p$ such that $N \cap S$ is a connected analytic submanifold. Then, by Theorem 2.1, $f^*$ is delineable over $N \cap S$. Let $\theta_1, \ldots, \theta_s$ be the sections of $f^*$ over $N \cap S$. Exactly one section is zero at $p$, call it $\theta_i$, and it must have multiplicity $m_i$ such that $n - m_i$ is the degree of $f$ at $p$. Refine $N$ so that none of the other sections are zero anywhere in $N \cap S$. In the refined $N$, $\theta_i$ is non-zero at point $q$ if and only if the degree of $f$ at $q$ is $n$. Since by assumption the leading coefficient of $f$ is zero in $S$, $\theta_i$ is zero everywhere in $N \cap S$, which implies that the degree of $f$ is $n - m_i$ at every point in $N \cap S$. □

Theorem 3.1 suggests a reduced McCallum projection in which only *leading* coefficients, discriminants and resultants appear.

DEFINITION. Let $A$ be a squarefree basis in $\mathbb{Z}[x_1, \ldots, x_k]$, where $k \geq 2$. We define the improved projection $\text{Proj}(A)$ of $A$ to be the union of the set of all leading coefficients of elements of $A$, the set of all discriminants of elements $f$ of $A$, and the set of all resultants of pairs $f, g$ of distinct elements of $A$.

Theorem 3.1 states that $f$ will be degree-invariant in a connected submanifold $S$ in which $D$ is order-invariant and the leading coefficient of $f$ is sign-invariant *provided that $f$ is not identically zero somewhere in $S$*. Thus, in addition to constructing a CAD in which the discriminant of $f$ is order-invariant and the leading coefficient of $f$ is sign-invariant, we must identify points at which elements of $A$ vanish identically.

As explained in Section 2, McCallum's projection requires that no projection factor vanish identically over any region of dimension greater than zero, so we are only looking for finitely many isolated points. Moreover, identifying these points means solving polynomial systems—zero-dimensional systems, in fact—which is typically much less computationally demanding than CAD construction. However these points are computed, they simply need to be added to the CAD of $\mathbb{R}^{k-1}$ before proceeding with lifting to construct cells in $\mathbb{R}^k$. Adding a point to a CAD is easy, and nothing involving the point needs to play a role in the projection process.

In fact, points at which some element of $A$ vanishes identically seem often to end up as zero-dimensional cells in the order-invariant CAD for $\text{Proj}(A)$ without having to be explicitly added to the CAD.

## 4. Constructing CADs with the Reduced McCallum Projection

The process of CAD construction—projection, lifting, representations and auxiliary algorithms are described in many papers (for example Collins, 1975; Arnon *et al.*, 1984; Collins and Hong, 1991). Therefore, this will be a high-level discussion of CAD construction using the reduced McCallum projection, focusing mainly on how it differs from the usual CAD construction.

It will be convenient to refer to the *level* of $p \in \mathbb{R}[x_1, \ldots, x_k]$, which is the largest $j$ such that $\deg_{x_j}(p) > 0$. For $P \subseteq \mathbb{R}[x_1, \ldots, x_k]$, $P_i$ is the set of polynomials in $P$ with level $i$.

### 4.1. the projection phase

Given an initial set of polynomials $A$, the projection phase constructs a projection factor set for a CAD in whose cells the elements of $A$ have invariant sign.

$P \longleftarrow$**Projection(**$A$**)**
Input: $A \subseteq \mathbb{R}[x_1, \ldots, x_k]$
Output: $P$, the projection factor set of a sign-invariant CAD for $A$

(1) $P = \text{IrreducibleFactorsOf}(A)$
(2) for $i$ from $k$ downto 2 do
    $P = P \cup \text{IrreducibleFactorsOf}(\text{Proj}(P_i))$
(3) return $P$

It is important to note that during the projection process, each element of $P$ may be tagged as being: $F_A$—an irreducible factor of an element of $A$, $F_D$—an irreducible factor of the discriminant of some higher level projection factor, or $F_{lc}$—an irreducible factor of the leading coefficient of some higher level projection factor. An element of $P$ may, of course, receive more than one tag.

### 4.2. the lifting phase

As described in Arnon *et al.* (1984), the *lifting* phase constructs a sequence of CADs:

$C_1$—a CAD of $\mathbb{R}^1$ defined by $P_1$,
$C_2$—a CAD of $\mathbb{R}^2$ defined by $P_1 \cup P_2$,
$\vdots$
$C_{k-1}$—a CAD of $\mathbb{R}^{k-1}$ defined by $P_1 \cup P_2 \cup \cdots \cup P_{k-1}$, and
$C_k$—a CAD of $\mathbb{R}^k$ defined by $P_1 \cup P_2 \cup \cdots \cup P_k$.

The CAD $C_1$ is used in the construction of $C_2$, which is used in the construction of $C_3$, etc. The elements of $P_{i+1}$ are delineable over each cell $c \in C_i$, so the maximal connected regions of $c \times \mathbb{R}$ in which the elements of $P_{i+1}$ have invariant sign are cylindrically arranged, and they are in fact cells in $C_{i+1}$. The process of constructing a representation for cells in $C_{i+1}$ from $c \in C_i$ and $P_{i+1}$ is called "lifting over $c$ with respect to $P_{i+1}$". All cells of $C_{i+1}$ are constructed by lifting over cells from $C_i$.

In the CAD construction algorithm of Arnon *et al.* (1984), all cells of $C_{i+1}$ are constructed by lifting over cells from $C_i$ with respect to $P_{i+1}$. In McCallum's CAD construction algorithm (algorithm $CADW$ from McCallum, 1998), lifting is still done with respect to $P_{i+1}$, except when some polynomial $q \in P_{i+1}$ vanishes identically over the cell in $C_i$; in this case, $q$ is replaced with a *delineating polynomial* for $q$ (McCallum, 1998), which is simply a certain partial derivative of $q$. The cell in question must be a single point, or McCallum's projection is declared invalid (unless, as McCallum points out, $q \in A$ and a CAD in whose cells the elements of $A$ are *sign*-invariant is sufficient).

Stack construction using the reduced projection may be done in the same manner as the $CADW$ algorithm, with three exceptions.

(1) In lifting over a zero-dimensional cell $c \in C_i$ over which some $q \in P_{i+1}$ vanishes identically, McCallum's delineating polynomial is used in place of $q$ only if $q$ is tagged $F_D$. If it is not tagged $F_D$, then it is sufficient for $q$ to be sign-invariant in each cell (which would certainly be true for any cell over $c$).
(2) In lifting over a cell of $c \in C_i$ of positive dimension over which some $q \in P_{i+1}$ vanishes identically, projection is *not* declared invalid unless $q$ is tagged as $F_D$. If $q$ is not tagged $F_D$, then it suffices for $q$ to be sign-invariant in each cell (which would certainly be true for any cell over $c$).
(3) In lifting over a zero-dimensional cell $c \in C_i$ such that $c = (\alpha_1, \ldots, \alpha_i)$, if $(\alpha_1, \ldots, \alpha_i, \alpha_{i+1})$ is a point on which some element of $P_{i+2}$ vanishes identically, lifting is done with respect to $P_{i+1} \cup \{x_{i+1} - \alpha_{i+1}\}$. This is how the isolated points over which projection factors vanish identically are "added" to the CAD.
As an example, suppose that $p(x, y, z) = p_1(x, y)z + p_0(x, y)$ is a three-level projection factor and $(\alpha_1, \alpha_2)$ is a zero of both $p_1$ and $p_0$, and therefore $(\alpha_1, \alpha_2)$ must be "added" to the CAD. In lifting over the base cell in the CAD of $\mathbb{R}^0$, the polynomial $x - \alpha_1$ will be added to the set of one-level projection factors, thus assuring that there will be a zero-dimensional cell at $\alpha_1$ in the CAD of $\mathbb{R}^1$. Eventually, the algorithm will lift over that cell, and the polynomial $y - \alpha_2$ will be added to the set of two-level projection factors for this lifting step, which assures that $(\alpha_1, \alpha_2)$ will be a zero-dimensional cell in the CAD of $\mathbb{R}^2$. Thus, $(\alpha_1, \alpha_2)$ has been "added" to the CAD.

Lifting with the reduced McCallum projection is substantially similar to lifting with the original McCallum projection, the primary difference being the points that must be "added" during stack construction.

### 4.3. DETECTING WELL-ORIENTEDNESS AND DETECTING POINTS TO ADD

McCallum's projection, in its most basic form, requires that the projection factors are well-oriented in order to produce an order-invariant CAD for the initial set of polynomials. The improved McCallum projection has the same requirement. However, McCallum's projection and CAD construction algorithm detects when well-orientedness fails, which is crucial to the practical utility of the method, and the improved projection needs to do this as well. Moreover, when the projection factors are well-oriented, the improved projection needs to compute the points over which projection factors vanish identically, since these points need to be "added" during CAD construction.

In essence, for each projection factor $p = p_n(\overline{x})z^n + \cdots + p_0(\overline{x})$, the system $p_n(\overline{x}) = p_{n-1}(\overline{x}) = \cdots = p_0(\overline{x}) = 0$ must be analyzed. If the system has positive dimension over the reals, $p$ is not well-oriented. If the system has no solution, no points need to be "added" during CAD construction in order to ensure the delineability of $p$ in each stack. Otherwise, however, the points in $\mathbb{R}^n$ over which $p$ vanishes identically must be computed and "added" during CAD construction.

One straightforward way of solving this system is to construct a sign-invariant CAD for $\{p_n(\overline{x}), \ldots, p_0(\overline{x})\}$. The dimension of the system's solution set, as well as the coordinates of all solutions in the zero-dimensional case, can be read off from the CAD. Since a system of equations is being considered, equational constraints can be used, which dramatically reduces the time and space required to solve the system. Various other timesaving techniques can be used as well. For example, the presence of even a single constant coefficient renders the system inconsistent.

At first glance, it may seem that the "improved McCallum Projection" might not actually be an improvement of McCallum's projection, since it needs to do the extra work of analyzing these systems of coefficients for each projection factor. This is, however, misleading. McCallum's projection includes all such coefficients, so that McCallum's projection actually contains the complete projection of $\{p_n(\overline{x}), \ldots, p_0(\overline{x})\}$ (without using equational constraints, or any other tricks that are applicable to system solving). Moreover, the CAD that would be constructed in solving the system $p_n(\overline{x}) = \cdots = p_0(\overline{x}) = 0$ is actually a simplification (in the sense of Brown, 1998) of the CAD constructed by McCallum's *CADW*. So McCallum's *CADW* does all the same work, but the polynomials $p_n(\overline{x}), \ldots, p_0(\overline{x})$ are mixed with other projection factors (resultants, discriminants, input polynomials, and coefficients of other projection factors) where they produce more and more extraneous projection factors with each projection.

Thus even when these systems of coefficients are analyzed by CAD, the improved projection is more efficient than the McCallum projection. However, while constructing a CAD for a set of polynomials is a way to answer fundamental questions about the system the polynomials define—for example, "What is the dimension of the solution set?", "Are there solutions?", "What are the coordinates of the isolated solutions?"—it may be overkill. Since we are restricted to systems of equalities, there is a variety of other methods that may be much faster in practice (and, of course, there is also a variety of methods that are asymptotically faster—Grigor'ev, 1988 or Renegar, 1992, for example). For instance, a Groebner Basis may detect inconsistency or determine dimension, and there are Groebner Basis implementations that perform very well in practice. Fast, practical algorithms for finding the real solutions of polynomial systems are a subject of on-going research (see, for example, Rouillier, 1999; Aubry *et al.*, 2000), and any progress on this front further increases the practical benefits of using the reduced McCallum projection rather than the original McCallum projection.

### 4.4. AN EXAMPLE

This section applies the new projection operator to an example problem. A classic toy problem for quantifier elimination algorithms is the quantified formula $\exists x[ax^2 + bx + c = 0]$. The CAD-based method of quantifier elimination solves this problem by constructing a CAD for the polynomial $f(a, b, c, x) = ax^2 + bx + c$.

McCallum's projection for $f$ proceeds as follows:

$$\begin{aligned}&\text{ProjMC}(\{ax^2+bx+c\}) = \{b^2-4ac, a, b, c\}, \text{factors} = \{b^2-4ac, a, b, c\}\\ &\text{ProjMC}(\{b^2-4ac, c\}) = \{-4a, b^2, -b^2\}, \text{factors} = \{a, b\}\\ &\text{ProjMC}(\{b\}) = \emptyset, \text{factors} = \emptyset\\ &P = \{ax^2+bx+c, b^2-4ac, a, b, c\}.\end{aligned}$$

This projection factor set decomposes $\mathbb{R}^4$ into 115 cells. QEPCAD, an implementation of quantifier elimination by partial CAD based on the ideas of Collins and Hong (1991) and Hong (1992), computes $P$ and constructs a representation of the CAD it defines in about 40 milliseconds.

The reduced McCallum projection of $f$ proceeds as follows:

$$\begin{aligned}&\text{Proj}(\{ax^2+bx+c\}) = \{b^2-4ac, a\}, \text{factors} = \{b^2-4ac, a\}\\ &\text{Proj}(\{b^2-4ac\}) = \{-4a\}, \text{factors} = \{a\}\\ &\text{Proj}(\emptyset) = \emptyset, \text{factors} = \emptyset\\ &P = \{ax^2+bx+c, b^2-4ac, a\}, \text{points } (0,0) \text{ and } (0,0,0) \text{ must be added.}\end{aligned}$$

Thus, the reduced projection factor set leaves out $b$ and $c$, which occur in McCallum's projection factor set. It is clear by inspection that $(0,0,0)$ must be added to the CAD of $\mathbb{R}^3$ because $f$ vanishes identically at this point. Similarly, $(0,0)$ must be added to the CAD of $\mathbb{R}^2$ because $-4ac+b^2$ vanishes identically at that point. The CAD that results from the reduced projection (with the two added points) consists of 27 cells in $\mathbb{R}^4$. QEPCAD computes the reduced projection factor set and constructs a representation of the CAD it defines in about 10 milliseconds. (Note: QEPCAD does not implement the reduced McCallum projection nor does it allow arbitrary points to be "added" to a CAD. However, both can be simulated through QEPCADs an interactive interface by directing the program to ignore "extra" projection factors generated by McCallum's projection.)

This example is so small that it is even possible to go through the projection phase by hand. Furthermore, the "extra" polynomials included by McCallum's projection are relatively benign, in that they do not interact to produce further "extra" polynomials in subsequent projections. Even so, both time and space requirements are about four times as high when McCallum's projection is used in place of the reduced projection.

## 5. Projecting Bounded Sets

Section 3 demonstrated that McCallum's projection can be reduced by leaving all coefficients save leading coefficients out of the projection. This section shows that even leading coefficients may be left out of the projection factor set when using CAD to solve certain kinds of quantifier elimination problems. For a complete description of the CAD-based quantifier elimination method, consult Collins and Hong (1991).

Consider a formula of the form $(\exists z)[F(x_1, \ldots, x_k, z)]$, where $F$ is a boolean combination of equalities and inequalities involving elements of $\mathbb{Z}[x_1, \ldots, x_k, z]$. This formula defines a set $T \subseteq \mathbb{R}^k$. Quantifier elimination by CAD calls for us to construct a CAD $C$ of $\mathbb{R}^k$ such that each cell of $C$ is either contained in $T$ or disjoint from $T$, so that $T$ can be described as the union of cells in $C$.

Typically, $C$ is defined by constructing $D$, a CAD of $\mathbb{R}^{k+1}$ in which the elements of $A$, the set of polynomials appearing in $F$, have invariant sign. The cells of $C$ are then the

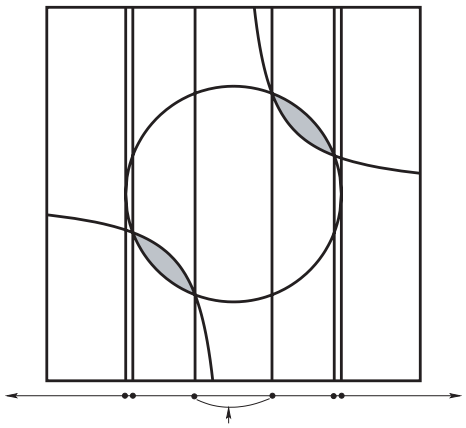

**Figure 1.** A projection that leaves out leading coefficients.

regions in $\mathbb{R}^k$ over which the cells of $D$ are cylindrically arranged. In other words, $C$ is an order-invariant CAD for Proj($A$). The formula $F$ is clearly either identically true or identically false in any cell of $D$. A cell $c \in C$ is contained in $T$ if and only if $F$ is true in at least one of the cells of $D$ that are cylindrically arranged over $c$. Thus, $T$ can be described as the union of cells in $C$.

However, $C$ need not be defined in this way to ensure that $T$ may be described as the union of cells in $C$. For example, consider the formula $(\exists y)[p_1 < 0 \ \wedge \ p_2 > 0]$, where $p_1 = x^2 + y^2 - 4$ and $p_2 = xy - 1$. We can construct the CAD of $\mathbb{R}^1$ defined by $\text{disc}_y(p_1)$, $\text{disc}_y(p_2)$, and $\text{res}_y(p_1, p_2)$, and as Figure 1 shows, the quantified formula is either identically true or identically false in each cell of the CAD, *despite the fact that leading coefficients were not included in projection*! By leaving leading coefficients out of the projection, we are not guaranteed that $p_1$ and $p_2$ are delineable over each cell in the CAD of $\mathbb{R}^1$. For example, consider the cell in the CAD of $\mathbb{R}^1$ that is marked in Figure 1. Polynomial $p_2$ is not delineable over this cell, and the reason is that $p_2$ has vertical asymptotes. However, these vertical asymptotes do not play a role in defining the set $(\exists y)[p_1 < 0 \ \wedge \ p_2 > 0]$. We know this will be the case *because we know the set* $p_1 < 0 \ \wedge \ p_2 > 0$ *is bounded in* $y$, and therefore no point in the set is near the asymptotes. Since the set we are projecting is contained within a circle, it is clear that it is bounded in $y$. For many quantifier elimination problems this kind of information about boundedness may be known *a priori* either from inspecting the formula, or from the application out of which the problem arose.

If it is known that the set defined by $F$ is bounded (in a sense to be made precise later), the following theorem shows that $C$ may be defined as an order-invariant CAD for the set of discriminants and pairwise resultants of elements of $A$.

THEOREM 5.1. *Let* $f \in \mathbb{R}[\overline{x}, z]$ *be a* $(k+1)$*-variate polynomial of positive degree* $n$ *in the variable* $z$*, with discriminant* $D(\overline{x}) \neq 0$*. Let* $S$ *be a connected submanifold of* $\mathbb{R}^k$ *on which* $D$ *is order-invariant and such that* $f$ *vanishes identically at no point in* $S$*. Let* $R$ *be a maximal connected region of* $S \times \mathbb{R}$ *in which* $f$ *has invariant order. If* $R$ *is bounded by continuous functions* $B_1$ *and* $B_2$*, then the projection of* $R$ *onto* $\mathbb{R}^k$ *is* $S$*.*

PROOF. As a matter of notational convenience, if $u = (u_1, \ldots, u_k) \in \mathbb{R}^k$ and $\alpha \in \mathbb{R}$, let $(u, \alpha)$ denote the point $(u_1, \ldots, u_k, \alpha) \in \mathbb{R}^{k+1}$. Given $u \in S$ and $\alpha \in \mathbb{R}$ such that $(u, \alpha) \in R$, we will show that for an arbitrary point $v \in S$ there is a $\beta$ such that $(v, \beta) \in R$.

Let $L : [0, 1] \longrightarrow \mathbb{R}^k$ be a path in $S$ connecting $u$ and $v$. Consider the set $H$ of all continuous real-valued functions on $[0, 1]$ whose value at zero is $\alpha$ and whose value at one is $\beta$. To each $h \in H$ we define the set $X_h = \{t \in [0, 1] | (L(t), h(t)) \notin R\}$, and the function $d(h)$ as $\inf X_h$, if $X_h \neq \emptyset$, and one otherwise. Thus, for any $h \in H$ we have $\{(L(t), h(t)) \mid t \in [0, d(h))\} \subseteq R$.

Let $t_0 \in [0, 1]$ be defined by $t_0 = \sup\{d(h) | h \in H\}$. We will suppose $t_0 \neq 1$. There are two cases to consider:

Case 1: The leading coefficient $l(\overline{x})$ of $f$ is non-zero at $L(t_0)$. By continuity of $l(\overline{x})$, there exists a neighborhood $N$ of $L(t_0)$ such that $l(\overline{x})$ is non-zero throughout $N$. By Lemma 8.2, $N$ can be refined to a neighborhood of $L(t_0)$ such that $N \cap S$ is a connected analytic submanifold. Therefore, by Theorem 2.1, the roots of $f$ over $N \cap S$ are given by analytic functions $g_1, \ldots, g_s$ satisfying $g_1 < \cdots < g_s$ for all points in $S \cap N$, and such that the $g_i$ define the order-invariant sections of $f$ over $S \cap N$.

We claim there must be a $t_1 \in [0, t_0]$ such that $L(t) \in N$ for all $t \in [t_1, t_0]$ and for some $h \in H$, $(L(t), h(t)) \in R$ for all $t \in [0, t_1]$. If $t_0 = 0$ then $t_1 = 0$ and any element of $H$ will satisfy the above condition. If $t_0 \neq 0$ then choose $t_1$ to be close enough to $t_0$ that, as $t$ goes from $t_1$ to $t_0$, $L(t)$ lies completely within $N$ (this must be possible, since $N$ is a neighborhood of $L(t_0)$ and $L$ is continuous). By the definition of $t_0$, there must be some $h \in H$ such that $\{(L(t), h(t)) \mid t \in [0, (t_1 + t_0)/2)\} \subseteq R$, and clearly $(L(t), h(t)) \in R$ for all $t \in [0, t_1]$.

Let $t_2 \in (t_0, 1]$ be such that $L(t) \in N$ for all $t \in [t_0, t_2]$. We will use $h$ to define a function $h^*$ such that $(L(t), h^*(t)) \in R$ for all $t \in [0, t_2]$, which contradicts the definition of $t_0$.

If $f$ is zero in $R$, then $h(t_1) = g_i(L(t_1))$ for some $i$, and we can define $h^*$ as:

$$h^*(t) = \begin{cases} h(t), & \text{if } t \in [0, t_1] \\ g_i(L(t)), & \text{if } t \in (t_1, t_2]. \end{cases}$$

Since $R$ is a maximal connected region in $S \times \mathbb{R}$ in which $f$ has invariant order, $(L(t), h^*(t)) \in R$ for all $t \in [0, t_2]$.

If $f$ is non-zero in $R$, then the fact that $R$ is bounded means that there is an $i$ such that $g_i(L(t_1)) < h(t_1) < g_{i+1}(L(t_1))$. Thus, there is some convex combination[†] $\delta g_i(L(t_1)) + \beta g_{i+1}(L(t_1))$ that equals $h(t_1)$. Thus, we may define $h^*$ as:

$$h^*(t) = \begin{cases} h(t), & \text{if } t \in [0, t_1] \\ \delta g_i(L(t)) + \beta g_{i+1}(L(t)), & \text{if } t \in (t_1, t_2]. \end{cases}$$

Since $R$ is a maximal connected region in $S \times \mathbb{R}$ in which $f$ has invariant order, $(L(t), h^*(t)) \in R$ for all $t \in [0, t_2]$.

Case 2: The leading coefficient of $f$ is zero at $L(t_0)$. In this case, let $f^*$ and $N$ be as defined in paragraph three of the proof of Theorem 3.1, with $L(t_0)$ taking the place of $p$ in that proof. Note that by construction the leading coefficient of $f^*$ is non-zero in $N$. By Lemma 8.2, $N$ can be refined to a neighborhood of $L(t_0)$ such that $N \cap S$ is a connected

[†]A *convex combination* of $a$ and $b$ is a linear combination $sa + tb$ with the additional requirement that $s, t \geq 0$ and $s + t = 1$.

analytic submanifold. Therefore, by Theorem 2.1, the roots of $f^*$ over $N \cap S$ are given by the analytic functions $g_1, \ldots, g_s$ such that $g_1 < \cdots < g_s$ for all points in $N \cap S$, and such that the $g_i$ define the order-invariant sections of $f^*$ over $S \cap N$. Note that Lemma 8.3 implies that the order of $f^*$ at point $(w, \zeta)$, $\zeta \neq 0$, is equal to the order of $f$ at point $(w, \gamma + 1/\zeta)$.

We claim there must be a $t_1 \in [0, t_0]$ such that $L(t) \in N$ for all $t \in [t_1, t_0]$ and for some $h \in H$, $(L(t), h(t)) \in R$ for all $t \in [0, t_1]$. If $t_0 = 0$ then $t_1 = 0$ and any element of $H$ will satisfy the above condition. If $t_0 \neq 0$ then choose $t_1$ to be close enough to $t_0$ that, as $t$ goes from $t_1$ to $t_0$, $L(t)$ lies completely within $N$ (this must be possible, since $N$ is a neighborhood of $L(t_0)$ and $L$ is continuous). By the definition of $t_0$, there must be some $h \in H$ such that $\{(L(t), h(t)) \mid t \in [0, (t_1 + t_0)/2)\} \subseteq R$, and clearly $(L(t), h(t)) \in R$ for all $t \in [0, t_1]$.

Let $t_2 \in (t_0, 1]$ be such that $L(t) \in N$ for all $t \in [t_0, t_2]$. We will use $h$ to define a function $h^*$ such that $(L(t), h^*(t)) \in R$ for all $t \in [0, t_2]$, which contradicts the definition of $t_0$.

If $f$ is zero in $R$, then $h(t_1) = \gamma + 1/g_i(L(t_1))$ for some $i$. Since $R$, a maximal connected region in $S \times \mathbb{R}$ in which $f$ has invariant order, is bounded, $g_i(t) \neq 0$ for $t \in [t_1, t_2]$. Therefore, we can define $h^*$ as:

$$h^*(t) = \begin{cases} h(t), & \text{if } t \in [0, t_1] \\ \gamma + 1/g_i(L(t)), & \text{if } t \in (t_1, t_2]. \end{cases}$$

According to Lemma 8.3, the order of $f$ at $(L(t), h^*(t))$ is the same for all $t \in [t1, t2]$, and therefore $(L(t), h^*(t)) \in R$ for all $t \in [0, t_2]$.

If $f$ is non-zero in $R$, then the fact that $R$ is bounded means that there is a root of $f(L(t_1), z)$ above and below $h(t_1)$. Let $\gamma + 1/g_i(L(t_1))$ be the root immediately below $h(t_1)$, and let $\gamma + 1/g_j(L(t_1))$ be the root immediately above. There is some convex combination $\delta(\gamma + 1/g_i(L(t_1))) + \beta(\gamma + 1/g_j(L(t_1)))$ that equals $h(t_1)$. Moreover, since $R$ is bounded, neither $g_i$ nor $g_j$ are zero anywhere in $N$. Thus, we may define $h^*$ as:

$$h^*(t) = \begin{cases} h(t), & \text{if } t \in [0, t_1] \\ \delta(\gamma + 1/g_i(L(t))) + \beta(\gamma + 1/g_j(L(t))), & \text{if } t \in (t_1, t_2]. \end{cases}$$

Since $R$ is a maximal connected region in $S \times \mathbb{R}$ in which $f$ has invariant order, $(L(t), h^*(t)) \in R$ for all $t \in [0, t_2]$. Therefore, our assumption that $t_0 \neq 1$ is false.

Since $t_0 = 1$, for any $\epsilon > 0$ there is a function $h_\epsilon \in H$ such that $(L(t), h_\epsilon(t)) \in R$ for all $t \in [0, 1 - \epsilon)$. The above argument can be used with minor modification to show that for some suitably small value of $\epsilon$, $h_\epsilon$ can be extended to a function $h$ such that $(L(t), h(t)) \in R$ for all $t \in [0, 1]$. Thus, the $\beta$ we require is $h(1)$. □

The region $R$ from Theorem 5.1 is, in fact, an analytic submanifold, which is shown by the following theorem.

THEOREM 5.2. *Let $f \in \mathbb{R}[\overline{x}, z]$ be a $(k+1)$-variate polynomial of positive degree $n$ in the variable $z$, with discriminant $D(\overline{x}) \neq 0$. Let $S$ be a connected submanifold of $\mathbb{R}^k$ on which $D$ is order-invariant and such that $f$ vanishes identically at no point in $S$. Let $R$ be a maximal connected region of $S \times \mathbb{R}$ in which $f$ has invariant order. Then $R$ is an analytic submanifold of dimension* $\dim(S)$*, if $f = 0$ in $R$, and dimension* $1 + \dim(S)$ *otherwise.*

PROOF. By definition, $R$ is an analytic submanifold of dimension $d$ if at every point $p \in R$ there is a mapping $F = (F_1, \ldots, F_{n+1-d})$ such that in some neighborhood $N$ of $p$, the $F_i$s are analytic and $R \cap N = \{q \in \mathbb{R}^{k+1} \mid F(q) = 0\}$, and such that the Jacobian matrix of $F$ has full rank at $p$. Therefore, let $p$ be a point in $R$. We will show that the required mapping exists.

If $f \neq 0$ in $R$, this is trivial. In this case, let $\overline{p}$ be the projection of $p$ onto $S$. Since $S$ is an analytic submanifold, there is some mapping $\overline{F} = (\overline{F}_1, \ldots, \overline{F}_{n-\dim(S)})$ such that in some neighborhood $\overline{N}$ of $\overline{p}$, the $\overline{F}_i$s are analytic and $S \cap \overline{N} = \{q \in \mathbb{R}^k \mid \overline{F}(q) = 0\}$, and such that the Jacobian matrix of $\overline{F}$ has full rank at $\overline{p}$. If $F$ is simply the extension of $\overline{F}$ to $\mathbb{R}^{k+1}$, then for some neighborhood $N$ of $p$, the $F_i$s are analytic and $R \cap N = \{q \in \mathbb{R}^{k+1} \mid F(q) = 0\}$, and the Jacobian matrix of $F$ has full rank at $p$. In other words, the required mapping for $p$ is simply inherited from $\overline{p}$. Since $F$ is a mapping from $\mathbb{R}^{k+1}$ to $\mathbb{R}^{n-\dim(S)}$, the dimension of $R$ is $1 + \dim(S)$.

So suppose $f = 0$ in $R$, and let $\overline{p}$ be the projection of $p$ onto $S$. There are two cases to consider:

Case 1: The leading coefficient of $p$ is non-zero at $\overline{p}$. Let $\overline{N}$ be a neighborhood of $\overline{p}$ in which the leading coefficient of $p$ is non-zero. By Lemma 8.2, $N$ may be refined to a neighborhood of $\overline{p}$ such that $N \cap S$ is a connected analytic submanifold. By Theorem 2.1, $f$ is analytic delineable over $N \cap S$, and therefore, by Theorem 2.2.3 of McCallum (1984), each section of $f$ over $N \cap S$ is an analytic submanifold of dimension $\dim(S)$. In particular, that means that the required mapping for $p$ exists.

Case 2: The leading coefficient of $p$ is zero at $\overline{p}$. This is the only non-trivial case. We essentially solve it by the same old trick—we construct the polynomial $f^*$ and neighborhood $N$ of $p$ as in Theorem 3.1. Since $f^*$ has the same discriminant as $f$, and since the leading coefficient of $f^*$ does not vanish at $\overline{p}$, $f^*$ is analytic delineable over some neighborhood of $\overline{p}$, and thus each of its sections are analytic submanifolds of dimension $\dim(S)$. Thus, for point $(p_1, \ldots, p_n, 1/(p_{n+1} - \gamma))$ we have a mapping $F^*$ of the proper form, and this yields the mapping $F = F^*(x_1, \ldots, x_n, \gamma + 1/x_{n+1})$ which is easily shown to have the desired properties in a sufficiently small neighborhood of $p$. □

With Theorems 5.1 and 5.2, we can prove that in projecting to eliminate variable $z$ for a quantifier-elimination problem in the variables $x_1, \ldots, x_n, z$, we may leave leading coefficients out of the projection when we know that the set being projected is bounded by two continuous functions of $x_1, \ldots, x_n$.

THEOREM 5.3. *Let $T$ be a subset of $\mathbb{R}^{n+1}$ such that $T$ is bounded by continuous real-valued functions $B_1$ and $B_2$, i.e.*

$$T \subseteq \{(\alpha_1, \ldots, \alpha_n, \beta) \mid B_1(\alpha_1, \ldots, \alpha_n) \leq \beta \leq B_2(\alpha_1, \ldots, \alpha_n)\}.$$

*Suppose that $A$ is a set of polynomials in $x_1, \ldots, x_n, z$, and $W$ a set of points such that any connected analytic submanifold not containing any point in $W$ and in which the elements of $A$ have invariant order is either contained in $T$ or disjoint from $T$. Suppose that the $(n+1)$-level factors of elements of $A$ are all well-oriented.*

*Let $T'$ be the projection of $T$ onto $\mathbb{R}^n$. Let $A'$ be the union of all irreducible factors of elements of $A$ of level less than $n+1$, and all discriminants and pairwise resultants of irreducible factors of $(n+1)$-level elements of $A$. Let $W'$ be the union of the projection*

*of $W$ onto $\mathbb{R}^n$ and the points of $\mathbb{R}^n$ at which any of the $(n+1)$-level factors of elements of $A$ vanish identically.*

*Then any connected analytic submanifold in $\mathbb{R}^n$ not containing any point of $W'$, and in which the elements of $A'$ have invariant order is either contained in $T'$ or disjoint from $T'$. Moreover, membership of $\alpha = (\alpha_1, \ldots, \alpha_n)$ in $T'$ can be determined by lifting over $\alpha$ with respect to $A \cup \{z - \beta \mid (\alpha_1, \ldots, \alpha_n, \beta) \in W\}$ (following McCallum's lifting method) and checking the membership of the resulting sample points in $T$.*

Proof. Let $S$ be a connected analytic submanifold in $\mathbb{R}^n$ not containing any point of $W'$, and in which the elements of $A'$ have invariant order. Let $f$ be the product of all the irreducible $(n+1)$-level factors of elements of $A$. The elements of $A$ are order-invariant in a subset of $S \times \mathbb{R}$ if and only if $f$ has invariant order in the set. Suppose $\alpha \in T \cap (S \times \mathbb{R})$, and let $R_\alpha$ be the maximal connected region in $S \times \mathbb{R}$ containing $\alpha$ and in which $f$ is order-invariant. By Theorem 5.2, $R_\alpha$ is an analytic submanifold. Thus, by hypothesis, $R_\alpha \subseteq T$. $T$ is bounded by $B_1$ and $B_2$, so $R_\alpha$ must be bounded by $B_1$ and $B_2$ as well. Since the discriminant of $f$ is order-invariant in $S$ and $f$ does not vanish identically at any point in $S$, Theorem 5.1 states that the projection of $R_\alpha$ onto $\mathbb{R}^n$ is $S$. This proves the first part of the theorem.

To prove the second part of the theorem, let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be a point in $\mathbb{R}^n$. If we lift over $\alpha$ with respect to $A$, following McCallum's lifting procedure (i.e. possibly adding delineating polynomials), we get at least one sample point from each maximal connected region of $\alpha \times \mathbb{R}$ in which the elements of $A$ have invariant order. By adding $\{z - \beta \mid (\alpha_1, \ldots, \alpha_n, \beta) \in W\}$, we ensure that we get at least one sample point from each maximal connected region not containing elements of $W$, as well as sample points at the elements of $W$. As each of these regions is either a point or an open interval, each region is in fact an analytic submanifold. By hypothesis then, each region is either completely in $T$ or disjoint from $T$. Thus, by checking each of these sample points for membership in $T$, we may decide whether $\alpha$ is in $T'$. □

Of course, there is an analogous theorem for the general improved McCallum projection. The only change would be that leading coefficients would be included, and there would be no requirement of boundedness. Therefore, if we are given a quantified formula

$$(Q_1 y_1) \cdots (Q_s y_s)[F(x_1, \ldots, x_r, y_1, \ldots, y_s)], \qquad \text{where } Q_i \in \{\exists, \neg\exists\}$$

we can project to eliminate $y_s, y_{s-1}, \ldots, y_1$, at each projection step using Theorem 5.3 when we know *a priori* that the set we are projecting is bounded (i.e. bounded by two continuous functions of the remaining variables) in the variable we are eliminating, and otherwise project using the general improved McCallum projection. Once we are down to free-variable space, every projection will use the general improved McCallum projection. Theorem 5.3 and the obvious analogue for the general improved McCallum projection ensure that we can determine truth values for cells in free-variable space using the lifting process in bound-variable space.

Obviously there is a question as to whether or not these "bounded projections" will occur often in practice. Constraints like "$-1 \leq x \leq 1$" or "$x$ and $y$ lie in some circle defined by parameters" are quite natural, however, so it is possible that this improvement will in fact often be applicable. Moreover, removing even one extraneous polynomial early

in the projection process can lead to a dramatically smaller projection factor set, so it is an improvement that is worth pursuing.

## 6. A Non-trivial Example

This section considers a non-trivial example problem, and describes how the results from this paper may be brought to bear on the problem. Kahan's "Ellipse Problem" is a well-known example of a quantifier elimination problem. Lazard (1988) has published a solution to this problem, though it was not obtained automatically. The problem is this: characterize the ellipses contained inside the unit circle. If we assume that these ellipses are oriented with the axes, this question can be phrased as the quantifier elimination problem:

$$\forall x, y[a > 0 \quad \wedge \quad b > 0 \quad \wedge \quad b(x-c)^2 + a(y-d)^2 - ab = 0 \Longrightarrow x^2 + y^2 < 1].$$

Note that the $a$ and $b$ from this formula are not the axis lengths of the ellipse, but rather their squares.

We will consider constructing a truth-invariant CAD for the complement of this set, as it will make it easier to see that the projection improvements we use are indeed justified. If a CAD can represent the complement, it can certainly represent the set as well ... just negate the truth values of all the cells. Thus, we consider the formula:

$$\exists x, y[a > 0 \quad \wedge \quad b > 0 \quad \wedge \quad b(x-c)^2 + a(y-d)^2 - ab = 0 \quad \wedge \quad x^2 + y^2 \geq 1].$$

CADs are constructed with respect to a variable order, and for this problem we will use $a < b < c < d < x < y$.

From this formulation it is clear that the equational constraint $b(x-c)^2+a(y-d)^2-ab = 0$ may be used during projection, as described in McCallum (1999) and Collins (1998). Furthermore, if $S$ is a bounded region in $\mathbb{R}^4$ satisfying $a > 0 \quad \wedge \quad b > 0$, the set defined by

$$b(x-c)^2 + a(y-d)^2 - ab = 0 \quad \wedge \quad x^2 + y^2 \geq 1$$

is clearly bounded over $S$. Thus, Theorem 5.1 states that no leading coefficients are needed in projecting to eliminate $y$ or $x$. So the first two projections will use the reduced McCallum projection without adding leading coefficients, and the subsequent three projections will use the reduced McCallum projection. Throughout the projection process, we must identify regions over which projection factors vanish identically. However, the problem formulation requires that both $a$ and $b$ be greater than zero, and regions on which projection factors vanish identically that do not meet this requirement can be ignored.

Proj($P_6$) We project two polynomials (both from input formula) using the reduced McCallum projection and the equational constraint mentioned above, because of boundedness leading coefficients are not required, and neither polynomial vanishes identically over any region satisfying $a > 0$ and $b > 0$.

Proj($P_5$) We project two polynomials using the reduced McCallum projection, because of boundedness leading coefficients are not required, and $(1, 1, 0, 0)$ is the only point satisfying $a > 0$ and $b > 0$ over which either polynomial vanishes identically.

Proj($P_4$) We project three polynomials using the reduced McCallum projection, and none of these polynomials vanishes identically over any point satisfying $a > 0$ and $b > 0$.

**Table 1.** The reduced McCallum projection.

| Level $i$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $\|P_i\|$ | 141 | 18 | 6 | 3 | 2 | 2 |

**Table 2.** The McCallum projection.

| Level $i$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $\|P_i\|$ | ??? | 129 | 17 | 7 | 2 | 2 |

Proj($P_3$) We project six polynomials using the reduced McCallum projection, and $(1, 1)$ is the only point satisfying $a > 0$ and $b > 0$ over which any polynomial vanishes identically.

Proj($P_2$) We project 18 polynomials using McCallum's projection.

This produces 141 projection factors of level 1. The polynomials $a-1$, $b-1$, $c$, and $d$ are all in the projection factor set, so the two points $(1, 1)$ and $(1, 1, 0, 0)$ do not need to be specially "added" as we construct a CAD. These points will end up as individual cells though the normal lifting process. Table 1 summarizes the counts of projection factors of various levels.

By contrast, suppose the McCallum projection is used for this problem. To make the comparison meaningful, we use the same equational constraint when projecting $P_6$. As McCallum suggests, in projecting a polynomial, we add coefficients from highest degree to lowest degree only until some coefficient is seen to be non-vanishing. We use the condition $a > 0 \quad \wedge \quad b > 0$ to conclude that any coefficient that is a power product of $a$ and $b$ is non-vanishing, and thus it, and any following coefficients, may be removed from the projection. Otherwise, the straightforward McCallum projection as implemented in QEPCAD is used.

The results are summarized in Table 2. QEPCAD was unable to complete the final projection after more than 16 hours of CPU time. Not only are there 129 discriminants and over 8000 resultants that need to be computed for this projection, but some of the polynomials involved are quite large—several have degrees in $b$ of 80 or more! It certainly seems reasonable to assume that if this projection were to be completed, there would be thousands of one-level projection factors.

The number of polynomials in a projection factor set is a very coarse metric for comparing projection factor sets. The degrees of those polynomials are also critically important. Using the reduced McCallum projection as described, the highest degree (in $b$) of any two-level projection factor was 11—with the McCallum projection it was 96. Using the reduced McCallum projection as described, the highest degree of any one-level projection factor was 37—with the McCallum projection it would certainly be much higher.

Constructing a CAD from the projection factor set produced by the reduced McCallum projection is still beyond what can be currently achieved in a reasonable amount of time and space. But it seems likely that this will change fairly soon, especially since progress in the fundamental algorithms of computing with real algebraic numbers—as opposed to progress in CAD-specific algorithms—is all that is required. However, constructing a CAD from the projection factor set produced by the McCallum projection, a much larger

set containing polynomials of much higher degree, seems likely to be impractical for a long time.

It is worth noting that the projection factor set for this problem could be reduced further if Theorem 5.1 could be applied to projections in free-variable space to allow us to ignore leading coefficients in projection. This is possible, but would require a considerably different idea of how the lifting process constructs a CAD from a projection factor set, and could cause problems in solution formula construction.

## 7. Conclusion

This paper presents an improved general projection for CAD, the *reduced* McCallum projection, and a still further improved projection for the special case of projecting sets that are bounded in a certain sense. The improved projections are proper subsets of previous projections, so there is no doubt as to their superiority. Section 6 provides an example illustrating that these improvements in projection can result in dramatically smaller projection factor sets, in terms both of the number of projection factors, and their degrees.

One interesting question is the relation between Theorem 3.1 and a projection operator suggested by Lazard. In Lazard (1994), he suggested a projection consisting of discriminants, resultants, leading coefficients, and trailing coefficients, but this has not been proven to be valid. Because the reduced projection from this paper has to separately treat points over which the polynomial being projected vanishes identically, it does not quite imply the correctness of Lazard's projection. It does say, however, that in order to prove Lazard's projection valid, it would suffice to show that if $S$ is a connected region in which the discriminant, leading coefficient, and trailing coefficient of a well-oriented polynomial $f$ are all order-invariant, and $f$ vanishes identically at some point in $S$, then $S$ has dimension zero. It also says that if you are looking for a counterexample to Lazard's projection, the only way it might possibly fail is by not identifying the isolated points over which some projection factor vanishes. In any event, the reduced McCallum projection is superior.

An issue that has not been addressed in this paper is what to do when a projection factor vanishes identically over a region of positive dimension. Sometimes problems are posed in such a way that this difficulty is side-stepped, as in the example considered in Section 6, in which the condition $a > 0 \ \wedge \ b > 0$ allowed us to ignore higher-dimensional regions over which projection factors vanished. Sometimes, however, the problem cannot be avoided. This issue may be addressed in a future paper.

## 8. Miscellaneous Lemmata

This section provides proofs of results used in proving Theorems 3.1 and 5.1. They are probably obvious enough to use without proof, but are included here for completeness.

The following lemma is used in the proof of Theorem 3.1. It says that a polynomial and its "reverse" have the same discriminant provided the polynomial has non-zero constant coefficient. This is actually a special case of the PGL(2)-invariance property of discriminants (see Gelfand *et al.*, 1994) which is a classical result.

LEMMA 8.1. *Let $f(x)$ be a polynomial over some integral domain $D$ and let $n$ be the degree of $f$. If the constant coefficient of $f$ is non-zero then* $\mathrm{disc}_x(f) = \mathrm{disc}_x(x^n f(1/x))$.

PROOF. Let $f(x)$ be a degree $n$ polynomial with non-zero constant coefficient. The polynomial $f$ may be written two ways

$$f = f_n x^n + \cdots + f_0 = f_n \Pi_{i=1}^n (x - \alpha_i)$$

where the $\alpha_i$ are the roots of $f$ in its splitting field. Note that $f_0 = (-1)^n f_n \Pi_{i=1}^n \alpha_i$. The discriminant of $f$ is defined as

$$\mathrm{disc}_x(f) = (-1)^{n(n-1)/2} f_n^{2n-2} \Pi_{i \neq j} (\alpha_i - \alpha_j).$$

Let $\beta_1, \ldots, \beta_n$ be the roots of $x^n f(1/x)$, and note that the $\beta_i$ are exactly the reciprocals of the roots of $f$. Consider the discriminant of $x^n f(1/x)$:

$$\begin{aligned}
\mathrm{disc}_x\left(x^n f(1/x)\right) &= (-1)^{n(n-1)/2} f_0^{2n-2} \Pi_{i \neq j} (\beta_i - \beta_j) \\
&= (-1)^{n(n-1)/2} f_0^{2n-2} \Pi_{i \neq j} (1/\alpha_i - 1/\alpha_j) \\
&= (-1)^{n(n-1)/2} f_0^{2n-2} \Pi_{i \neq j} \left( \frac{\alpha_j - \alpha_i}{\alpha_j \alpha_i} \right) \\
&= (-1)^{n(n-1)/2} f_0^{2n-2} \frac{\Pi_{i \neq j} \alpha_j - \alpha_i}{\Pi_{i \neq j} \alpha_j \alpha_i} \\
&= (-1)^{n(n-1)/2} f_0^{2n-2} \frac{\Pi_{i \neq j} \alpha_i - \alpha_j}{\left(\Pi_{i=1}^n \alpha_i\right)^{2n-2}} \\
&= (-1)^{n(n-1)/2} \left((-1)^n f_n \Pi_{i=1}^n \alpha_i\right)^{2n-2} \frac{\Pi_{i \neq j} \alpha_i - \alpha_j}{\left(\Pi_{i=1}^n \alpha_i\right)^{2n-2}} \\
&= (-1)^{n(n-1)/2} f_n^{2n-2} \Pi_{i \neq j} \alpha_i - \alpha_j. \quad \square
\end{aligned}$$

The following lemma is used in the proof of Theorem 3.1. It follows fairly directly from Theorem 2.2 of McCallum (1988).

LEMMA 8.2. *Let $S$ be a connected analytic submanifold, let $p$ be a point in $S$, and let $N$ be a neighborhood of $p$. There is a neighborhood $N'$ of $p$ such that $N' \subseteq N$ and $N \cap S$ is a connected analytic submanifold.*

PROOF. Let $s$ be the dimension of $S$ and let $n$ be the dimension of the ambient space. By Theorem 2.2 of McCallum (1988), there is a neighborhood $U$ of $p$ and a coordinate system (see McCallum, 1988, p. 144, for a definition of coordinate system) $\Phi = (\phi_1, \ldots, \phi_n)$ such that

$$S \cap U = \{x \in U | \phi_{s+1}(x) = 0, \ldots, \phi_n(x) = 0\}.$$

Let $U' = \Phi(U \cap N)$, and note that $U'$ is a neighborhood of $\Phi(p)$. Let $B$ be an $\epsilon$-ball centered at $\Phi(p)$ and contained in $U'$. Let $N' = \Phi^{-1}(B)$. Clearly, $N' \subseteq N$, $p \in N'$, and $N'$ is open.

To see that $N' \cap S$ is connected, note that $B \cap \{q \in \mathbb{R}^n | q_{s+1} = 0, \ldots, q_n = 0\}$ is a connected set, and is precisely $\Phi(N' \cap S)$. So for any two points $a$ and $b$ in $N' \cap S$, we can construct a path in $B \cap \{q \in \mathbb{R}^n | q_{s+1} = 0, \ldots, q_n = 0\}$ connecting $\Phi(a)$ and $\Phi(b)$, and that maps back under $\Phi^{-1}$ to a path in $N' \cap S$ connecting $a$ and $b$.

Finally, $N' \cap S$ is clearly an analytic submanifold by Theorem 2.2 of McCallum (1988), because $\Phi$ provides a coordinate system for every point in $N' \cap S$. $\square$

The following lemma is used in the proof of Theorem 5.1. It essentially says that the orders of a polynomial and its reverse are the same at corresponding points.

LEMMA 8.3. *Let $f(\overline{x}, z) \in \mathbb{R}[x_1, \ldots, x_k, z]$ be a polynomial of degree $n$. Let $f^* = z^m f(1/z)$, where $m \geq n$. If $(w, \zeta) \in \mathbb{R}^{k+1}$ is a point such that $\zeta \neq 0$, then the order of $f^*$ at $(w, \zeta)$ is equal to the order of $f$ at $(w, 1/\zeta)$.*

PROOF. This is obvious if the order of $f^*$ at $(w, \zeta)$ is zero. So assume that $f^*(w, \zeta) = 0$. Consider

$$\frac{\partial^s}{\partial x_1^{e_1} \cdots \partial x_k^{e_k} \partial z^t} f^*.$$

Since $f^*_{x_i} = z^m f_{x_i}(1/z)$, it suffices to show that

$$\left(\frac{\partial^s}{\partial z^s} f^*\right)\Big|_{(\overline{x},z)=(w,\zeta)} = 0 \Longleftrightarrow \left(\frac{\partial^s}{\partial z^s} f\right)\Big|_{(\overline{x},z)=(w,1/\zeta)} = 0.$$

This is equivalent to

$$\frac{\partial^s}{\partial z^s} f^*(w, z)\Big|_{z=\zeta} = 0 \Longleftrightarrow \frac{\partial^s}{\partial z^s} f(w, z)\Big|_{z=1/\zeta} = 0$$

which simply means that the multiplicity of $f^*(w, z)$ at $\zeta$ is the same as the multiplicity of $f(w, z)$ at $1/\zeta$. This is obvious from the definition of $f^*$. □

## Acknowledgements

I would like to thank Scott McCallum for his help in reviewing Theorem 3.1 and improving its proof, and George Nakos for pointing out that Lemma 8.1 is a special case of the PGL(2)-invariance property of discriminants. This research was supported by a grant from the Naval Academy Research Council.

## References

Arnon, D. S., Collins, G. E., McCallum, S. (1984). Cylindrical algebraic decomposition I: the basic algorithm. *SIAM J. Comput.*, **13**, 865–877.

Aubry, P., Rouillier, F., Safey El Din, M. Real solving for positive dimensional systems.Technical Report RR-3992, INRIA, September 2000.

Brown, C. W. (1998). Simplification of truth-invariant cylindrical algebraic decompositions. In *Proceedings of International Symposium on Symbolic and Algebraic Computation*, pp. 295–301.

Caviness, B. F., Johnson, J. R. eds, (1998). *Quantifier Elimination and Cylindrical Algebraic Decomposition, Texts and Monographs in Symbolic Computation*. Vienna, Springer.

Collins, G. E. (1975). In *Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition*, *LNCS* **33**, pp. 134–183. Berlin, Springer, Reprinted in Caviness and Johnson (1998).

Collins, G. E. (1998). Quantifier elimination by cylindrical algebraic decomposition—20 years of progress. In Caviness, B., Johnson, J. eds, *Quantifier Elimination and Cylindrical Algebraic Decomposition, Texts and Monographs in Symbolic Computation*. Vienna, Springer.

Collins, G. E., Hong, H. (Sep. 1991). Partial cylindrical algebraic decomposition for quantifier elimination. *J. Symb. Comput.*, **12**, 299–328.

Gelfand, I. M., Kapranov, M. M., Zelevinsky, A. V. (1994). *Discriminants, Resultants, and Multidimensional Determinants*. Berlin, Springer.

Grigor'ev, D. Yu. (1988). The complexity of deciding tarski algebra. *J. Symb. Comput.*, **5**, 65–108.

Hong, H. (1992). Simple solution formula construction in cylindrical algebraic decomposition based quantifier elimination. In *Proceedings of International Symposium on Symbolic and Algebraic Computation*, pp. 177–188.

Hong, H., Liska, R., Steinberg, S. (1997). Testing stability by quantifier elimination. *J. Symb. Comput.*, **24**, 161–187. Special Issue on Applications of Quantifier Elimination.
Lazard, D. (1988). Quantifier elimination: optimal solution for two classical examples. *J. Symb. Comput.*, **5**, 261–266.
Lazard, D. (1994). An improved projection for cylindrical algebraic decomposition. In Bajaj, C. L. ed., *Algebraic Geometry and its Applications*, pp. 467–476. Berlin, Springer, Collections of Papers from Abhyankar's 60th Birthday Conference.
McCallum, S. (1984). An Improved Projection Operator for Cylindrical Algebraic Decomposition. Ph.D. Thesis, University of Wisconsin-Madison.
McCallum, S. (1988). An improved projection operation for cylindrical algebraic decomposition of three-dimensional space. *J. Symb. Comput.*, **5**, 141–161.
McCallum, S. (1998). An improved projection operator for cylindrical algebraic decomposition. In Caviness, B., Johnson, J. eds, *Quantifier Elimination and Cylindrical Algebraic Decomposition, Texts and Monographs in Symbolic Computation*. Vienna, Springer-Verlag.
McCallum, S. (1999). On projection in CAD-based quantifier elimination with equational constraint. In Dooley, Sam ed., *Proceedings of International Symposium on Symbolic and Algebraic Computation*, pp. 145–149.
Renegar, J. (1992). On the computational complexity and geometry of the first-order theory of the reals, parts I-III. *J. Symb. Comput.*, **13**, 255–352.
Rouillier, F. (1999). Solving zero-dimensional systems through the rational univariate representation. *J. Appl. Algebra Eng., Commun. Comput.*, **9**, 433–461.
Strzebonski, A. (2000). Solving systems of strict polynomial inequalities. *J. Symb. Comput.*, **29**, 471–480.

*Originally Received 23 October 2000*
*Accepted 4 April 2001*