Cylindrical Algebraic Decomposition I: The Basic Algorithm

Dennis S. Arnon

George E. Collins

Scot McCallum

Report Number:
82-427
Given a set of \( r \)-variate integral polynomials, a \emph{cylindrical algebraic decomposition (cad)} of euclidean \( r \)-space \( E^r \) partitions \( E^r \) into connected subsets compatible with the zeros of the polynomials. Collins (1975) gave an algorithm for cad construction as part of a new decision procedure for real closed fields. This algorithm has since been implemented and applied to diverse problems (optimization, curve display). New applications of it have been proposed (program verification, motion planning). Part I of the present paper has several purposes. First, it provides an exposition of the essential aspects of the algorithm. Second, it corrects minor errors in the 1975 paper, and develops certain concepts introduced there. Third, it provides a framework for the adjacency algorithm presented in Part II. In addition, it surveys the applications of cad's and provides a detailed example of the operation of the algorithm.

Keywords: polynomial zeros, computer algebra, computational geometry, semi-algebraic geometry, real closed fields, decision procedures, real algebraic geometry.
1. Introduction. Given a set of \( \tau \)-variate integral polynomials, a \textit{cylindrical algebraic decomposition (cad)} of euclidean \( r \)-space \( E^r \) partitions \( E^r \) into connected subsets compatible with the zeros of the polynomials (Section 2 below gives a precise definition). For example, consider the bivariate polynomial

\[ y^4 - 2y^3 + y^2 - 3x^2y + 2x^4. \]

Its zeros comprise the curve shown in Figure 1. Figure 2 shows a cad of the plane compatible with its zeros.

Cad's were introduced by Collins in 1973 (see [COL75]) as part of a new quantifier elimination, and hence decision, method for elementary algebra and geometry. He gave an algorithm for cad construction, and proved that for any fixed number of variables, its computing time is a polynomial function of the remaining parameters of input size. As can be seen from the

\[ Figure 1 \]
example above, cad's are closely related to the classical simplicial and CW-complexes of algebraic topology. In fact, the essential strategy of Collins' cad algorithm, induction on dimension, can be found in van der Waerden's 1929 argument ([WAE29], pp. 360-361) that real algebraic varieties are triangulable.

Collins' cad-based decision procedure for elementary algebra and geometry is the best known (see [FER79]; very little besides a cad is needed for the decision procedure). J. Schwartz and M. Sharir used the cad algorithm to solve a motion planning problem ([SCH82]). D. Lankford [LAN78] and N. Dershowitz [DER79] pointed out that a decision procedure for elementary algebra and geometry could be used to test the termination of term-rewriting systems. P. Kahn used cad's to solve a problem on rigid frameworks in algebraic topology ([KAH79]). Kahn also observed ([KAH78]) that a cad algorithm provides a basis for a constructive proof that real
algebraic varieties are triangulable, and thus for computing the homology groups of a real algebraic variety.

Implementation of Collins' cad algorithm began soon after its introduction, culminating in the first complete program in 1981 [ARN81a]. The program has begun to find use; in May, 1982 the termination of a term-rewriting system for group theory (given by Lankford [LAN78]), was verified using it. It has also been utilized for display of algebraic curves [ARN81b]. In 1977, Müller implemented certain subalgorithms of the cad algorithm and used them to solve algebraic optimization problems [MUE77].

Part I of the present paper has several purposes. One is to provide an exposition of the essential aspects of Collins' cad algorithm that is as simple and accessible as possible, while still being complete. Minor errors in [COL75], [COL76], [ARN79], and [ARN81a] are corrected in our new exposition. A second purpose is to provide a framework for the adjacency algorithm presented in Part II. We also give a detailed example of the cad algorithm's operation.

In Part I we have given simplicity and clarity priority over efficiency, so the reader may well notice ways in which the efficiency of the algorithm we present here could be improved. A forthcoming Part III of the present paper will discuss efficient ways to implement the algorithms of Parts I and II, and report on experience with computer programs for these algorithms.

Part I is organized as follows: In Section 2 we give a rigorous definition of cad and establish notation for later sections. Sections 3, 4, and 5 present the cad algorithm. Section 6 traces the algorithm on an example.
2. Definition of cylindrical algebraic decomposition. The many ingredients of a precise definition of cad lead us to devote this entire section to that definition.

Connectivity plays an important role in the theory of cad's. It is convenient to have a term for a nonempty connected subset of $E^r$; we will call such sets regions. For a region $R$, the cylinder over $R$, written $Z(R)$, is $R \times E$. A section of $Z(R)$ is a set $s$ of points $<\alpha, f(\alpha)>$, where $\alpha$ ranges over $R$, and $f$ is a continuous, real-valued function on $R$. $s$, in other words, is the graphs of $f$. We say such an $s$ is the $f$-section of $Z(R)$. A sector of $Z(R)$ is a set $S$ of all points $<\alpha, b>$, where $\alpha$ ranges over $R$ and $f_1(\alpha) < b < f_2(\alpha)$ for (continuous, real-valued) functions $f_1 < f_2$. The constant functions $f_1 = -\infty$, and $f_2 = +\infty$, are allowed. Such an $S$ is the $(f_1, f_2)$-sector of $Z(R)$. Clearly sections and sectors of cylinders are regions. Note that if $r = 0$ and $R = E^0 = \text{a point}$, then $Z(R) = E^1$, any point of $E^1$ is a section of $Z(R)$, and any open interval in $E^1$ is a sector of $Z(R)$.

For any subset $X$ of $E^r$, a decomposition of $X$ is a finite collection of disjoint regions whose union is $X$. Continuous, real-valued functions $f_1 < f_2 < \ldots < f_k$, $k \geq 0$, defined on $R$, naturally determine a decomposition of $Z(R)$ consisting of the following regions: (1) the $(f_i, f_{i+1})$-sectors of $Z(R)$ for $0 \leq i \leq k$, where $f_0 = -\infty$ and $f_{k+1} = +\infty$, and (2) the $f_i$-sections of $Z(R)$ for $1 \leq i \leq k$. We call such a decomposition a stack over $R$ (determined by $f_1, \ldots, f_k$).

A decomposition $D$ of $E^r$ is cylindrical if either (1) $r = 1$ and $D$ is a stack over $E^0$, or (2) $r > 1$, and there is a cylindrical decomposition $D'$ of $E^{r-1}$ such that for each region $R$ of $D'$, some subset of $D$ is a stack over $R$. 
It is clear that $D'$ is unique for $D$, and thus associated with any cylindrical decomposition $D$ of $E^r$ are unique induced cylindrical decompositions of $E^i$ for $i = r-1, r-2, ..., 1$. Conversely, given a cad $\mathcal{D}$ of $E^i$, $i < r$, a cad $D$ of $E^r$ is an extension of $\mathcal{D}$ if $D$ induces $\mathcal{D}$.

For $0 \leq i \leq r$, an $i$-cell in $E^r$ is a subset of $E^r$ which is homeomorphic to $E^i$. It is not difficult to see that if $c$ is an $i$-cell, then any section of $Z(c)$ is an $i$-cell, and any sector of $Z(c)$ is an $(i+1)$-cell (these observations are due to P. Kahn [Kahn76]). It follows by induction that every element of a cylindrical decomposition is an $i$-cell for some $i$.

A subset of $E^r$ is semi-algebraic if it can be constructed by the operations of finite union, finite intersection, and complementation applied to sets of the form

$$\{ x \in E^r \mid F(x) \geq 0 \},$$

where $F$ is an element of $\mathbb{Z}[x_1, \ldots, x_r]$, the ring of integral polynomials in $r$ variables. We write $I_r$ to denote $\mathbb{Z}[x_1, \ldots, x_r]$. As we shall now see, a different definition of semi-algebraic set is possible, from which one obtains a useful characterization of such sets. By a formula we will mean a well-formed formula of the first order theory of real closed fields. (The "first order theory of real closed fields" is a precise name for what we referred to above as "elementary algebra and geometry"; see [Kre82].) The formulas of the theory of real closed fields involve elements of $I_r$. A definable set in $E^k$ is a set $S$ such that for some formula $\Psi(x_1, \ldots, x_k)$, $S$ is the set of points in $E^k$ satisfying $\Psi$. $\Psi$ is a defining formula for $S$. (We follow the convention that $\varphi(x_1, \ldots, x_k)$ denotes a formula $\varphi$ in which all occurrences of $x_1, \ldots, x_k$ are free, each $x_i$ may or may not occur in $\varphi$, and no variables
besides \( x_1, \ldots, x_n \) occur free in \( \varphi \).) A definable set is *semi-algebraic* if it has a defining formula which is quantifier-free. It is well-known that there exists a quantifier elimination method for real closed fields ([TAR48]). Hence a subset of \( \mathbb{E}^r \) is semi-algebraic if and only if it is definable.

A decomposition is *algebraic* if each of its regions is a semi-algebraic set. A *cylindrical algebraic decomposition* of \( \mathbb{E}^r \) is a decomposition which is both cylindrical and algebraic.

Let \( X \) be a subset of \( \mathbb{E}^r \), and let \( F \) be an element of \( I_r \). \( F \) is *invariant on \( X \)* (and \( X \) is *\( F \)-invariant*), if one of the following three conditions holds:

1. \( F(\alpha) > 0 \) for all \( \alpha \) in \( X \). ("\( F \) has positive sign on \( X \)).
2. \( F(\alpha) = 0 \) for all \( \alpha \) in \( X \). ("\( F \) has zero sign on \( X \)).
3. \( F(\alpha) < 0 \) for all \( \alpha \) in \( X \). ("\( F \) has negative sign on \( X \)).

Let \( A = \{A_1, \ldots, A_n\} \) be a subset of \( I_r \) ("subset of \( I_r \)" will always mean "finite subset"). \( X \) is *\( A \)-invariant* if each \( A_i \) is invariant on \( X \). A collection of subsets of \( \mathbb{E}^r \) is \( A \)-invariant if each element of the collection is.

This completes the definition of "\( A \)-invariant cylindrical algebraic decomposition". The cad shown in Section 1 is an \( A \)-invariant cad of \( \mathbb{E}^2 \) for \( A = [y^4 - 2y^3 + y^2 - 3x^2y + 2x^4] \). Note that an \( A \)-invariant cad is not unique. Since any subset of an \( A \)-invariant region is \( A \)-invariant, we can always find a way to subdivide one or more regions of an \( A \)-invariant cad to obtain another, "finer", one.

3. The cylindrical algebraic decomposition algorithm: first phase The cad algorithm we present can be divided into three phases. In this and the next two sections we describe each phase in turn. Before taking up the first phase, we give general specifications for a "cad algorithm", and a synopsis of
the particular cad algorithm we will be occupied with in this and the next two sections.

A "cad construction algorithm", or "cad algorithm" for short, has the following specifications. Its input is a set $A \subseteq I_r$, $r \geq 1$. Its output is a description of an $A$-invariant cad $D$ of $E^r$. This description should inform one of the number and arrangement of the cells in the cad, and the sign of each element of $A$ on each cell. As will be seen (Section 4), the cad algorithm we give meets the first of these requirements by producing a list of cell indices of the cells in the cad that the algorithm determines. It meets the second requirement by constructing, for each cell of the cad, an exact description of a particular point (a sample point) belonging to that cell. The sign of any $A_i \in A$ on a particular cell can then be determined by evaluating $A_i$ (exactly) at the sample point for the cell.

Let us turn now to the algorithm we will present in this paper. For $r \geq 2$, its strategy is to construct from the input set $A$, a set $\text{PROJ}(A) \subseteq I_{r-1}$, such that for any $\text{PROJ}(A)$-invariant cad $D'$ of $E^{r-1}$, there is an $A$-invariant cad $D$ of $E^r$ which induces $D'$. ("PROJ" stands for "projection"). The algorithm calls itself recursively on $\text{PROJ}(A)$ to get $D'$, then extends $D'$ to $D$. When $r = 1$, the algorithm constructs an $A$-invariant cad of $E^1$ directly.

Thus for $r \geq 2$, if we were to trace the algorithm from its initiation we would see it compute $\text{PROJ}(A)$, then $\text{PROJ}(\text{PROJ}(A)) = \text{PROJ}^2(A)$, and so on, until $\text{PROJ}^{r-1}(A)$ has been computed. These computations we call the first, or "projection", phase of the algorithm. The construction of a $\text{PROJ}^{r-1}(A)$-invariant cad of $E^1$ we call the second, or "base", phase. The successive extensions of the cad of $E^1$ to a cad of $E^2$, the cad of $E^2$ to a cad
of $E^3$, and so on, until an $A$-invariant cad of $E^r$ is obtained, we call the third, or "extension", phase of the algorithm.

In light of developments of recent years, only the first phase needs extensive description and justification. The second and third phases consist of algorithms which by now are standard and well-documented. Thus this section is much longer than the two that follow, and in fact is the heart of the paper.

Our agenda for this section is to define the map $\text{PROJ}$ from subsets of $I_r$ to subsets of $I_{r-1}$, and to prove that it has the desired property. This property was stated above as: any $\text{PROJ}(A)$-invariant cad of $E^{r-1}$ is induced by some $A$-invariant cad of $E^r$. To establish this, clearly it suffices to show that over any $\text{PROJ}(A)$-invariant region in $E^{r-1}$ there exists an $A$-invariant algebraic stack, and that is what we will do.

For $F \in I_r$, $r \geq 1$, let $V(F)$ denote the real variety of $F$, i.e. the set of all $\langle x_1, \ldots, x_r \rangle \in E^r$ such that $F(x_1, \ldots, x_r) = 0$. Let $R$ be a region in $E^{r-1}$. $F$ is delineable on $R$ if $V(F) \cap Z(R)$ consists of $k$ disjoint sections of $Z(R)$, for some $k \geq 0$. When $F$ is delineable on $R$, it gives rise to a stack over $R$, namely the stack determined by the continuous functions whose graphs make up $V(F) \cap Z(R)$. We write $S(F, R)$ to denote this stack, and speak of the $F$-sections of $Z(R)$. One easily sees that $S(F, R)$ is $F$-invariant. We now show that if $R$ is semi-algebraic, then $S(F, R)$ is an algebraic stack.

**Theorem 3.1.** Let $F \in I_r$, $r \geq 2$, be delineable on a semi-algebraic region $R \subset E^{r-1}$. Then $S(F, R)$ is algebraic.

**Proof.** Let $\varphi$ be a defining formula for $R$. Let the sections of $V(F) \cap Z(R)$ be $s_1 < s_2 < \ldots < s_k$, $k \geq 1$, and let $s_i$ be an $f_i$-section. By our remarks in
Section 2, to show that $S(F,R)$ is algebraic, it suffices to show that each region of $S(F,R)$ is definable. Let $x$ denote the $(r-1)$-tuple $<x_1, \ldots, x_{r-1}>$, and let $y$ stand for $x_r$. Then for $2 \leq j \leq k-1$, we can define $s_j$ as the set of all points $<x,y>$ satisfying a formula which asserts that "$x \in R$ and $y$ is the $j^{th}$ real root of $F(x,y)$". The following is such a formula:

$$
\varphi(x) \land (\exists y_1)(\exists y_2) \cdots (\exists y_{j-1})[ y_1 < y_2 < \cdots < y_{j-1} < y \\
\land F(x,y_1) = 0 \land F(x,y_2) = 0 \land \cdots \land F(x,y_{j-1}) = 0 \land F(x,y) = 0 \\
\land (\forall y_{j+1})\{ (y_{j+1} \neq y_1 \land y_{j+1} \neq y_2 \land \cdots \land y_{j+1} \neq y_{j-1} \land \\
y_{j+1} \neq y \land F(x,y_{j+1}) = 0 \Rightarrow y_{j+1} > y \}].
$$

Defining formulas for $s_1$ and $s_k$ can be obtained by obvious modifications to the above formula. For $1 \leq j \leq k$, let $\varphi_j$ denote the defining formula for $s_j$. For $2 \leq j \leq k$, we can define the $(f_{j-1},f_j)$-sector of $S(F,R)$ as the set of all points $<x,y>$ satisfying a formula which asserts that "$x \in R$ and $y$ is between the $(j-1)^{st}$ and $j^{th}$ real roots of $F(x,y)$". The following is such a formula:

$$
\varphi(x) \land (\exists y_{j-1})(\exists y_j)[ y_{j-1} < y < y_j \land \varphi_{j-1}(x,y_{j-1}) \land \varphi_j(x,y_j) ].
$$

Defining formulas for the $(-\infty,f_1)$-sector and the $(f_k,\infty)$-sector of $S(F,R)$ can be obtained by straightforward modifications to the formula just given.

Thus $S(F,R)$ is algebraic.

Principal subresultant coefficients (psc's), which we now introduce, are a vital and characteristic feature of the cad algorithm we are presenting. As will be seen, they are the chief means by which the geometric idea of induction on dimension is translated into an algorithm. For they are eminently computable, being determinants of certain matrices of polynomials.
Let $J$ be a unique factorization domain. Let $F$ and $G$ be nonzero elements of $J[x]$. If $\deg(F) \geq \deg(G)$, let $F_1 = F$ and $F_2 = G$, else let $F_1 = G$ and $F_2 = F$. Let $F_1, F_2, \ldots, F_k, k \geq 2$, be a polynomial remainder sequence as defined in [BRT71]. Let $n_i = \deg(F_i), 1 \leq i \leq k$. Then $n_1, n_2, \ldots, n_k$ is the degree sequence of $F$ and $G$. Let $n = \min(\deg(F), \deg(G))$. For $0 \leq j < n$, we write $S_j(F,G)$ to denote the $j^{th}$ subresultant of $F$ and $G$ [BRT71]. For $0 \leq j < n$, the $j^{th}$ principal subresultant coefficient of $F$ and $G$, written $\text{psc}_j(F,G)$, is the coefficient of $x^j$ in $S_j(F,G)$. We define $\text{psc}_n(F,G)$ to be $1 \in J$.

The following theorem states the properties of $\text{psc}'s$ that are important for us.

**Theorem 3.2.** Let $F$ and $G$ be nonzero elements of $J[x]$, $J$ a unique factorization domain. Let $n_1, n_2, \ldots, n_k, k \geq 2$, be the degree sequence of $F$ and $G$. Then

1. $n_k = \deg(\gcd(F,G))$, and
2. For any $j$, $0 \leq j \leq n_2$, $\text{psc}_j(F,G) \neq 0$ if and only if $j = n_i$ for some $i$, $2 \leq i \leq k$.

**Proof.** Let $F_1, F_2, \ldots, F_k$ be a polynomial remainder sequence whose first two terms are $F$ and $G$; thus $n_i = \deg(F_i), 2 \leq i \leq k$. As pointed out on p. 506 of [BRT71], $F_k \sim \gcd(F,G)$, where $\sim$ denotes similarity. Hence $n_k = \deg(\gcd(F,G))$. Suppose for some $j$, $0 \leq j \leq n_2$, that $\text{psc}_j(F,G) \neq 0$. If $j = n_2$ we are done, so suppose $j < n_2$. Then by the Fundamental Theorem of polynomial remainder sequences [BRT71], either $j = n_i$ for some $i$, $3 \leq i \leq k$, or $j = n_{m-1} - 1$, for some $m$, $3 \leq m \leq k$. If $j = n_i$ we are done, so suppose $j = n_{m-1} - 1$. Then $n_{m-1} - 1 \geq n_m$. Suppose $n_{m-1} - 1 > n_m$. By the
fundamental theorem of p.r.s., $S_{n_{m-1}}(F,G) \sim S_{n_m}(F,G)$, so

$$\deg(S_{n_{m-1}}(F,G)) = \deg(S_{n_m}(F,G)) = n_m < n_{m-1} - 1 = j.$$ 

Hence $psc_j(F,G) = 0$, a contradiction. So $j = n_{m-1} - 1 = n_m$, and we are done. Suppose conversely that $j = n_i$ for some $i$, $2 \leq i \leq k$. If $i = 2$, then $psc_{n_1}(F,G) = 1 \neq 0$. If $i \geq 3$, then by the fundamental theorem of p.r.s., $S_{n_i}(F,G) \sim F_i$, hence $\deg(S_{n_i}(F,G)) = \deg(F_i) = n_i$, hence $psc_{n_i}(F,G) \neq 0$.

An immediate consequence of this theorem is:

**Corollary 3.3.** Let $F$ and $G$ be as in Theorem 3.2. Then $\deg(gcd(F,G)) = k$ if and only if $k$ is the least $j$ such that $psc_j(F,G) \neq 0$.

We will put Corollary 3.3 to work in the next Lemma, for which we need some definitions. Let $F$ be an element of $I_r$. The derivative of $F$, written $F'$, is the partial derivative of $F$ with respect to $x_r$. We view $I_r$ as $I_{r-1}[x_r]$, and hence by the degree of $F$, written $deg(F')$, mean the degree of $F$ in $x_r$. The zero polynomial has degree $-\infty$. Let $R$ be a region in $E^{r-1}$. For $\alpha \in R$, we write $F_{\alpha}(x_r)$ or $F_{\alpha}$ to denote $F(\alpha,x_r)$.

**Lemma 3.4.** Let $F \in I_r$, $r \geq 2$, and let $R$ be a region in $E^{r-1}$. Suppose that $\deg(F_{\alpha})$ is constant and nonnegative for $\alpha \in R$, and that if it is positive, then the least $k$ such that $psc_k(F_{\alpha}, F'_{\alpha}) \neq 0$ is constant for $\alpha \in R$. Then the number of distinct roots of $F_{\alpha}$ is constant for $\alpha \in R$.

**Proof.** Let $n$ be the constant degree of $F_{\alpha}$ for $\alpha \in R$. If $n = 0$, then $F_{\alpha}$ has no roots for every $\alpha \in R$, so suppose $n \geq 1$. Let $m$ be the nonnegative integer such that for all $\alpha \in R$, $m$ is the least $k$ such that $psc_j(F_{\alpha}, F'_{\alpha})$ is nonzero. Then by Corollary 3.3, $\deg(gcd(F_{\alpha}, F'_{\alpha})) = m$ is constant for $\alpha \in R$. Let $p_{\alpha}$ be the number of distinct roots of $F_{\alpha}$ for $\alpha \in R$. Then by standard algebra,
\( p_a = n - m \), for any \( a \in R \). Hence \( p_a \) is constant for \( a \in R \).

Let \( p(x) \) be a univariate polynomial with complex coefficients. We let \( \text{sep}(p) \) denote the minimum distance in the complex plane between any two distinct roots of \( p(x) \). A complex number is strictly complex if it is non-real.

**Lemma 3.5.** Suppose that \( F \subseteq \mathbb{F}_r, \ r \geq 2 \), that \( R \) is a region in \( \mathbb{F}^{r-1} \), that \( \deg(F_\gamma) \) is constant and nonnegative for \( \gamma \in R \), and that the number of distinct roots of \( F_\gamma \) is constant for \( \gamma \in R \). Let \( \alpha \in R \). Let \( 0 < \varepsilon < \text{sep}(F_\alpha)/2 \), and let \( z_1, \ldots, z_p \) be the distinct roots of \( F_\alpha \). Suppose that \( z_1, \ldots, z_k \) are real and \( z_{k+1}, \ldots, z_p \) are strictly complex. Let \( e_i \geq 1 \) be the multiplicity of \( z_i \) for \( 1 \leq i \leq p \). Let \( C_1, \ldots, C_p \) be disjoint circles of radius \( \varepsilon \) in the complex plane, such that \( C_i \) is centered at \( z_i \). Then there is a neighborhood \( M \) of \( \alpha \) in \( R \) such that for all \( \beta \in M \) and for each \( C_i \), \( F_\beta \) has exactly one root \( u_i \), of multiplicity \( e_i \), in \( C_i \). Furthermore, \( u_i \) is real for \( 1 \leq i \leq k \) and strictly complex for \( k+1 \leq i \leq p \).

**Proof.** By Theorem (1.4) of [MAR66], there is a neighborhood \( M \) in \( R \) of \( \alpha \) such that for all \( \beta \in M \), and for \( 1 \leq i \leq p \), \( F_\beta \) has \( e_i \) roots, multiplicities counted, in \( C_i \). Consider any particular \( \beta \in M \). Since \( F_\beta \) and \( F_\alpha \) each have \( p \) distinct roots, and since the interiors of the \( C_i \)'s are disjoint, for \( 1 \leq i \leq p \), \( F_\beta \) has exactly one root, of multiplicity \( e_i \), in \( C_i \). Consider any \( C_i \) for \( 1 \leq i \leq k \). \( C_i \) is centered on the real axis in the complex plane, hence for every strictly complex point in \( C_i \), its complex conjugate is also in \( C_i \). Also, recall that the complex roots of a polynomial with real coefficients occur in conjugate pairs. Hence since \( C_i \) contains only one root of \( F_\beta \), that root is real. Now consider any \( C_i \) for \( k+1 \leq i \leq p \). Since the strictly complex roots
of $F_a$ occur in conjugate pairs, and since the radius of $C_i$ is less than \( \text{sep}(F_a)/2 \), $C_i$ contains no real points. Hence the root of $F_a$ in $C_i$ is strictly complex. 

**Theorem 3.6.** Let $F \in \mathcal{F}_r$, $r \geq 2$, and let $R$ be a region in $E^{r-1}$. Suppose that $\text{deg}(F_a)$ is constant and nonnegative for $a \in R$, and that if positive, then the least $k$ such that $\text{psc}_k(F_a,F_0) \neq 0$ is constant for $a \in R$. Then $F$ is delineable on $R$.

*Proof.* By Lemmas 3.4 and 3.5, the number of distinct of real roots of $F_a$ is constant for $a \in R$; suppose $F_a$ has $k \geq 0$ real roots for all $a$. For $1 \leq i \leq k$, and for $a \in R$, define $f_i(a)$ to be the $i^{th}$ real root of $F_a$. From Lemmas 3.4 and 3.5 it is easily seen that $f_i$ is continuous for $1 \leq i \leq k$. Hence $F$ is delineable on $R$. 

Let $R$ be a region in $E^r$, $r \geq 1$, and let $a \in R$. An open neighborhood of $a$ in $R$ is $M \cap R$ for some set $M$ which is open in the usual topology on $E^r$, and which contains $a$. Let $T$ be a function defined on $R$. $T$ is locally constant on $R$ if for every $a \in R$, there is an open neighborhood $M$ of $a$ in $R$ such that $T(\beta) = T(a)$ for all $\beta \in M$. From the connectivity of $R$ one easily sees that if $T$ is locally constant on $R$, then $T$ is constant on $R$.

**Theorem 3.7.** Let $A \subseteq \mathcal{F}_r$, $r \geq 2$, and let $R$ be a region in $E^{r-1}$. Suppose that for every $F \in A$, $\text{deg}(F_a)$ is constant and nonnegative for $a \in R$, and that if positive, then the least $k$ such that $\text{psc}_k(F_a,F_0) \neq 0$ is constant for $a \in R$. Suppose also that for every $F,G \in A$, $F \neq G$, the least $k$ such that $\text{psc}_k(F_a,G_0) \neq 0$ is constant for $a \in R$. Then where $H = \prod A$, $H$ is delineable on $R$. 


Proof. By Theorem 3.6, every $F \in A$ is delineable on $R$. Hence $V(H) \cap Z(R)$ is the union of certain sections of $Z(R)$. If every pair of these sections is either disjoint or identical, then $H$ is delineable on $R$. Hence it suffices to show that if an $F$-section and a $G$-section meet, for any $F, G \in A$, $F \neq G$, then they are identical.

To establish this last proposition, it suffices to show that (the truth value of) the predicate "$s_F$ and $s_G$ meet over $\gamma \in R$" is locally constant on $R$. For if it is locally constant on $R$, then it is constant on $R$, which means that if $s_F$ and $s_G$ meet over one point of $R$, then they meet everywhere over $R$, i.e. they are identical. Establishing the following two assertions will show that this predicate is locally constant: (1) for any $\beta \in R$ over which $s_F$ and $s_G$ do not meet, there exists an open neighborhood of $\beta$ in $R$ over which $s_F$ and $s_G$ do not meet (at all); and (2) for any $\alpha \in R$ over which $s_F$ and $s_G$ do meet, there exists an open neighborhood $M$ of $\alpha$ in $R$ over which $s_F$ and $s_G$ do meet (over every point of $M$). (1) is an immediate consequence of the fact that sections are graphs of continuous functions. The remainder of this proof will be devoted to establishing (2).

For any $\gamma \in R$, let $g_{\gamma} = \text{gcd}(F_{\gamma}, G_{\gamma})$. Since the least $k$ such that $\text{gcd}(F_{\gamma}, G_{\gamma}) \neq 0$ is constant for $\gamma \in R$, by Corollary 3.3, $\text{deg}(g_{\gamma})$ is constant for $\gamma \in R$. We now proceed to show that if $s_F$ and $s_G$ meet at $< \alpha, z^* >$, i.e. meet over $\alpha$, then there exists a neighborhood $M$ of $\alpha$ in $R$, such that for any $\beta$ in $M$ over which $s_F$ and $s_G$ do not meet, $\text{deg}(g_{\beta}) \prec \text{deg}(g_{\alpha})$. Since $\text{deg}(g_{\beta}) = \text{deg}(g_{\alpha})$ for all $\beta \in M$, we will have established (2).

Consider any $\alpha \in R$ such that $s_F$ and $s_G$ meet at $< \alpha, z^* >$. Let $K = FG$. For some positive $\varepsilon < \text{sep}(K_a)/2$, consider the circles of radius $\varepsilon$ in the
complex plane centered at the roots of $K_\alpha$. Since the least $k$ such that $\rho_{e_k}(F, F') \neq 0$ is constant for $\gamma \in \mathcal{R}$, Lemmas 3.4 and 3.5 applied to $F$ imply that there is an open neighborhood $\mathcal{M}_F$ of $\alpha$ in $\mathcal{R}$, such that for every circle $C$, if the root of $K_\alpha$ at the center of $C$ is a root of $F_\alpha$ of multiplicity $\varepsilon \geq 1$, then for all $\beta \in \mathcal{M}_F$, $F_\beta$ has exactly one root in $C$, and this root has multiplicity $\varepsilon$. Also, if the root of $K_\alpha$ at the center of $C$ is not a root of $F_\alpha$, but only a root of $G_\alpha$, then $F_\beta$ has no roots in $C$ for all $\beta \in \mathcal{M}_F$, since every root of $F_\beta$ is contained in some other circle. By an identical argument for $G$ in place of $F$, we obtain an open neighborhood $\mathcal{M}_G$ of $\alpha$ in $\mathcal{R}$. Let $\mathcal{H} = \mathcal{M}_F \cap \mathcal{M}_G$. $\mathcal{H}$ is an open neighborhood of $\alpha$ in $\mathcal{R}$.

Let $C_1, \ldots, C_k$ be all the circles such that the root of $K_\alpha$ at the center is a common root of $F_\alpha$ and $G_\alpha$, i.e. a root of $g_\alpha$. Note that $z^*$ is the center of one of the $C_i$'s, call it $C^*$. For $1 \leq i \leq k$, let $\varepsilon_i$ be the minimum of: the multiplicity of the center of $C_i$ as a root of $F_\alpha$, and its multiplicity as a root of $G_\alpha$. By our remarks above, for any $\beta \in \mathcal{M}$ and any $C_i$, $g_\beta$ either has one root of multiplicity $\varepsilon_i$ in $C_i$ or no roots in $C_i$, depending on whether the root of $F_\beta$ in $C_i$ is equal to the root of $G_\beta$ in $C_i$. Also by our remarks above, for all $\beta \in \mathcal{H}$, $C_1, \ldots, C_k$ are the only circles which could possibly contain roots of $g_\beta$.

Recall that the degree of a polynomial in one variable is equal to the sum of the multiplicities of its distinct roots. Hence if there exists $\beta \in \mathcal{M}$ and a $C_i$ such that the root of $F_\beta$ in $C_i$ is not equal to the root of $G_\beta$ in $C_i$, then $\deg(g_\beta)$ is less than $\deg(g_\alpha)$, which is impossible. Hence for all $\beta \in \mathcal{H}$, and for every $C_i$, the root of $F_\beta$ in $C_i$ is equal to the root of $G_\beta$ in $C_i$. This holds in particular for $C^*$, and so $s_F$ and $s_G$ meet (everywhere) over $\mathcal{H}$. This completes the proof of (2). \(\blacksquare\)
Suppose \( F \) is an element of \( I_r, r \geq 2 \), which is delineable on a region \( R \) in \( \mathbb{B}^{r-1} \). Suppose \( s \) is a subset of \( V(F) \), and also a section of \( Z(R) \). Then since \( s \) is contained in a section of \( S(F,R) \), and since it is itself a section of \( Z(R) \), it must belong to \( S(F,R) \). Hence it is a section of \( S(F,R) \). This elementary observation will be useful in the following theorem.

**Theorem 3.8.** Let \( A \subset I_r, r \geq 2 \) and let \( R \) be a region in \( \mathbb{B}^{r-1} \). Suppose that each \( F \in A \) is delineable on \( R \), and that \( H = \bigsqcup A \) is delineable on \( R \). Then \( S(H,R) \) is \( A \)-invariant.

**Proof.** For each \( F \in A \), \( V(F) \subset V(H) \), hence by our observation above, every section of \( S(F,R) \) is a section of \( S(H,R) \). Hence \( S(H,R) \) is a refinement of \( S(F,R) \) for every \( F \in A \), in the sense that each element of \( S(F,R) \) is the union of certain elements of \( S(H,R) \). Hence since each \( S(F,R) \) is \( F \)-invariant, so is \( S(H,R) \). Hence \( S(H,R) \) is \( A \)-invariant. 

With the above theorems, we are now ready to define \( \text{PROJ} \). For any nonzero \( F \in I_r = I_{r-1} \), \( \text{ldcf}(F) \) denotes the leading coefficient of \( F \). The leading term of \( F \), written \( \text{ldt}(F) \), is

\[
\text{ldcf}(F) \cdot x_r^{\text{deg}(F)}.
\]

The reduced of \( F \), written \( \text{red}(F) \), is \( F - \text{ldt}(F) \). If \( F = 0 \), we define \( \text{red}(F) = 0 \). For any \( k \geq 0 \), the \( k \text{-th reduced of } F \), written \( \text{red}^k(F) \), is defined by induction on \( k \):

\[
\text{red}^0(F) = F,
\]

\[
\text{red}^{k+1}(F) = \text{red}(\text{red}^k(F)).
\]

For any \( F \in I_r \), the reduced set of \( F \), written \( \text{RED}(F) \), is
Arnon, Collins, McCallum: Cylindrical algebraic decomposition

\[ \{\text{red}^k(F) \, | \, 0 \leq k \leq \deg(F) \, \& \, \text{red}^k(F) \neq 0\} \]

Let \( F \) and \( G \) be nonzero elements of \( I_r[x] \). Let \( n = \min(\deg(F), \deg(G)) \). The pse set of \( F \) and \( G \), written \( PSC(F, G) \), is

\[ \{pse_j(F, G) \, | \, 0 \leq j \leq n \, \& \, pse_j(F, G) \neq 0\} \]

If either \( F = 0 \) or \( G = 0 \) then \( PSC(F, G) \) is defined to be the empty set. Let

\[ A = \{A_1, \ldots, A_n\}, n \geq 1, \]

be a set of polynomials in \( I_r, r \geq 2 \). The projection of \( A \), written \( PROJ(A) \), is a set of polynomials in \( I_{r-1} \) defined as follows. For each \( 1 \leq i \leq n \), let \( R_i = \text{RED}(A_i) \). Let

\[ PROJ_1(A) = \bigcup_{i=1}^{n} \bigcup_{e_i \in R_i} (\text{ldeg}(G_i) \cup PSC(G_i, G_i')) \]

\[ PROJ_2(A) = \bigcup_{i \neq j} \bigcup_{e_i \in R_i \, \& \, e_j \in R_j} PSC(G_i, G_j) \]

Then \( PROJ(A) \) is the union of \( PROJ_1(A) \) and \( PROJ_2(A) \).

The following simple observation is needed for the theorem which follows. Suppose \( F \) and \( G \) are nonzero elements of \( I_r \), and suppose that for some \( \alpha \in E^{r-1} \), \( \deg(F) = \deg(F_\alpha) \geq 0 \), and \( \deg(G) = \deg(G_\alpha) \geq 0 \). Let

\[ n = \min(\deg(F), \deg(G)) \]

Then for every \( j, 0 \leq j \leq n \), it is the case that

\[ (pse_j(F, G))_\alpha = pse_j(F_\alpha, G_\alpha) \]

We see this as follows. For \( j < n \), since \( \deg(F) = \deg(F_\alpha) \) and \( \deg(G) = \deg(G_\alpha) \), the matrix obtained by evaluating the entries of the Sylvester matrix of \( F \) and \( G \) at \( \alpha \) is just the Sylvester matrix of \( F_\alpha \) and \( G_\alpha \), hence if \( j < n \) then \( (S_j(F, G))_\alpha \) is equal to \( S_j(F_\alpha, G_\alpha) \), and so \( (pse_j(F, G))_\alpha = pse_j(F_\alpha, G_\alpha) \). If \( j = n \), then \( (pse_j(F, G))_\alpha = pse_j(F_\alpha, G_\alpha) = 1 \).

For \( F \in I_r \) and \( X \subset E^{r-1} \), \( F \) is identically zero on \( X \) if \( F_\alpha = 0 \) for all \( \alpha \in X \).

Let \( A \) be a subset of \( I_r, r \geq 2 \), and let \( X \subset E^{r-1} \). The nonzero product of \( A \) on
written \(A_X\), is the product of all the elements of \(A\) which are not identically zero on \(X\). If there are no such elements, then \(A_X\) is the constant polynomial \(1\in I_r\).

**Theorem 3.9.** For \(A \subset I_r\), \(r \geq 2\), if \(R\) is a \(\text{PROJ}(A)\)-invariant region in \(E^{r-1}\), every element of \(A\) is either delineable or identically zero on \(R\), and \(A_R\) is delineable on \(R\).

**Proof.** Consider any \(F \in A\). If \(F = 0\), then \(F\) is identically zero on \(R\). Suppose \(F \neq 0\). By definition, \(\text{PROJ}(A)\) includes every nonzero coefficient of \(F\), so each coefficient of \(F\) either vanishes everywhere or nowhere on \(R\). Hence \(\deg(F_a)\) is constant for \(\alpha \in R\). For any \(K \in I_r\) for which \(\deg(K_a)\) is constant for \(\alpha \in R\), let \(\deg_R(K)\) denote this constant value. If \(\deg_R(F) = -\infty\), then \(F\) is identically zero on \(R\). If \(\deg_R(F) = 0\), then obviously \(F\) is delineable on \(R\). Suppose \(\deg_R(F) \geq 1\). Then there is a unique reductum \(Q\) of \(A\) such that \(\deg(Q) = \deg_R(Q) = \deg_R(F)\). Then \(F_a = Q_a\) for all \(\alpha \in R\), hence if \(Q\) is delineable on \(R\), then \(F\) is delineable on \(R\). Since \(\text{PSC}(Q, Q') \subset \text{PROJ}(A)\), the least \(k\) such that \((\text{PSC}_t(Q, Q'))_{t \in \alpha} \neq 0\) is constant for \(\alpha \in R\). Hence by our observation above, the least \(k\) such that \(\text{PSC}_k(Q_a, Q_a') \neq 0\) is constant for \(\alpha \in R\). Hence by Theorem 3.6, \(Q\) is delineable on \(R\), hence \(F\) is delineable on \(R\). Thus every element of \(A\) is either identically zero or delineable on \(R\).

Let \(B\) be the set of elements of \(A\) which are delineable on \(R\). Now by an argument similar to the above, using Theorem 3.7 applied to \(B\) in place of Theorem 3.6 applied to \(A\), it follows that \(\bigcap B\) is delineable on \(R\). But \(\bigcap B = A_R\), hence \(A_R\) is delineable on \(R\).
We complete our agenda for this section with the following

**Corollary 3.10.** For \( A \subseteq l_r, r \geq 2 \), if \( R \) is a \( \text{PROJ}(A) \)-invariant region in \( E^{r-1} \), then there exists an algebraic, \( A \)-invariant stack over \( R \).

**Proof.** From Theorems 3.9, 3.8, and 3.1, three assertions follow: (1) every element of \( A \) is either definable or identically zero on \( R \), (2) \( A_K \) is definable on \( R \), and (3) \( S(A_K, R) \) is an algebraic stack over \( R \), which is \( F \)-invariant for every \( F \in A \) which is definable on \( R \). Since obviously \( S(A_K, R) \) is \( F \)-invariant for any \( F \in A \) which is identically zero on \( R \), \( S(A_K, R) \) is \( A \)-invariant.


Recall that the input to the CAD algorithm is a set \( A \subseteq l_r \). In the first phase of the algorithm we computed \( \text{PROJ}(A) \), \( \text{PROJ}^2(A) \), and finally \( \text{PROJ}^{r-1}(A) \subseteq l_1 \). Let \( K = \text{PROJ}^{r-1}(A) \). It is the task of the second phase to construct a \( K \)-invariant CAD \( D^* \) of \( E^1 \), that is, to construct cell indices and sample points for the cells of such a CAD. Let us now define cell indices.

Consider first a CAD of \( E^1 \). We define the index of the leftmost 1-cell, i.e., that 1-cell which viewed as an open interval in the \( x \)-axis has a left endpoint of \( -\infty \), to be \((1) \). The index of the 0-cell (if any) immediately to its right is defined to be \((2) \), the index of the 1-cell to the right of that 0-cell (if any) is defined to be \((3) \), etc. Now suppose that cell indices have been defined for CAD's of \( E^{r-1}, r \geq 2 \), and consider a CAD \( D \) of \( E^r \). \( D \) induces a CAD \( D' \) of \( E^{r-1} \).

Any cell \( d \) of \( D \) is an element of a stack \( S(c) \) over a cell \( c \) of \( D' \). Let \( (i_1, \ldots, i_{r-1}) \) be the index of \( c \). The cells of \( S(c) \) may be numbered from bottom to top, with the bottommost sector being called cell 1, the second above 1 (if any) cell 2, the sector above that (if any) cell 3, etc. If \( d \) is the \( j \)-th cell of the stack by this numbering, then its cell index is defined to be
It is interesting to note that the sum of the parities of the components of a cell index is equal to the dimension of the cell (where even parity = 0 and odd parity = 1). In a cad of $E^2$, for example, a cell with index $(2,4)$ is a 0-cell, $(2,5)$ is a 1-cell, $(3,2)$ is a 1-cell, and $(1,5)$ is a 2-cell.

We begin cad construction in $E^1$ by constructing the set of all distinct (i.e., relatively prime) irreducible factors of the various elements of $K$ (see [KAL82] for information on polynomial factorization algorithms). Let $M = [M_1, \ldots, M_k] \subset I_1$ be the set of these factors. The real roots $\alpha_1 < \cdots < \alpha_n, n \geq 0,$ of $\prod M$ will be the 0-cells of $D^*$ (if $n = 0$ then $D^*$ consists of the single 1-cell $E^1$). We determine the $\alpha_j$'s by isolating the real roots of each $M_i$. Algorithms for this task are described in [CL082]. Note that by their relative primeness, no two elements of $M$ have a common root. Hence by refining the isolating intervals for the $\alpha_j$'s we obtain a collection of disjoint left-open and right-closed intervals $(\tau_1, s_1], (\tau_2, s_2], \ldots, (\tau_n, s_n]$ with rational endpoints, each containing exactly one $\alpha_j$, and with $\tau_1 < s_1 \leq \tau_2 < \cdots$

As soon as we know $n$, we can write down the indices of the $2n+1$ cells of $D^*$. Thus constructing cell indices in $E^1$ is straightforward. In the third phase of the cad algorithm there will be root isolation steps following which it will similarly be straightforward to write down the indices for the cells in certain stacks that will be part of cad's of $E^i, i \geq 2$. Thus we will not discuss cell index determination further in detail, but simply assume that it can be done.
We now construct sample points for the cells of $D^*$. For the 1-cells of $D^*$ we can use appropriately chosen endpoints from the isolating intervals above, giving us a rational sample point for each 1-cell (if $D^* = \{ E^1 \}$, we arbitrarily pick some rational element of $E$). Obviously the only point in a 0-cell is the cell itself. Its value may be an irrational algebraic number. The use to be made of sample points in the third phase of the cad algorithm leads us to adopt a particular representation for them that we now describe.

This representation is applicable to algebraic points in any $E^i$, that is, points each of whose coordinates is a real algebraic number. Loos ([LOOS2a], Section 1) describes the representation for a real algebraic number $\gamma$ by its minimal polynomial $M(x)$ and an isolating interval for a particular root of $M(x)$. With $\gamma$ so represented, and setting $m$ to be the degree of $M(x)$, one can represent an element of $Q(\gamma)$ as an element of $Q[x]$ of degree $\leq m - 1$ (as Loos describes). For any algebraic point, there exists a real algebraic $\gamma$ such that each coordinate of the point is in $Q(\gamma)$; $\gamma$ is a primitive element for the point. Our representation for an algebraic point in $E^i$ is: a primitive element $\gamma$ and an $i$-tuple of elements of $Q(\gamma)$, all represented as described by Loos. It is straightforward to express our above-specified sample points for $D^*$ in this representation, and we henceforth assume that this has been done.

5. The cylindrical algebraic decomposition algorithm: third phase. Let us begin by examining the extension of the cad $D^*$ of $E^1$ to a cad of $E^2$. In phase one, we computed a set $J = PROJ^{r-2}(A) \subset I_2$, where $A \subset I_r$ is the set of input polynomials. Consider any cell $c$ of $D^*$. $J_c$ is delineable on $c$. $S(J_c,c)$ is a $J$-invariant stack over $c$ which is a subset of the cad of $E^2$ that
we want. Let $\alpha$ be the sample point for $c$. Clearly $J_c$ is the product of all elements $G$ of $J$ for which $G(\alpha,x_2) \neq 0$. Using the algorithms for arithmetic in $\mathbb{Q}(\alpha)$ described in [L0082a], we construct $J_c$. As described in Section 2 of [L0082a], we can isolate the real roots of $J_c(\alpha,x_2) \in \mathbb{Q}(\alpha)[x_2]$, and thereby determine the number of sections in $S(J_c,c)$. If $\beta$ is a root of $J_c(\alpha,x_2)$, then $<\alpha,\beta>$ is a sample point for a section of $S(J_c,c)$. Using the representation for $\alpha$, the isolating interval for $\beta$, and the algorithms NORMAL and SIMPLE of [L0082a], we construct a primitive element $\gamma$ for $\mathbb{Q}(\alpha,\beta)$, and use it to construct the representation we require for $<\alpha,\beta>$. Sector sample points for $S(J_c,c)$ can be obtained from $\alpha$ and the (rational) endpoints of the isolating intervals for the roots of $J_c(\alpha,x_2)$, much as was done above for $E^1$. Thus sector sample points are of the form $<\alpha,\tau>$, $\tau$ rational, so we can take $\gamma = \alpha$.

After processing each cell $c$ of $E^*$ in this fashion, we have determined a cad of $E^2$ and constructed a sample point for each cell.

Extension from $E^{i-1}$ to $E^i$ for $3 \leq i \leq r$ is essentially the same as extending $E^1$ to $E^2$. A sample point in $E^{i-1}$ has $i-1$ coordinates, as contrasted with the single coordinate of a point in $E^1$. Where $\alpha$ is the primitive element of a sample point in $E^{i-1}$ and $F = F(x_1, \ldots, x_i)$ is an element of $k_i$, we use arithmetic in $\mathbb{Q}(\alpha)$ to explicitly determine the univariate polynomial over $\mathbb{Q}(\alpha)$ that results from substituting the coordinates $<x_1, \ldots, x_{i-1}>$ for $<x_1, \ldots, x_{i-1}>$ in $F$.

The following abstract algorithm summarizes our discussion of the cad algorithm.

```
CAD(A,E-A,E)
[Cylindrical algebraic decomposition. A is a list of $n \geq 0$ integral polynomials
```
in \( r \) variables, \( r \geq 1 \). \( I \) is a list of the indices of the cells comprising an \( A \)-invariant cad \( D \) of \( E^r \). \( S \) is a list of sample points for \( D \), such that the \( i^{th} \) element of \( S \) is a sample point for the cell whose index is the \( i^{th} \) element of \( I \).]

1. \([r = 1.]\) If \( r > 1 \) then go to 2. Set \( I \leftarrow \) the empty list. Set \( S \leftarrow \) the empty list. Set \( H(x) \leftarrow \) the product of the nonzero elements of \( A \). Isolate the real roots of \( H(x) \) to determine the 0-cells of \( D \). Construct the indices of the cells of \( D \) and add them to \( I \). Construct sample points for the cells of \( D \) and add them to \( S \). Exit.

2. \([r > 1.]\) Set \( P \leftarrow PROJ(A) \). Call CAD recursively with inputs \( r-1 \) and \( P \) to obtain outputs \( I' \) and \( S' \) that specify a cad \( D' \) of \( E^{r-1} \). Set \( I \leftarrow \) the empty list. Set \( S \leftarrow \) the empty list. For each cell \( c \) of \( D' \), let \( i \) denote the index of \( c \), let \( \alpha \) denote the sample point for \( c \), and carry out the following four steps: first, set \( h(x_r) \leftarrow \prod [A_i(\alpha,x_r)]_{A_i \in A \& A_i(\alpha,x_r) \neq 0} \), second, isolate the real roots of \( h(x_r) \), third, use \( i \), \( \alpha \), and the isolating intervals for the roots of \( h \) to construct cell indices and sample points for the sections and sectors of \( S(c) \), fourth, add the new indices to \( I \) and the new sample points to \( S \). Exit.

C. An example. We now show what algorithm CAD does for a particular example in \( E^2 \). Let

\[
A_1(x,y) = 144y^2 + 60xy + 9x^2 + 105x^2 + 70x - 90,
\]

\[
A_2(x,y) = 2y^2 + 6xy + x^3 + 8x,
\]

and \( A = [A_1, A_2] \). When CAD is called with input \( A \), its first action will be to compute \( PROJ(A) \). Following the definition in Section 3, we get
By techniques described in [COL75] and [ARN81], it can be determined that if we retain only $p_1(x) = x^4 - 15x^2 - 10x + 14$, $p_2(x) = x$, and $p_3(x) = 81x^8 + 3330x^6 + 1260x^3 - 37395x^4 - 45780x^3 - 32098x^2 + 167720x + 1435204$, then
32096x^2 + 167720x + 143520\frac{x}{x}, in \text{PROJ}(A), this smaller \text{PROJ}(A) will still suffice for the construction of an \text{A-invariant cad} of \text{E}^2. It turns out that \text{p}_0(x) has no real roots, and so has no effect on the cad. Hence let us set PROJ(A) = \{p_1(x), p_2(x)\}.

\text{p}_1 and \text{p}_2 are both irreducible, so we have \text{M}_1 = \text{p}_1 and \text{M}_2 = \text{p}_2 in the notation of Section 5. \text{M}_1 has four real roots with approximate values -3.26, -1.51, 0.7, and 4.08; \text{M}_2 has the unique root \text{z} = 0. The following collection of isolating intervals for these roots satisfies the conditions set out in Section 5:

\((-4.3], (-2,-1], (-1.0], (-\frac{1}{2},1], (4,6].\)

Since there are five 0-cells, the cell indices for the cad are (1), (2), ..., (11).

We now construct representations for the sample points of the induced cad of \text{E}^1. Each 1-cell will have a rational sample point, hence any rational \text{y} will be a primitive element. We arbitrarily choose \text{y} = 0. \((-1,0]\) is an isolating interval for \text{y} as a root of its minimal polynomial. We may take the 1-cell sample points to be -4, -2, -1, \frac{1}{2}, 4, and 9.

The four irrational 0-cells have as their primitive elements the four roots of \text{M}_1(x). The representation for the leftmost 0-cell, for example, consists of \text{M}_1(x), the isolating interval \((-4.3], and the 1-tuple \langle x \rangle, where \text{x} corresponds to the element \text{y} of \text{Q}(\text{y}). The 0-cell \text{z} = 0 is represented in the same fashion as the rational 1-cell sample points.

We now come to the extension phase of the algorithm. Let \text{c} be the leftmost 1-cell of the cad \text{D}' of \text{E}^1. \text{A}_1(\text{-4,y})\neq 0 and \text{A}_2(\text{-4,y})\neq 0, hence \text{A}_c = \text{A}_1\text{A}_2. We have
\[ A_c(-4,y) = 24(y^2 + 6y + 25)(24y^2 + 256y + 601). \]

\[ y^2 + 6y + 24 \] has no real roots, but \( 24y^2 + 256y + 601 \) has two real roots, which can be isolated by the intervals \((-8,-7]\) and \((-4,-2]\). Thus the stack \( S(c) \) has two sections and three sectors; the indices for these cells are \((1,1), (1,2), \ldots, (1,5)\). From the endpoints of the isolating intervals we obtain sector sample points of \(<-4,-8>\), \(<-4,-4>\), and \(<-4,-1>\) (which will be represented in the customary fashion). The two roots \( \gamma_1 \) and \( \gamma_2 \) of \( 24y^2 + 256y + 601 \) are both \( y \)-coordinates for the section sample points and primitive elements for these sample points. Thus the (representations for the) section sample points are

\[ \{24y^2 + 256y + 601, (-8,-7], <-4,y]\} \]

and

\[ \{24y^2 + 256y + 601, (-4,-2], <-4,y]\}. \]

Now let \( c \) be the leftmost 0-cell of \( D' \); let \( \alpha \) also denote this point. \( A_1(\alpha,y) \neq 0 \) and \( A_2(\alpha,y) \neq 0 \), so again \( A_c = A_1A_2 \). We find that, up to constant factor,

\[ A_c(\alpha,y) = (y^2 + 6y + \alpha^2 + 9)(y + \frac{1}{3}\alpha^2)^2. \]

\[ y^2 + 6y + \alpha^2 + 9 \in Q(\alpha)[y] \] has no real roots, but obviously \( y + \frac{1}{3}\alpha^2 \) has exactly one; \((-8,8)\) is an isolating interval for it. Hence \( S(c) \) has one section and two sectors; the indices of these cells are \((2,1), (2,2), \) and \((2,3)\). The appropriate representations for \(<-\alpha,-8>\) and \(<-\alpha,9>\) are the sector sample points. Since \( y + \frac{1}{3}\alpha^2 \) is linear in \( y \), its root is an element of \( Q(\alpha) \). Hence
\{U_1(x), (-\infty,2], \langle x, -\frac{1}{3}x^2 > \}

is the representation of the section sample point.

Thus in this particular case it was not necessary to apply the NORMAL and SIMPLE algorithms of [LC062a] to find primitive elements for the sections of \(S(x)\), and it is also not necessary for the other sample points of this example. In general, however, for a 0-cell \(\alpha\), \(A_e(\alpha,y)\) will have nonlinear factors with real roots, and it will be necessary to apply NORMAL and SIMPLE. Saying this another way, where \(\alpha\) is a 0-cell of \(D'\) and \(\langle \alpha,\beta \rangle\) is a section sample point of \(D\), we had in our example above \(Q(\alpha,\beta) = Q(\alpha)\), but in general, \(Q(\alpha)\) will be a proper subfield of \(Q(\alpha,\beta)\).

The steps we have gone through above for a 1-cell and a 0-cell are carried out for the remaining cells of \(D'\) to complete the determination of the \(A\)-invariant cad \(D\) of \(E^2\).

Although information of the sort we have described is all that would actually be produced by CAD, it may be useful to show a picture of the decomposition of the plane to which the information corresponds. The curve defined by \(A_1(x,y) = 0\) has three connected components which are easily identified in Figure 3 below. The curve defined by \(A_2(x,y) = 0\) is just the \(y\)-axis, i.e. the same curve as defined by \(x = 0\). The \(A\)-invariant cad of \(E^2\) which CAD determines is shown in Figure 3. We remark that the curve \(A_1(x,y)\) is from ([HIL32], p. 329).

7. References

Figure 3


