Cylindrical Algebraic Decomposition - an Introduction

Mats Jirstrand
Department of Electrical Engineering
Linköping University
S-581 83 Linköping
Sweden

email: matsj@isy.liu.se

1995-10-18

REGLERTEKNIK

AUTOMATIC CONTROL

LINKÖPING

Technical reports from the Automatic Control group in Linköping are available as UNIX-compressed Postscript files by anonymous ftp at the address 130.236.20.24 (ftp.control.ee.liu.se).

Cylindrical Algebraic Decomposition - an Introduction

Mats Jirstrand
Department of Electrical Engineering
Linköping University, S-581 83 Linköping, Sweden
email: matsj@isy.liu.se

1995-10-18

Abstract. In this report we give an introduction to a constructive way of treating systems of polynomial equations and inequalities. We present a method called cylindrical algebraic decomposition (CAD) discovered 1973 by Collins. The method constructs a decomposition of $\mathbb{R}^n$ such that a given set of polynomials have constant sign on each component. All concepts needed to understand the algorithm is presented, e.g., polynomial remainder sequences, subresultants, principal subresultant coefficients, Sturm chains and algebraic number representations.

Keywords: cad, inequalities, real polynomial systems, semi-algebraic sets, real algebra

1 Introduction

The aim of this report is to describe a constructive method in real algebraic geometry to obtain a so called *Cylindrical Algebraic Decomposition*, (CAD) of $\mathbb{R}^n$. A CAD is a decomposition of the n-dimensional real space into regions over which a given set of polynomials have constant sign. Given such a decomposition it is easy to give a solution of a system of inequalities and equations defined by the polynomials, so called real polynomial systems.

The CAD-algorithm was discovered by Collins in 1973 [6] as a sub-algorithm in his work on an effective method for quantifier elimination (QE) in real closed fields. The first algorithm for the solution of this problem was given by Tarski 1948 [18] but was completely impractical. The sub-algorithms of CAD has been improved over the years see e.g., [16, 14, 11] and it is now possible to run nontrivial examples on a computer with realistic runtimes. For an extensive bibliography on QE and CAD see [1].

The report is organized as follows: section 2 presents an introductory example of the use of CAD. In Section 3 and 4 we present the machinery needed to understand the CAD algorithm. Section 5 is a presentation of the algorithm. In Section 6 we consider some examples and finally in Section 7 we give a summary of the report.

2 An Introductory Example

To get a feeling of what kind of problems CAD may solve we present an introductory example.

Example 2.1 Suppose we are given the following real polynomial system:

$$\begin{aligned} x_1^2 + x_2^2 - 1 &< 0 \\ x_1^3 - x_2^2 &= 0 \end{aligned} \tag{1}$$

For system (1) the set of solutions is very easy to find. It consists of the part of the cuspidal cubic inside the unit circle, see Figure 1.

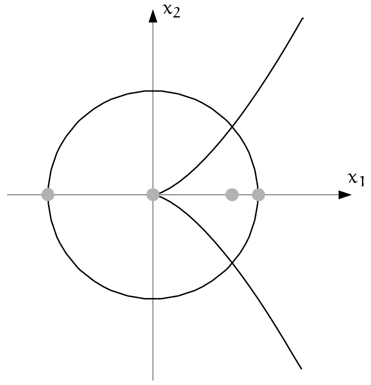

Figure 1: The zero sets of the polynomials in system (1) and some projections onto the x_1-axis (gray dots).

In this case it was easy to solve the system by inspection but is there a systematic approach which can be used for more complicated problems? The answer is yes and we will now give an outline of a procedure for finding the solution of system (1). Let $f_1 = x_1^2 + x_2^2 - 1$ and $f_2 = x_1^3 - x_2^2$. The procedure can be divided into three steps:

(i) Find the projections onto the x_1-axis of all points of the zero sets of f_1 and f_2 corresponding to vertical tangents, singularities and intersections (gray dots). The projections of these points of system (1) is

$$-1,\ 0,\ \alpha,\ 1,$$

where $\alpha \approx 0.7549$ is the real zero of $x^3 + x^2 - 1$. The projected points induce a decomposition of the x_1-axis into 9 components (4 points and 5 open intervals).

(ii) Evaluate f_1 and f_2 over a "sample point" of each component (dot or interval). This gives $2 \cdot 9$ polynomials in x_2.

(iii) Evaluate the signs of the obtained polynomials, i.e., evaluate the signs of f_1 and f_2 on a vertical line over each "sample point".

Notice that a vertical line over each component intersects the zero sets of f_1 and f_2 a constant number of times, since the points of the x_1-axis over which the zero sets change "character" is exactly the points picked out by the projection. Enumerating the components of the decomposition from left to right Table 1 summarizes the number of intersections over each component.

Component	1	2	3	4	5	6	7	8	9
# of intersections	0	1	2	3	4	2	4	3	2

Table 1: Number of intersections with $\left\{ (x_1, x_2) \in \mathbb{R}^2 \mid f_1 = 0 \text{ and } f_2 = 0 \right\}$.

To illustrate step (ii) and (iii) we just consider "sample points" of component 2 and 5, $\alpha_2 = -1$ (which is the only choice for this particular component) and $\alpha_5 = \frac{1}{2}$. The evaluation of f_1 and f_2 is summarized in Table 2.

x_1	$f_1(x_1,x_2)$	$f_2(x_1,x_2)$	# real roots of $f_1,\ f_2$	$\begin{bmatrix} \text{sign}(f_1) \\ \text{sign}(f_2) \end{bmatrix},\ x_2 : -\infty \to +\infty$
α_2	x_2^2	$-1 - x_2^2$	$2,\ 0$	$\left[\begin{array}{c\|c\|c} + & 0 & + \\ - & - & - \end{array}\right]$
α_5	$x_2^2 - \frac{3}{4}$	$\frac{1}{8} - x_2^2$	$2,\ 2$	$\left[\begin{array}{c\|c\|c\|c\|c\|c\|c\|c\|c} + & 0 & - & - & - & - & - & 0 & + \\ - & - & - & 0 & + & 0 & - & - & - \end{array}\right]$

Table 2: Evaluation of f_1 and f_2 over α_2 and α_5.

Since $f_1 < 0$ and $f_2 = 0$ for a solution of system (1) Table 2 shows that there are two sets of solutions of (1) over component 5, i.e., over the interval

$0 < x_1 < \alpha$ which consists of parts of the zero set of f_2. We also see that there are no solutions over component 2.

The whole solution of system (1) is given by

$$\begin{aligned} x_1^3 - x_2^2 &= 0 \\ 0 \le x_1 &< \alpha, \end{aligned} \tag{2}$$

where α is the real zero of $x^3 + x^2 - 1$.

In Figure 2 $(\mathrm{sign}(f_1(x_1, x_2)), \mathrm{sign}(f_2(x_1, x_2))$ along the lines $x_1 = -1$ and $x_1 = \frac{1}{2}$ is displayed.

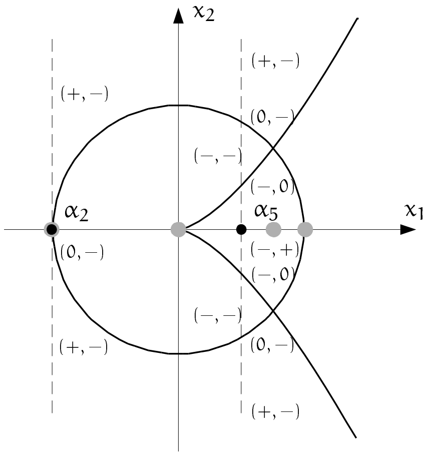

Figure 2: A part of the construction of the solution.

□

In this example it was easy to find the projections and evaluate the polynomials over different sample points. However, the general projection operation is more intricate and for the evaluation step one usually need to do calculations with algebraic numbers. In the rest of this report we will treat these problems in detail.

3 A Semi-Algebraic Dictionary

In this section we will introduce the reader to some of the basic concepts of the CAD-machinery and their geometrical interpretation. The definitions essentially follows [2]. A very detailed description of CAD is given in [17] and some briefer presentations may be found in [9, 10].

Since one of the aims of this report is to understand algorithmic ways of treating systems of equations and inequalities, important objects to study is so called *semi-algebraic* sets.

Definition 3.1 A set is *semi-algebraic* if it can be constructed by finitely many applications of union, intersection and complementation operations on sets of the form

$$\{ x \in \mathbb{R}^n \mid f(x) \geq 0 \},$$

where $f \in \mathbb{R}[x_1, \ldots, x_n]$. □

An interesting property of semi-algebraic sets is that they are closed under projection, i.e., the projection of a semi-algebraic set to some lower dimensional space is again a semi-algebraic set. This is not true for algebraic sets, i.e., sets defined by a system of polynomial equations (consider the unit circle). We also observe that the set of points which satisfies a system of equalities and inequalities is a semi-algebraic set.

Example 3.1 An example of a semi-algebraic set $\mathcal{S} \in \mathbb{R}^2$,

$$\begin{aligned} \mathcal{S} = \Big\{ x \in \mathbb{R}^2 \mid & \left(x_1^2 + x_2^2 - 1 \leq 0 \ \wedge \ x_1^2 - x_2 = 0 \right) \ \bigvee \\ & \left((x_1-1)^2 + (x_2-1)^2 - 1 \leq 0 \ \wedge \ (x_1-2)^2 + (x_2-2)^2 - 1 \leq 0 \right) \Big\}. \end{aligned}$$

The projection of the set onto the x_1-axis

$$\mathcal{S}_{x_1} = \left\{ x \in \mathbb{R}^2 \mid x_1^2 + x_1^4 - 1 \leq 0 \ \vee \ 1 \leq x_1 \leq 2 \right\},$$

is again a semi-algebraic set, see Figure 3. □

We now introduce some terminology for describing how algebraic curves and surfaces partition $\mathbb{R}^n$.

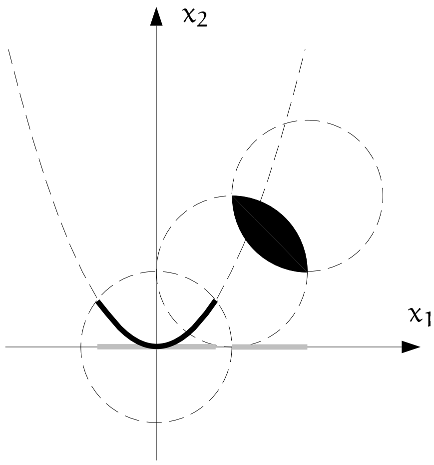

Figure 3: A semi-algebraic set (black region) and its projection onto the x_1-axis (gray region). The dashed sets are the zero sets of the defining polynomials.

Definition 3.2

- A *region*, R is a connected subset of $\mathbb{R}^n$.
- The set $Z(R) = R \times \mathbb{R} = \{(\alpha, x) \mid \alpha \in R,\ x \in \mathbb{R}\}$ is called a *cylinder* over R.
- Let f, f_1, f_2 be continuous, real-valued functions on R.
  A f-*section* of $Z(R)$ is the set

  $$\{(\alpha, f(\alpha)) \mid \alpha \in R\}$$

  and a (f_1, f_2)-*sector* of $Z(R)$ is the set

  $$\{(\alpha, \beta) \mid \alpha \in R,\ f_1(\alpha) < \beta < f_2(\alpha)\}.$$

$\square$

Notice that an algebraic equation implicitly defines a set of real-valued, piecewise continuous functions. The real roots of an polynomial equation in one variable are piecewise continuous functions of its coefficients.

Definition 3.3 Let $X \subseteq \mathbb{R}^n$. A *decomposition* of X is a finite collection of disjoint regions (components) whose union is X:

$$X = \bigcup_{i=1}^{k} X_i, \quad X_i \cap X_j = \emptyset, \quad i \neq j$$

□

Definition 3.4 A *stack* over R is a decomposition which consists of f_i-sections and (f_i, f_{i+1})-sectors, where $f_0 < \ldots < f_{k+1}$ for all $x \in R$ and $f_0 = -\infty$, $f_{k+1} = +\infty$. □

Observe the strict inequalities in Definition 3.4. Geometrically this means that the graphs of different functions may not intersect each other over R.

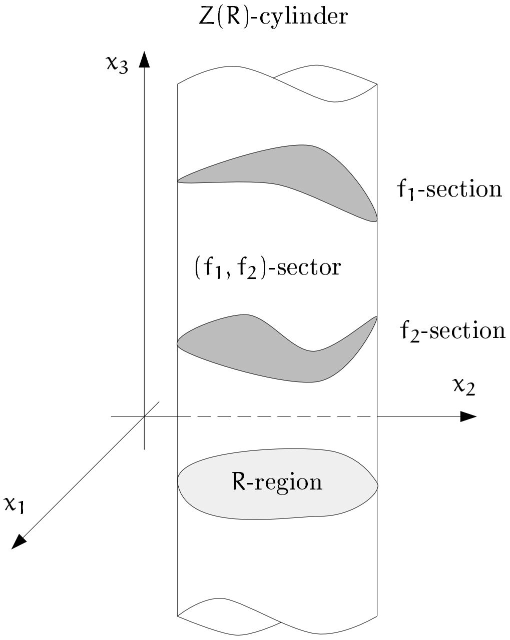

Figure 4: A geometrical interpretation of the definitions of region, cylinder, sections, sectors and stack.

Definition 3.5 A decomposition $\mathcal{D}$ of $\mathbb{R}^n$ is *cylindrical* if

$n = 1$ $\mathcal{D}$ is a partition of $\mathbb{R}^1$ into a finite set of numbers, and the finite and infinite open intervals bounded by these numbers.

$n > 1$ $\mathcal{D}' = F_1 \cup \ldots \cup F_m$ is a cylindrical decomposition of $\mathbb{R}^{n-1}$ and over each F_i there is a stack which is a subset of $\mathcal{D}$.

□

From the definition of a cylindrical decomposition it is clear that any cylindrical decomposition of $\mathbb{R}^n$ induces a cylindrical decomposition of $\mathbb{R}^{n-1}$ etc. down to $\mathbb{R}^1$.

Definition 3.6 Let $X \subseteq \mathbb{R}^n$ and $f \in k[x_1, \ldots, x_n]$. Then f is *invariant* on X if one of the following conditions holds:

$$
\begin{array}{lll}
\text{(i)} & \forall x \in X & : \; f(x) > 0 \\
\text{(ii)} & \forall x \in X & : \; f(x) = 0 \\
\text{(iii)} & \forall x \in X & : \; f(x) < 0
\end{array}
$$

The set $\mathcal{F} = \{f_1, \ldots, f_r\} \in \mathbb{R}[x_1, \ldots, x_n]$ of polynomials is *invariant* on X if each f_i is invariant on X. We also say that X is $\mathcal{F}$-invariant if $\mathcal{F}$ is invariant on X. □

Example 3.2 Let $\mathcal{F} = \{x_1^2 + x_2^2 - 1,\; (x_1 - 1)^2 - x_2^2 - 1\}$. Then the set $\mathcal{I}$ is $\mathcal{F}$-invariant, see Figure 5.

□

Definition 3.7 A decomposition is *algebraic* if each of its components is a semi-algebraic set. □

Example 3.3 Let $f(x) = (x_1 - 2)^2 + (x_2 - 2)^2 - 1$. Then

$$\{\, x \mid f(x) > 0 \,\} \cup \{\, x \mid f(x) = 0 \,\} \cup \{\, x \mid f(x) < 0 \,\}$$

is an algebraic decomposition of $\mathbb{R}^2$. □

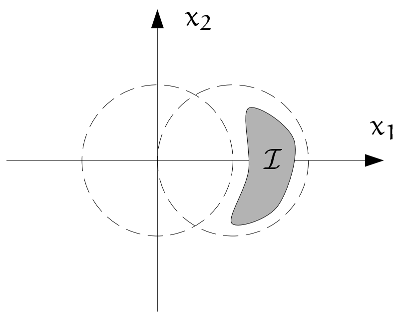

Figure 5: The zero set of $\mathcal{F}$ in Example 3.2 (dashed lines) and the $\mathcal{F}$-invariant set $\mathcal{I}$.

Notice that when the decomposition is defined by a set of polynomials it is algebraic since all boundaries are zero sets of the defining polynomials.

Definition 3.8 A *Cylindrical Algebraic Decomposition* (*CAD*) of $\mathbb{R}^n$ is a decomposition which is both cylindrical and algebraic. The components of a CAD is called *cells*. □

Example 3.4 Let $\mathcal{F} = \{(x_1-2)^2+(x_2-2)^2-1,\ (x_1-3)^2+(x_2-2)^2-1\}$. The CAD consists of the distinct black "dots", "arcs" and "patches of white space" in Figure 6. The induced CAD of $\mathbb{R}^1$ consists of the gray dots on the x_1-axis and the intervals between.

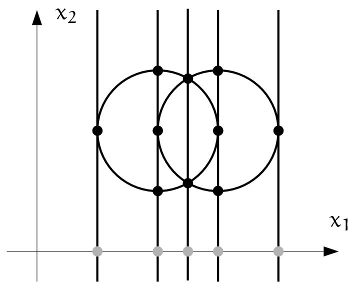

Figure 6: A CAD of $\mathbb{R}^2$ and the induced CAD of $\mathbb{R}^1$.

One of the components may be characterized semi-algebraically as

$$\begin{array}{lll}\{x \in \mathbb{R}^2 & \mid & (x_1-2)^2+(x_2-2)^2-1>0 \wedge \\ & & (x_1-3)^2-(x_2-2)^2-1<0 \wedge \\ & & x_1<3 \ \wedge \ x_2<2\,\}.\end{array}$$

Which one? □

4 Basic Tools

In this section we will present some theoretical tools which are important for the understanding of the different steps of the CAD-algorithm. These are polynomial remainder sequences, subresultants, principal subresultant coefficients, Sturm chains and representations of algebraic numbers. All concepts are treated in [17]. These are also the main tools for other constructive methods in real algebra and real algebraic geometry, see [4, 3, 12].

4.1 Common Factors of Multivariate Polynomials

We start with the univariate case and then generalize the ideas to multivariate polynomials. Given two polynomials $f, g \in k[x]$. How many common zeros do f and g have? How many distinct zeros do f have? These two questions may be answered knowing the *greatest common divisor* (gcd) of two polynomials. In the rest of this section k denotes a field of characteristic zero.

Lemma 4.1 *The number of common zeros of* $f,\ g \in k[x]$ *is*

$$\deg(\gcd(f, g))$$

Proof. The lemma follows from the definition of gcd and the fact that the number of zeros (counting multiplicity) of a univariate polynomial is equal to its degree. □

Lemma 4.2 *The number of distinct zeros of* $f \in k[x]$ *is*

$$\deg(f) - \deg(\gcd(f, f')).$$

Proof. Let $f \in k[x]$ have l distinct zeros $\alpha_1, \ldots \alpha_l$. Then

$$f(x) = a(x-\alpha_1)^{e_1} \cdots (x-\alpha_l)^{e_l}.$$

Differentiating $f(x)$ it is easy to see that

$$\deg(\gcd(f, f')) = \deg(f) - l$$

and the lemma follows. $\square$

How do one calculate the gcd of two univariate polynomials? The answer is provided by the Euclidean algorithm for polynomials. By repeated polynomial division we end up with the gcd of the two original polynomials. The process may be described as

$$\begin{aligned}
f_1 &= q_1 f_2 + f_3, && \deg(f_3) < \deg(f_2) \\
f_2 &= q_2 f_3 + f_4, && \deg(f_4) < \deg(f_3) \\
&\vdots \\
f_{p-2} &= q_{p-2} f_{p-1} + f_p, && \deg(f_p) < \deg(f_{p-1}) \\
f_{p-1} &= q_{p-1} f_p + 0
\end{aligned}$$

where $f_p = \gcd(f_1, f_2)$, see [13] or [8] for a detailed treatment. The algorithm terminates since the degree decreases in each step. The sequence $(f_1, f_2, \ldots, f_p)$ is called a *polynomial remainder sequence* (PRS).

Example 4.1 Let $f_1 = (1+x)(3+x)(1+x+x^2)$ and $f_2 = (1+x)(2+x)^2$. The PRS of f_1, f_2 in expanded form is

$$\begin{aligned}
f_1(x) &= 9 + 24x + 31x^2 + 23x^3 + 8x^4 + x^5 \\
f_2(x) &= 4 + 8x + 5x^2 + x^3 \\
f_3(x) &= 9 + 12x + 3x^2 \\
f_4(x) &= 1 + x,
\end{aligned}$$

where $f_4(x) = 1 + x = \gcd(f_1, f_2)$. $\square$

We now extend the above ideas to multivariate polynomials. Let $f, g \in k[x_1, \ldots, x_{n-1}][x_n]$, i.e., f and g is considered as polynomials in the variable x_n with polynomial coefficients in the variables $x_1, \ldots, x_{n-1}$. Hence the coefficients of f and g is no longer fixed numbers but depends on over which point $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{R}^{n-1}$ they are evaluated. This implies that both the number of zeros and their location varies for different $\alpha \in \mathbb{R}^{n-1}$.

Example 4.2 Let

$$f = (x_1^2 + x_2^2 - 1)x_3^2 + (x_2 - 1)x_3 + x_2^2.$$

Consider f as a polynomial in x_3. Then $\deg_{x_3}(f) = 2$ everywhere except on the cylinder $x_1^2 + x_2^2 - 1 = 0$. On the cylinder $\deg_{x_3}(f) = 1$ except on the line $(x_1, x_2) = (0, 1)$ where $\deg_{x_3}(f) = 0$. □

For some $\alpha \in \mathbb{R}^{n-1}$ there might be common factors of f and g but not for others, i.e., the gcd(f, g) and hence its degree depends on α. To calculate a gcd of two polynomials we use the Euclidean algorithm with pseudo division in each step since the polynomial coefficients no longer belongs to a field. Here is a brief exposition of pseudo division.

Lemma 4.3 *Let* $f, g \in k[x_1, \ldots, x_{n-1}][x_n]$,

$$\begin{aligned} f &= f_p x_n^p + \ldots f_0 \\ g &= g_m x_n^m + \ldots g_0 \end{aligned}$$

i.e., f_i, g_j *are polynomials in* $k[x_1, \ldots, x_{n-1}]$ *and* $m \leq p$. *Then*

$$g_m^s f = qg + r,$$

where $q, r, \in k[x_1, \ldots, x_{n-1}][x_n]$ *are unique,* $s \geq 0$ *and* $\deg_{x_n}(r) < m$.

Proof. A proof can be found in e.g., [8]. □

The remainder, r of the pseudo division is called the pseudo remainder of f_1 and f_2 and is denoted prem(f_1, f_2).

If we allow denominators pseudo division can be seen as

- Ordinary polynomial division for polynomials in x_n with coefficients from the rational function field $k(x_1, \ldots, x_{n-1})$, followed by
- Clearing denominators. The only term which needs to be inverted in the division is the leading coefficient, g_m of g. Hence we get the equation $g_m^s f = qg + r$.

Definition 4.1 Let R be a unique factorization domain. Two polynomials in $R[x]$ are *similar*, denoted

$$f(x) \sim g(x)$$

if there exist $a, b \in R$ such that $af(x) = bg(x)$. □

We can now generalize the concept of *polynomial remainder sequences.*

Definition 4.2 Let $R = k[x_1, \dots, x_{n-1}]$ and $f_1, f_2 \in R[x_n]$ with $\deg_{x_n}(f_1) \geq \deg_{x_n}(f_2)$. The sequence $f_1, f_2, \dots, f_k$ is a *polynomial remainder sequence* (PRS) for f_1 and f_2 if:

(i) For all $i = 3, \dots, k$

$$f_i \sim \mathrm{prem}(f_{i-2}, f_{i-1})$$

(ii) The sequence terminates with

$$\mathrm{prem}(f_{k-1}, f_k) = 0$$

□

Since we only claim similarity there are infinitely many PRS to every pair $f_1, f_2 \in k[x_1, \dots, x_{n-1}][x_n]$ of polynomials.

Immediately one thinks of the following two sequences:

- *Euclidean* Polynomial Remainder Sequence (EPRS):

$$\begin{aligned} f_i = \mathrm{prem}(f_{i-2}, f_{i-1}) &\neq 0 \\ \mathrm{prem}(f_{k-1}, f_k) &= 0 \end{aligned}$$

- *Primitive* Polynomial Remainder Sequence (PPRS):

$$\begin{aligned} f_i = \mathrm{pp}(\mathrm{prem}(f_{i-2}, f_{i-1})) &\neq 0 \\ \mathrm{prem}(f_{k-1}, f_k) &= 0 \end{aligned}$$

where pp stands for *primitive part*, i.e. the remaining part of the polynomial when we have removed all common factors of the coefficients.

We observe that a PRS is unique up to similarity since pseudo division is unique. Furthermore,

$$\gcd(f_1, f_2) \sim \ldots \sim \gcd(f_{k-1}, f_k) \sim f_k,$$

i.e., PRS essentially computes the gcd of two polynomials up to similarity.

From a computational point of view both EPRS and PPRS suffers from complexity problems. EPRS has an exponential coefficient growth and the PPRS algorithm involves calculations of gcd of the coefficients, which in our case again is polynomials. However, this computational complexity is not inherent in the problem. The *Subresultant Polynomial Remainder Sequence* (SPRS) offers a tradeoff between coefficient growth and the cost of gcd calculations of the coefficients. We will now take a closer look at subresultants and SPRS.

4.2 Subresultants

In this subsection we will present a way of calculating the SPRS, see e.g., [13, 15, 17].

To do this we observe that the process of pseudo division may be organized as row operations on a matrix containing the coefficients of the polynomials.

Example 4.3 Pseudo division applied to $f = x^3 + 2x^2 + 3x + 1$ and $g = 2x^2 + x + 2$ gives

$$2^2 f = (2x + 3)g + \boxed{5x - 2}.$$

One way of organizing the calculations is

$$M = \begin{bmatrix} 1 & 2 & 3 & 1 \\ 2 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 \end{bmatrix} \sim \begin{bmatrix} 2 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 \\ 0 & 0 & \boxed{5 \quad -2} \end{bmatrix} = M^-$$

where M^- is obtained from M by row operations. Observe the correspondence between the pseudo remainder coefficients and the last row of M^-. In fact multiplying the first row of M with 2^2, M^- can be obtained by just subtracting integer multiples of the other rows from the first row. Finally, permuting the rows gives the triangular form. According to the triangular structure of M^- the pseudo remainder coefficients may be found, modulo a common factor, by determinant calculations on a matrix consisting of the first two columns of M^- augmented by either column three or four. □

Since M and M^- only differs by row operations their minors are strongly related. Hence the coefficients of a polynomial similar to the pseudo remainder may be calculated as minors of the original matrix M. In fact, by calculating minors of matrices whose elements are the coefficients of two polynomials f and g we can construct a whole PRS of f and g. To see this we first need a couple of definitions. Throughout the rest of this subsection R is a *unique factorization domain* (UFD).

Definition 4.3 Let $f_i = \sum_{j=0}^{n_i} f_{ij} x^j \in R[x],\ i = 1, \dots, k$. The *matrix associated* with $f_1, \dots, f_k$ is

$$\mathrm{mat}(f_1, \dots, f_k) = \left[\ f_{i,l-j}\ \right],$$

where $l = 1 + \max_{1 \le i \le k}(n_i)$. □

Definition 4.4 Let $M \in R^{k \times l}, l \le k$. The *determinant polynomial* of M is

$$\mathrm{detpol}(M) = \det(M^{(k)})x^{l-k} + \dots + \det(M^{(l)}),$$

where $M^{(j)} = \left[\begin{array}{cccc} M_{\cdot,1} & \dots & M_{\cdot,k-1} & M_{\cdot,j} \end{array}\right]$. □

In Example 4.3 we have $M = \mathrm{mat}(f, x\,g, g)$, $\mathrm{detpol}(M) = 5x - 2 = \mathrm{prem}(f, g)$ and $\mathrm{detpol}(M^-) = 2^2(5x - 2)$.

Definition 4.5 Let $f, g \in R[x]$ and $\deg(f) = m, \deg(g) = n$, $m \ge n$.

- The k^{th} *subresultant* of f and g is

$$\mathrm{subres}_k(f, g) = \mathrm{detpol}(M_k),$$

  where $M_k = \mathrm{mat}(x^{n-k-1}f, \dots, f, x^{m-k-1}g, \dots, g)$.

- The *subresultant chain* of f and g is $(S_j)_{j=0}^{n+1}$, where

$$\begin{array}{rcl} S_{n+1} & = & f, \\ S_n & = & g, \\ S_{n-1} & = & \mathrm{subres}_{n-1}(f, g), \\ & \vdots & \\ S_0 & = & \mathrm{subres}_0(f, g). \end{array}$$

□

Observe that M_0 is the Sylvester matrix of f and g and $\text{subres}_0 = \text{detpol}(M_0) = \det(M_0)$ is the resultant of f and g. Furthermore, the M_k matrices is obtained by deleting rows and columns of M_0.

The importance of the definition of subresultants and subresultant chains lies in the fact that all PRS of f and g is embedded in the subresultant chain of f and g up to similarity.

We illustrate the definitions with a numerical example.

Example 4.4 Let $f = x^5 - 2x^4 + 3x^3 - 4x^2 + 5x - 6$ and $g = 3x^3 + 5x^2 + 7x + 9$. Then

$$M_0 = \begin{bmatrix} 1 & -2 & 3 & -4 & 5 & -6 & 0 & 0 \\ 0 & 1 & -2 & 3 & -4 & 5 & -6 & 0 \\ 0 & 0 & 1 & -2 & 3 & -4 & 5 & -6 \\ 3 & 5 & 7 & 9 & 0 & 0 & 0 & 0 \\ 0 & 3 & 5 & 7 & 9 & 0 & 0 & 0 \\ 0 & 0 & 3 & 5 & 7 & 9 & 0 & 0 \\ 0 & 0 & 0 & 3 & 5 & 7 & 9 & 0 \\ 0 & 0 & 0 & 0 & 3 & 5 & 7 & 9 \end{bmatrix}$$

$$M_1 = \left[\begin{array}{ccccc|cc} 1 & -2 & 3 & -4 & 5 & -6 & 0 \\ 0 & 1 & -2 & 3 & -4 & 5 & -6 \\ 3 & 5 & 7 & 9 & 0 & 0 & 0 \\ 0 & 3 & 5 & 7 & 9 & 0 & 0 \\ 0 & 0 & 3 & 5 & 7 & 9 & 0 \\ 0 & 0 & 0 & 3 & 5 & 7 & 9 \end{array}\right], \quad M_2 = \left[\begin{array}{ccc|ccc} 1 & -2 & 3 & -4 & 5 & -6 \\ 3 & 5 & 7 & 9 & 0 & 0 \\ 0 & 3 & 5 & 7 & 9 & 0 \\ 0 & 0 & 3 & 5 & 7 & 9 \end{array}\right].$$

Observe how M_1 and M_2 is obtained by deleting rows and columns of M_0. The $M_k^{(l)}$ matrices are formed by the left part of the partitioned matrices and one column from the right part. Now, the subresultants is the determinant polynomials of M_0, M_1 and M_2 , i.e.,

$$\begin{aligned}
S_4 &= x^5 - 2x^4 + 3x^3 - 4x^2 + 5x - 6 \\
S_3 &= 3x^3 + 5x^2 + 7x + 9 \\
S_2 &= \det(M_2^{(4)})x^2 + \det(M_2^{(5)})x + \det(M_2^{(6)}) = 263x^2 - 5x + 711 \\
S_1 &= \det(M_1^{(6)})x + \det(M_1^{(7)}) = -2598x - 11967 \\
S_0 &= \det(M_0) = 616149 = 3^2 \cdot 223 \cdot 307
\end{aligned}$$

Compare the subresultant chain with the EPRS and PPRS for f and g:

$$\begin{aligned}
f_1 &= x^5 - 2x^4 + 3x^3 - 4x^2 + 5x - 6 & \tilde{f}_1 &= x^5 - 2x^4 + 3x^3 - 4x^2 + 5x - 6\\
f_2 &= 3x^3 + 5x^2 + 7x + 9 & \tilde{f}_2 &= 3x^3 + 5x^2 + 7x + 9\\
f_3 &= -263x^2 + 5x - 711 & \tilde{f}_3 &= -263x^2 + 5x - 711\\
f_4 &= -70146x - 323109 & \tilde{f}_4 &= -866x - 3989\\
f_5 &= -3^8 \cdot 223 \cdot 263^2 \cdot 307 & \tilde{f}_5 &= -1
\end{aligned}$$

where $f_4 = 81\,\tilde{f}_4 = 3\,S_1$. Notice the tremendous coefficient growth in the EPRS compared with the modest growth in the subresultant chain. In this example there is a one to one correspondence between the PRS and the subresultant chain. This is due to the fact that the degree drops by one for each pseudo division. If the degree drops with more than one some of the subresultants becomes similar. □

What is the connection between a polynomial in a PRS and the determinant polynomial of M_k? By row operations on M_k a number of pseudo divisions may be carried out consecutively. The process is described by the following example which is a generalization of Example 4.3.

Example 4.5 Let $f = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ and $g = b_3x^3 + b_2x^2 + b_1x + b_0$. The corresponding M_1 matrix becomes

$$M_1 = \begin{bmatrix} a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & \\ & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & & & \\ & b_3 & b_2 & b_1 & b_0 & & \\ & & b_3 & b_2 & b_1 & b_0 & \\ & & & b_3 & b_2 & b_1 & b_0 \end{bmatrix} \overset{(1)}{\sim} \begin{bmatrix} b_3 & b_2 & b_1 & b_0 & & & \\ & b_3 & b_2 & b_1 & b_0 & & \\ & & b_3 & b_2 & b_1 & b_0 & \\ & & & b_3 & b_2 & b_1 & b_0 \\ & & & \tilde{a}_2 & \tilde{a}_1 & \tilde{a}_0 & \\ & & & & \tilde{a}_2 & \tilde{a}_1 & \tilde{a}_0 \end{bmatrix} \overset{(2)}{\sim}$$

$$\begin{bmatrix} b_3 & b_2 & b_1 & b_0 & & & \\ & b_3 & b_2 & b_1 & b_0 & & \\ & & b_3 & b_2 & b_1 & b_0 & \\ & & & \tilde{a}_2 & \tilde{a}_1 & \tilde{a}_0 & \\ & & & & \tilde{a}_2 & \tilde{a}_1 & \tilde{a}_0 \\ & & & & & \tilde{b}_1 & \tilde{b}_0 \end{bmatrix} = M_1^-$$

Row operations in detail:

(1) Multiply the first row with b_3^3 and subtract multiplicities of row 3, 4 and 5 to eliminate a_5, a_4 and a_3. A similar treatment of the second row

followed by interchanging rows gives the second matrix. The resulting matrix elements $\tilde{a}_i$ are the coefficients of $\mathrm{prem}(f, g)$.

(2) The same process as in (1) repeated on row 4, 5 and 6. The matrix elements $\tilde{b}_i$ are the coefficients of $\mathrm{prem}(g, \mathrm{prem}(f, g))$.

□

As pointed out earlier the only operations needed to get from M_k to the last triangular matrix, M_k^- are row operations. It is then clear that the minors $\det(M_k^{(l)})$ and the corresponding minors of the triangular matrix only differs by a common factor.

Our original motivation for calculating PRS was to determine the gcd of two polynomials and especially its degree. Hence we are interested in the coefficient of the highest power of a gcd.

Definition 4.6 Let $f, g \in R[x]$ and $\deg(f) = m, \deg(g) = n$, $m \geq n$. The k^{th} *principal subresultant coefficient* of f and g is

$$\mathrm{psc}_k(f, g) = \det(M_k^{(k)}), \quad 0 \leq k \leq n.$$

□

In other words $\mathrm{psc}_k(f, g)$ is the coefficient of x^k in $\mathrm{subres}_k(f, g)$. The following lemma, which is not hard to believe in knowing the connection between a PRS and the corresponding subresultant chain, tells us that knowing the psc chain of two polynomials we know the degree of their gcd.

Lemma 4.4 *Let* $f,\ g \in R[x]$ *where* $\deg(f) = m$ *and* $\deg(g) = n$. *Then for all* $0 < i \leq \min(m, n)$

$$f \text{ and } g \text{ have a common factor of degree} = i$$

$$\Longleftrightarrow$$

$$\mathrm{psc}_j(f, g) = 0, j = 0, \ldots, i-1 \text{ and } \mathrm{psc}_i(f, g) \neq 0$$

Proof. See Corollary 7.7.9. in [17]. □

In this subsection we have worked with polynomials in $R[x]$ where R is a unique factorization domain (UFD). For simplicity the examples were done for polynomials over the integers but any UFD will do e.g., multivariate polynomials. In the following we use $R = \mathbb{R}[x_1, \ldots, x_{n-1}]$, i.e., polynomials in $\mathbb{R}[x_1, \ldots, x_{n-1}][x_n]$.

4.3 Delineable Sets

The key idea in the so called projection phase of the CAD-algorithm is to find regions over which the given polynomials have a constant number of real roots, cf. Example 2.1. This is formalized by the concept of delineability.

Let $f_i \in \mathbb{R}[x_1, \ldots, x_{n-1}][x_n]$ be a real polynomial in n-variables:

$$f_i(x_1, \ldots, x_{n-1}, x_n) = f_i^{d_i}(x_1, \ldots, x_{n-1})x_n^{d_i} + \cdots + f_i^0(x_1, \ldots, x_{n-1})$$

and $\xi = (\xi_1, \ldots, \xi_{n-1}) \in \mathbb{R}^{n-1}$. Then we write $f_{i,\xi}(x_n) = f(\xi_1, \ldots, \xi_{n-1}, x_n)$ for the univariate polynomial obtained by substituting ξ for the first $n-1$ variables.

We also introduce the *reductum*, $\hat{f}_i^{k_i}$ of a polynomial. Let

$$\hat{f}_i^{k_i}(x_1, \ldots, x_{n-1}, x_n) = f_i^{k_i}(x_1, \ldots, x_{n-1})x_n^{k_i} + \cdots + f_i^0(x_1, \ldots, x_{n-1}),$$

where $0 \le k_i \le d_i$. Thus, if $f_i^{d_i}(\xi) = \cdots = f_i^{k_{i+1}}(\xi) = 0$ and $f_i^{k_i}(\xi) \neq 0$, then

$$f_{i,\xi}(x_n) = \hat{f}_i^{k_i}(\xi, x_n) = f_i^{k_i}(\xi)x_n^{k_i} + \cdots + f_i^0(\xi).$$

Definition 4.7 Let $\mathcal{F} = \{f_1, f_2, \ldots, f_r\} \subset \mathbb{R}[x_1, \ldots, x_{n-1}][x_n]$ be a set of multivariable real polynomials and $C \subset \mathbb{R}^{n-1}$. We say that $\mathcal{F}$ is *delineable* on C, if it satisfies the following invariant properties:

(i) For every $1 \le i \le r$, the *total number of complex roots* of $f_{i,\xi}$ (counting multiplicity) remains invariant as ξ varies over C.

(ii) For every $1 \le i \le r$, the *number of distinct complex roots* of $f_{i,\xi}$ remains invariant as ξ varies over C.

(iii) For every $1 \le i < j \le r$, the *total number of common complex roots* of $f_{i,\xi}$ and $f_{j,\xi}$ (counting multiplicity) remains invariant as ξ varies over C.

□

Consider one of the polynomials $f_i \in \mathcal{F}$. Since it has real coefficients its complex roots have to occur in conjugate pairs. Let ξ and ξ' be two points in $C \subset \mathbb{R}^{n-1}$. The only way for a pair of complex conjugated roots of $f_{i,\xi}$ to become real when ξ varies to ξ' is to coalesce into a real double root, i.e. the number of distinct roots of f_i drops. Hence a transition from a nonreal root to a real root is impossible over C. Similar arguments holds for the reversed problem.

Lemma 4.5 *Let $\mathcal{F} \subset \mathbb{R}[x_1, \dots, x_{n-1}][x_n]$ be a set of polynomials and let $\mathcal{F}$ be delineable over $C \subset \mathbb{R}^{n-1}$. Then the total number of distinct real roots of $\mathcal{F}$ is invariant over C.*

Proof. See Lemma 8.6.3. in [17]. □

We are now able to formulate the main theorem of this section.

Theorem 4.1 *Let $\mathcal{F} \subset \mathbb{R}[x_1, \dots, x_{n-1}][x_n]$ be a set of polynomials and let $C \subset \mathbb{R}^{n-1}$ be a connected maximal $\mathcal{F}$-delineable set. Then C is semi-algebraic.*

Proof. A complete proof may be found in [6] or in the errata of [17]. Here we only sketch the ideas. The idea is to show that the three invariant properties of Definition 4.7 have semi-algebraic characterizations. Let $\mathrm{psc}_i^{x_n}$ denote the i^{th} principal resultant coefficient w.r.t. x_n and D_{x_n} denote the formal derivative operator w.r.t. x_n.

(i) Total number of complex roots of $f_{i,\xi}$ remains invariant over C. This corresponds to the claim that

$$(\forall 1 \leq i \leq r)(\exists 0 \leq k_i \leq d_i)$$

$$\Big[(\forall k > k_i)[f_i^k(x_1, \dots, x_{n-1}) = 0] \wedge f_i^{k_i}(x_1, \dots, x_{n-1}) \neq 0\Big]$$

holds for all $\xi \in C$.

(ii) The number of distinct complex roots of $f_{i,\xi}$ remains invariant over C, which corresponds to

$$(\forall 1 \leq i \leq r)(\exists 0 < k_i \leq d_i)(\exists 0 \leq l_i \leq k_i - 1)$$

$$\Big[(\forall k > k_i)[f_i^k(x_1, \dots, x_{n-1}) = 0] \wedge f_i^{k_i}(x_1, \dots, x_{n-1}) \neq 0 \wedge$$

$$(\forall l < l_i)[\mathrm{psc}_l^{x_n}(\hat{f}_i^{k_i}(x_1, \dots, x_n), D_{x_n}(\hat{f}_i^{k_i}(x_1, \dots, x_n))) = 0] \wedge$$

$$\mathrm{psc}_{l_i}^{x_n}(\hat{f}_i^{k_i}(x_1, \dots, x_n), D_{x_n}(\hat{f}_i^{k_i}(x_1, \dots, x_n))) \neq 0\Big],$$

holds for all $\xi \in C$.

(iii) The total number of common complex roots of $f_{i,\xi}$ and $f_{j,\xi}$ (counting multiplicity) remains invariant over C, which is characterized by

$$(\forall 1 \leq i < j \leq r)(\exists 0 < k_i \leq d_i)(\exists 0 < k_j \leq d_j)(\exists 0 \leq m_{i,j} \leq \min(d_i, d_j))$$

$$\Big[(\forall k > k_i)[f_i^k(x_1,\ldots,x_{n-1}) = 0] \wedge f_i^{k_i}(x_1,\ldots,x_{n-1}) \neq 0 \wedge$$
$$(\forall k > k_j)[f_j^k(x_1,\ldots,x_{n-1}) = 0] \wedge f_j^{k_j}(x_1,\ldots,x_{n-1}) \neq 0 \wedge$$
$$(\forall m < m_{i,j})[\mathrm{psc}_m^{x_n}(\hat{f}_i^{k_i}(x_1,\ldots,x_n), \hat{f}_j^{k_j}(x_1,\ldots,x_n)) = 0] \wedge$$
$$[\mathrm{psc}_{m_{i,j}}^{x_n}(\hat{f}_i^{k_i}(x_1,\ldots,x_n), \hat{f}_j^{k_j}(x_1,\ldots,x_n)) \neq 0]\Big],$$

holds for all $\xi \in C$.

$\square$

In summary, given a set of polynomials $\mathcal{F} \subset \mathbb{R}[x_1,\ldots,x_{n-1}][x_n]$ we can compute another set of $(n-1)$-variate polynomials $\mathrm{proj}(\mathcal{F}) \subset \mathbb{R}[x_1,\ldots,x_{n-1}]$, which characterizes the maximal connected $\mathcal{F}$-delineable subsets of $\mathbb{R}^{n-1}$. Let

$$\mathcal{F} = \{f_1, f_2, \ldots, f_r\}$$

then

$$\mathrm{proj}(\mathcal{F}) = \mathrm{proj}_1(\mathcal{F}) \ \cup \ \mathrm{proj}_2(\mathcal{F}) \ \cup \ \mathrm{proj}_3(\mathcal{F})$$

where

$$\mathrm{proj}_1 = \{f_i^k(x_1,\ldots,x_{n-1}) \mid 1 \le i \le r,\ 0 \le k \le d_i\}$$

$$\mathrm{proj}_2 = \{\mathrm{psc}_l^{x_n}(\hat{f}_i^k(x_1,\ldots,x_n), D_{x_n}(\hat{f}_i^k(x_1,\ldots,x_n))) \mid \\ 1 \le i \le r,\ 0 \le l < k \le d_i - 1\}$$

$$\mathrm{proj}_3 = \{\mathrm{psc}_m^{x_n}(\hat{f}_i^{k_i}(x_1,\ldots,x_n), \hat{f}_j^{k_j}(x_1,\ldots,x_n)) \mid \\ 1 \le i < j \le r,\ 0 \le m \le k_i \le d_i,\ 0 \le m \le k_j \le d_j\}$$

Suppose that the set $\mathrm{proj}(\mathcal{F})$ is invariant over $C \subset \mathbb{R}^{n-1}$. The invariance of the set $\mathrm{proj}_1(\mathcal{F})$ implies that the degree w.r.t. x_n of the polynomials is constant over C and hence the number of roots of each polynomial is constant over C (condition (i) in Definition 4.7).

The invariance of $\mathrm{proj}_2(\mathcal{F})$ implies that the gcd of each polynomial and its derivative has constant degree according to Lemma 4.4. Together with the invariance of $\mathrm{proj}_1(\mathcal{F})$ the number of distinct zeros of each polynomial in $\mathcal{F}$ is constant, cf. Lemma 4.2 (condition (ii) in Definition 4.7).

The invariance of $\mathrm{proj}_3(\mathcal{F})$ together with the invariance of $\mathrm{proj}_1(\mathcal{F})$ implies that the number of common zeros of each pair of polynomials in $\mathcal{F}$ is constant, cf. Lemma 4.4 (condition (iii) in Definition 4.7).

According to Lemma 4.5 the set $\mathrm{proj}(\mathcal{F})$ characterize the sets over which there are a constant number of real zeros of the polynomials in $\mathcal{F}$.

4.4 Real Roots of a Polynomial

In this subsection we will describe a method for calculating the number of distinct real zeros of a univariate polynomial using so called Sturm chains. This is important in both the so called base and extension phase of the CAD-algorithm since we then need to isolate the real roots of a number of univariate polynomials. We will also take a brief look on how one may do calculations with and represent algebraic numbers.

Definition 4.8 Let $f_1, \ldots, f_r \in \mathbb{R}[x]$ have the following properties with respect to the interval (a, b):

(i) $f_k(x) = 0 \Rightarrow f_{k-1}(x) f_{k+1}(x) < 0, \; a < x < b$

(ii) $f_r(x) \neq 0, \; a < x < b$

Then $f_1, \ldots, f_r$ is called a *Sturm chain* in the interval (a, b). If each polynomial of the Sturm chain is multiplied by the same arbitrary polynomial $d(x)$ the chain obtained is called a *generalized Sturm chain.* □

Example 4.6 Let $f_1 \in \mathbb{R}[x]$. We will now construct an important Sturm chain whose first two elements are f_1 and f_1'. Let $f_2 = f_1'$ and consider the following PRS:

$$\begin{aligned}
f_1 &= q_1 f_2 - f_3 \\
f_2 &= q_2 f_3 - f_4 \\
&\vdots \\
f_{r-2} &= q_{r-2} f_{r-1} - f_r \\
f_{r-1} &= q_{r-1} f_r + 0,
\end{aligned}$$

where $f_r = \gcd(f_1, f_2)$. This sequence is a Sturm chain in (a, b) by construction if $f_r \neq 0$ in (a, b) or a generalized sturm chain in $(-\infty, \infty)$, since

$f_1, \ldots, f_r$ may be seen as Sturm chain multiplied by the gcd of all f_i. Observe the reversed sign of each remainder, which guarantees property (ii) of Definition 4.8. □

Definition 4.9 Let $(a_i)_{i=1}^r$ be a finite sequence of real numbers. Then let $\mathrm{var}(a_1, \ldots, a_r)$ denote the number of variations in sign of the sequence. □

Example 4.7

$$\mathrm{var}(-1, 0, -2, 0, 0, 4, 3, -1) = 2 \quad \text{and} \quad \mathrm{var}(3, 5, 0, -1, 2, 0, -2, 1) = 4.$$

□

Theorem 4.2 *Let* $f_1, \ldots, f_r$ *be the chain obtained in Example 4.6 and* $V(x) = \mathrm{var}(f_1(x), \ldots, f_r(x))$. *Then the number of distinct real zeros of* f_1 *in* (a, b)[1] *is*

$$V(a) - V(b)$$

Proof. See [9, 17]. □

Example 4.8 Let $f_1 = (x^2 + x + 1)(x + 1)(x - 1)(x - 3)$. Then $f_2 = f_1' = 5x^4 - 8x^3 - 9x^2 - 2x + 2$ and the Sturm chain in Example 4.6 of f_1 and f_2 becomes:

$$\begin{aligned}
f_1 &= x^5 - 2x^4 - 3x^3 - x^2 + 2x + 3 \\
f_2 &= 5x^4 - 8x^3 - 9x^2 - 2x + 2 \\
f_3 &= \tfrac{46}{25}x^3 + \tfrac{33}{25}x^2 - \tfrac{36}{25}x - \tfrac{79}{25} \\
f_4 &= -\tfrac{6825}{2116}x^2 + \tfrac{2625}{1058}x + \tfrac{37875}{2116} \\
f_5 &= -\tfrac{321632}{29575}x - \tfrac{50784}{4225} \\
f_6 &= -\tfrac{2142075}{190969}
\end{aligned}$$

According to Theorem 4.2 we can calculate the number of distinct real zeros of f_1 in $(-2, 2)$. We have

$$V(-2) = \mathrm{var}(-, +, -, +, +, -) = 4, \quad V(2) = \mathrm{var}(-, -, +, +, -, -) = 2$$

[1] Here a may be $-\infty$ and b may be ∞.

where only the signs of the evaluated Sturm chain is presented. Hence the number of real zeros of f_1 in $(-2, 2)$ is 2.

The total number of distinct real zeros of f_1 is 3 since

$$V(-\infty) = \text{var}(-, +, -, -, +, -) = 4, \quad V(\infty) = \text{var}(+, +, +, -, -, -) = 1.$$

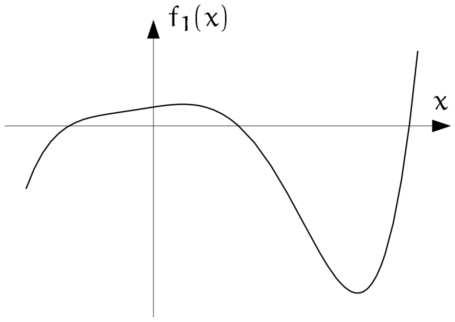

Figure 7: A plot of $f_1(x)$.

$\square$

We now have a method for counting the number of distinct real zeros of a univariate polynomial in an interval. Together with a bound on the modulus of the zeros it is easy to state an algorithm which separates or isolates the real zeros of a polynomial, e.g., using some bisection method, see [9] and [17].

In the so called extension phase of the CAD-algorithm multivariate polynomials are evaluated over algebraic numbers, i.e., zeros of univariate polynomials. Then one needs both representations and algorithms for calculations with these numbers.

A real algebraic number, α may be represented in a number of different ways. Perhaps the most intuitive way is by a polynomial and an isolating interval. Usually one choose a polynomial of lowest degree which has α as a zero:

$$\alpha \; : \; [p_\alpha(x), \, I_\alpha],$$

where $p_\alpha \in \mathbb{Z}[x]$, $I_\alpha = (a, b) \in \mathbb{Q}^2$ and I_α contains no other real zero of p_α than α.

The main tool for arithmetic operations with algebraic numbers is resultants. We will not go into details here but there are algorithms for e.g., addition, multiplication, inverse and sign evaluation of polynomials.

More about representation of and calculation with algebraic numbers can be found in [17, 9, 7]. There are also a library of C routines called SACLIB offering algebraic number arithmetic, see [5].

5 The CAD-Algorithm

In this section we will describe the CAD-algorithm in detail. The algorithm can be divided into three phases: projection, base and extension.

The input of the algorithm is a set, $\mathcal{F}$ of n-variate polynomials. The projection phase consists of a number of steps, each in which new sets of polynomials is constructed. The zero sets of the resulting polynomials of each step is the projection of "significant" points of the zero set of the preceding polynomials, i.e., self-crossings, isolated points, vertical tangent points etc. In each step the number of variables is decreased by one and hence the projection phase consists of $n-1$ steps.

The base phase consists of isolation of real roots, $\alpha_i \in \mathbb{R}^1$ of the monovariate polynomials, which are the outputs from the projection phase. Each root and one point in the each interval between two roots are chosen as sample points of a decomposition of $\mathbb{R}^1$.

The purpose of the extension phase is to construct sample points of all cells of the CAD of $\mathbb{R}^n$. The extension phase consists of $n-1$ steps. In the first step a sample point, $(\alpha_i, \beta_j) \in \mathbb{R}^2$ of each cell of the stack over the cells of the base phase is constructed. In the following steps the above procedure is repeated until we have sample points of all cells of the CAD of $\mathbb{R}^n$.

Observe that to determine if a real polynomial system has a solution, it is enough to determine the signs of $\mathcal{F}$ in a sample point of each cell since $\mathcal{F}$ is invariant on each cell by construction.

The algorithm can be summarized as:

Input: $\mathcal{F} = \{f_1, \dots, f_r\} \subset \mathbb{R}[x_1, \dots, x_n]$.

Output: An $\mathcal{F}$-invariant CAD of $\mathbb{R}^n$.

- Projection:

  $$\mathcal{F}_0 = \mathcal{F} \subset \mathbb{R}[x_1, \dots, x_n],\ \mathcal{F}_1 \subset \mathbb{R}[x_1, \dots, x_{n-1}], \dots, \mathcal{F}_{n-1} \subset \mathbb{R}[x_1].$$

- Base: Root isolation and sample point construction of a CAD of $\mathbb{R}^1$.

- Extension: Sample point construction of CADs of $\mathbb{R}^k$, $k = 2, \dots, n$.

We now describe the details of each phase.

5.1 The projection phase

In the projection phase the proj-operator of Section 4 is applied recursively $n-1$ times.

Let $\mathcal{F} = \{f_1, \dots, f_r\}$, $\mathrm{proj}^0 = \mathcal{F}$ and $\mathrm{proj}^i(\mathcal{F}) = \mathrm{proj}(\mathrm{proj}^{i-1}(\mathcal{F}))$ for $1 \leq i \leq n-1$. Then

$$\begin{aligned}
&\mathcal{F} \subset \mathbb{R}[x_1, \dots, x_n] \\
&\mathrm{proj}(\mathcal{F}) \subset \mathbb{R}[x_1, \dots, x_{n-1}] \\
&\mathrm{proj}^2(\mathcal{F}) \subset \mathbb{R}[x_1, \dots, x_{n-2}] \\
&\quad \vdots \\
&\mathrm{proj}^{n-1}(\mathcal{F}) \subset \mathbb{R}[x_1],
\end{aligned}$$

where the corresponding zero sets are the successive projections of the "significant" points of the original zero set.

Example 5.1 Consider the 3D-sphere of radius 1 centered at $(2, 2, 2)$ which is given by the real zero set of f,

$$f = (x_1 - 2)^2 + (x_2 - 2)^2 + (x_3 - 2)^3 - 1.$$

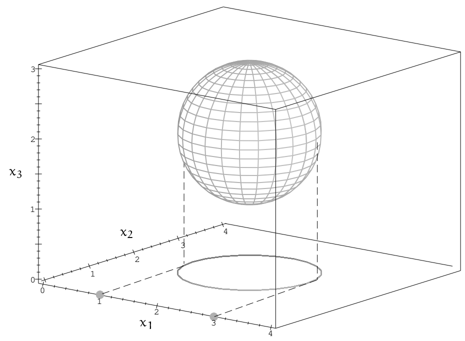

Figure 8: The real zero set of f and the projections of its "significant" points.

Now, the projection polynomials is

$$\begin{aligned}
\mathrm{proj}(f) &= \{\,4((x_1-2)^2+(x_2-2)^2-1),\ (x_1-2)^2+(x_2-2)^2+3\,\} \\
\mathrm{proj}^2(f) &= \{\,4(x_1-1)(x_1-3)(x_1^2-4x_1+19), \\
&\quad 16(x_1^4-8x_1^3+30x_1^2-56+113), \\
&\quad 4(x_1^2-4x_1+7), \\
&\quad x_1^2-4x_1+11, \\
&\quad 256(x_1-1)(x_1-3)\,\}
\end{aligned}$$

The only real zeros of the polynomials in $\mathrm{proj}(f)$ correspond to the circle in the x_1x_2-plane in Figure 8 and the only real zeros of the polynomials in $\mathrm{proj}^2(f)$ is 1 and 3, i.e., the gray dots on the x_1-axis in Figure 8.

□

5.2 The base phase

The zeros of the monovariate polynomials in $\mathrm{proj}^{n-1}(\mathcal{F})$ define a sign invariant decomposition of $\mathbb{R}^1$. Enumerate the real zeros of the polynomials in $\mathrm{proj}^{n-1}(\mathcal{F})$ according to

$$-\infty < \xi_1 < \xi_2 < \cdots < \xi_s < +\infty,$$

The $\mathrm{proj}^{n-1}(\mathcal{F})$-invariant decomposition of $\mathbb{R}^1$ consists of these zeros and the intermediate open intervals. The purpose of the base phase is to isolate the above zeros and find sample points for each component in the decomposition, i.e., the zeros and a sample point in each interval. For an open interval we may choose a rational sample point but for a zero we must store an exact representation of the algebraic number. There are several ways of doing this, as was discussed in Section 4.

The base phase may thus be described briefly as:

Input: A set of monovariate polynomials, $\mathrm{proj}^{n-1}(\mathcal{F})$.

Output: Sample points of each component of the decomposition of $\mathbb{R}^1$.

- Real root isolation: $\xi_1 \in (u_1, v_1], \ldots, \xi_s \in (u_s, v_s]$, where $u_i, v_i \in \mathbb{Q}$.
- Choice of sample points: $\alpha_1 = u_1$, $\alpha_2 = \xi_1, \ldots, \alpha_{2s+1} = v_s + 1$.

Example 5.2 Given the $\mathrm{proj}^2(f)$ set from the projection phase of Example 5.1 we isolate the real roots of its polynomials. The number of real roots of each polynomial may be calculated using Theorem 4.2. This gives the real roots 1 and 3 with isolating intervals $(\frac{1}{2}, 2]$ and $(2, \frac{7}{2}]$, respectively. The x_1-axis is decomposed into 5 cells with the following sample points:

$$\frac{1}{2},\ 1,\ 2,\ 3,\ \frac{7}{2}.$$

□

5.3 The extension phase

In the extension phase we "lift" a sign invariant decomposition, $\mathcal{D}_{i-1}$ of $\mathbb{R}^{i-1}$ to a sign invariant decomposition, $\mathcal{D}_i$ of $\mathbb{R}^i$ using the technique of the base phase repetitively.

Consider the "lift" from $\mathbb{R}^1$ to $\mathbb{R}^2$. According to the way $\mathrm{proj}^{n-2}(\mathcal{F})$ is constructed it is delineabel over each cell of $\mathcal{D}^1$. We will construct the sample points of those cells of $\mathcal{D}^2$ which belongs to the stack over the cell $C \subset \mathcal{D}^1$. Evaluate the polynomials in $\mathrm{proj}^{n-2}(\mathcal{F})$ over the sample point, α of C. We then get a set of monovariate polynomials in x_2 corresponding to the values of $\mathrm{proj}^{n-2}(\mathcal{F})$ on the "vertical" line $x_1 = \alpha$.

These monovariate polynomials is then treated in the same way as the polynomials in the base phase, i.e., root isolation and choice of sample points. Hence the "lift" from $\mathbb{R}^1$ to $\mathbb{R}^2$ corresponds to the construction of the second component of the sample points of $\mathcal{D}^n$.

Having sample points for all cells of $\mathcal{D}^2$ the above process may be repeated to construct sample points of the cells of $\mathcal{D}^3, \ldots, \mathcal{D}^n$.

A geometrical picture of the steps in the extension phase consists of so to speak raising vertical lines over each sample point of the lower dimensional decomposition and calculate the intersections between these lines with the zero set of the next higher dimensional set of polynomials.

The result of the extension phase is a list of cells (indexed in some way) and their sample points.

Hence, the decomposition may be represented as a tree structure where the first level of nodes under the root corresponds to the cells of $\mathbb{R}^1$, the second level of nodes represents the cells of $\mathbb{R}^2$, i.e., the stacks over the cells of $\mathbb{R}^1$ etc, see Figure 10. The leaves represents the cells of the CAD of $\mathbb{R}^n$. In each node or leaf a sample point of the corresponding cell is stored. To each level of the tree there are a number of projection polynomials $\mathrm{proj}^k(\mathcal{F})$ whose signs when evaluated over a sample point defines a cell.

Notice that the projection polynomials $\mathrm{proj}^k(\mathcal{F}), k = 0, \ldots, n-1$ together with the sample points describes the set of solutions of a system of polynomial equations and inequalities. The signs of the projection polynomials gives us information about the restrictions on the solution set imposed by the original system on smaller and smaller sets of variables.

Example 5.3 We now extend the CAD of $\mathbb{R}^1$ from Example 5.2 to a CAD of $\mathbb{R}^2$ and $\mathbb{R}^3$.

The base phase gives a decomposition of the x_1-axis into five cells and a sample point of each cell, see the top left plot in Figure 9.

Now, specializing the polynomials of $\mathrm{proj}(f)$ over each sample point gives five univariate polynomials in x_2. For each specialized polynomial we use the same algorithms as in the base phase to construct sample points of the cells of $\mathbb{R}^2$. We may choose the following sample points

$$\begin{aligned}
&(\tfrac{1}{2}, 2),\\
&(1,1),\ (1,2),\ (1,3),\\
&(2,\tfrac{1}{2}),\ (2,1),\ (2,2),\ (2,3),\ (2,\tfrac{7}{2}),\\
&(3,1),\ (3,2),\ (3,3),\\
&(\tfrac{7}{2}, 2).
\end{aligned}$$

In the same way we specialize f over each sample point of $\mathbb{R}^2$ and construct the 25 sample points of the CAD of $\mathbb{R}^3$. In Figure 10 the structure of a tree representation of the CAD is given.

$\square$

Observe that even for this trivial example the number of cells become quite large. In general the number of cells of a CAD grow very fast as the number of variables increase.

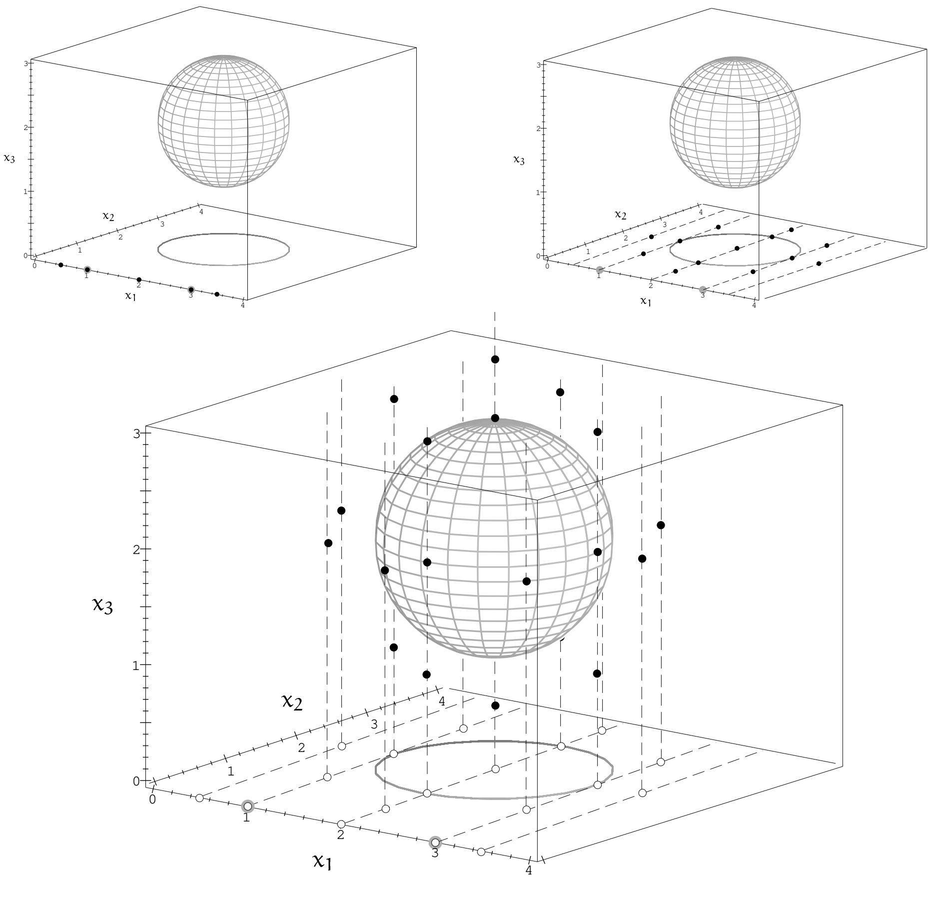

Figure 9: The sample points of each step of the extension phase.

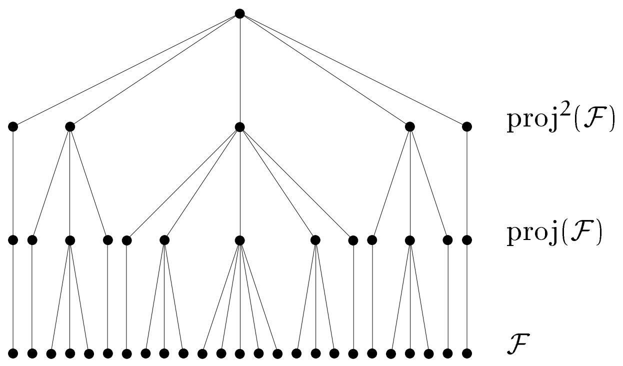

Figure 10: A tree representation of the CAD.

6 Examples

Example 6.1 Given the following polynomials

$$\begin{aligned} f_1 &= x_2^2 - 2x_1x_2 + x_1^4 \\ f_2 &= (2431x_1 - 3301)x_2 - 2431x_1 + 2685, \end{aligned} \tag{3}$$

determine a corresponding CAD of $\mathbb{R}^2$.

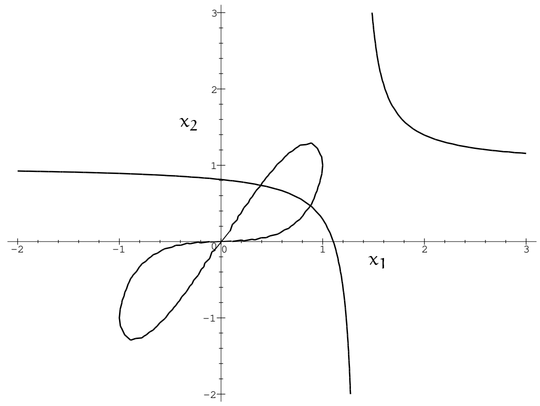

Figure 11: A plot of the real zero set of the polynomials in (3).

- Projection:

$$\begin{aligned}
\mathrm{proj}_1(f_1) &= \{-2\,x_1, 1, x_1{}^4\} \\
\mathrm{proj}_1(f_2) &= \{-2431\,x_1 + 2685, 2431\,x_1 - 3301\} \\
\mathrm{proj}_2(f_1) &= \{4\,x_1{}^2\,(x_1 - 1)\,(x_1 + 1)\} \\
\mathrm{proj}_2(f_2) &= \{\} \\
\mathrm{proj}_3(\{f_1, f_2\}) &=
\end{aligned}$$

$$\Big\{ -x_1 \left(-4862\,x_1 + 5370 + 2431\,x_1{}^4 - 3301\,x_1{}^3\right), \\ (17\,x_1 - 15)\,(13\,x_1 - 5)\left(26741\,x_1{}^4 - 38742\,x_1{}^3 - 8854\,x_1{}^2 - 51552\,x_1 + 96123\right)\Big\}$$

- Base: The real roots of $\mathrm{proj}(\{f_1, f_2\})$ are

$$-1,\ 0,\ \frac{5}{13},\ \frac{15}{17},\ \alpha \approx 0.93208,\ 1,\ \frac{2685}{2431},\ \frac{3301}{2431},\ \beta \approx 1.59982$$

where α and β is the real zeros of $2431x_1^4 - 3301x_1^3 - 4862x_1 + 5370$. It turns out that we only need five of these roots to determine a CAD of $\mathbb{R}^2$. These are

$$-1,\ 0,\ \frac{5}{13},\ \frac{15}{17},\ 1,\ \frac{3301}{2431}.$$

We also need sample points from each interval between the above roots, e.g.,

$$-2,\ -\frac{1}{2},\ \frac{1}{4},\ \frac{1}{2},\ \frac{9}{10},\ \frac{5}{4},\ 2.$$

Hence the base phase produces 13 sample points.

- Extension: We calculate the sample points for the stack over cell 7 ($x_1 = \frac{1}{2}$) of the decomposition of $\mathbb{R}^1$ to illustrate the procedure. We have

$$\begin{aligned}
f_1(\tfrac{1}{2}, x_2) &= x_2{}^2 - x_2 + 1/16 \\
f_2(\tfrac{1}{2}, x_2) &= -\tfrac{4171}{2}\,x_2 + \tfrac{2939}{2},
\end{aligned}$$

with real roots

$$\frac{1}{2} \pm \frac{1}{4}\sqrt{3} \quad \text{and} \quad \frac{2939}{4171}$$

respectively. Together with four points in the intermediate intervals we get seven sample points, see Table 3.

Sample point (x_1, x_2)	$\mathrm{sign}(f_1)$	$\mathrm{sign}(f_2)$
$(\frac{1}{2}, 0)$	$+$	$+$
$(\frac{1}{2}, \frac{1}{2} - \frac{1}{4}\sqrt{3})$	0	$+$
$(\frac{1}{2}, \frac{1}{2})$	$-$	$+$
$(\frac{1}{2}, \frac{2939}{4171})$	$-$	0
$(\frac{1}{2}, \frac{3}{4})$	$-$	$-$
$(\frac{1}{2}, \frac{1}{2} + \frac{1}{4}\sqrt{3})$	0	$-$
$(\frac{1}{2}, 2)$	$+$	$-$

Table 3: Sample points and signs of f_1 and f_2 over cell 7.

The information in one row of Table 3 is typically what is stored in a leaf of a tree representation of a CAD, i.e., the sample point and the signs of the polynomials. The whole CAD of $\mathbb{R}^3$ consists of 63 cells, see Figure 12. Given the sign of f_1 and f_2 in all cells we can "solve" any real polynomial system defined by f_1 and f_2.

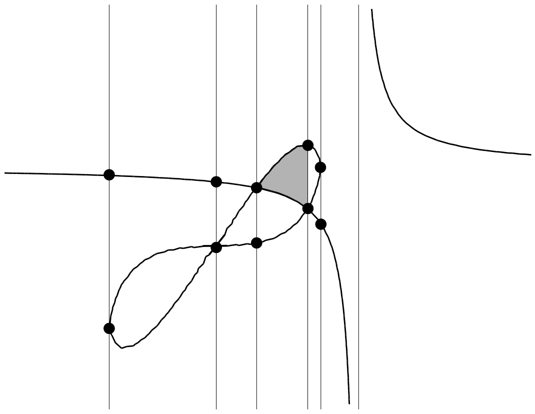

Figure 12: The CAD, where the gray region corresponds to row five in Table 3, i.e., $f_1 < 0$ and $f_2 < 0$.

□

Example 6.2 Given the following polynomials

$$\begin{aligned} f_1 &= x_2^2 - x_1^3 - x_1^2 \\ f_2 &= (x_1 - 1)x_2^2 + x_1^3 x_2 - x_1^3 + 1, \end{aligned} \tag{4}$$

determine a corresponding CAD of $\mathbb{R}^2$.

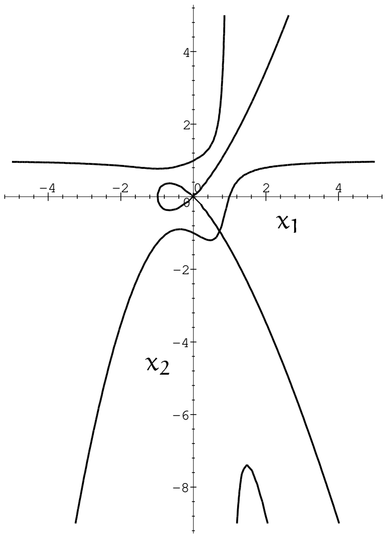

Figure 13: A plot of the real zero set of the polynomials in (4).

- Projection:

$$\begin{aligned} \text{proj}(\{f_1, f_2\}) = \; & \{x_1{}^3, x_1 - 1, \\ & -(x_1 - 1)\left(x_1{}^2 + x_1 + 1\right), \\ & -4\,x_1{}^2\,(x_1 + 1), \\ & -(x_1 - 1)\left(x_1{}^6 + 4\,x_1{}^4 - 4\,x_1{}^3 - 4\,x_1 + 4\right), \\ & -x_1{}^9 - 2\,x_1{}^7 - x_1{}^6 + 2\,x_1{}^5 + 3\,x_1{}^4 - 2\,x_1{}^3 - 2\,x_1{}^2 + 1, \\ & -x_1{}^2\,(x_1 + 1), \\ & -x_1{}^9 - x_1{}^8 + x_1{}^6 - 2\,x_1{}^3 + 1\} \end{aligned}$$

- Base: The real roots of $\text{proj}(\{f_1, f_2\})$ are

$$-1,\ 0,\ \alpha \approx 0.72685,\ \beta \approx 0.78694,\ 1$$

where α is the real zero of

$$x_1{}^9 + 2\,x_1{}^7 + x_1{}^6 - 2\,x_1{}^5 - 3\,x_1{}^4 + 2\,x_1{}^3 + 2\,x_1{}^2 - 1$$

and β the real zero of

$$x_1{}^9 + x_1{}^8 - x_1{}^6 + 2\,x_1{}^3 - 1.$$

We end this example here and just show a part of the resulting CAD, see Figure 14.

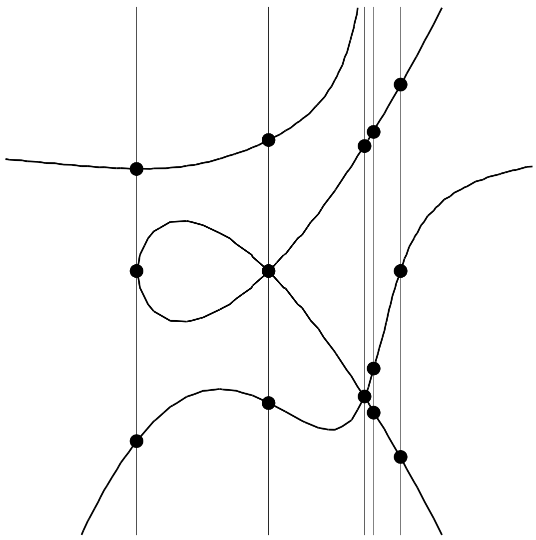

Figure 14: A part of the CAD for (4).

□

7 Conclusions

We have described an algorithm which takes a number of multivariate polynomials as input and produce a decomposition (CAD) of $\mathbb{R}^n$ as output. The decomposition has the following properties:

- The signs of the input polynomials is invariant on each component.
- It is cylindrical, i.e., a "vertical" line through an sample point, α of a lower dimensional component, C intersects the same components above and below C regardless of the choice of $\alpha \in C$.
- It is algebraic, i.e., all components may be described by a set of polynomial equations and inequalities.

The decomposition may be represented as a tree structure where the leaves corresponds to the cells of a CAD of $\mathbb{R}^n$. Given such a tree it is easy to answer questions such as: is this real polynomial system solvable or which constraints does it impose on a subset of the variables, i.e., elimination of variables. We may also treat logical combinations of real polynomial systems.

The complexity of the CAD-algorithm is very high which is not surprising since there are a huge number of problems which may be formulated as solutions to real polynomial systems.

Acknowledgement

This work was supported by the Swedish Research Council for Engineering Sciences (TFR), which is gratefully acknowledged.

References

[1] D.S. Arnon. A bibliography of quantifier elimination for real closed fields. *J. Symbolic Comput.*, 5(1-2):267–274, Feb-Apr 1988.

[2] D.S. Arnon, G.E. Collins, and S. McCallum. Cylindrical algebraic decomposition I: The basic algorithm. *SIAM J. Comput.*, 13(4):865–877, November 1984.

[3] R. Benedetti and J. Risler. *Real Algebraic and Semi-Algebraic Sets.* Hermann, Paris, 1990.

[4] J. Bochnak, M. Coste, and M-F. Roy. *Géometrie algébrique réelle.* Springer, 1987.

[5] B. Buchberger, H. Hong, R. Loos, G. Collins, J. Johnson, A. Mandache, M. Encarnacion, W. Krandick, A. Neubacher, and H. Vielhaber. Saclib 1.1 user's guide. Technical Report 93-19, RISC, Johannes Kepler University, A-4040 Linz, Austria, 1993.

[6] G.E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Second GI Conf. Automata Theory and Formal Languages, Kaiserslauten*, volume 33 of *Lecture Notes Comp. Sci.*, pages 134–183. Springer, 1975.

[7] M. Coste and M.F. Roy. Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. *J. Symbolic Computation*, 5:121–129, 1988.

[8] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer, 1992.

[9] J.H. Davenport, Y. Siret, and E. Tournier. *Computer Algebra. Systems and Algorithms for Algebraic Computation.* Academic Press, 1988.

[10] J. Hollman and L. Langemyr. Algorithms for non-linear algebraic constraints. In F. Benhamou and A. Colmerauer, editors, *Constraint Logic Programming. Selected Research*, pages 113–131. The MIT Press, 1993.

[11] H. Hong. An improvement of the projection operator in cylindrical algebraic decomposition. In *Proceedings ISAAC '90*, pages 261–264, 1990.

[12] M. Knebusch and C. Schneiderer. *Einführung in die reelle Algebra.* Vieweg, Braunschweig, 1989.

[13] D.E. Knuth. *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms.* Addison-Wesley, second edition, 1981.

[14] D. Lazard. An improved projection for cylindrical algebraic decomposition. Technical report, Informatique, Universite Paris VI, F-75252 Paris Cedex 05, France, April 1990.

[15] R. Loos. Generalized polynomial remainder sequences. In B. Buchberger, G.E. Collins, and R. Loos, editors, *Computer Algebra. Symbolic*

and Algebraic Computation, pages 115–137. Springer, second edition, 1983.

[16] S. McCallum. An improved projection operator for cylindrical algebraic decomposition of three dimensional space. *J. Symbolic Computation*, 5:141–161, 1988.

[17] B. Mishra. *Algorithmic Algebra.* Texts and Monographs in Computer Science. Springer-Verlag, 1991.

[18] A. Tarski. *A Decision Method for Elementary Algebra and Geometry.* University of California Press, second edition, 1948.