Interval Gröbner System and its Applications*

B. M.-Alizadeh
Benyamin.M.Alizadeh@gmail.com

S. Rahmany
S_Rahmani@du.ac.ir

A. Basiri
Basiri@du.ac.ir

School of Mathematics and Computer Sciences, Damghan University, Damghan, P.O. Box 36716-41167, Iran.

Abstract

In this paper, the concept of the interval Gröbner system together with an algorithm for its computation are proposed to analyze algebraic polynomial systems with interval coefficients (interval polynomial systems). These systems appear in many computational problems arising from both the engineering and mathematical sciences. As opposed to linear interval polynomial systems, there is no method to solve and/or analyze a non-linear interval polynomial system. Interval Gröbner systems enable us to determine whether an interval polynomial system has any solutions or not. If so, a finite decomposition of the solution set will be constructed by the elements of the computed interval Gröbner system. Furthermore, this concept allows us to verify whether two interval polynomial systems share a common solution or not. The concept of the interval Gröbner system is based on elimination tools on the set of interval polynomials. It is worth noting that this is not a trivial extension of usual techniques, since the set of interval polynomials does not satisfy the distributivity and additive inverse axioms of a ring with usual interval arithmetic. In doing so, we introduce the concept of the ideal family associated to an interval polynomial system which contains an infinite number of (non-interval) polynomial ideals. Then we analyze all of these ideals using an equivalence relation with a finite number of equivalence classes. This method is based on a novel computational algebraic tool, the concept of comprehensive Gröbner system, equipped with an interval-based criterion to omit unnecessary computations. We also provide some applications of

*Submitted: December 17, 2016; Revised: November 6, 2017, January 27, 2017; Accepted: June 20, 2018.

interval Gröbner systems to analyze interval polynomial systems, finding multiple roots and solving the divisibility problem of interval polynomials. Our algorithm for the computation of interval Gröbner systems has been implemented in both `Maple` and `Magma` software packages.

Keywords: Interval Polynomial System, Interval Gröbner system, Elimination Method, Gröbner Basis, Comprehensive Gröbner System, Multiple Roots, Real Factors
AMS subject classifications: 65G40, 13P10

1 Introduction

Many computational problems arising from applied sciences deal with floating-point computation and therefore need to import polynomial equations containing error terms in computers. The error terms make the polynomial equations to appear with perturbed coefficients, i.e. the coefficients range in specific intervals and thus are called *interval polynomial equations*. Interval polynomial equations come naturally from several problems in engineering sciences such as control theory [8, 34] and dynamical systems [31]. One of the most important problems in the context of interval polynomial equations is to analyze and study the stability and solutions of an (or a system of) interval polynomial(s). More generally, the problem is to gain as much information as possible from an interval polynomial system. Many scientific works in this direction use interval arithmetic [2], for instance, computation of the roots in certain cases [6, 33]; however, they do not enable us to obtain the desired roots, even approximately [6]. Another example consists of those works which contain (the most popular) method to solve an interval polynomial equation by computing the roots of some exact algebraic polynomials. However, it is hard to solve an algebraic equation of high degree which has its own challenging complexity problems [10, 12]. In [13], a method is devoted to solving an interval polynomial system by constructing two boundary systems of equality and inequalities depending on the sign of the variables to determine a decomposition on the solution set. There is also a new method described in [38] which counts the zeros of a univariate interval polynomial.

In addition to numerical methods, there are some attempts to combine numeric and symbolic methods to solve an interval polynomial system. In [9], Falai et al. state a modification of Wu's characteristic set method for interval polynomial systems, and use numerical approximation to find an interval containing the roots. The essential strategy in this work is to omit all the terms with interval coefficients containing zero, which simply permits the division of interval coefficients. This consideration may cause the lose of some important polynomials.

In this paper, we try to use exact symbolic methods to facilitate analyzing interval polynomial systems. It is worth noting that, in some published texts such as [16, 17], it has been attempted to approximate the solution set of a polynomial system by presenting an interval box containing the solution set. These methods are devoted to solving a polynomial system in the usual sense (with non-interval coefficients) and thus differ from our method which is focused on polynomial systems with interval coefficients. In our proposed method, it is very important to keep trace of interval coefficients during computations. Roughly speaking, we associate an auxiliary parameter to each interval coefficient provided that each parameter ranges over its own related interval only. Nowadays there are important results [36, 35], efficient algorithms [20, 21, 23, 24, 25, 27, 28] and powerful implementations in the context of parametric computations and analyzing parametric polynomial systems. We introduce the new concept *interval Gröbner system* for a system of interval polynomials using the concept of *comprehensive Gröbner system* [35] which is used to describe all different behaviors of a parametric polynomial system. An interval Gröbner system contains a finite number of systems where each one is a Gröbner basis for (non-interval) polynomial systems obtained from the main system. It is worth noting that unlike [9], we do not omit any interval coefficient and cover all possible cases for the exact coefficients arising from the intervals. Using an interval Gröbner system of an interval polynomial system, one can verify in a simple way whether the system has any solution or not, and if so, find all the solutions. Furthermore, it enables us to compute the common solutions of two interval polynomial systems. We design also an algorithm to compute an interval Gröbner system for an interval polynomial system. Our algorithm has been implemented in `Maple` software which involves all the criteria and techniques that are explained in this paper. Also, we have implemented this algorithm in the `Magma` computer algebra system, but this implementation does not contain some of the techniques [1].

This paper is organized as follows. In Section 2 we state introductory definitions and review interval arithmetic. In Section 3 we explain interval polynomials and their related concepts. Section 4 states the main idea behind the paper. To review the concepts of computational algebraic tools we present Section 5 which contains a brief introduction to the concept of the Gröbner basis and the comprehensive Gröbner system, together with their related algorithms. Subsequently, we describe our elimination method for interval polynomial systems in Section 6. Finally, in Section 7, we describe some applications of the interval Gröbner system.

2 Preliminaries

In this section we present the interval arithmetic and related concepts which are needed for the rest of this text. The main references of this section are [19] and [29]. Let $\mathbb{R}$ denote the set of real numbers while $\mathbb{R}^*$ is used to show the *extended real numbers set* i.e. $\mathbb{R} \cup \{-\infty, \infty\}$.

Definition 1 *Let $a, b \in \mathbb{R}^*$. We define four kinds of real intervals defined by a and b as follows:*

$$\begin{array}{l}\text{Closed interval}: \ [a,b] = \{x \mid a \leq x \leq b\} \ (a, b \neq \pm\infty) \\ \text{Left half open interval}: \ (a,b] = \{x \mid a < x \leq b\} \ (b \neq \pm\infty) \\ \text{Right half open interval}: \ [a,b) = \{x \mid a \leq x < b\} \ (a \neq \pm\infty) \\ \text{Open interval}: \ (a,b) = \{x \mid a < x < b\}\end{array} \tag{1}$$

The set of all real intervals is denoted by $[\mathbb{R}]$.

It should be said that approximately all existing texts on the subject of interval computation deal with closed intervals. In must cases, closed intervals are denoted by capitals and their lower (resp. upper) bounds by underbars (resp. overbars), as

$$X = [\underline{X}, \overline{X}].$$

However, as there are some practical problems including non-closed intervals we consider all different types of intervals.

[1] These implementations are available at `http://faculty.du.ac.ir/rahmani/softwares/`.

Remark 2.1 *Having all different kinds of intervals at once, we use the notion* $[a, b, i, j]$ *where* $i, j \in \{0, 1\}$ *to denote the intervals in (1), as follows,*

$$[a,b,i,j] = \begin{cases} [a,b] & \text{if} \quad i=j=1 \\ (a,b] & \text{if} \quad i=0, j=1 \\ [a,b) & \text{if} \quad i=1, j=0 \\ (a,b) & \text{if} \quad i=j=0 \end{cases}$$

However when all intervals come from one sort of presentation, we prefer to use the form in (1).

Now we review the interval arithmetic and discuss the interval dependencies that will occur in the evaluation of interval expressions.

Definition 2 *Suppose that* A *and* B *are two intervals, which are considered as two sets of real numbers. Four essential arithmetic operations on* A *and* B *are defined as*

$$A \; op \; B = \{a \; op \; b \;\mid\; a \in A, \; b \in B\},$$

where $op \in \{+, -, \times, /\}$.

As a consequence of the above definition, we can also define interval arithmetic when the intervals are shown by their bounds. Let $[a_1, b_1, i_1, j_1]$ and $[a_2, b_2, i_2, j_2]$ be two real intervals. Note that each real number a is considered as $[a, a, 1, 1]$ which is called a degenerate interval. Four essential arithmetic operations are defined as follows,

$$\begin{aligned} [a_1,b_1,i_1,j_1] + [a_2,b_2,i_2,j_2] &= [a_1+a_2, b_1+b_2, \min(i_1,i_2), \min(j_1,j_2)] \\ [a_1,b_1,i_1,j_1] - [a_2,b_2,i_2,j_2] &= [a_1-b_2, b_1-a_2, \min(i_1,j_2), \min(j_1,i_2)] \\ [a_1,b_1,i_1,j_1] \times [a_2,b_2,i_2,j_2] &= [a_k b_\ell, a_{k'} b_{\ell'}, \min(i_k,j_\ell), \min(i_{k'},j_{\ell'})], \end{aligned}$$

where $a_k b_\ell$ and $a_{k'} b_{\ell'}$ are the minimum and maximum of the set $\{a_1a_2, a_1b_2, b_1a_2, b_1b_2\}$ respectively, and finally

$$[a_1,b_1,i_1,j_1]/[a_2,b_2,i_2,j_2] = [a_1,b_1,i_1,j_1] \times [1/b_2, 1/a_2, j_2, i_2],$$

provided that $a_2 > 0$ or $b_2 < 0$ or $a_2 = i_2 = 0$ or $b_2 = j_2 = 0$. Note in the above relations that all ambiguous cases $\infty - \infty$, $\pm\infty \times 0$, $\frac{\pm\infty}{\pm\infty}$ and $\frac{0}{0}$ will induce the biggest possible interval i.e. $\mathbb{R}$.

As an easy observation, when an interval $X = [a, b, i, j]$ with $a \neq b$ contains zero, we can compute $1/X$ as follows,

- If $a = 0$ then
$$\frac{1}{X} = \frac{1}{[a,b,0,j]} = [\frac{1}{b}, +\infty, j, 0],$$
- If $b = 0$ then
$$\frac{1}{X} = \frac{1}{[a,b,i,0]} = [-\infty, \frac{1}{a}, 0, i],$$
- If $ab < 0$ then by seperating X as $X = [a, 0, i, 0] \cup [0, b, 0, j]$ we have
$$\frac{1}{X} \quad = \quad \frac{1}{[a,0,i,0] \cup [0,b,0,j]} = [-\infty, \frac{1}{a}, 0, i] \cup [\frac{1}{b}, +\infty, j, 0].$$

Remark 2.2 *Although interval arithmetic seems to be compatible with real numbers arithmetic, but this affects the distributivity of multiplication over addition and the existence of inverse elements. More precisely, if* X, Y *and* Z *are three intervals then*

- $X \times (Y + Z) \subseteq X \times Y + X \times Z$,
  and if X *is non-degenerated then*
- $X \times \frac{1}{X} \neq 1$, *but* $1 \in X \times \frac{1}{X}$ *and*
- $X + (-X) \neq 0$, *but* $0 \in X + (-X)$.

Furthermore, if X *contains some negative real numbers, then*

$$X^n = \{x^n \mid x \in X\} \neq \underbrace{X \times \cdots \times X}_{n \ times}.$$

To see this, let for instance $X = [a, b, i, j]$ *where* $a < 0$ *and* $|a| < b$. *Then,* $X^2 = [0, b^2, 1, j]$ *while* $X \times X = [ab, b^2, \min(i, j), j]$. *To solve this inconsistency, we define the n'th power of an interval for each non-negative integer* n *as follows,*

$$[a, b, i, j]^n = \begin{cases} 1 & n = 0 \\ [a^n, b^n, i, j] & 0 \leq a \\ [b^n, a^n, j, i] & b \leq 0 \\ [0, \max(a^n, b^n), 1, c] & a < 0 < b \end{cases}$$

where $c = \begin{cases} i & |b| < |a| \\ j & otherwise. \end{cases}$

Let us now evaluate some expressions to illustrate more challenging problems dealing with interval arithmetic. Let $f(x, y) = \frac{x}{x+y}$, $X = [1, 2]$ and $Y = [1, 3]$. We compute $f(X, Y)$ in two ways. The first is to compute $f(X, Y)$ as a usual evaluation using interval arithmetic:

$$\frac{X}{X + Y} = [1/5, 1]. \tag{2}$$

However, one can manipulate the expression to see

$$\frac{X}{X + Y} \quad = \quad \frac{1}{1 + \frac{Y}{X}} = [1/4, 2/3]. \tag{3}$$

Let us separate x and y first depending on $f(x, y)$: we call y (resp. x), a *first* (resp. *second*) *class* variable of f if it appears one (resp. more than one) time(s) in the structure of f. As is obvious, the answer of (3) is a narrower interval and in fact the exact value. The reason is that X is a second class variable for (2) and so it brings *dependency* between two parts of the expression. This is while there is no dependency in (3) given that $\frac{Y}{X}$ appears only one time, and so it is a first class variable. Dependency is one of the crucial points of this paper in finding the solution set of interval polynomial systems. Dependency is the main reason that causes the appearance of an amount of error by introducing larger intervals than the exact solution. Nevertheless, it is possible to cancel dependencies by considering $X - X = 0$ as well as $X/X = 1$ easily, while sometimes this becomes difficult (see [19] for more details) .

3 Interval Polynomials

Let $\mathbb{R}$ be the field of real numbers, considered as the ground field of computations throughout the current text and let the set $\{x_1, \ldots, x_n\}$ be the set of variables.

Definition 3 *Each polynomial of the form*

$$[f] = \sum_{i=1}^{m} [a_i, b_i, \ell_i, k_i] x_1^{\alpha_{i1}} \cdots x_n^{\alpha_{in}}, \tag{4}$$

is called an interval polynomial, where $[a_i, b_i, \ell_i, k_i]$ *is a real interval for each* $i = 1, \ldots, m$*, and each power product* $x_1^{\alpha_{i1}} \cdots x_n^{\alpha_{in}}$ *is called a monomial where the powers are non negative integers. We denote the set of all interval polynomials by*

$$[\mathbb{R}][x_1, \ldots, x_n].$$

Definition 4 *Let* $[f]$ *be an interval polynomial as defined in (4). The set of all polynomials arising from* $[f]$ *for different values of intervals in coefficients is called the family of* $[f]$ *and is denoted by* $\mathcal{F}([f])$*. More preciesly:*

$$\mathcal{F}([f]) = \{\sum_{i=1}^{m} c_i x_1^{\alpha_{i1}} \cdots x_n^{\alpha_{in}} \mid c_i \in [a_i, b_i, \ell_i, k_i], i = 1, \ldots, m\}.$$

Similar to the family of an interval polynomial, we can define the family of a set of interval polynomials as follows:

Definition 5 *Let* $S = \{[f]_1, \ldots, [f]_\ell\}$ *be a set of interval polynomials with* $\mathcal{F}([f]_j) = \mathcal{F}_j$ *for each* $j = 1, \ldots, \ell$*. We define the family of* S *to be the set* $\mathcal{F}_1 \times \cdots \times \mathcal{F}_\ell$*, denoted by* $\mathcal{F}(S)$*.*

We now define the concept of the solution set of an interval polynomial.

Definition 6 *For an interval polynomial* $[f] \in [\mathbb{R}][x_1, \ldots, x_n]$*, we say that* $r \in \mathbb{R}^n$ *is a real solution or a real root of* $[f]$*, if there exists a polynomial* $p \in \mathcal{F}([f])$ *such that* $p(r) = 0$*. Similarly, we say that a system* $S = \{[f]_1, \ldots, [f]_\ell\}$ *of interval polynomials has a solution, if there exists* $r \in \mathbb{R}^n$ *such that for each* $i = 1, \ldots, \ell$*,* r *is a root of* $[f]_i$*.*

Example 3.1 *Let us find the solution set of*

$$[-2, -1]x^2 + [1, 5]x + [3, 6] = 0$$

where all intervals are closed. When $x \geq 0$*, we have*

$$[-2, -1]x^2 + [1, 5]x + [3, 6] = [-2x^2 + x + 3, -x^2 + 5x + 6],$$

So we must have

$$0 \leq -x^2 + 5x + 6 \text{ and } -2x^2 + x + 3 \leq 0,$$

which implies that

$$x = -1.$$

Similarly when $x \leq 0$*, we have*

$$[-2, -1]x^2 + [1, 5]x + [3, 6] = [-2x^2 + 5x + 3, -x^2 + x + 6],$$

which concludes

$$x = 3$$

Thus the solution set of this interval polynomial is

$$\{-1, 3\}$$

It is notable that using interval arithmetic in the well-known method of calculating the roots of a quadratic polynomial equation due to the discriminant, we attain

$$[-3.77, 0.70] \cup [1.15, 6.77].$$

However, this solution set contains an amount of error, due to dependencies occurring in the discriminant.

4 The Idea

In this section we describe some problems which may occur when using an elimination method on a system of interval polynomials. To facilitate the description, let us give an example of a linear interval polynomial system. It is worth noting that, as the main elimination method for a system of linear interval polynomials, one can use the interval Gaussian elimination method described in [1, 37]. As explained in the ongoing example, we impose only one simple linear operation which is of course a part of interval Gaussian elimination method. Consider the system

$$\begin{cases} f_1 = [1,2]x_1 + x_2 + 2x_3, \\ f_2 = [1,4]x_1 + x_2 + 1, \\ f_3 = [3,4]x_1 + x_2 + 4x_3. \end{cases}$$

By eliminating the variable x_2, we have

$$\begin{cases} f_1 - f_2 = [-3,1]x_1 + 2x_3 - 1, \\ f_3 - f_2 = [-1,3]x_1 + 4x_3 - 1 \end{cases}$$

Now, if we choose 0 from both intervals $[-3, 1]$ and $[-1, 3]$, it will be concluded that the system has no solution because $2x_3 - 1 = 4x_3 - 1 = 0$.

However, this case is impossible since both the intervals $[-3, 1]$ and $[-1, 3]$ can not be zero at once. To see this, notice that $[-3, 1]$ comes from $[1, 2] - [1, 4]$ and so for $[-3, 1]$ to be zero, $[1, 4]$ must give some values in $[1, 2]$. On the other hand, $[-1, 3]$ comes from $[3, 4] - [1, 4]$ and so this interval can be zero only when $[1, 4]$ gives some values in $[3, 4]$ and this is a contradiction. This simple linear system shows that the usual elimination method can result in a wrong conclusion or the appearance of some extra values in the solution set. The main reason is that we forgot the dependencies between $[-3, 1]$ and $[-1, 3]$ during the computation while they are both dependent on $[1, 4]$ and thus they are dependent on each other.

To solve this problem, we must keep trace of each interval coefficient. In doing so, our idea is to use a parameter instead of each interval, to see how new coefficients are built. For instance, let us substitute $[1, 2]$, $[1, 4]$ and $[3, 4]$ with a, b and c as parameters in the above example. So we have

$$\begin{cases} \tilde{f}_1 = ax_1 + x_2 + 2x_3, \\ \tilde{f}_2 = bx_1 + x_2 + 1, \\ \tilde{f}_3 = cx_1 + x_2 + 4x_3. \end{cases}$$

and applying the elimination steps we observe

$$\begin{cases} \tilde{f}_1 - \tilde{f}_2 = (a-b)x_1 + 2x_3 - 1, \\ \tilde{f}_3 - \tilde{f}_2 = (c-b)x_1 + 4x_3 - 1. \end{cases}$$

Now one can conclude that under the assumption that $a-b=0$, the coefficient $c-b$ can not be zero. The reason is that if $c-b=0$ then $a=c$ while $1 \leq a \leq 2$ and $3 \leq c \leq 4$. Therefore, using parameters in the mentioned manner, prevents us reaching wrong conclusions regarding the solution set.

The main question here, is how to use the elimination method when the coefficients contain a number of parameters. In fact, as we will state in the following sections, we carry out the elimination steps thanks to the method of the Gröbner basis and for the parametric case, we use the concept of the comprehensive Gröbner system, to see the simplest possible polynomials to solve. Thus, our idea is to convert each interval polynomial system into a parametric polynomial system and use the parametric algorithmic aspects, with some modifications, to solve the parametric system by dividing the solution set into a finite number of components. Finally, we convert the result to see the solution set of the interval polynomial system.

5 Gröbner Bases and Comprehensive Gröbner Systems

In this section we review the concepts and notations of ordinary and parametric polynomial rings. Let K be a field and $x_1, \ldots, x_n$ be n (algebraically independent) variables. Each power product $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is called a monomial where $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_{\geq 0}$. For simplicity, we abbreviate such monomials by $\mathbf{x}^\alpha$ where $\mathbf{x}$ is used for the sequence $x_1, \ldots, x_n$ and $\alpha = (\alpha_1, \ldots, \alpha_n)$. We can sort the set of all monomials over K by special types of total orderings, the so called monomial orderings, given in the following definition.

Definition 7 *The total ordering $\prec$ on the set of monomials is called a monomial ordering whenever for each monomials $\mathbf{x}^\alpha, \mathbf{x}^\beta$ and $\mathbf{x}^\gamma$ we have:*

- $\mathbf{x}^\alpha \prec \mathbf{x}^\beta \Rightarrow \mathbf{x}^\gamma \mathbf{x}^\alpha \prec \mathbf{x}^\gamma \mathbf{x}^\beta$*, and*
- $\prec$ *is well-ordering.*

There are an infinite number of monomial orderings, each one is convenient for a special type of problem. Among them, we point to pure and graded-reverse lexicographic orderings denoted by $\prec_{lex}$ and $\prec_{grevlex}$ as follows. Assume that $x_n \prec \cdots \prec x_1$. We say that

- $\mathbf{x}^\alpha \prec_{lex} \mathbf{x}^\beta$ whenever
$$\alpha_1 = \beta_1, \ldots, \alpha_i = \beta_i \text{ and } \alpha_{i+1} < \beta_{i+1},$$
for an integer $1 \leq i < n$.
- $\mathbf{x}^\alpha \prec_{grevlex} \mathbf{x}^\beta$ if
$$\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i,$$
breaking ties when there exists an integer $1 \leq i < n$ such that
$$\alpha_n = \beta_n, \ldots, \alpha_{n-i} = \beta_{n-i} \text{ and } \alpha_{n-i-1} > \beta_{n-i-1}.$$

It is worth noting that the former has much theoretical importance while the latter speeds up the computations and carries less information out.

Each $K-$linear combination of monomials is called a polynomial on $x_1, \ldots, x_n$ over K. The set of all polynomials has a ring structure with the usual polynomial addition and multiplication, and is called the polynomial ring on $x_1, \ldots, x_n$ over K and denoted by $K[x_1, \ldots, x_n]$ or just by $K[\mathbf{x}]$. Let f be a polynomial and $\prec$ be a monomial ordering. The greatest monomial w.r.t. $\prec$ contained in f is called the leading monomial of f, denoted by $\mathrm{LM}(f)$ and the coefficient of $\mathrm{LM}(f)$ is called the leading coefficient of f which is shown by $\mathrm{LC}(f)$. Further, if F is a set of polynomials, $\mathrm{LM}(F)$ is defined to be $\{\mathrm{LM}(f) | f \in F\}$ and if I is an ideal, $in(I)$ is the ideal generated by $\mathrm{LM}(I)$ and is called the initial ideal of I. Now, we state the concept of the Gröbner basis of a polynomial ideal which provides much useful information about the ideal.

Definition 8 *Let I be a polynomial ideal of $K[\mathbf{x}]$ and $\prec$ be a monomial ordering. A finite set $G \subset I$ is called a Gröbner basis of I if for each non zero polynomial $f \in I$, $\mathrm{LM}(f)$ is divisible by $\mathrm{LM}(g)$ for some $g \in G$.*

Using the well-known Hilbert basis theorem (See [4] for example), it is proved that each polynomial ideal possesses a Gröbner basis with respect to each monomial ordering. There are efficient algorithms also to compute a Gröbner basis. The first and simplest one is the Buchberger algorithm presented simultaneously with the introduction of the Gröbner basis concept while the most efficient known algorithms are Faugère's F_5 algorithm [11], $\mathrm{G}^2\mathrm{V}$ [14] and GVW [15]. As a witness of the efficiency of these algorithms, we refer to [5] for instance, where the F_5 algorithm is used to cryptanalyze the HFE system. Also, a full discussion on the complexity of signature-based algorithms is given in [3].
It should be said that a polynomial ideal has not a unique Gröbner basis. To have unicity, we define the reduced Gröbner basis concept. As an important fact, the reduced Gröbner basis of an ideal is unique up to the monomial ordering.

Definition 9 *Let G be a Gröbner basis for the ideal I w.r.t. $\prec$. Then G is called the reduced Gröbner basis of I whenever each $g \in G$ is monic, i.e. $\mathrm{LC}(g) = 1$ and none of the monomials appearing in g is divisible by $\mathrm{LM}(h)$ for each $h \in G \setminus \{g\}$.*

One of the most important applications of Gröbner basis is its role in solving a polynomial system. Let

$$\left\{ \begin{array}{lcl} f_1 & = & 0 \\ & \vdots & \\ f_k & = & 0, \end{array} \right.$$

be a polynomial system and $I = \langle f_1, \ldots, f_k \rangle$ be the ideal generated by $f_1, \ldots, f_k$. We define the affine variety associated to the above system or equivalently to the ideal I to be

$$\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_k) = \{\alpha \in \overline{K}^n | f_1(\alpha) = \cdots = f_k(\alpha) = 0\},$$

where $\overline{K}$ is used to denote the algebraic closure of K. Now let G be a Gröbner basis for I with respect to an arbitrary monomial ordering. Interestingly, $I = \langle G \rangle$ which implies that $\mathbf{V}(I) = \mathbf{V}(G)$. This is the key computational technique to solve a polynomial system. Let us continue with an example.

Example 5.1 *We will solve the following polynomial system,*

$$\left\{ \begin{array}{ccc} x^2 - xyz + 1 & = & 0 \\ y^3 + z^2 - 1 & = & \\ xy^2 + z^2 & = & 0 \end{array} \right.$$

Due to the properties of pure lexicographical ordering, the reduced Gröbner basis of the ideal $I = \langle x^2 - xyz + 1, y^3 + z^2 - 1, xy^2 + z^2\rangle \subset \mathbb{Q}[x, y, z]$ has the form

$$G = \{g_1(z), x - g_2(z), y - g_3(z)\},$$

w.r.t. $z \prec_{lex} y \prec_{lex} x$, where

$$\begin{cases} g_1(z) &=& z^{15} - 3z^{14} + 5z^{12} - 3z^{10} - z^9 - z^8 + 4z^6 \\ && -6z^4 + 4z^2 - 1 \\ g_2(z) &=& 2z^{14} - 9z^{13} + 11z^{12} + 2z^{11} - 7z^{10} - 3z^9 \\ && +2z^8 - z^7 + 4z^6 + 7z^5 - 10z^4 - 6z^3 \\ && +11z^2 + 2z - 4 \\ g_3(z) &=& z^{13} - 3z^{12} + z^{11} + 2z^{10} + z^9 - z^8 - 2z^6 \\ && +2z^4 - z^3 - 3z^2 + 1. \end{cases}$$

This special form of this Gröbner basis for the system allows us to find $\mathbf{V}(G)$ by solving only one univariate polynomial $g_1(z)$ and putting the roots into the two last polynomials in G.

Suppose now that the same system of Example 5.1 is given as follows with parametric coefficients, where the parameters are a, b and c:

$$\begin{cases} ax^2 - (a^2 - b + 1)xyz + 1 &=& 0 \\ y^3 + c^2z^2 - 1 &=& \\ (a + b + c)xy^2 + z^2 &=& 0 \end{cases}$$

The solutions of this system depend on the values of the parameters; as can be seen the system has no solutions whenever $a = 0$ and $b = 1$ while it converts to the system of Example 5.1 for $a = 1, b = 1$ and $c = -1$ whereby it has a number of solutions. To manage all the different behaviors of the parameters which cause difference in the behavior of the main system, we recall the concept of the comprehensive Gröbner system in the sequel. By this, we can divide the space of the parameters, i.e. $\overline{K}^t$ into a finite number of partitions, for which the general form of the polynomials in the assigned Gröbner basis is determined.

Let K be a field and $\mathbf{a} := a_1, \ldots, a_t$ and $\mathbf{x} := x_1, \ldots, x_n$ be the sequences of parameters and variables respectively. We call $K[\mathbf{a}][\mathbf{x}]$, the parametric polynomial ring over K, with parameters $\mathbf{a}$ and variables $\mathbf{x}$. This ring is in fact the set of all parametric polynomials as

$$\sum_{i=1}^{m} p_i \mathbf{x}^{\alpha_i}$$

where $p_i \in K[\mathbf{a}]$ is a polynomial on $\mathbf{a}$ with coefficients in K, for each i.

Definition 10 *Let $I \subset K[\mathbf{a}][\mathbf{x}]$ be a parametric ideal and $\prec$ be a monomial ordering on $\mathbf{x}$. Then the set*

$$\mathcal{G}(I) = \{(E_i, N_i, G_i) \mid i = 1, \ldots, \ell\} \subset K[\mathbf{a}] \times K[\mathbf{a}] \times K[\mathbf{a}][\mathbf{x}]$$

is called a comprehensive Gröbner system for I if for each $(\lambda_1, \ldots, \lambda_t) \in \overline{K}^t$ and each specialization

$$\begin{array}{rccc} \sigma_{(\lambda_1,\ldots,\lambda_t)}: & K[\mathbf{a}][\mathbf{x}] & \to & \overline{K}[\mathbf{x}] \\ & \sum_{i=1}^{m} p_i \mathbf{x}^{\alpha_i} & \mapsto & \displaystyle\sum_{i=1}^{m} p_i(\lambda_1, \ldots, \lambda_t)\mathbf{x}^{\alpha_i} \end{array}$$

there exists an $1 \le i \le \ell$ *such that* $(\lambda_1, \ldots, \lambda_t) \in \mathbf{V}(E_i) \setminus \mathbf{V}(N_i)$ *and* $\sigma_{(\lambda_1,\ldots,\lambda_t)}(G_i)$ *is a Gröbner basis for* $\sigma_{(\lambda_1,\ldots,\lambda_t)}(I)$ *with respect to* $\prec$*. For simplicity, we call* E_i *and* N_i *the null and non-null conditions respectively.*

See that, by [35, Theorem 2.7], every parametric ideal has a comprehensive Gröbner system. Now we give an example from [24] to illustrate the definition of the comprehensive Gröbner system.

Example 5.2 *Consider the following parametric polynomial system in* $\mathbf{Q}[a, b, c][x, y]$*:*

$$\Sigma : \begin{cases} ax - b & = & 0 \\ by - a & = & 0 \\ cx^2 - y & = & 0 \\ cy^2 - x & = & 0 \end{cases}$$

Choosing the graded reverse lexicographical ordering $y \prec x$*, we have the following comprehensive Gröbner system: For instance, for the specialization* $\sigma_{(1,1,1)}$ *for which*

G_i	E_i	N_i
$\{1\}$	$\{\ \}$	$\{a^6 - b^6, a^3c - b^3, b^3c - a^3, ac^2 - a, bc^2 - b\}$
$\{bx - acy, by - a\}$	$\{a^6 - b^6, a^3c - b^3, b^3c - a^3, ac^2 - a, bc^2 - b\}$	$\{b\}$
$\{cx^2 - y, cy^2 - x\}$	$\{a, b\}$	$\{c\}$
$\{x, y\}$	$\{a, b, c\}$	$\{\ \}$

Table 1: An example of a comprehensive Gröbner system.

$a \mapsto 1, b \mapsto 1$ *and* $c \mapsto 1$*,*

$$\sigma_{(1,1,1)}(\{bx - acy, by - a\}) = \{x - y, y - 1\}$$

is a Gröbner basis of $\sigma_{(1,1,1)}(\langle\Sigma\rangle)$*.*

It is worth noting that if $\mathbf{V}(E_i) \setminus \mathbf{V}(N_i) = \emptyset$ for some i, then the triple (E_i, N_i, G_i) is useless, and must be omitted from the computed comprehensive Gröbner system. In this case we say that the pair (E_i, N_i) is *inconsistent*. It is easy to see that inconsistency occurs if and only if $N_i \subset \sqrt{\langle E_i \rangle}$ and we need an efficient radical membership test to determine inconsistencies. In [23, 24] there is a new and efficient algorithm to compute a comprehensive Gröbner system of a parametric polynomial ideal which uses a new and powerful radical membership criterion. Therefore, we prefer to employ this algorithm, the so called PGB algorithm, in our computations. Another essential technique which is used in [24] is the usage of the *minimal Dickson basis* which reduces the extent of computations in PGB. Before explaining it, let us recall some notations which are used in the structure of PGB. Let $\prec_{\mathbf{x}}$ and $\prec_{\mathbf{a}}$ be two monomial orderings on $K[\mathbf{x}]$ and $K[\mathbf{a}]$ respectively. Let also $\prec_{\mathbf{x},\mathbf{a}}$ be the block ordering of $\prec_{\mathbf{x}}$ and $\prec_{\mathbf{a}}$, comparing two parametric monomials by $\prec_{\mathbf{x}}$, breaking the tie by $\prec_{\mathbf{a}}$. For a parametric polynomial $f \in K[\mathbf{a}][\mathbf{x}]$, we denote by $\mathrm{LM}_{\mathbf{x}}(f)$ (resp. by $\mathrm{LC}_{\mathbf{x}}(f)$) the leading monomial (resp. the leading coefficient) of f when it is considered as a polynomial in $K[\mathbf{a}][\mathbf{x}]$, and thus $\mathrm{LC}_{\mathbf{x}}(f) \in K[\mathbf{a}]$.

Definition 11 *By the above notations, let $P \subset K[\mathbf{a}][\mathbf{x}]$ be a set of parametric polynomials and $G \subset P$. Then, G is called a minimal Dickson basis of P denoted by $MDBasis(P)$, if:*

- *For each $p \in P$, there exists some $g \in G$ such that $\mathrm{LM}_{\mathbf{x}}(g) \mid \mathrm{LM}_{\mathbf{x}}(p)$ and,*
- *For each two distinct polynomials in G as g_1 and g_2, neither of the $\mathrm{LM}_{\mathbf{x}}(g_1)$ and $\mathrm{LM}_{\mathbf{x}}(g_2)$ divides the other.*

In PGB, we need to compute a minimal Dickson basis for P only when P is a Gröbner basis for $\langle P \rangle$ itself w.r.t. $\prec_{\mathbf{x},\mathbf{a}}$ and $P \cap K[\mathbf{a}] = \{0\}$. In this situation, it suffices by Definition 11 to omit all polynomials p from P for which there exists a $p' \in P$ such that $\mathrm{LM}_{\mathbf{x}}(p') \mid \mathrm{LM}_{\mathbf{x}}(p)$.

The PGB algorithm, as shown below, uses the PGB-MAIN algorithm to introduce new branches in computations.

Algorithm 1 PGB

procedure PGB($P, \prec_{\mathbf{a}}, \prec_{\mathbf{x}}$)
  $E, N := \{\ \}, \{1\}$;
  $\prec_{\mathbf{x},\mathbf{a}}$:=The block ordering of $\prec_{\mathbf{x}}, \prec_{\mathbf{a}}$
  Return PGB-MAIN($P, E, N, \prec_{\mathbf{x},\mathbf{a}}$);
end procedure

The main work of PGB-MAIN is to create all necessary branches and import them in the comprehensive Gröbner system at output. In this algorithm $A * B$ is defined to be the set $\{ab \mid a \in A, b \in B\}$.

Algorithm 2 PGB-MAIN

procedure PGB-MAIN($P, E, N, \prec_{\mathbf{x},\mathbf{a}}$)
  $G :=$ The reduced Gröbner basis for $P \cup E$ w.r.t. $\prec_{\mathbf{a},\mathbf{x}}$;
  if $1 \in G$ **then**
    Return $(E, N, \{1\})$;
  end if
  $G_r := G \cap K[\mathbf{a}]$;
  if IsConsistent($E, N * G_r$) **then**
    $PGB := \{(E, N * G_r, \{1\})\}$;
  else
    $PGB := \emptyset$;
  end if
  if IsConsistent(G_r, N) **then**
    $G_m :=$MDBasis($G \setminus G_r$);
  else
    Return (PGB);
  end if
  $h := \mathrm{lcm}(h_1, \ldots, h_k)$, where $h_i = \mathrm{LC}_{\mathbf{x}}(g_i)$ and $g_i \in G_m$;
  if IsConsistent($G_r, N * \{h\}$) **then**
    $PGB := PGB \cup \{(G_r, N * \{h\}, G_m)\}$;
  end if
  for $i = 1, \ldots, k$ **do**
    $PGB := PGB \cup$ PGB-MAIN($G \setminus G_r, G_r \cup \{h_i\}, N * \{\prod_{j=1}^{i-1} h_j\}, \prec_{\mathbf{a},\mathbf{x}}$)
  end for
end procedure

As is shown in the algorithm, it first computes a Gröbner basis of the ideal $\langle P \rangle$ over $K[\mathbf{a}, \mathbf{x}]$ i.e. G, before performing any branches based on parametric constraints [24, Lemma 3.2]. After this, the algorithm computes a minimal Dickson basis i.e. G_m and continues by making a decision for each situation in which one of the leading coeffiecients of G_m is zero. By this, PGB-MAIN constructs all necessary branches to import in the comprehensive Gröbner system at output. Throughout the algorithm, when a new branch (E_i, N_i, G_i) is needed in the system, the algorithm IsConsistent is used as follows to test the consistency of parametric conditions (E_i, N_i).

Algorithm 3 IsConsistent

procedure IsConsistent(E, N)
  $flag :=$false;
  for $g \in N$ **while** $flag =$false **do**
    if $g \notin \sqrt{\langle E \rangle}$ **then**
      $flag :=$true;
    end if
  end for
  Return $flag$;
end procedure

The main part of this algorithm is the radical membership test. The powerful technique which is used in [23, 24] for the radical membership check is based on linear algebra methods accompanied with a probabilistic check. We refer the reader to [24, Section 5] for more details.

6 Interval Gröbner System

In this section we introduce the new concept of *interval Gröbner system* and its related definitions and statements. Let us state first, the following proposition as an immediate consequence of Definition 6. Recall that for a polynomial system $S \subset \mathbb{R}[x_1, \ldots, x_n]$ the variety of S is the set of all complex solutions of S, denoted by $\mathbf{V}(S)$.

Definition 12 *Let $[S] \subset [\mathbb{R}][x_1, \ldots, x_n]$. Then, the interval polynomial system $[S]$ has a solution if there exists a polynomial system S in $\mathcal{F}([S])$ such that $\mathbf{V}(S) \cap \mathbb{R}^n \neq \emptyset$.*

It is worth noting that, in the case of (non-interval) polynomial systems, there is an efficient criterion due to the well-known Hilbert Nullestelensatz theorem which determines the emptiness of $\mathbf{V}(S)$ by applying the reduced Gröbner basis: $\mathbf{V}(S) \neq \emptyset$ if and only if the reduced Gröbner basis of $\langle S \rangle$ with respect to an arbitrary monomial ordering does not contain 1. However, this is not the case for the interval polynomial systems due to Definition 12, because of two main difficulties: first, we can not define the concept of the Gröbner basis in $[\mathbb{R}][x_1, \ldots, x_n]$ as it is not a polynomial ring and second, the solutions of an interval polynomial system are real points while the elements of the variety may be purely complex. The following theorem states the modified version of the Hilbert Nullestelensatz theorem for interval polynomial systems:

Theorem 6.1 *(Interval Hilbert Nullestelensatz)*
Let $[S] \subset [\mathbb{R}][x_1, \ldots, x_n]$. Then, the interval polynomial system $[S]$ has a solution if and only if there exists a polynomial system S in $\mathcal{F}([S])$ such that for G, the reduced Gröbner basis of $\langle S \rangle$ with respect to an arbitrary monomial ordering, $\mathbf{V}(G) \cap \mathbb{R}^n \neq \emptyset$.

Proof: First, from $\mathbf{V}(G) \cap \mathbb{R}^n \neq \emptyset$ it is concluded that $1 \notin G$. It is easy to see by Definition 6 that $r \in \mathbb{R}^n$ is a solution of $[S]$ if and only if there exists a polynomial system $S \in \mathcal{F}([S])$ for which $r \in \mathbf{V}(S)$. Therefore, by the Hilbert Nullestelensatz theorem, r is a solution of $[S]$ if and only if $1 \notin G$ and also $\mathbf{V}(G) \cap \mathbb{R}^n \neq \emptyset$, where G is the reduced Gröbner basis of $\langle S \rangle$ with respect to an arbitrary monomial ordering, for at least one $S \in \mathcal{F}([S])$. $\square$

Remark 6.2 *It is worth noting in the above theorem that, from the theoretical point of view, it is sufficient that $\mathbf{V}(G) \cap \mathbb{R}^n \neq \emptyset$. However, from the algorithmic point of view, it is easier to check first if $1 \in G$. In the affirmative case, it is concluded by the Hilbert Nullestelensatz theorem that the system has no solution. Else, it is necessary to check whether $\mathbf{V}(G) \cap \mathbb{R}^n \neq \emptyset$ or not.*

Note that there are an infinite number of polynomial systems in $\mathcal{F}([S])$ for an interval polynomial system $[S]$ and so it is practically impossible to check all of them by the Interval Hilbert Nullestelensatz theorem. Nevertheless, we give a finite partition on the set of all polynomial systems arising from $[S]$ using the concept of comprehensive Gröbner system.

Definition 13 *Let $[S] = \{[f]_1, \ldots, [f]_\ell\}$ be a system of interval polynomials. We define the ideal family of $[S]$, denoted by $\mathcal{IF}([S])$ to be the set*

$$\mathcal{IF}([S]) = \{\langle p_1, \ldots, p_\ell \rangle \mid (p_1, \ldots, p_\ell) \in \mathcal{F}([S])\}$$

Theorem 6.3 *Let $[S]$ be a system of interval polynomials and $\prec$ be a monomial ordering on $\mathbb{R}[x_1, \ldots, x_n]$. Then*

- *The set of initial ideals $\{in(I) \mid I \in \mathcal{IF}([S])\}$ is a finite set, and*
- *For each set $\mathcal{J}$ of ideals of $\mathcal{IF}([S])$ with the same initial ideal, there exists a set of parametric polynomials which induces the ideals in $\mathcal{J}$ by different specializations.*

Proof: To prove this theorem, we use the concept of the comprehensive Gröbner system. Suppose that S^* is obtained by replacing each interval coefficient by a parameter. Note that if an interval appears in $t \geq 1$ coefficients, then we assign t distinct parameters to it. It is easy to check that each element of $\mathcal{IF}([S])$ is the image of S^* under a suitable specialization. On the other hand, by [35, Theorem 2.7], S^* has a finite comprehensive Gröbner system as $\mathcal{G} = \{(E_1, N_1, G_1), \ldots, (E_k, N_k, G_k)\}$, where for each specialization σ there exists a $1 \leq j \leq k$ such that $\mathrm{LM}(\sigma(S^*)) = \mathrm{LM}(G_j)$. It should be said that although there is a finite number of branches in $\mathcal{G}$, we can also remove the specializations with complex values, and also those with values out of the assigned interval. Thus, for each $I \in \mathcal{IF}([S])$ there exists an $1 \leq i \leq k$ with $in(I) = \langle \mathrm{LM}(G_i) \rangle$ and this finishes the proof. □

What is explained in the proof of Theorem 6.3 allows to extend the concept of the comprehensive Gröbner system to the concept of the interval Gröbner system.

Definition 14 *Let $[S] \subset [\mathbb{R}][x_1, \ldots, x_n]$ be a system of interval polynomials with t interval coefficients, and $\prec$ be a monomial ordering on $\mathbb{R}[x_1, \ldots, x_n]$. Let also that*

$$\mathcal{G} = \{(E_1, N_1, G_1), \ldots, (E_k, N_k, G_k)\},$$

be a set of triples such that

$$(E_i, N_i, G_i) \in \mathbb{R}[a_1, \ldots, a_t] \times \mathbb{R}[a_1, \ldots, a_t] \times \mathbb{R}[a_1, \ldots, a_t][x_1, \ldots, x_n],$$

where each a_i is a parameter which is assigned to an interval appearing in a coefficient. Then we call $\mathcal{G}$ an interval Gröbner system for $[S]$ denoted by $\mathcal{G}_\prec([S])$ if for each $t-$tuple $(\alpha_1, \ldots, \alpha_t)$ of the inner values of interval coefficients there exists an $1 \leq i \leq k$, and also for each $1 \leq i \leq k$ there exists $(\alpha_1, \ldots, \alpha_t)$ of the inner values of interval coefficients such that:

- *For each $p \in E_i$, $p(\alpha_1, \ldots, \alpha_t) = 0$,*
- *There exist some $q \in N_i$ such that $q(\alpha_1, \ldots, \alpha_t) \neq 0$, and*
- *$\sigma(G_i)$ is a Gröbner basis for $\langle \sigma([S]) \rangle$ with respect to $\prec$, where σ is the specialization $a_j \mapsto \alpha_j$ for $j = 1, \ldots, t$.*

Theorem 6.4 *Each interval polynomial system possesses an interval Gröbner system.*

Proof: Let S^* be the parametric polynomial system obtained by assigning each interval coefficient to a parameter. As mentioned in the proof of Theorem 6.3, $\mathcal{G}_\prec([S])$ is the same comprehensive Gröbner system of S^* where each parameter is bounded to give values from its assigned ideal. On the other hand, it is proved that each system of parametric polynomials has a comprehensive Gröbner system, which terminates the proof. □

We now give an easy example to illustrate what was described above.

Example 6.5 *Consider the interval polynomial system*

$$[S] = \begin{cases} [-1,2)xy + [-1,1)y + [3,5) = 0, \\ [-3,1)xy^2 + [1,3)y = 0. \end{cases} \quad (5)$$

To obtain a parametric polynomial system, we must assign to each one of the intervals $[-1,2), [-1,1), [3,5), [-3,1)$ *and* $[1,3)$ *one parameter from* $\{h_1, \ldots, h_5\}$ *respectively. Then we observe the parametric polynomial system*

$$S^* = \{a_1xy + a_2y + a_3, a_4xy^2 + a_5y\} \subset \mathbb{R}[a_1, \ldots, a_5][x, y].$$

Using the lexicographic monomial ordering $y \prec x$ *we can compute a comprehensive Gröbner system for* $\langle S^* \rangle$ *which contains about* 19 *triples. However some of them are admissible only for some values of parameters out of their assigned intervals. For instance the triple*

$$(\{1\}, \{a_1, a_2, a_4, a_5\}, \{a_3\})$$

is not acceptable in this example, since by applying this triple, $a_5 = 0$ *while from the main structure of the system,* $a_5 \in [1,3]$ *and so it is a contradiction. By removing such triples, there remains only* 8 *triples shown in the following table. Therefore the following table shows* $\mathcal{G}_\prec([S])$.

E_i	N_i	G_i
$\{a_1, a_2, a_4\}$	$\{\ \}$	$\{1\}$
$\{a_1, a_2\}$	$\{a_4\}$	$\{1\}$
$\{a_1, a_4\}$	$\{a_2\}$	$\{1\}$
$\{a_4\}$	$\{a_1\}$	$\{1\}$
$\{a_2\}$	$\{a_1a_4(a_1a_5 - a_3a_4)\}$	$\{1\}$
$\{a_1a_5 - a_3a_4\}$	$\{a_1a_2a_4\}$	$\{1\}$
$\{a_1\}$	$\{a_2a_4\}$	$\{a_2y + a_3, a_4x - a_2a_5\}$
$\{a_2, a_1a_5 - a_3a_4\}$	$\{a_1a_4\}$	$\{a_1xy + a_3\}$
$\{\ \}$	$\{a_1a_2a_4(a_1a_5 - a_3a_4)\}$	$\{a_2a_4y - a_1a_5 + a_3a_4,$ $(a_1^2a_5 - a_1a_3a_4)x + a_2^2a_4y + a_2a_3a_4\}$

Table 2: Interval Gröbner system of System (5)

Let us explain some rows of Table 3. Suppose that one selects $1, 0, 4, -1$ *and* 2 *from* $[-1,2), [-1,1), [3,5), [-3,1)$ *and* $[1,3)$, *respectively. By this choice, system 5 converts to*

$$S_{1,0,4,-1,2} = \begin{cases} xy + 4 = 0, \\ -xy^2 + 2y = 0. \end{cases} \quad (6)$$

Now, using Table 3, it can be observed by the fifth row of the Table that the evaluations satisfy the null and non-null conditions of this row. This implies that the reduced Gröbner basis of $\langle S_{S_{1,0,4,-1,2}} \rangle$ *equals* $\{1\}$ *and so there is no solution given by the Hilbert Nullestelensatz theorem. Suppose now that we change our selected values by choosing* $1/2$ *instead of* 0 *from* $[-1,1)$. *In this case, we observe the system*

$$S_{1,1/2,4,-1,2} = \begin{cases} xy + 1/2y + 4 = 0, \\ -xy^2 + 2y = 0. \end{cases} \quad (7)$$

However, the new values satisfy the conditions of the last row of the table, which shows that (after dividing by the leading coefficients) the reduced Gröbner basis of $\langle S_{1,1/2,4,-1,2}\rangle$ *is*

$$\{y + 12, x - 1/24y - 1/3\}.$$

It can be concluded that in this case we have a unique solution $x = -1/6, y = -12$.

6.1 Computing Interval Gröbner Systems

In this section we state our algorithm, called IGS, to compute an interval Gröbner system for an interval polynomial system. This algorithm is based on the PGB algorithm with some conditions for consistency. To begin, let $[S] = \{[f]_1, \ldots, [f]_\ell\} \subset [\mathbb{R}][x_1, \ldots, x_n]$ be a system of interval polynomials, where for each $1 \le j \le \ell$,

$$[f]_j = \sum_{i=1}^{m_j} [a_{ij}, b_{ij}] x_1^{\alpha_{ij,1}} \cdots x_n^{\alpha_{ij,n}}$$

and $(\alpha_{ij,1}, \ldots, \alpha_{ij,n}) \in \mathbb{Z}^n_{\ge 0}$, for each i. As is mentioned in Theorem 6.3, we assign to each interval coefficient $[a_{ij}, b_{ij}]$ a parameter h_{ij} to convert $[S]$ to a parametric polynomial system S^*. The following proposition describes the relations between the comprehensive Gröbner systems of S^* and the interval Gröbner systems of $[S]$.

Proposition 6.6 *Using the above notations, let* $[\mathcal{G}]$ *and* $\mathcal{G}$ *be an interval Gröbner basis for* $[S]$ *and a comprehensive Gröbner basis for* S^* *respectively with respect to the same monomial ordering* $\prec$*. Then, for each* $(E, N, G) \in [\mathcal{G}]$*, there exists* $(E', N', G') \in \mathcal{G}$ *such that*

$$\mathbf{V}(E) \setminus \mathbf{V}(N) \subset \mathbf{V}(E') \setminus \mathbf{V}(N')$$

and G *and* G' *have the same initial ideals.*

Proof: This comes from Definitions 14 and 10. □

According to the above proposition, to compute an interval Gröbner basis for $[S]$, it is enough to compute a comprehensive Gröbner basis for S^*, and use a criterion to omit the triples (E, N, G) lying in $\mathcal{G} \setminus [\mathcal{G}]$, which we consider *redundant* triples.

Remark 6.7 *Note that for each triple* (E, N, G) *in* $\mathcal{G} \setminus [\mathcal{G}]$*, the intersection of* $\mathbf{V}(E) \setminus \mathbf{V}(N)$ *with the Cartesian product of the interval coefficients is empty.*

We will now present a criterion to determine the elements of $\mathcal{G} \setminus [\mathcal{G}]$. This criterion is based on the answer to this question:

How can we be sure that a system of polynomials $E \subset \mathbb{R}[a_1, \ldots, a_t]$ *has a real root in the interval* $[\alpha_1, \beta_1) \times \cdots \times [\alpha_t, \beta_t)$*?*

In the following items, a brief survey of existing methods which can answer the above question is presented:

- In the case for which $\langle E\rangle$ is zero-dimensional (i.e. $\mathbf{V}(E)$ is a finite set), this question is answered generally with efficient computational tools such as Sturm's chain by isolating the real roots (see [30]).
- In the case of a positive dimensional $\langle E\rangle$, there exist certain algorithms to isolate the real roots. Among them there exists an algorithm which determines whether a multivariate polynomial system has real roots or not (see [7]).

- In [16, 17], the authors have used the Bernstein expansion to find a suitable box which contains real solutions of a polynomial system. The cornerstone of their methods relies on computing Bernstein polynomials.
- There are also some computational methods based on interval computations ([29]) and also quantifier elimination (QE) methods ([22]) which are devoted to finding the real solutions of polynomial equations.

In addition to what was mentioned, we convert the above key question to the problem of determining whether a polynomial system has a real root or not. This conversion makes it also possible to use the first two methods to here.

Theorem 6.8 *Let $E \subset \mathbb{R}[a_1, \ldots, a_t]$ be a finite set of polynomials. Let also*

$$F = E \cup \{a_i + (a_i - \beta_i)b_i^2 - \alpha_i \mid i = 1, \ldots, t\} \subset \mathbb{R}[a_1, \ldots, a_t, b_1, \ldots, b_t],$$

where b_j's are algebraically independent of a_i's and suppose that $[\alpha_i, \beta_i)$ is a real interval for each $i = 1, \ldots, t$. Then the system $E = 0$ has a solution in $[\alpha_1, \beta_1) \times \cdots \times [\alpha_t, \beta_t)$ if and only if the system $F = 0$ has a real solution.

Proof: Let $E = 0$ has a solution $(\gamma_1, \ldots, \gamma_t) \in [\alpha_1, \beta_1) \times \cdots \times [\alpha_t, \beta_t)$. Let also

$$\eta_i = \sqrt{\frac{\alpha_i - \gamma_i}{\gamma_i - \beta_i}}$$

for each $i = 1, \ldots, t$. It is seen that

$$\gamma_i + (\gamma_i - \beta_i)\eta_i^2 - \alpha_i = 0$$

which implies that $(\gamma_1, \ldots, \gamma_t, \eta_1, \ldots, \eta_t)$ is a solution of $F = 0$.

Conversely, suppose that there exists

$$(\gamma_1, \ldots, \gamma_t, \eta_1, \ldots, \eta_t) \in \mathbb{R}^{2t}$$

which is a solution of $F = 0$, i. e. $f(\gamma_1, \ldots, \gamma_t) = 0$ for each $f \in F$ and $\gamma_i + (\gamma_i - \beta_i)\eta_i^2 - \alpha_i = 0$, for each $i = 1 \ldots, t$. It is enough to show that $\gamma_i \in [\alpha_i, \beta_i)$. In doing so, we see that

$$\gamma_i = \frac{\alpha_i + \beta_i\eta_i^2}{1 + \eta_i^2} = (\beta_i - \alpha_i)\frac{\eta_i^2}{1 + \eta_i^2} + \alpha_i.$$

Indeed, $0 \leq \frac{\eta_i^2}{1+\eta_i^2} < 1$ and this shows that

$$\alpha_i \leq \underbrace{(\beta_i - \alpha_i)\frac{\eta_i^2}{1 + \eta_i^2} + \alpha_i}_{\gamma_i} < \beta_i$$

which finishes the proof. $\square$

Remark 6.9 *Note that for the intervals $[\alpha, \infty)$ and $(-\infty, \beta]$ we can use the auxiliary polynomials $a - \alpha - b^2$ and $a - \beta + b^2$ respectively.*

The following example shows the importance of Theorem 6.8.

Example 6.10 *Let* $a_1 = [3,5)$*,* $a_2 = [2,3)$ *and* $f = a_1a_2^2 - a_2 - 42$*. We will use Theorem 6.8, to find whether* $f = 0$ *has a solution in* $[3,5) \times [2,3)$ *or not. For this, we construct the polynomial ideal*

$$I = \langle a_1 + (a_1 - 2)b_1^2 - 1, a_2 + (a_2 - 3)b_2^2 - 2, a_1a_2^2 - a_2 - 42\rangle.$$

Computing a Gröbner basis for I *with respect to* $b_2 \prec_{grevlex} b_1 \prec_{grevlex} a_2 \prec_{grevlex} a_1$*, we will see that*

$$29b_1^2b_2^2 + 18b_2^4 + 24b_1^2 + 53b_2^2 + 32 \in I.$$

This concludes that no b_1 *or* b_2 *can be specialized to a real value. So,* $f = 0$ *has no real solution. It is worth noting that if we use interval arithmetic to solve this problem, we will see that* $f([2,3),[3,5)) = [-33,1)$*, which contains zero. But as was seen above, it is impossible for* f *to have a real solution. Thus, interval arithmetic is unable to solve this problem.*

Using Theorem 6.8 and the Remarks 6.7 and 6.9, we can determine the elements of $\mathcal{G} \setminus [\mathcal{G}]$ exactly (see Proposition 12).

Corollary 6.11 *Let* $(E,N,G) \in \mathcal{G}$ *and suppose that* $[\alpha_1,\beta_1),\ldots,[\alpha_t,\beta_t)$ *are* t *real intervals. Then* (E,N,G) *is redundant if and only if the system* $F = 0$ *has no real roots, where*

$$\begin{aligned} F &= E \cup \{a_i + (a_i - \beta_i)b_i^2 - \alpha_i \mid i = 1,\ldots,t\} \cup \{\prod_{g\in N}(c_g g - 1)\} \\ &\subset \mathbb{R}[a_1,\ldots,a_t,b_1,\ldots,b_t,c_g : g \in N]. \end{aligned}$$

Proof: The proof comes from Theorem 6.8 and the fact that if $\prod_{g\in N}(c_g g - 1) = 0$ then, there exist some $g \in N$ for which $c_g g - 1 = 0$, which implies that $g \neq 0$. □

The above corollary states the criterion which determines all redundant triples, and by installing this criterion on the PGB algorithm, we can design our new algorithm to compute interval Gröbner systems. We now design the IGS algorithm by its main procedure.

Algorithm 4 IGS

procedure IGS($[S], \prec_{\mathbf{x}}$)
  Assign $a_1,\ldots,a_t$ to interval coefficients and name it S^*;
  $\prec_{\mathbf{a}}$:= an arbitrary monomial ordering on $a_1,\ldots,a_t$;
  $E, N := \{\ \}, \{1\}$;
  $\prec_{\mathbf{x},\mathbf{a}}$:=The block ordering of $\prec_{\mathbf{x}}, \prec_{\mathbf{a}}$
  Return PGB-MAIN($P, E, N, \prec_{\mathbf{x},\mathbf{a}}, L$); \\$L$ is the ordered set of interval coefficients which is needed to check consistency.
end procedure

The PGB-MAIN algorithm is the same as that which was used in the PGB algorithm. We only change the definition of consistency as below.

Definition 15 *Let* $[\alpha_1,\beta_1),\ldots,[\alpha_t,\beta_t)$ *be* t *real intervals and* $E, N \subset \mathbb{R}[a_1,\ldots,a_t]$*. The pair* (E,N) *is called consistent if it is not redundant, or equivalently,*

$$[\mathbf{V}(E) \setminus \mathbf{V}(N)] \cap [\alpha_1,\beta_1) \times \cdots \times [\alpha_t,\beta_t) \neq \emptyset.$$

According to the above definition, we change the IsConsistent algorithm to Interval-IsConsistent, which checks the consistency for radical membership and redundancy determination.

Algorithm 5 Interval-IsConsistent

procedure Interval-IsConsistent($E, N, [\alpha_1, \beta_1), \ldots, [\alpha_t, \beta_t)$)
    $test$:=false;
    $flag$:=false;
    if (E, N) is not redundant **then**
        $test$:=true;
    end if
    if test **then**
        $flag$:=false;
        for $g \in N$ **while** $flag$ =false **do**
            if $g \notin \sqrt{\langle E \rangle}$ **then**
                $flag$:=true;
            end if
        end for
    end if
    Return $flag$;
end procedure

Example 6.12 *The* Interval-IsConsistent *algorithm returns false for the pair* $(\{a_1a_2^2 - a_2 - 42\}, \{a_1, a_2\})$*, as regards the Example 6.10; this pair is redundant.*

Remark 6.13 *It is worth noting that redundant triples will be omitted before the algorithm continues with them. This property causes* IGS *to return fewer triples than* PGB.

In the following, we clarify the complexity of the IGS algorithm. In doing so, we state an upper bound for the number of operations which are done in the first branch of the algorithm. Recall that an interval polynomial is homogeneous if all of its monomials have the same degree.

Theorem 6.14 *Let* $[S] = \{[f]_1, \ldots, [f]_\ell\} \subset [\mathbb{R}][x_1, \ldots, x_n]$ *be a system of homogeneous interval polynomial system with* t *intervals and maximum degree* d*. The number of operations required to compute an interval Gröbner system for* $[S]$*, in the first branch is bounded by* $d^{2^{O(t+n)}}$.

Proof: It is well-known that in the worst case, the complexity of the computation of a Gröbner basis is doubly exponential in the number of variables ([18, 26]). On the other hand, in the first branch of the PGB-Main algorithm, all parameters (which are the intervals) are considered as variables and so $t + n$ variables are encountered. Thus, the above upper bound for the number of operations in the first branch of IGS is given. □

Indeed, a similar bound exists for each branch, provided that the degree of the polynomials dose not increase. Otherwise, the bound for each branch depends on the degree of the result of previous branches. To see an upper bound for the degree of a Gröbner basis see [3].

Remark 6.15 *It is worth noting that the worst case estimations of the complexity of the computation of a Gröbner basis have led to the belief that Gröbner basis is not a useful tool in practice. However, there are quite efficient implementations to compute a Gröbner basis which have surprisingly good results in practical challenges ([3]). This is while the cornerstone of the* IGS *algorithm is based on the computation of some Gröbner bases and so each efficient implementation to compute a Gröbner basis results in an efficient implementation of the* IGS *algorithm. For instance, in [21] signature-based algorithms are used to compute comprehensive Gröbner systems which can be modified and be used to compute interval Gröbner systems.*

In the following part, we give an illustrative example to show the steps of computing an interval Gröbner system.

Example 6.16 *In this example, we declare the execution details of the* IGS *algorithm to compute an interval Gröbner system with respect to the monomial ordering* $y \prec_{grevlex} x$*, for*

$$[S] = \begin{cases} [-1,2]x^2 + [-2,2]y + 1 = 0 \\ [2,3]xy + y^2 + 2 = 0 \end{cases} . \tag{8}$$

As the first step, we assign the parameters a_1, a_2 *and* a_3 *to intervals* $[-1,2], [-2,2]$ *and* $[2,3]$ *respectively, and put a monomial ordering on them such as* $a_1 \prec_{lex} a_2 \prec_{lex} a_3$*. So, the system assigns to the parametric ideal*

$$I = \langle ax^2 + by + 1, cxy + y^2 + 2 \rangle.$$

The IGS *algorithm evaluates* E *(resp.* N*) to* $\{\ \}$ *(resp.* $\{1\}$*) and continues by the* PGB-Main *sub-algorithm. In the first step of this algorithm,* G *as the reduced Gröbner basis of* I *with respect to* $\prec_{\mathbf{x},\mathbf{a}}$*, will be computed as follows:*

$$\begin{aligned} G \;=\; & \{2a_1a_3x - a_1y^3 - a_2a_3^2y^2 - (a_3^2 + 2a_1)y, \\ & a_1xy^2 - a_2a_3y^2 + 2a_1x - a_3y, a_1x^2 + a_2y + 1, a_3xy + y^2 + 2\}. \end{aligned}$$

From this, $G_r = \emptyset$ *and so* G_r *and* N *are consistent, since* $N = \{1\}$*. So, a minimal Dickson basis must be computed which equals*

$$G_m = \{2a_1a_3x - a_1y^3 - a_2a_3^2y^2 - (a_3^2 + 2a_1)y, a_1x^2 + a_2y + 1, a_3xy + y^2 + 2\}.$$

Also, $h = \mathrm{lcm}(a_1, a_1, a_3) = a_1a_3$ *denotes the least common multiple of leading coefficients of the elements of* G_m *with respect to* $y \prec_{grevlex} x$*. Now,* $(G_r, N * \{h\}) = (\{\ \}, \{a_1a_3\})$ *enters the* Interval-IsConsistent *sub-algorithm to determine whether they are consistent or not. As the assigned intervals to* a_1 *and* a_3 *contain non-zero elements, it is possible for* a_1 *and* a_3 *to be non-zero and consequently* $(\{\ \}, \{a_1a_3\})$ *is not redundant. In the sequel, since* $E = \{\ \}$ *the sub-algorithm returns true and, therefore,* $(\{\ \}, \{a_1a_3\}, G_m)$ *adds to PGB as a branch. In the sequel,* PGB-Main *begins with* $E = \{a_1\}, N = \{1\}$ *and* G*. In this step, we will see that*

$$G = \{a_1, a_2y + 1, a_3x + y - 2a_2\},$$

and thus $G_r = \{a_1\}$ *and consequently,* $G_m = \{a_3x + y - 2a_2, a_2y + 1\}$ *as a minimal Dickson basis of* $G \setminus G_r$*. Here,* $h = a_2a_3$*, and so* $(G_r, N * \{h\}) = (\{a_1\}, \{a_2a_3\})$ *will be checked by the* Interval-IsConsistent *algorithm to determine consistency.*

Obviously, $0 \in [-1,2]$ *and there are elements in* $[-2,2]$ *and* $[2,3]$ *which are non-zero. Thus, the algorithm returns true since the radical conditions are also satisfied. Consequently,* $(\{a_1\}, \{a_2a_3\}, \{a_3x + y - 2a_2, a_2y + 1\})$ *appears as a new branch in* PGB. *Next,* PGB-MAIN *gives* $E := \{a_1, a_3\}, N = \{1\}$ *and* $\{a_3x + y - 2a_2, a_2y + 1\}$. *However, in this step the* INTERVAL-ISCONSISTENT *sub-algorithm does not allow the algorithm to continue with this branch, as* a_3 *is assigned to* $[2,3]$ *which can not be zero. Therefore, the algorithm begins with* $E := \{a_1, a_2\}, N = \{1\}$ *and* $G = \{a_3x + y - 2a_2, a_2y + 1\}$. *But in this case, the reduced Gröbner basis equals* 1 *and so* $(E, N, \{1\})$ *adds to* PGB. *Finally, verifying different branches in a similar way to that described above, the algorithm finds some branches which are involved in the above branches, or inconsistent conditions. Therefore, the algorithm terminates with the interval Gröbner system for* $[S]$*, which is shown in the following Table,*

E_i	N_i	G_i
$\{a_1, a_2\}$	$\{\}$	$\{1\}$
$\{\ \}$	$\{a_1a_3\}$	$\{2a_1a_3x - a_1y^3 - a_2a_3^2y^2 - (a_3^2 + 2a_1)y,$ $a_1x^2 + a_2y + 1, a_3xy + y^2 + 2\}$
$\{a_1\}$	$\{1\}$	$\{a_3x + y - 2a_2, a_2y + 1\}$

Table 3: Interval Gröbner system of $[S]$ in Example 8

7 Applications of Interval Gröbner System

Interval Gröbner systems have some novel properties which make it possible to analyze interval polynomial systems. This section aims to declare some applications of interval Gröbner systems.

7.1 Solving Interval Polynomial Systems

In this section we state an application of the interval Gröbner system to discuss the solution set of an interval polynomial system. Furthermore, we state another application to find the solutions which two interval polynomial systems may share. The following theorem shows how the interval Gröbner system can be used to find out whether an interval polynomial system has a solution or not.

Theorem 7.1 *Let* $[S]$ *be an interval polynomial system, and* $\mathcal{G}_{\prec}([S])$ *be an interval Gröbner system for* $[S]$*, with respect to* $\prec$*. Then,*

(a) If for each $(E, N, G) \in \mathcal{G}_{\prec}([S])$*,* $G = \{1\}$ *then,* $[S]$ *has no solution.*

(b) If $[S]$ *has no solution then, for each* $(E, N, G) \in \mathcal{G}_{\prec}([S])$*, either* $G = \{1\}$ *or* $\mathbf{V}(G) \cap \mathbb{R}^n = \emptyset$*, where* n *denotes the number of variables.*

Proof: Rewriting the Interval Hilbert Nullestelensatz theorem (see Theorem 6.1) by the notion of the ideal family in Definition 13 implies that the interval polynomial system $[S]$ has a solution, if for each ideal in $\mathcal{IF}([S])$, neither the reduced Gröbner basis equals $\{1\}$ nor has any real solutions. On the other hand, the interval Gröbner system gives a full decomposition on $\mathcal{IF}([S])$ by presenting all different possible Gröbner bases. So,

$[S]$ has a solution if and only if none of the reduced Gröbner bases of $\mathcal{G}_{\prec}([S])$ equals $\{1\}$ and all have some real solutions. This proves both parts of the theorem. $\square$

The following illustrative example shows the ability of the above theorem.

Example 7.2 *Consider the interval polynomial system described as follows:*

$$[S] = \begin{cases} a_1 xy^2 + a_2 x^2 y + a_3 = 0 \\ a_4 x^3 y^3 + a_5 xy + a_6 y = 0 \\ x^3 y^2 - \frac{1}{2} a_5 x - \frac{1}{2} a_6 = 0 \end{cases} \tag{9}$$

where,

$$a_1 = [2,3], a_2 = [3,7], a_3 = [7,12], a_4 = [1,2], a_5 = [4,6], a_6 = [2,4].$$

The interval Gröbner system of $[S]$ contains only one possible Gröbner basis which equals $\{1\}$ and by Theorem 7.1 (a), has no solution. To verify this, note that from the third equation, $2x^3y^3 = a_5 xy + a_6 y$. So, by the second equation, $a_4 x^3 y^3 + 2x^3 y^3 = 0$, which implies that $x^3y^3 = 0$. Thus, $x = 0$ or $y = 0$, each of which together with the first equation implies that $a_3 = 0$. However, this is a contradiction and so this system has no solution.

When Theorem 7.1 can not assert that an interval polynomial system has no solution, we will try to solve and find the solutions of the system, as shown in the following example.

Remark 7.3 *Suppose that $\mathcal{G} = \{(E_1, N_1, G_1), \ldots, (E_k, N_k, G_k)\}$, is an interval Gröbner system for an interval polynomial system $[S]$. Then,*

$$\mathbf{V}([S]) \subset \bigcup_{i=1}^{k} \mathbf{V}(G_i).$$

In the sequel, we state an example which illustrates how interval Gröbner systems solve interval polynomial systems.

Example 7.4 *Consider the following system of interval polynomials,*

$$[S] = \begin{cases} [1,3]x^2 + [-2,-1]y^2 + [2,4](z + [-2,1])^2 = 0 \\ [-4,-1]y^2 + x^3 y = 0 \\ x^3 y^3 + [2,5]x^2 = 0 \end{cases} \tag{10}$$

By computing an interval Gröbner system for this system, we attain only one branch (E, N, G), where $E = \{\ \}$ and N contains the non-nullity conditions over all intervals except $[-2,1]$. Therefore, all of the conditions are satisfied. Thus, it is enough to solve G to find out all solutions of $[S]$. It is worth noting that G contains $[-4,-1]y^4 - [2,5]x^2$ among its 8 elements, which implies that $x = y = 0$. Putting these values in the first equation of $[S]$, we see that $z = [-1,2]$, and so the solution set of $[S]$ is a segment on the $z-$axis.

The following lemma states a way to find the common solutions of two interval polynomial systems.

Lemma 7.5 *Let $[S]$ and $[S']$ be two interval polynomial systems. Then, $\mathbf{V}([S] \cup [S']) \cap \mathbb{R}^n$ equals the set of all common solutions of $[S]$ and $[S']$, where n denotes the number of variables.*

Proof: It is easy to see that $\mathbf{V}([S]) = \bigcup_{S\in\mathcal{F}([S])} \mathbf{V}(S)$ (and similarly for $[S']$). On the other hand, $a \in \mathbb{R}^n$ is a common solution of $[S]$ and $[S']$, if there exist $S \in \mathcal{F}([S])$ and $S' \in \mathcal{F}([S'])$ such that $a \in \mathbf{V}(S) \cap \mathbf{V}(S')$. Therefore, the set of all common solutions equals

$$\begin{aligned} \bigcup_{S\in\mathcal{F}([S]),S'\in\mathcal{F}([S'])} \mathbf{V}(S)\cap\mathbf{V}(S') &= \bigcup_{S\in\mathcal{F}([S])} \mathbf{V}(S)\cap \bigcup_{S'\in\mathcal{F}([S'])} \mathbf{V}(S') \\ &= \mathbf{V}([S])\cap\mathbf{V}([S']). \end{aligned} \tag{11}$$

However, as a simple fact, for each two sets of polynomials S and S', $\mathbf{V}(S)\cap\mathbf{V}(S') = \mathbf{V}(S\cup S')$ and so

$$\begin{aligned} \bigcup_{S\in\mathcal{F}([S]),S'\in\mathcal{F}([S'])} \mathbf{V}(S)\cap\mathbf{V}(S') &= \bigcup_{S\in\mathcal{F}([S]),S'\in\mathcal{F}([S'])} \mathbf{V}(S\cup S') \\ &= \bigcup_{S''\in\mathcal{F}([S]\cup[S'])} \mathbf{V}(S'') \\ &= \mathbf{V}([S]\cup[S']). \end{aligned} \tag{12}$$

Thus, relations (11) and (12) imply that

$$\mathbf{V}([S])\cap\mathbf{V}([S']) = \mathbf{V}([S]\cup[S']),$$

which proves the assertion. □

Remark 7.6 *It is easy to see that the above lemma can be extended to find the common solutions of an arbitrary number of interval polynomial systems.*

The following illustrative example explains the application of interval Gröbner systems in finding the common solutions of two interval polynomial systems.

Example 7.7 *Consider the interval polynomial system*

$$[S] = \begin{cases} [3,5]x^4z - y = 0 \\ [3,7]x^2y^2 + yz^3 = 0 \end{cases},$$

and let $[f] = [2,4]x^2 + [1,5]y^2 + [-4,-2]xz$. In this example, we will apply the concept of interval Gröbner system to find the common solutions of $[S]$ and $[f]$. In doing so, by Lemma 7.5, we construct a new interval polynomial system $[S'] = [S] \cup \{[f]\}$, and compute an interval Gröbner system for $[S']$, which contains only one branch (E, N, G). Here, $E = \{\ \}$ and N contains non-nullity conditions on interval coefficients which are all satisfied. Also, G has no non-zero real solution and this shows that there is no common solution between $[S]$ and $[f]$ except $(0,0,0)$.

7.2 Multiple zeros of an interval polynomial

In this section we state another application of interval Gröbner systems to find multiple roots of interval polynomials which can be useful in the study of the stability of polynomial roots. It should be said that the concepts related to multiple roots, come from [32].

Definition 16 *An interval polynomial $[f]$ has a multiple root of order ℓ if there exists $f \in \mathcal{F}([f])$ with a multiple root of order ℓ.*

We first state a criterion to verify whether an univariate interval polynomial has a multiple root, and then generalize it for the multivariate case. Note that in the following, $[f]^{(i)}$ denotes the $i-$th derivation of $[f]$.

Theorem 7.8 *Let $[f]$ be an univariate interval polynomial and $\mathcal{G}_\prec$ be an interval Gröbner system of $\{[f],[f]',\ldots,[f]^{(\ell-1)}\}$ with respect to an arbitrary monomial ordering $\prec$. Then, $[f]$ has a multiple root of order at least ℓ if and only if $\mathcal{G}_\prec$ contains a triple (E,N,G) in which $\mathbf{V}(G)\cap\mathbb{R}\neq\emptyset$. Furthermore, $\mathbf{V}(G)\cap\mathbb{R}$ contains all multiple roots of $[f]$ of order at least ℓ.*

Proof: Let $[f]$ have a multiple root of order at least ℓ. From Definition 16, there exists $f\in\mathcal{F}([f])$ with a multiple root of order ℓ. Suppose that $f=\sigma([f])$ where σ is a suitable evaluation of intervals. This implies that there exists a non-constant polynomial h such that

$$gcd(f,f',\ldots,f^{(\ell-1)})=h.$$

Now, from a well-known theorem from polynomial algebra

$$\langle f,f',\ldots,f^{(\ell-1)}\rangle=\langle h\rangle,$$

and so by the definition of the interval Gröbner system, there exists a triple (E,N,G) such that $\{h\}=\sigma(G)$. Therefore, $\mathbf{V}(G)\neq\emptyset$. Conversely, let $(E,N,G)\in\mathcal{G}_\prec$ such that $\mathbf{V}(G)\cap\mathbb{R}\neq\emptyset$ and σ be a suitable evaluation of intervals compatible with (E,N). By a fact from polynomial algebra,

$$\langle\sigma([f]),\sigma([f]'),\ldots,\sigma([f]^{(\ell-1)})\rangle=\langle gcd(\sigma([f]),\sigma([f]'),\ldots,\sigma([f]^{(\ell-1)}))\rangle,$$

and so by the definition of the interval Gröbner system,

$$\langle gcd(\sigma([f]),\sigma([f]'),\ldots,\sigma([f]^{(\ell-1)}))\rangle=\langle\sigma(G)\rangle.$$

Now, as $\mathbf{V}(G)\cap\mathbb{R}\neq\emptyset$, $gcd(\sigma([f]),\sigma([f]'),\ldots,\sigma([f]^{(\ell-1)}))$ has a real root and so $[f]$ has a multiple root of order at least ℓ. $\square$

The following example shows the application of interval Gröbner systems to find multiple roots of interval polynomials.

Example 7.9 *Suppose that $[f]=x^8-4x^6+[4,8]x^4+[-6,-3]x^2+[-1,2]$. We use Theorem 7.8 to find whether $[f]$ has a multiple root of order at least 3 or not. In doing so, we compute an interval Gröbner system for $\{[f],[f]',[f]''\}$ with respect to a lexicographical ordering. It contains a triple (E,N,G), where*

$$E=\{a_3^2-a_3,a_2+4a_3,a_1-6a_3\},N=\{1\},G=\{x^4-2a_3x^2+a_3\},$$

in which $a_1=[4,8],a_2=[-6,-3]$ and $a_3=[-1,2]$. The one evaluation σ which arises from E is $a_1\mapsto 6,a_2\mapsto -4$ and $a_3\mapsto 1$. Now, we have $\sigma(G)=\{x^4-2x^2+1\}$ which concludes that $[f]$ has two multiple roots 1 and -1 with an order of at least 3.

Remark 7.10 *To find whether an interval polynomial $[f]\in[\mathbb{R}][x]$ has a multiple root of order exactly ℓ, it is enough to solve the system*

$$\{[f],[f]',\ldots,[f]^{(\ell-1)},y[f]^{(\ell)}-1\},$$

where y is a new variable. Indeed, the last polynomial ensures that $[f]^{(\ell)}\neq 0$, and thus $[f]$ has a multiple root of order exactly ℓ if and only if the interval Gröbner system of the above system contains a triple (E,N,G) with $\mathbf{V}(G)\cap\mathbb{R}^2\neq\emptyset$.

In the sequel, we describe a method to find multiple zeros of multivariate interval polynomials. It is easy to see that a multivariate function has a multiple root of order at least ℓ whenever the function and all of its partial derivatives up to order $\ell - 1$ share a common zero. We apply this fact to state the following theorem. It is worth noting that the proof of this theorem is similar to that of Theorem 7.8 and so we leave it without proof. In the following theorem, $[f]_{x_i^j}$ denotes the partial derivation of $[f]$ with respect to x_i of order j.

Theorem 7.11 *Let $[f] \in [\mathbb{R}][x_1, \ldots, x_n]$ be a multivariate interval polynomial. Then, $[f]$ has a multiple root of order at least ℓ, if and only if the interval Gröbner system of*

$$\{[f]\} \cup \{[f]_{x_i^j} \mid i = 1, \ldots, n, j = 1, \ldots, \ell - 1\}$$

contains some triples (E, N, G) such that $\mathbf{V}(G) \cap \mathbb{R}^n \neq \emptyset$. Furthermore, $\mathbf{V}(G) \cap \mathbb{R}^n$ contains all multiple roots of $[f]$ of order at least ℓ.

In the following example, we apply the above theorem to verify whether a given multivariate interval polynomial has multiple roots or not.

Example 7.12 *Let $[f] = [7, 10]x^3 + [1, 3]y^3 - [9, 12]xy^2 + 12x^2y \in [\mathbb{R}][x, y]$. We will determine the multiple roots of $[f]$ of order at least 2. In doing so, we compute a reduced interval Gröbner system for $[S] = \{[f], [f]_x, [f]_y\}$ with respect to a lexicographical monomial ordering. This system contains two triples $(E_1, N_1, G_1) = (\{\alpha\}, \{a_3, a_1a_3 + 48\}, \{(2a_1a_3 + 96)xy + (-3a_1a_2 - 4a_3)y^2, (3a_1a_3 + 144)x^2 + (36a_2 - a_3^2)y^2\})$, and $(E_2, N_2, G_2) = (\{\ \}, \{\alpha, a_3, a_1a_3 + 48\}, G_1 \cup \{\alpha y^3\})$, in which $\alpha = 27a_1^2a_2^2 - 4a_1a_3^3 + 216a_1a_2a_3 - 144a_3^2 + 6912a_2$, and a_1, a_2 and a_3 are assigned to $[7, 10], [1, 3]$ and $[9, 12]$ respectively. It concludes by Theorem 7.11 that each real solution of G_1 and also G_2 determines a multiple root of $[f]$ of order at least 2.*

More precisely, from (E_2, N_2, G_2), we observe that $y = 0$, provided that at least one of the α, a_3 and a_1a_3+48 does not equal zero (note that such an evaluation exists). But, this implies that $x = 0$ and so $(0, 0)$ is one of the multiple roots of $[f]$. Furthermore, by evaluating under the specialization σ for which $a_1 \mapsto 9, a_2 \mapsto 2$ and $a_3 \mapsto 11$, we see that $\sigma(\alpha) = 0$ and the conditions of (E_1, N_1, G_1) are satisfied (note that $\sigma(a_3) \neq 0$). However, under this evaluation, G_1 converts to $\{3xy - y^2, 9x^2 - y^2\}$ which shows that each point over the line $3x - y = 0$ is a multiple root of $[f]$ with order at least 2. So, $[f]$ has infinite number of multiple roots of order at least 2.

7.3 Real Factors

In this section, we apply interval Gröbner systems to find real factors of interval polynomials. One of the interesting problems in the context of interval polynomials is the *Divisibility Problem* stated as follows ([32]):

For an interval polynomial $[f] \in [\mathbb{R}][x_1, \ldots, x_n]$ and a real polynomial $g \in \mathbb{R}[x_1. \ldots, x_n]$, determine whether there is a polynomial $p \in \mathcal{F}([f])$ such that g is a factor of p.

In the following, we state a criterion based on the interval Gröbner system which determines a solution for the above problem. It is worth noting that g i-divides $[f]$ whenever the answer of the above problem is *yes*.

Theorem 7.13 *Let $[S] = \{[f], g\} \subset [\mathbb{R}][x_1, \ldots, x_n]$ and $\mathcal{G}_\prec$ be a reduced interval Gröbner system for $[S]$ with respect to a monomial ordering $\prec$. Then g i-divides $[f]$ if and only if there exists a triple $(E, N, G) \in \mathcal{G}_\prec$ such that $G = \{g\}$.*

Proof: It is easy to see that g i-divides $[f]$ if and only if there exists a specialization σ for which $g|\sigma([f])$ and of course $\sigma([f]) \neq 0$. This implies that for such evaluation, $\sigma([S])$ can be expressed only by $\{g\}$ and therefore there exists a pair of parametric sets (E, N) such that $(E, N, \{g\}) \in \mathcal{G}_{\prec}$. $\square$

Example 7.14 *We will solve the divisibility problem for*

$$[f] = [-1, 1]x^2 + [-3, 1]y^2 + [1/2, 2]xy \in [\mathbb{R}][x, y],$$

and $g = x - \sqrt{2}y \in \mathbb{R}[x, y]$. *By computing a reduced interval Gröbner system for* $[S] = \{[f], g\}$ *with respect to a lexicographical monomial ordering, we find the triple*

$$(\{a_3\sqrt{2} + 2a_1 + a_2\}, \{1\}, \{x - \sqrt{2}y\})$$

where a_1, a_2 *and* a_3 *denote inner values of the intervals* $[-1, 1]$, $[-3, 1]$ *and* $[1/2, 2]$. *This means that if the values of* a_1, a_2 *and* a_3 *satisfy the equation* $a_3\sqrt{2} + 2a_1 + a_2 = 0$, *then there exists some* $p \in \mathcal{F}([f])$ *such that* $g|p$. *For instance, by evaluating under the specialization* σ *for which* $a_1 \mapsto 1/3, a_2 \mapsto -2$ *and so* $a_3 \mapsto 2\sqrt{2}/3$ *we find* $p = 1/3x^2 - 2y^2 + (2\sqrt{2}/3)xy \in \mathcal{F}([f])$ *which is divisible by* g *(note that* $p = 1/3(x + 3\sqrt{2}y)g$*). Therefore* g *i-divides* $[f]$.

Remark 7.15 *We can use Theorem 7.13 for further aims. Let* $f, g \in \mathbb{R}[x_1, \ldots, x_n]$ *where* g *does not divide* f. *Then one can use Theorem 7.13 to find a polynomial* $\tilde{f}$ *with the same coefficients of* f *which contain little perturbations and* $g \mid \tilde{f}$. *In doing so, one can convert* f *to an interval polynomial* $[f]$ *by putting the interval* $[c - \epsilon, c + \epsilon]$ *instead of the coefficient* c*, for each coefficient* c *appearing in* f. *Then, using Theorem 7.13 one can increase* ϵ *enough such that* g *i-divides* $[f]$ *with the desired precision.*

It should be pointed out that the proposed method can also be used for the divisibility problem of two interval polynomials. Given $[f], [g] \in [\mathbb{R}][x_1, \ldots, x_n]$, the following theorem determines if there exists $g \in \mathcal{F}([g])$ such that g i-divides $[f]$. As the proof of this theorem is similar to the proof of Theorem 7.13, we leave it without proof.

Theorem 7.16 *Let* $[S] = \{[f], [g]\} \subset [\mathbb{R}][x_1, \ldots, x_n]$ *and* $\mathcal{G}_{\prec}$ *be a reduced interval Gröbner system for* $[S]$ *with respect to a monomial ordering* $\prec$. *Then there exists* $g \in \mathcal{F}([g])$ *such that* g *i-divides* $[f]$ *if and only if there exists a triple* $(E, N, G) \in \mathcal{G}_{\prec}$ *such that* $G = \{\tilde{g}\}$ *and* $\tilde{g}$ *is the parametric form of* $[g]$ *which is simplified by* E.

The following example illustrates the above criterion to solve the divisibility problem for two interval polynomials.

Example 7.17 *Let* $[f] = x^4 + [1, 4]x^2z^2 + x^3y + [1, 4]x^2y^2 + [3, 7]y^2z^2 + 3y^3x$ *and* $[g] = x^2 + [-1, 4]y^2$. *By computing a reduced interval Gröbner system for* $[S] = \{[f], [g]\}$ *with respect to a lexicographical monomial ordering, we observe that this system contains the triple* $(E, N, G) = (\{3a_1 - a_3, a_2 - 3, a_4 - 3\}, \{\ \}, \{x^2 + 3y^2\})$, *in which* a_1, a_2, a_3 *and* a_4 *are assigned to* $[1, 4], [1, 4], [3, 7]$ *and* $[-1, 4]$ *respectively. This shows that* $g = x^2 + 3y^2 \in \mathcal{F}([g])$ *i-divides* $[f]$. *Furthermore, as the equations in* E *show,* $x^2 + 3y^2$ *divides* $p = x^4 + a_1x^2z^2 + x^3y + 3x^2y^2 + 3a_1y^2z^2 + 3y^3x \in \mathcal{F}([f])$ *where* a_1 *is an arbitrary value of* $[1, 4]$ *(note that* $p/g = x^2 + xy + a_1z^2$*).*

8 Conclusion and Future Works

In the current paper we have introduced the concept of the interval Gröbner system as a novel computational tool to analyze interval polynomial systems. We have further designed a complete algorithm for its computation using the existing methods to analyze parametric polynomial systems. There are also sufficient conditions on the interval Gröbner systems to determine whether an interval polynomial system has any solutions or not, and help to find the solution set. There are also some applications of interval Gröbner system such as computing the common solutions of two interval polynomial systems and computing the multiple roots of interval polynomials.

In future works, we hope to apply the interval Gröbner system to find the approximate gcd and the nearest polynomials with some specific properties. Moreover, we can use this concept to solve optimization problems in which the objective function and constraints are in the form of interval polynomials.

Acknowledgement

We would like to give special thanks to Prof. Prungchan Wongwises (who generously posted a hard copy of her Ph.D dissertation for the first author), Prof. Evgenija D. Popova and Prof. Amir Hashemi for valuable comments. We also thank the anonymous referees for their helpful comments.

References

[1] Götz Alefeld. Inclusion methods for systems of nonlinear equations-the interval newton method and modifications. *Topics in Validated Computations*, pages 7–26, 1994.

[2] Götz Alefeld and Dalcidio Moraes Claudio Claudio. The basic properties of interval arithmetics, its software realization and some applications. *Journal of Computers and Structures*, 67:3–8, 1998.

[3] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of the F_5 Gröbner basis algorithm. *J. Symb. Comput.*, 70(C):49–70, September 2015.

[4] Thomas Becker and Volker Weispfenning. *Gröbner bases: a computational approach to commutative algebra*. Springer-Verlag, London, UK, 0 edition, 4 1993.

[5] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69(1):1–52, Oct 2013.

[6] Dalcidio Moraes Claudio and Paul W. Oliveira. Interval approximation. *ZAMM - Journal of Applied Mathematics and Mechanics, ICIAM/GAMM 95 Numerical Analysis*, 76(S1):363–412, 1996.

[7] Mohab Safey El Din. Polynomial system solver over the reals: Algorithms, complexity, implementations and applications, 2010.

[8] Abbas Emami-Naeini and Paul Van Dooren. Computation of zeros of linear multivariable systems. *Automatica*, 18(4):415 – 430, 1982.

[9] Chen Falai and Wu Yang. Applications of interval arithmetic in solving polynomial equations by Wu's elimination method. *SCIENCE CHINA Mathematics*, 48(9):1260, 2005.

[10] Xuchuan Fan, Jiansong Deng, and Falai Chen. Zeros of univariate interval polynomials. *Journal of Computational and Applied Mathematics*, 216(2):563 – 573, 2008.

[11] Jean Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (f5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

[12] J. A. Ferreira, F. Patrício, and F. Oliveira. A priori estimates for the zeros of interval polynomials. *Journal of Computational and Applied Mathematics*, 136(1):271 – 281, 2001.

[13] J. A. Ferreira, F. Patrício, and F. Oliveira. On the computation of solutions of systems of interval polynomial equations. *Journal of Computational and Applied Mathematics*, 173(2):295 – 302, 2005.

[14] Shuhong Gao, Yinhua Guan, and Frank Volny IV. A new incremental algorithm for computing Gröbner bases. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ISSAC '10, pages 13–19, New York, NY, USA, 2010. ACM.

[15] Shuhong Gao, Frank Volny IV, and Mingsheng Wang. A new algorithm for computing Gröbner bases, 2010.

[16] Jürgen Garloff and Andrew P. Smith. Investigation of a subdivision based algorithm for solving systems of polynomial equations. *Nonlinear Analysis*, 47(1):167–178, 2001.

[17] Jürgen Garloff and Andrew P. Smith. Solution of systems of polynomial equations by using Bernstein expansion. In *Symbolic Algebraic Methods and Verification Methods*, pages 87–97. Springer Vienna, 2001.

[18] Mark Giusti. Some effectivity problems in polynomial ideal theory. In *EUROSAM 84*, pages 159–171. Springer-Verlag, 1984.

[19] Eldon Hansen and G. William Walster. *Global Optimization Using Interval Analysis*. CRC Press, 2003.

[20] Amir Hashemi, Mahdi Dehghani Darmian, and Benyamin M.-Alizadeh. Applying Buchberger's criteria on montes's DisPGB algorithm. *Bulletin of the Iranian Mathematical Society*, 38(3):715–724, 2012.

[21] Amir Hashemi, Benyamin M.-Alizadeh, and Mahdi Dehghani Darmian. Computing comprehensive Gröbner systems: A comparison of two methods. *Computer Science Journal of Moldova*, 25(3(75)):278–302, 2017.

[22] Nikolaos I. Ioakimidis. Quantifier elimination in applied mechanics problems with cylindrical algebraic decomposition. *International Journal of Solids and Structures*, 34(30):4037 – 4070, 1997.

[23] Deepak Kapur, Yao Sun, and Dingkang Wang. A new algorithm for computing comprehensive Gröbner systems. *ISSAC, Technische Universität München, München, Germany, July 25 - 28*, 2010.

[24] Deepak Kapur, Yao Sun, and Dingkang Wang. An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system. *Journal of Symbolic Computation*, 49:27 – 44, 2013. The International Symposium on Symbolic and Algebraic Computation.

[25] Montserrat Manubens and Antonio Montes. Improving the DISPGB algorithm using the discriminant ideal. *Journal of Symbolic Computation*, 41(11):1245 – 1263, 2006. Special Issue on the Occasion of Volker Weispfennings 60th Birthday.

[26] H. Michael Möller and Ferdinando Mora. Upper and lower bounds for the degree of Gröbner bases. In John Fitch, editor, *EUROSAM 84*, pages 172–183, Berlin, Heidelberg, 1984. Springer Berlin Heidelberg.

[27] Antonio Montes. A new algorithm for discussing Gröbner bases with parameters. *Journal of Symbolic Computation*, 33(2):183 – 208, 2002.

[28] Antonio Montes and Michael Wibmer. Gröbner bases for polynomial systems with parameters. *Journal of Symbolic Computation*, 45(12):1391 – 1425, 2010. MEGA2009.

[29] Ramon E. Moore, Ralph Baker Kearfott, and Michael J. Cloud. *Introduction to Interval Analysis*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2009.

[30] P. Pedersen, Marie-Françoise Roy, and Aviva Szpirglas. Counting real zeros in the multivariate case. In Frédéric Eyssette and André Galligo, editors, *Computational Algebraic Geometry*, pages 203 – 224, Boston, MA, 1993. Birkhäuser Boston.

[31] Howard Harry Rosenbrock. *State-space and multivariable theory*. London : Nelson, 1970.

[32] Hiroshi Sekigawa and Kiyoshi Shirayanagi. Locating real multiple zeros of a real interval polynomial. In *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation*, ISSAC '06, pages 310–317, New York, NY, USA, 2006. ACM.

[33] Ye. M. Smagina and Irina V. Brewer. Problem of asymptotic tracking for system with interval parameters. *IFAC Proceedings Volumes*, 29(1):3294 – 3298, 1996. 13th World Congress of IFAC, 1996, San Francisco USA, 30 June - 5 July.

[34] C. B. Soh and C.S. Berger. Damping ratio of polynomials with perturbed coefficients. *IEEE Transactions on Automatic Control*, 33:1180–1182, 12 1988.

[35] Volker Weispfenning. Comprehensive Gröbner bases. *Journal of Symbolic Computation*, 14(1):1 – 29, 1992.

[36] Volker Weispfenning. Canonical comprehensive Gröbner bases. *Journal of Symbolic Computation*, 36(3):669 – 683, 2003. ISSAC 2002.

[37] Prungchan Wongwises. Experimentelle Untersuchungen zur numerische Auflösungen von linearen Gleichungssystemen mit Fehlershranken, 1975.

[38] Mingbo Zhang and Jiansong Deng. Number of zeros of interval polynomials. *Journal of Computational and Applied Mathematics*, 237(1):102 – 110, 2013.