Trends in Mathematics
Information Center for Mathematical Sciences
Volume 2, December 1999, Pages 208–218

ON ALGEBRAIC ANALYSIS II

SUN T. SOH

Abstract. As a continuation of my article, "*On Algebraic Analysis I*", an underlying theory for computational mathematics called, Algebraic Analysis, is discussed with some examples and helpful remarks. Based on thse results, some important elementary algorithms in Algebraic Analysis are accordingly discussed.

1. Introduction

In [9], the author discussed very shortly the Theory of Groebner Bases and some of its applications. In this article, a more detailed version of the theory is discussed. All of the results in this article are well developed, for instance, in [3] or [1]. But, this does not means, by no means, that the results covered in this article are all of those so far developed.

In the followings, the most important algorithms for exact computation, i.e., Algebraic Analysis, are listed with some necessary definitions, theoretical results but with no proofs, and some helpful remarks. They are a theoretical backbone of exact computation or Algebraic Analysis.

Among several algorithms, the division algorithm for polynomials in more than one variables and the Buchberger's algorithm for Groebner bases are the most fundamental ones in the sense that others are based on these two.

2. The Division Algorithm In Several Variables

One starts with a simple example.

Example 1. *Decide whether the following system of polynomial equations over the field* $\mathbf{C}$ *of complex numbers is solvable, and if so, find all the solutions of it:*

$$\begin{cases} x^2+y^2+z^2 &= 1 \\ x^2+z^2 &= y \\ x &= z \end{cases}$$

We compute a Groebner basis of $I = (x^2+y^2+z^2-1, x^2+z^2-y, x-z)$ *with respect to the lex order under* $x > y > z$. *The basis is*

$$\begin{array}{rcl} g_1 &=& x-z \\ g_2 &=& -y+2z^2 \\ g_3 &=& z^4+(1/2)z^2-1/4 \end{array} .$$

Received by the editors July 24, 1999.
1991 *Mathematics Subject Classification.* 01-08, 01A67.
Key words and phrases. Key words and phrases: symbolic computation,approximation.
This work was supported by Korea Research Foundation (1998-015-D00011).

so that it is solvable and its solutions are completely determined by solving $g_3 = 0, g_2 = 0$, *and* $g_1 = 0$, *successively, since* $I = (g_1, g_2, g_3)$.

Remark 1. *One recalls that* $k[x_1, ..., x_n]$ *is a UFD but it is not a PID in general, unless* $n = 1$. *This fact causes a big trouble to mathematicians for a long time, ever since the discovery of the division algorithm for integers in at least Greek period.*

The division algorithm for polynomials in more than one variables described in Theorem 1 below is still incomplete in the sense that both the quotients $a_1, ..., a_s$ *and the remainder* r *in there are not uniquely determined. But, the amazing discovery of Buchberger made this division algorithm quite significant since the remainder is going to be unique, although not complete because, for an obvious reason, making the quotients furthermore unique is still impossible and will be impossible.*

By Buchberger's discovery of an algorithm for a Groebner basis for a polynomial ideal, which changes the generating set of a given polynomial ideal I *into another generating set* G *of* I *which is still finite but with an amazing property that the remainder* r *is now guaranteed to be unique when one attempts to divide a given polynomial* f *with the elements of this new generating set* G *of* I.

In addition to this, the above example explicitly shows the strength of the algorithm under the lex order. Namely, it allows us to solve a system of non-linear equations step by step by the so-called backward substitution. (In the case of the above example, one first solves $g_3 = 0$, *and substitute its solutions (called partial solutions) to* $g_2 = 0$ *in order to obtain a little bit bigger partial solutions, and then substitute these to* $g_1 = 0$ *to finally obtain the whole solutions.*

To understand the theory behind exact computation i.e., symbolic computation i.e., Algebraic Analysis, one has to study the subject from a strong computational point of view. The author decided to present the following summary of the theory of Groebner bases which should be sufficient enough for the beginners.

Definition 1. *A* ***monomial ordering*** *on* $k[x_1, ..., x_n]$ *under a given ordering between unknowns is any relation* $>$ *on* $\mathbf{Z}^n_{\geq 0}$, *or equivalently, any relation on the set of monomials* $x^\alpha, \alpha \in \mathbf{Z}^n_{\geq 0}$, *such that*

1. $>$ *is a total ordering on* $\mathbf{Z}^n_{\geq 0}$.
2. *If* $\alpha > \beta$ *and* $\gamma \in \mathbf{Z}^n_{\geq 0}$, *then* $\alpha + \gamma > \beta + \gamma$.
3. $>$ *is a well-ordering.*

Example 2. *Some examples of monomial ordering under a given ordering between unknowns are*

- *Lexicographic order (Lex order)*
- *Graded lex order*
- *Graded reverse lex order*

Their definitions are

Definition 2. ***(Lexicographic Order)*** *Let* $\alpha = (\alpha_1, ..., \alpha_n)$ *and* $\beta = (\beta_1, ..., \beta_n)$ *be two elements in* $\mathbf{Z}^n_{\geq 0}$. *We say that* $\alpha <_{lex} \beta$ *if, in the vector difference* $\alpha - \beta$, *the left-most nonzero entry is* positive.

Definition 3. ***(Graded Lex Order)*** *Let* $\alpha, \beta \in \mathbf{Z}^n_{\geq 0}$. *We say* $\alpha <_{grlex} \beta$ *if*

1. $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, *or*
2. $|\alpha| = |\beta|$ *but* $\alpha <_{lex} \beta$.

Definition 4. *(**Graded Reverse Lex Order**) Let $\alpha, \beta \in \mathbf{Z}^n_{\geq 0}$. We say $\alpha <_{grlex} \beta$ if*

1. $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, *or*
2. $|\alpha| = |\beta|$ *but in $\alpha - \beta \in \mathbf{Z}^n$, the right-most nonzero entry is* negative.

These are not all of them. In fact, it is well known that there are infinitely many monomial orders.

Let

$$f = \sum_{\alpha} c_\alpha x^\alpha,$$

be a polynomial in $k[x_1, ..., x_n]$, for uniquely determined $c_\alpha \in k$, $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where by definition $\alpha = (\alpha_1, ..., \alpha_n)$. Then a monomial order $<$ always allows us to compare which monomial is the biggest one among those x^α's, with respect to this $<$, showing up in writing f in a unique manner as above.

Definition 5. *The biggest one is usually called the **leading monomial** of f, and denoted by*

$$LM(f).$$

*If a particular x^α is $LM(f)$, then $c_\alpha x^\alpha$ is called the **leading term** of f, and denoted by*

$$LT(f),$$

*and $\alpha = (\alpha_1, ..., \alpha_n)$ is called the **multidegree** of f, and denoted by*

$$multi\deg(f).$$

Theorem 1. *(**The Division Algorithm for polynomials in** $k[x_1, ..., x_n]$). Under a fixed monomial order $>$ on polynomials, let $F = (f_1, ..., f_s)$ be an ordered s-tuple of polynomials in $k[x_1, ..., x_n]$. Then any $f \in k[x_1, ..., x_n]$ can be written as*

$$f = a_1 f_1 + ... + a_s f_s + r,$$

where $a_i, r \in k[x_1, ..., x_n]$, and r is a k-linear combination of monomials, none of which is divisible by any of the leading terms $LT(f_1), ..., LT(f_s)$ of the $f_1, ..., f_s$. Furthermore, if $a_i f_i \neq 0$, we have

$$multi\deg(f) \geq multi\deg(a_i f_i).$$

One should note that this theorem *never* claims that either the quotients $a_1, ..., a_s$ or the remainder r are uniquely determined. In this sense, this division is far from complete.

Example 3. *Would like to divide $x^2y + xy^2 + y^2$ by $xy - 1$ and $y^2 - 1$. Assume $x > y$ and assume lex order. Then*

$$x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1$$

But the remainder $x + y + 1$ is not uniquely determined when the order of dividend is changed:

$$x^2y + xy^2 + y^2 = (x + 1) \cdot (y^2 - 1) + x \cdot (xy - 1) + 2x + 1$$

where the remainder is $2x + 1$.

Example 4. *Let $f = xy^2 - x$ and $f_1 = xy + 1, f_2 = y^2 - 1$. With $x > y$ and lex order, we have*

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y)$$
$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Thus, the remainder $= 0$ implies $f \in (f_1, f_2)$, but not conversely in general.

3. Groebner Bases

On the other hand, Buchberger ingeniously invented an algorithm in 1965 which allows us, when combined with the division algorithm in several variables, to compute the remainder of the division algorithm in a unique manner under a fixed monomial order. Thanks to his algorithm, the division algorithm gained a strong power as one shall see below. One starts with an axiomatic definition of Groebner basis:

Definition 6. *Fix a monomial order. A finite subset $G = \{g_1, ..., g_t\}$ of an ideal $I = (g_1, ..., g_t)$ is said to be a* ***Groebner basis*** *if*

$$(LT(g_1), ..., LT(g_t)) = (LT(I)),$$

where $(LT(I))$ is the ideal generated by all the leading terms of polynomials in I.

Remark 2. *The problem of this version of definition of Groebner basis* of purely axiomatic nature *is computationally useless.*

Remark 3. *One may easily prove that a set $\{g_1, ..., g_t\} \subset I$ is a Groebner basis if and only if the leading term of any element I is divisible by one of the $LT(g_i)$.*

Remark 4. *A Groebner basis is a Hilbert basis, but not conversely.*

The next result says that when one divides a polynomial with a Groebner basis according to the division algorithm in Theorem 1, the remainder is always uniquely determined.

Theorem 2. *Let $G = \{g_1, ..., g_t\}$ be a Groebner basis for an ideal $I \subset k[x_1, ..., x_n]$ and let $f \in I$. Then there exists a unique $r \in k[x_1, ..., x_n]$ satisfying:*

1. *No term of r is divisible by one of $LT(g_1), ..., LT(g_t)$;*
2. *There exists $g \in I$ such that $f = g + r$.*

One has an immediate corollary.

Corollary 3. *$f \in I$ if and only if the remainder on division of f by G is zero.*

Remark 5. *These axiomatic results suddenly gain their strong points by the works of Buchberger in discovering an algorithm for Groebner bases in 1965, and it is the main subject of the next section.*

4. Buchberger's Algorithm for Groebner Bases

The following result is computationally very important, since it is the main criterion utilized in Buchberger's algorithm for actually converting the given set of generating set of a polynomial ideal I into its Groebner basis.

Theorem 4. *Let I be a polynomial ideal. Then a basis $G = \{g_1, ..., g_t\}$ for I is a Groebner basis for I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero, where*

$$S(f,g) = \frac{LCM((LM(f), LM(g))}{LT(f)} \cdot f - \frac{LCM(LM(f), LM(g))}{LT(g)} \cdot g.$$

The most important result in Algebraic Analysis is the following algorithm.

Theorem 5. ***(Buchberger's Algorithm to construct a Groebner basis in a finite number of steps)***. *There exists an algorithm which computes a Groebner basis of I from a given generating set of a polynomial ideal I.*

Remark 6. *The time efficiency of Buchberger's algorithm is still quite controversial, since it generally requires an exponential time efficiency although it is very dependent on the choice of a monomial order. This means that the complexity analysis of Buchberger's algorithm is still remained as an active research area. But, when the number of unknowns are not too many and when the coefficients of polynomials are not too much big and strange, it is generally known that the fine-tuned version of his algorithm is fast enough to tolerate. The important point is that we never really had such a remarkable algorithm until 1965.*

Definition 7. *A **reduced Groebner basis** for a polynomial ideal I is a Groebner basis G for I such that*

1. *$LC(p) = 1$ for all $p \in G$;*
2. *For all $p \in G$, no monomial of p belongs to $(LT(G - \{p\}))$.*

Remark 7. *The combination of the division algorithm in Theorem 1 and the Buchberger's algorithm in Theorem 5 is computationally very important.*

Lemma 6. *Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial ordering, I has a unique reduced Groebner basis.*

Remark 8. *Any computer algebra systems which has "SOLVE" command, for instance, MAPLE, REDUCE, MACSYMA, MATHEMATICA, etc., are already equipped with some version of Buchberger's algorithm which produces the reduced Groebner basis of a polynomial ideal. This enables us to check the result of a particular problem under a particular computer algebra system loaded in a particular machine is indeed correct by comparing it with that obtained under a different computer algebra system in a different machine.*

5. Elimination and Extension Theory

Definition 8. *Given $I = (f_1, ..., f_s) \subset k[x_1, ..., x_n]$, the **ideal I_k of elimination** at k-th step of I is the ideal of $k[x_{k+1}, ..., x_n]$ defined by*

$$I_k = I \cap k[x_{k+1}, ..., x_n].$$

Theorem 7. ***(The Elimination Theorem)***. *Let $I \subset k[x_1, ..., x_n]$ be an ideal and let G be a Groebner basis of I with respect to lex order where $x_1 > x_2 > ... > x_n$. Then, for each $0 \leq k \leq n$, the subset*

$$G_k = G \cap k[x_{k+1}, ...x_n]$$

is a Groebner basis of the ideal of elimination at k-th step.

Theorem 8. *(**The Extension Theorem**). Let $I = (f_1, ..., f_s) \subset k[x_1, ..., x_n]$ and I_1 be the ideal of elimination at first step of I. For each $1 \leq i \leq s$, write f_i in the form*

$$f_i = g_i(x_2, ..., x_n)x_1^{N_i} + \text{ terms in which } x_1 \text{ has degree } < N_i,$$

where $N_i \geq 0$ and $g_i \in k[x_1, ..., x_n]$ (where k is algebraically closed) is nonzero. (Set $g_i = 0$ if $f_i = 0$). Suppose that we have a partial solution $(a_2, ..., a_n) \in \mathbf{V}(I_1)$. If $(a_2, ..., a_n) \notin \mathbf{V}(g_1, ..., g_s)$, then there exists $a_1 \in k$ such that $(a_1, ..., a_n) \in \mathbf{V}(I)$.

Remark 9. *The proof of this theorem is done by the theory of resultants, well-developed by those who worked in the Invariant Theory.*

Theorem 9. *(**Polynomial Implicitization**). If k is an infinite field, let $F : k^m \to k^n$ be the function determined by the polynomial parametrization as is in the next Lemma. Let I be the ideal $I = (x_1 - f_1, ..., x_n - f_n) \subset k[t_1, ..., t_m, x_1, ..., x_n]$ and let $I_m = I \cap k[x_1, ..., x_n]$ be the ideal of elimination at m-th step. Then $\mathbf{V}(I_m)$ is the smallest variety in k^n containing $F(k^m)$.*

Lemma 10. *If V is a variety over an infinite field k defined parametrically by*

$$x_i = f_i(t_1, ..., t_m), \qquad i = 1, ..., n,$$

where the f_i are polynomials in $k[t_1, ..., t_m]$, then V is irreducible.

Theorem 11. *(**Rational Implicitization**). If k is an infinite field, let $F : k^m - W \to k^n$ be the function determined by the rational parametrization as in the next Lemma. Let J be the ideal $J = (g_1x_1 - f_1, ..., g_nx_n - f_n, 1 - gy) \subset k[y, t_1, ..., t_m, x_1, ..., x_n]$, where $g = g_1 \cdot g_2 \cdots g_n$, and let $J_{m+1} = J \cap k[x_1, ..., x_n]$ be the ideal of elimination at $(m+1)$st step. Then $\mathbf{V}(J_{m+1})$ is the smallest variety in k^n containing $F(k^m - W)$.*

Lemma 12. *If V is a variety over an infinite field k defined parametrically by*

$$x_i = \frac{f_i(t_1, ..., t_m)}{g_i(t_1, ..., t_m)}$$

where the f_i and the g_i are polynomials in $k[t_1, ..., t_m]$, then V is irreducible.

Remark 10. *The converse process of implicitization, called parametrization, is not always possible.*

Theorem 13. *Let k be an algebraically closed field. Suppose $V = \mathbf{V}(f_1, ..., f_s) \subset k^n$, and let $\pi_k : k^n \to k^{n-k}$ be projection onto the last $n-k$ factors. If I_k is the ideal of elimination at k-th step of $I = (f_1, ..., f_s)$, i.e., $I_k = (f_1, ..., f_s) \cap k[x_{k+1}, ..., x_n]$, then $\mathbf{V}(I_k)$ is the **Zariski closure** of $\pi_k(V)$ (i.e., the smallest affine algebraic variety containing $\pi_k(V)$).*

Theorem 14. *(**Radical Membership**). Let k be an arbitrary field and let $I = (f_1, ..., f_s) \subset k[x_1, ..., x_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal $\bar{I} = (f_1, ..., f_s, 1 - yf) \subset k[x_1, ..., x_n, y]$ (in which case, $\bar{I} = k[x_1, ..., x_n, y]$).*

Theorem 15. *Let I, J be ideals in $k[x_1, ..., x_n]$. Then*

$$I \cap J = (tI + (1 - t)J) \cap k[x_1, ..., x_n].$$

Lemma 16. *The intersection $I \cap J$ of two principal ideals $I = (f), J = (g) \subset k[x_1, ..., x_n]$ is a principal ideal generated by $LCM(f, g)$.*

Theorem 17. *Let I be an ideal and g an element of $k[x_1, ..., x_n]$. If $\{h_1, ..., h_p\}$ is a basis of the ideal $I \cap (g)$, then $\{h_1/g, ..., h_p/g\}$ is a basis of $I : (g)$.*

Theorem 18. *Let $V = \mathbf{V}(I)$ be an affine variety in k^n where k is an algebraically closed field and fix a monomial ordering in $k[x_1, ..., x_n]$. Then the following statements are equivalent:*

1. *V is a finite set.*
2. *For each $i, 1 \leq i \leq n$, there exists some $m_i \geq 0$ such that $x_i^{m_i} \in LT((I))$.*
3. *Let G be a Groebner basis for I. Then for each $i, 1 \leq i \leq n$, there exists some $m_i \geq 0$ such that $x_i^{m_i} = LM(g)$ for some $g \in G$.*
4. *The k-vector space $S = Span(x^\alpha : x^\alpha \notin (LT(I)))$ is finite-dimensional.*
5. *The k-vector space $k[x_1, ..., x_n]/I$ is finite-dimensional.*

Now we consider the projective situation.

Definition 9. *A **graded monomial order** on $k[x_1, ..., x_n]$ is a monomial order that orders first by total degree:*

$$x^\alpha < x^\beta$$

whenever $|\alpha| < |\beta|$, where $|\alpha|$ = the sum of α_i's.

Example 5. *Graded lex order and graded reverse lex order are graded monomial orders, but lex order is not.*

Theorem 19. *Let I be an ideal in $k[x_1, ..., x_n]$ and let $G = \{g_1, ..., g_s\}$ be a Groebner basis for I with respect to a graded monomial order in $k[x_1, ..., x_n]$. Then $G^h = (g_1^h, ..., g_s^h)$ is a basis for $I^h \subset k[x_0, x_1, ..., x_n]$.*

Theorem 20. *Let k be an algebraically closed field, and let $I \subset k[x_1, ..., x_n]$ be an ideal. Then $\mathbf{V}(I^h) \subset \mathbf{P}^n(k)$ is the **projective closure** of $\mathbf{V}_a(I) \subset k^n$.*

Definition 10. *Let k be a field.*

1. *A polynomial $F \in k[x_0, ..., x_n, y_1, ..., y_m]$ is $(x_0, ..., x_n)$-**homogeneous** polynomial if there exists an integer $k \geq 0$ such that*

$$F = \sum_{|\alpha|=k} h_\alpha(y_1, ..., y_m) x^\alpha,$$

   where x^α is a monomial in $x_0, ..., x_n$ of multidegree α and $h_\alpha \in k[y_1, ..., y_m]$.
2. *The **variety** $\mathbf{V}(F_1, ..., F_s) \subset \mathbf{P}^n \times k^m$ defined by $(x_0, ..., x_n)$-homogeneous polynomials $F_1, ..., F_s \in k[x_0, ..., x_n, y_1, ..., y_m]$ is the set*

$$\{(a_0, ..., a_n, b_1, ..., b_m) \in \mathbf{P}^n \times k^m : F_i(a_0, ..., a_n, b_1, ..., b_m) = 0 \text{ for } 1 \leq i \leq s\}.$$

Definition 11. *Given an ideal $I \subset k[x_0, ..., x_n, y_1, ..., y_m]$ generated by $(x_0, ..., x_n)$-homogeneous polynomials, the **projective elimination ideal of** I is the set*

$$\hat{I} = \{f \in k[y_1, ..., y_m] : \text{ for each } 0 \leq i \leq n, \text{ there exists } e_i \geq 0 \text{ with } x_i^{e_i} f \in I\}.$$

Theorem 21. *Let $I = (F_1, ..., F_s) \subset k[x_0, ..., x_n, y_1, ..., y_m]$ be an ideal generated by $(x_0, ..., x_n)$-homogeneous polynomials $F_1, ..., F_s$. Then*

$$\hat{I} = I_n^{(0)} \cap I_n^{(1)} \cap \cdots \cap I_n^{(n)},$$

where $I_n^{(i)} = I^{(i)} \cap k[y_1, ..., y_m]$ *is the ideal of* n*-th elimination of* $I^{(i)}$ *where*

$$I^{(i)} = (F_1^{(i)}, ..., F_s^{(i)})$$

where $F_j^{(i)} = F_j(x_0, ..., x_{i-1}, 1, x_{i+1}, y_1, ..., y_m)$ *is the dehomonization of* F_j *at* i*-th place, for each* $1 \leq j \leq s$.

Theorem 22. *(**The Projective Extension Theorem**). Assume that* k *is algebraically closed and that* $V = \mathbf{V}(F_1, ..., F_s) \subset \mathbf{P}^n \times k^m$ *is defined by* $(x_0, ..., x_n)$*-homogeneous polynomials in* $k[x_0, ..., x_n, y_1, ..., y_m]$. *Write* $I = (F_1, ..., F_s)$. *If*

$$\pi : \mathbf{P}^n \times k^m \to k^m$$

is projection onto the last m *coordinates, then*

$$\pi(V) = \mathbf{V}(\hat{I}).$$

Theorem 23. *Let* k *be algebraically closed and let* $F : \mathbf{P}^n \to \mathbf{P}^m$ *be defined by homogeneous polynomials* $f_0, ...f_m \in k[x_0, ..., x_n]$ *which have the same total degree and no common zeroes in* $\mathbf{P}^n$. *In* $k[x_0, ..., x_n, y_0, ..., y_m]$, *let* $I = (y_0 - f_0, ..., y_m - f_m)$ *and let* $I_{n+1} = I \cap k[y_0, ..., y_m]$. *Then* I_{n+1} *is a homogenous ideal in* $k[y_0, ..., y_m]$ *and*

$$F(\mathbf{P}^n) = \mathbf{V}(I_{n+1}).$$

6. Dimension Theory

Remark 11. *In the past, the dimension of an irreducible affine variety* V *was defined as the transcendence degree of the field of fractions* $k(V)$ *of its coordinate ring* $k[X]$. *The problem with this axiomatic definition is that one cannot compute it since it is very difficult to know which collection of elements of* $k(V)$ *is indeed algebraically independent over* k.

Theorem 24. *(**The Dimension Theorem**). Let* $V = \mathbf{V}(I)$ *be an affine variety, where* $I \subset k[x_1, ..., x_n]$ *is an ideal. If* k *is algebraically closed, then*

$$\dim V = \deg^a HP_I(s),$$

where ${}^aHP_I(s)$ *is an affine Hilbert polynomial of* I. *Furthermore, if* $>$ *is a graded order on* $k[x_1, ..., x_n]$, *then*

$$\begin{aligned} \dim V &= \deg^a HP_{(LT(I))}(s) \\ &= \max.\dim. \text{ of a coordinate subspace in } \mathbf{V}((LT(I)). \end{aligned}$$

Finally, the last two equalities hold over any field k *when* $I = \mathbf{I}(V)$.

Theorem 25. *(**the dimension theorem**). Let* $V = \mathbf{V}(I) \subset \mathbf{P}^n$ *be a projective variety, where* $I \subset k[x_0, ..., x_n]$ *is a homogeneous ideal. If* V *is nonempty and* k *is algebraically closed, then*

$$\dim V = \deg HP_I(s),$$

where $HP_I(s)$ *is the Hilbert polynomial of* I. *Furthermore, for any monomial order on* $k[x_0, ..., x_n]$, *we have*

$$\begin{aligned} \dim V &= \deg HP_{(LT(D))}(s) \\ &= \max.\dim. \text{ of a projective coordinate subspace in } \mathbf{V}((LT(I))). \end{aligned}$$

Finally, the last two equalities holds over any field k *when* $I = \mathbf{I}(V)$.

Thus, by computing the (affine) Hilbert polynomial of I in each case, one can figure out the dimension of a variety.

For more advanced results, one may refer to, for instance, [4] and its references.

7. Algorithms Based on Buchberger's Algorithm

Algorithms in this section are immediate application of the basic algorithms introduced in Section 2 and Section 4. The author is quite sure that some of the readers will be surprised by the availability of those algorithms discussed now. One can find enough examples of these algorithms, for instance, in [3] or [1].

7.1. **Algorithm for ideal membership.** Apply Cor. 3.

7.2. **Algorithm for ideal equality.** Let $I = (f_1, ..., f_s)$ and $J = (g_1, ..., g_t)$ be two ideals in $k[x_1, ..., x_n]$. Then $I = J$ if and only if their reduced Groebner bases are the same for a fixed monomial order (cf. Lemma 6).

7.3. **Algorithm for consistency (i.e. Solvability question of system of polynomial equations).** If we have polynomials $f_1, ..., f_s \in k[x_1, ..., x_n]$ where k is algebraically closed, compute a reduced Groebner basis for the ideal they generate with respect to any ordering. If this basis is $\{1\}$, the polynomials have no common zero in k^n; otherwise, they have a common zero. (cf. Lemma 6).

7.4. **Algorithm for detecting zero-dimensional varieties.** Apply Theorem 18.

7.5. **Implicitization algorithm for polynomial parametrizations.** If we have $x_i = f_i(t_1, ..., t_m)$ for polynomials $f_1, ..., f_n \in k[t_1, ..., t_m]$, consider the ideal

$$I = (x_1 - f_1, ..., x_n - f_n) \in k[t_1, ..., t_m, x_1, ..., x_n]$$

and compute a Groebner basis with respect to a lex ordering where every t_i is greater than every x_i. Then by the **Elimination Theorem 7,** the element of the Groebner basis not involving $t_1, ..., t_m$ form a basis of I_m, and by the **Polynomial Implicitization Theorem 9,** they define the smallest variety in k^n containing the parametrization.

7.6. **Implicitization algorithm for rational parametrizations.** If we have $x_i = f_i(t_1, ..., t_m)/g_i(t_1, ..., t_m)$ for polynomials $f_1, g_1 ..., f_n, g_n \in k[t_1, ..., t_m]$, consider the new variable y and the ideal

$$I = (g_1 x_1 - f_1, ..., g_n x_n - f_n, 1 - gy) \in k[y, t_1, ..., t_m, x_1, ..., x_n]$$

where $g = g_1 \cdots g_n$. Compute a Groebner basis with respect to a lex ordering where y and every t_i are greater than every x_i. Then by the **Elimination Theorem 7,** the element of the Groebner basis not involving $y, t_1, ..., t_m$ form a basis of I_m, and by the **Rational Implicitization Theorem 11,** they define the smallest variety in k^n containing the parametrization.

7.7. **Algorithm for computing intersection of ideals.** If $I = (f_1, ..., f_r)$ and $J = (g_1, ..., g_s)$ are ideals in $k[x_1, ..., x_n]$, consider the ideal

$$(tf_1, ..., tf_r, (1-t)g_1, ..., (1-t)g_s) \subset k[x_1, ..., x_n, t]$$

and compute a Groebner basis with respect to lex order in which t is greater than the x_i. Then the elements of this basis which do not contain the variable t is a Groebner basis of $I \cap J$. (cf. Theorem 15).

7.8. **Algorithm for computing the l.c.m.** To compute the *l.c.m.* of two polynomials $f, g \in k[x_1, ..., x_n]$, we compute the intersection $(f) \cap (g)$ using the algorithm for computing intersection of ideals and then by Lemma 16, we get the result. (cf. Theorem15).

7.9. **Algorithm for computing the g.c.d.** Compute *l.c.m.* of $f, g \in k[x_1, ..., x_n]$ and apply the division algorithm to get the result by the formula

$$GCD(f, g) = \frac{f \cdot g}{LCM(f, g)}.$$

7.10. **Algorithm for computing a basis of an ideal quotient I:J.** Given $I = (f_1, ..., f_r)$ and $J = (g_1, ..., g_s) = (g_1) + ... + (g_s)$, to compute $I : J$, first compute a basis for $I : (g_i)$ for each i. In view of Theorem 17 we first compute a basis of $(f_1, ..., f_r) \cap (g_i)$ by the algorithm above. Then using the division algorithm, divide each of these elements by g_i to get a basis for $I : (g_i)$. Finally compute a basis for $I : J$ by apply the intersection algorithm $s - 1$ times, computing first a basis for $I : (g_1, g_2) = (I : (g_1)) \cap (I : (g_2))$, then a basis for $I : (g_1, g_2, g_3) = (I : (g_1, g_2)) \cap (I : (g_3))$, and so on.

7.11. **Algorithm for computing the projective closure of an affine variety.** Given $W = \mathbf{V}(f_1, ..., f_s) \subset k^n$ where k is algebraically closed, compute a Groebner basis G of $(f_1, ..., f_n)$ with respect to a graded monomial order. Then the projective closure in $\mathbf{P}^n(k)$ is defined by $g^h = 0$ for $g \in G$. (cf. Theorem 20).

7.12. **Algorithm for radical membership.** Let $I = (f_1, ..., f_s)$ be an ideal in $k[x_1, ..., x_n]$ and let f be a polynomial in $k[x_1, ..., x_n]$. To determine if $f \in \sqrt{I} \subset k[x_1, ..., x_n]$, compute a reduced Groebner basis of the ideal $(f_1, ..., f_s, 1 - yf) \subset k[x_1, ..., x_n, y]$ with respect to some ordering. If the result is $\{1\}$, then $f \in \sqrt{I}$. Otherwise, $f \notin \sqrt{I}$. (cf. Theorem 14).

8. Further Results

The algorithms discussed so far are somewhat oriented to Algebraic Geometry. Once understanding the materials presented in this article, one may then refer to [1] and [2] for Commutative Algebra oriented materials. For example, the following algorithms for commutative algebra and the needed theoretical results for them are presented in these references.

8.1. **Algorithm for associated primes.** Can we find bases for the associated primes $P_i = \sqrt{Q_i}$? Yes.

8.2. **Algorithm for radical generators.**

8.3. **Algorithm for radical ideal.**

8.4. **Algorithm for primality.** Is there an algorithm for deciding if a given ideal is prime? Yes.

8.5. **Algorithm for irreducibility.** Is there an algorithm for deciding if a given affine variety is irreducible? Yes.

8.6. **Algorithm for decomposition.** Is there an algorithm for finding the minimal decomposition of a given variety or radical ideal? Yes.

8.7. **Algorithm for primary decomposition.** Is there an algorithm for finding bases for the primary ideals Q_i in a minimal primary decomposition of an ideal I? Yes.

For more advanced results, the readers may also refer to [4], [5], [10], and references of these literatures.

References

[1] W.W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases,* GSM Vol. 3, 1994, AMS

[2] T. Becker and V. Weispfenning, *Groebner Bases: A Computational Approach to Commutative Algebra*, 1993, Springer Verlag

[3] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra,* 1992, Springer-Verlag

[4] D. Eisenbud and L. Robbiano, *Computational Algebraic Geometry and Commutative Algebra*, Symposia Mathematica Vol. XXXIV, Istituto Nazionale di Alta Mathematica Francesco Severi, 1993, Cambridge Univ. Press

[5] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, 1995, Springer-Verlag

[6] George R. Kempf, *Algebraic Varieties*, London Math. Soc. LNS 172, 1993, Cambridge Univ. Press

[7] _____, *Algebraic Structures,* 1995, Friedrich Vieweg & Sohn,

[8] D. Mumford, *Algebraic Geometry I, Complex Projective Varieties,* 1976, Springer-Verlag

[9] Sun T. Soh, *A Global Object, Algebraic Geometry,* Proc. of Workshops in Pure Math., Vol. 14, Part I (1994), pp.139-145, Pure Math. Research Assoc., The Korean Academic Council

[10] B. Sturmfels, *Algorithms in Invariant Theory,* Texts and Monographs in Symbolic Computation, 1993, Springer-Verlag

Current address: Department of Mathematics, Myong Ji University, Yong In, Rep. of Korea
E-mail address: sunsoh@wh.myongji.ac.kr