

Computing dimension of affine varieties using Groebner basis approach

Mohammad Salah Uddin

Department of Natural Sciences, Daffodil International University, Bangladesh

Abstract: Given a set of polynomials $F \subseteq k[X]$, what is the dimension of the affine variety $\mathbf{V}(F)$? Giving an affirmative answer to this question was never so easier in algebraic geometry until the development of Groebner basis. Groebner bases are nice because we can compute these; and this is Buchberger algorithm which makes Groebner bases so fruitful. Given a polynomial collection $F \subseteq k[X]$, Groebner basis helps in computing free set in $k[X]$ with respect to the ideal $\langle F \rangle$. Then dimension of $\mathbf{V}(F)$ equals the cardinality of the free set with respect to $\langle F \rangle$. Here we describe an algorithm for computing such free set and answer the aforementioned question from computational point of view. We see that, in case of finding dimension of affine variety, computational technique is much more informative and motivating than theoretical method.

Keywords: Affine variety, Dimension, Free set, Groebner basis

I. Introduction

Affine varieties are the solution sets to systems of polynomial equations in several unknowns. Let $F = \{f_1, f_2, \dots, f_s\}$ be a subset of the polynomial ring $k[X]$ where k is a field of scalars and $X = \{x_1, x_2, \dots, x_n\}$. Then an **affine variety** defined by F , denoted by $\mathbf{V}(F)$ or $\mathbf{V}(f_1, f_2, \dots, f_s)$, is the common zero locus of the polynomial collection F i.e. $\mathbf{V}(F)$ equals the set $\{(a_1, a_2, \dots, a_n) \in k^n : f_i(a_1, a_2, \dots, a_n) = 0, 1 \leq i \leq s\}$. In words, affine varieties are points, curves, surfaces and higher dimensional objects defined by polynomial equations. For example, consider the polynomial collection $F_1 = \{9x^2 + 4y^2 - 36, x^2 - y^2 - 9\} \subseteq \mathbb{C}[x, y]$. In \mathbb{R}^2 , $\mathbf{V}(9x^2 + 4y^2 - 36)$ is an ellipse and $\mathbf{V}(x^2 - y^2 - 9)$ is a hyperbola where $\mathbf{V}(F_1) = \emptyset$ because no point of \mathbb{C}^2 satisfies $9x^2 + 4y^2 - 36 = 0$ and $x^2 - y^2 - 9 = 0$ simultaneously (Fig. 1). Now interchanging the coefficients of x^2 and y^2 in the first polynomial of F_1 , we have $F_2 = \{4x^2 + 9y^2 - 36, x^2 - y^2 - 9\}$ and $\mathbf{V}(F_2) = \{(3, 0), (-3, 0)\}$, (Fig. 2), which is a nonempty finite subset of \mathbb{C}^2 containing the points $(3, 0)$ and $(-3, 0)$. Let us now consider the polynomial collection $F_3 = \{y - x^2, z - x^3\} \subseteq \mathbb{C}[x, y, z]$. Then the variety $\mathbf{V}(F_3)$ is an infinite subset of \mathbb{C}^3 . It is a curve in \mathbb{R}^3 known as the twisted cubic (Fig. 3). It is the intersection of the varieties $\mathbf{V}(y - x^2)$ and $\mathbf{V}(z - x^3)$, which are the surfaces $y = x^2$ and $z = x^3$ in \mathbb{R}^3 .

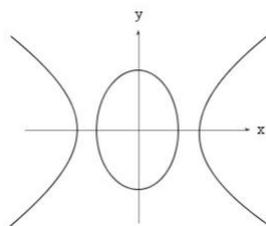


Figure 1: $\mathbf{V}(F_1) \cap \mathbb{R}^2$

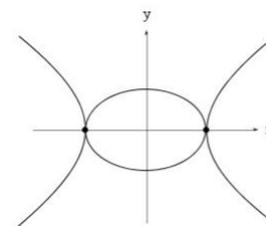


Figure 2: $\mathbf{V}(F_2) \cap \mathbb{R}^2$

The **dimension** of a variety V , denoted by $\dim V$, is defined to equal the length d of the longest possible chain $V = V_d \supset V_{d-1} \supset \dots \supset V_2 \supset V_1 \supset V_0$. With this definition, since the smallest irreducible varieties are singletons, finite varieties are zero-dimensional, lines are one-dimensional, planes are of dimension two and so on. When we have one equation in \mathbb{R}^2 , we get curve(s), for example $\mathbf{V}(9x^2 + 4y^2 - 36)$ and $\mathbf{V}(x^2 - y^2 - 9)$ (Fig 1); when we have one equation in \mathbb{R}^3 , we get a surface, for example $\mathbf{V}(y - x^2)$ and $\mathbf{V}(z - x^3)$ (Fig 3). Thus in each case the dimension drops by 1. Now consider the case of two equations. For two equations in \mathbb{R}^2 , we get a set of points, for example $\mathbf{V}(F_2)$ (Fig 2); two equations in \mathbb{R}^3 give a curve, for example $\mathbf{V}(F_3)$ (Fig 3). Thus in these cases the dimension drops by 2. Since each equation imposes an extra constraint, intuition suggests that each equation drops the dimension by 1. Unfortunately, this is not the case in general. To see this, consider the variety $\mathbf{V}(F_1)$ shown in the Fig 1, where two equations in \mathbb{R}^2 give an empty set. A more confusing situation occurs in case of the variety $\mathbf{V}(xz, yz) \cap \mathbb{R}^3$, shown in the Fig 4, which contains both the Z axis and the XY plane. However throughout this paper we want to answer the following question from a computational point of view.

Given $F \subseteq k[X]$, what is the dimension of the affine variety $\mathbf{V}(F)$?

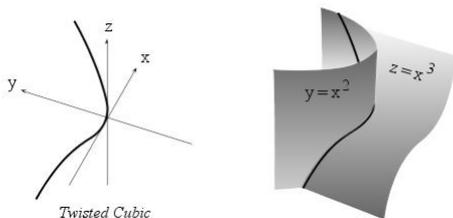


Figure 3: $V(F_3) \cap \mathbb{R}^3$

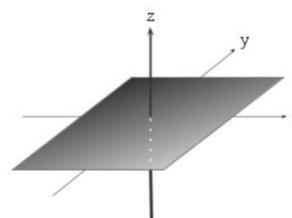


Figure 4: $V(xz, yz) \cap \mathbb{R}^3$

Since, in algebraic geometry we study geometry through algebraic method, it becomes abstract and difficult by its nature. Groebner basis removes this abstractness and presents algebraic geometry as much more practical and experimental subject. In many problems in the polynomial rings, we have to operate with ideals and finite sets of their generators. For a given polynomial ideal, Groebner basis is one of such generating sets with many nice properties. Groebner bases are so useful mainly because we can compute these. The main contribution of Buchberger was to give an algorithm, known as Buchberger algorithm, whose input is a finite set of polynomials F and whose output is a Groebner basis for the ideal generated by the elements of F . Here in Section 2, we give a very short note on the construction of Groebner basis. In Section 3, we show that how Groebner basis helps us computing free set which directly determines dimension of affine varieties.

II. Groebner Basis

The simplest polynomials in the ring $k[X]$ are the **monomials**, which are the polynomials of the form $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, where we define $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. We set $|\alpha| = \alpha_1 + \alpha_2 + \dots + \alpha_n$ and call $|\alpha|$, the **degree** of the monomial x^α . For $0 \neq a_\alpha \in k$, $a_\alpha x^\alpha$ is called a **term** in $k[X]$ and a_α is called the **coefficient** of the term $a_\alpha x^\alpha$. Every polynomial $f \in k[X]$ is a finite sum of terms. For algorithmic purposes, we need to impose an ordering ($>$) on the monomials in $k[X]$ so that the terms in a polynomial are always ordered. One of the most commonly used monomial order on $k[X]$ is lexicographic (*lex*) monomial order. Please see [1] for more detailed. For $x^\alpha, x^\beta \in k[X]$, $x^\alpha >_{lex} x^\beta$ if in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most nonzero entry is positive. Now let $f = a_\alpha x^\alpha$ be a nonzero polynomial in $k[X]$ and let $>$ be a monomial order. Then $\max_{(\alpha \in \mathbb{Z}_{\geq 0}^n : a_\alpha \neq 0)} (\alpha \in \mathbb{Z}_{\geq 0}^n : a_\alpha \neq 0)$ is called **multi-degree** of f and is denoted by $multideg(f)$ and the term $a_\alpha x^\alpha$ such that $\alpha = multideg(f)$ is called the **leading term** of f and is denoted by $LT(f)$.

For an ideal $I \subseteq k[X]$, the ideal generated by the leading terms of I is called **leading ideal** of I and it is denoted by $\langle LT(I) \rangle$. Then a generating set $G = \{g_1, g_2, \dots, g_t\}$ is said to be a **Groebner basis** for the ideal I if $\langle LT(g_1), LT(g_2), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$. Since every leading ideal is finitely generated Groebner basis always exists. The algorithm $G \leftarrow GroebnerBasis(f_1, f_2, \dots, f_s, >)$ [2] returns Groebner basis with respect to the monomial order $>$ for the polynomial collection $F = \{f_1, f_2, \dots, f_s\}$. But Groebner bases computed in this way varies according to the monomial order chosen. However, this confusing is removed by introducing reduced Groebner basis which uniquely exists for any polynomial ideal and does not depend on monomial ordering [1]. A **reduced Groebner basis** for a polynomial ideal I is a Groebner basis G for I such that for all $g \in G$, coefficient of $LT(g)$ equals 1 and no monomial of g lies in the ideal $\langle LT(G - \{g\}) \rangle$. The algorithm $G_{red} \leftarrow RedGroebnerBasis(f_1, f_2, \dots, f_s, >)$ [2] returns reduced Groebner basis for the polynomial collection $F = \{f_1, f_2, \dots, f_s\}$. We note that the reduced Groebner basis for the whole ideal $k[X]$, the collection of all polynomials in the variables in X , equals $\{1\}$ [1].

III. Computing Free Set

Free sets are closely related to the dimension of affine varieties. The dimension of an affine variety equals the cardinality of the free set. Therefore computing free set is the other word of determining dimension of affine variety. Let $F = \{f_1, f_2, \dots, f_s\} \subseteq k[X]$ be given. Then a set $S \subseteq \{x_1, x_2, \dots, x_n\}$ is said to be **free** in $k[X]$ with respect to the ideal $\langle F \rangle$ if no monomial in the variables in S appear in the leading ideal $\langle LT(F) \rangle$. For example, consider the ideal $\langle H \rangle \subseteq \mathbb{C}[x, y]$ where $\langle LT(H) \rangle = \langle x^2 y, y^4 \rangle$. Then the free set S in $\mathbb{C}[x, y]$ with respect to $\langle H \rangle$ contains only the variable x i.e. $S = \{x\}$, because in this case no monomial only in the variable x is in $\langle x^2 y, y^4 \rangle$. The following proposition shows that we can describe an algorithm for computing the free set with respect to a given ideal.

Proposition: Let $F = \{f_1, f_2, \dots, f_s\} \subseteq \mathbb{Q}[X]$ and a monomial order $>$ be given. Then there is an algorithm for computing the free set in $\mathbb{Q}[X]$ with respect to $\langle F \rangle$.

Proof: Here we present the algorithm $S \leftarrow CompFreeSet(F, >)$ in pseudo code which returns the free set S in $\mathbb{Q}[X]$ with respect to the ideal $\langle F \rangle$.

```

Algorithm:  $S \leftarrow \text{CompFreeSet}(F, >)$ 
Input:  $F = \{f_1, f_2, \dots, f_s\} \subseteq \mathbb{Q}[X]$  and a term order  $>$ 
Output:  $S$ , the free set in  $\mathbb{Q}[X]$  w.r.t.  $\langle F \rangle$ 

begin
 $G_{red} := \text{RedGroebnerBasis}(f_1, f_2, \dots, f_s, >)$ 
 $S := \emptyset$ 
if  $G_{red} = \{1\}$  then
    return
end if
for each  $x_i \in \{x_1, x_2, \dots, x_n\}$  do
     $S := S \cup \{x_i\}$ 
    monomialfound := false
    for each  $f_j \in G_{red}$  do
        if  $\text{multideg}(LM(f_j)) = \sum_{x_k \in S} \beta_k \times \text{multideg}(x_k)$  then
            monomialfound := true
             $G_{red} := G_{red} - \{f_j\}$ 
            if  $G_{red} = \{1\}$  then
                 $S := S - \{x_i\}$ 
                return
            end if
        end if
    end for
    if monomialfound := true then
         $S := S - \{x_i\}$ 
    end if
end for
end

```

Let us now see how this algorithm works and computes S successfully. On computing the reduced Groebner basis G_{red} for $\langle F \rangle$, this algorithm checks whether G_{red} equals $\{1\}$. If so, it returns with S as an empty set, because in this case monomials in each variables in $\{x_1, x_2, \dots, x_n\}$ is in the ideal $\langle LT(F) \rangle$. In case of nontrivial outputs it executes two loops with finite number of indices. Hence there is no cause to fall into infinite loop. In $i - th$ step in the outer loop x_i is added to S considering x_i is free in $\mathbb{Q}[X]$. For each polynomial $f_j \in G_{red}$, in the inner loop it checks if $\text{multideg}(LM(f_j))$ equals $\sum_{x_k \in S} \beta_k (0, \dots, 0, 1, 0, \dots, 0)$ [$\because \text{multideg}(x_k) = 0, \dots, 0, 1, 0, \dots, 0$ i.e. if LMf_j equals a monomial $x_k^{\beta_k}$ in the variables in S . Each time it finds such an $f_j \in G_{red}$ for any x_i , it updates S by removing x_k from it so that S contains only those x_i which are free in $\mathbb{Q}[X]$ with respect to the ideal $\langle F \rangle$. It also updates G_{red} by removing f_j to prevent the repetition of same monomial match. Once continuation of the process stops either if $G_{red} = \{1\}$ or if every $x_i \in \{x_1, x_2, \dots, x_n\}$ is added to S and checked for monomial match. Therefore, at the end S is left containing only those variables x_i which are free in $\mathbb{Q}[X]$ with respect to the ideal $\langle F \rangle$. \square

IV. Computing Dimension

Here we recall the dimension criterion theorem [3] and the algorithm " $S \leftarrow \text{CompFreeSet}(F, >)$ ", to complete our answer. The dimension theorem states that "For given $F \subseteq k[X]$ and a monomial order $>$, the cardinality of the free set in $k[X]$ with respect to $\langle F \rangle$ equals dimension of $\mathbf{V}(F)$ i.e. $|S| = \dim \mathbf{V}(F)$." Therefore, to compute the dimension of the variety of a given polynomial collection $F \subseteq k[X]$, we need only two steps- $S := \text{CompFreeSet}(F, >)$ and then $\dim \mathbf{V}(F) := |S|$. For example, since no monomial consisting only the variables x and y is present in the ideal $I = \langle xz, yz \rangle$, the set $S = \{x, y\}$ is free in $\mathbb{C}[x, y, z]$ with respect to I . Hence the dimension of the variety $\mathbf{V}(I)$ equals $|S| = 2$. On the other hand, dimension of a variety containing more than one irreducible component is same as the maximum dimension of its irreducible components [4]. Since the only irreducible components of variety $\mathbf{V}(xz, yz)$ are the XY plane and the Z axis (Fig 4), the dimension of $\mathbf{V}(xz, yz)$ equals two, the dimension of the XY plane.

V. Conclusions

Developing a good theory of dimension is a challenging problem in the area of algebraic geometry. Idea of free set gives easier option to this demand and more others. Recalling the dimension criterion theorem and our algorithm for computing free set allow us to solve the dimension problem completely. Since this algorithm uses directly the definition of free set it becomes time consuming in case of the polynomial collections with big Groebner basis. However, the ability of computing dimension of affine varieties must give strength to further studies in this area.

References

- [1] D. Cox, J. Little and D. O'Shea, *An introduction to computational algebraic geometry and commutative algebra* (New York Inc, Springer-Verlage, 1997).
- [2] Mohammad Salah Uddin, *Computational algebraic geometry and Groebner bases*, Diploma dissertation, The Abdus Salam International Center for Theoretical Physics, Trieste, Italy, 2009.
- [3] B. Sturmfels, *Lectures on Groebner bases*, Mathematical Science and Research Institute, Berkeley.
- [4] Karen E. Smith, Lauri Kahanpaa, Pekka Kekalainen, William Traves, *An Invitation to algebraic geometry*, (New York Inc, Springer-Verlage, 2000)