Groebner Basis and its Applications

Yengkhom Satyendra Singh, Benaki Lairenjam

Abstract: This paper is a survey on Groebner basis and its applications on some areas of Science and Technology. Here we have presented some of the applications of concepts and techniques from Groebner basis to broader area of science and technology such as applications in steady state detection of chemical reaction network (CRN) by determining kinematics equations in the investigation and design of robots. Groebner basis applications could be found in vast area in circuits and systems. In pure mathematics, we can encounter many problems using Groebner basis to determine that a polynomial is invertible about an ideal, to determine radical membership, zero divisors, hence so forth. A short note is being presented on Groebner basis and its applications.

Keywords: Groebner basis, polynomials, polynomials rings, ideals, division algorithm, applications of Groebner basis.

I. INTRODUCTION

Polynomial systems are available in many areas of mathematics, natural sciences and engineering, and the theory of Groebner basis is one of the most advance tools for solving polynomial systems. Groebner basis are the basis for the finitely generated ideals of a polynomial ring with several variables. The three steps monomial ordering, division algorithm and Hilbert basis theorem are the shortest way which leads to the definition of Groebner basis [15]. The notion of Groebner basis was introduced by Buchberger in 1965 to describe ideals of commutative algebras. This notion generalizes both the Gaussian elimination method for solving systems of polynomial equations and the division of polynomials in multiple indeterminates. In the case of systems of linear polynomial equations, Groebner basis give the Gaussian elimination algorithm. In the case of the division, of a polynomial by a set of polynomials, the remainder is not always unique. Hence if the remainder of the division of f by $f_1, f_2, \dots, f_s$ is equal to zero then f is in the ideal generated by $f_1, f_2, \dots, f_s$, but if the remainder is not equal to zero we cannot determine whether f is in the ideal generated by $f_1, f_2, \dots, f_s$. Also, if we choose any divisor and the remainder is unique regardless of the order of divisors. These divisors are the Groebner basis. Groebner basis can also be used to decide whether or not an element of a commutative algebra is in some ideal. Given I an ideal of the ring $K[x_1, \dots, x_n]$ of polynomials in n indeterminates, a Groebner basis of I gives us an algorithm deciding whether or not an element of $K[x_1, \dots, x_n]$ is in I. A Groebner basis is a set of multivariate nonlinear polynomials that reduces many fundamental problems in mathematics into simple algorithmic solutions such as finding intersection of ideal, finding Hilbert dimension and envelopes in commutative algebra; geometric theorem proving, graph coloring, summation and integration, linear integer optimization in the field of mathematics; also it has many applications in coding theory, robotics, software engineering and in petroleum industry for natural sciences and engineering [3]. Groebner basis theory in [1] and [2], is of great importance in various scientific fields with the progress in Computer Algebra System (CAS) such as mathematical modeling and simulations for problems. To name a few problems that the Groebner basis technique solved recently are determining genetic connection between the species, reverse engineering problems, inverse kinematics in robotics and to control oil platforms using artificial intelligence.

Revised Manuscript Received on October 15, 2019
* Correspondence Author
Yengkhom Satyendra Singh, Department of Mathematics, School of Applied Sciences, Reva University, Bangalore, India.
Email: yengkhom123@gmail.com
Benaki Lairenjam, Department of Mathematics, School of Applied Sciences Reva University, Bangalore, India.
Email: benaki_lai@yahoo.co.in

II. PRELIMINARIES

Let K indicate a field generally $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ or Z_p where p is prime. Let $R = K[x_1, x_2, \dots, x_n]$ represent the polynomial ring in the indeterminates $x_1, x_2, \dots, x_n$ over the field K. A monomial is nothing but a product of the variables, that is $x^\alpha = x_1^{\alpha_1}, x_2^{\alpha_2}, \dots, x_n^{\alpha_n}$ where $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n \in N^n$. Furthermore, the total degree of the monomial x^α could be define as $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$.

A polynomial of R can be define as a linear combination of monomials such as $f = c_1 x_1^{\alpha_1} + c_2 x_2^{\alpha_2} + \cdots + c_n x_n^{\alpha_n}$. That is all the polynomials of R is of the form

$$f = c_t x^t + c_{t-1} x^{t-1} + \cdots + c_1 x + c_0$$

where t is the degree of f.

And so, each polynomial will have a largest monomial of degree t. We call $c_t x^t$ the leading term of f and x^t the leading monomial.

A. Example: x^7y^2z, x^6y^3, y^5 and x^3z are monomials in x, y, z. They are of total degree $10, 9, 5$ and 3 respectively.

B. Definition: A multivariate polynomial f in $x_1, x_2, \dots, x_n$ with coefficients in a field K is a finite linear combination $\sum_\alpha a_\alpha x^\alpha$, where x^α is the monomials and $a_\alpha \in K$ are the coefficients. The total degree of the polynomial f is the maximum $|\alpha|$ such that $a_\alpha \neq 0$ [18].

C. Definition: A monomial ordering is a total ordering on the variables $x_1, x_2, \dots, x_n$ (that is there are no elements which are not comparable) $>$ on the set of monomials of $R = K[x_1, x_2, \dots, x_n]$ such that

i. $x^\alpha > x^\beta \Rightarrow x^\alpha x^\gamma > x^\beta x^\gamma \forall x^\gamma$

ii. $x^\alpha > 1 \quad \forall x^\alpha \neq 1$.

We know that a monomial ordering is well-ordering, for every set of monomials there is a minimal element on the set of monomials.

I. A Lexicographic order is an ordering $\alpha >_{lex} \beta$ iff, the left-most nonzero entry in $\alpha - \beta$ is positive.

II. A Graded Lex order is an ordering $\alpha >_{grlex} \beta$ iff, $|\alpha| > |\beta|$ or $(|\alpha| = |\beta|)$ and $\alpha >_{lex} \beta$.

III. A Graded Reverse Lex order is an ordering $\alpha >_{grevlex} \beta$ iff, $|\alpha| > |\beta|$ or $(|\alpha| = |\beta|)$ and the right most nonzero entry in $\alpha - \beta$ is negative.

D. Definition: Let us suppose $>$ be a monomial ordering and f be a polynomial of $K[x]$. Let us also assume that $f = cx^\alpha +$ monomial terms of the form x^β with $\beta \neq \alpha$, where $c \neq 0$ and for every term of the form x^β, $x^\alpha > x^\beta$ with respect to the ordering $>$. Then

I. $LT(f) = cx^\alpha$ is the leading term.

II. $LM(f) = x^\alpha$ is the leading monomial.

E. Definition: Let us suppose $>$ be a monomial ordering and f be a polynomial of $K[x]$, we can write $f = c_1x^{\alpha_1} + c_2x^{\alpha_2} + \dots + c_rx^{\alpha_r}$ where $a_i \in K/\{0\}, x^{\alpha_i}$ are power products, and $x^{\alpha_1} > x^{\alpha_2} > \dots > x^{\alpha_r}$. Then the leading power product of f, $LP(f) = x^{\alpha_1}$.

F. Definition: The multivariate division algorithm consists of a sequence of reduction steps as follows: Let $f, g, h \in K[x_1, x_2, \dots, x_n]$ with $g \neq 0$.We say that f reduces to h modulo g in one step, denoted by $f : g \longrightarrow h$, if and only if $LP(g)$ divides a nonzero term cx^α that appears in f and $h = f - \left(\frac{cx^\alpha}{LT(g)}\right) g$.

G. Division Algorithm [8]:

Input: $f, f_1, f_2, \ldots, f_s \in K[x_1, x_2, \ldots, x_n]$ with

$f_i \neq 0, (1 \leq i \leq s)$

Output: $a_1, a_2, \ldots, a_s, r$ such that

$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r$ and r is

reduced with respect to $\{f_1, f_2, \ldots, f_s\}$ and

$$\max(LP(a_1)LP(f_1), \ldots, LP(a_s)LP(f_s), LP(r)) = LP(f).$$

Initialization:
$a_1 := 0, a_2 := 0, \ldots, a_s := 0, h = f$

While $h \neq 0$ **Do**

IF $LP(f_i)$ divides $LP(h)$ **THEN** take i least such

that $LP(f_i)$ divides $LP(h)$

$$a_i := a_i + \frac{LT(h)}{LT(f_i)}$$

$$h := h - \left(\frac{LT(h)}{LT(f_i)}\right) f_i$$

ELSE
$r := r + LT(h)$

$h := h - LT(h)$

End

H. Definition: The notion of S-polynomial is very important in determining the Groebner basis. Let f, g be non-zero polynomials in $K[x_1, x_2, \ldots, x_n]$ and let $L = lcm(LP(f), LP(g))$. Then the polynomial $S(f,g) = \left(\frac{L}{LT(f)}\right) f - \left(\frac{L}{LT(g)}\right) g$ is called the S-polynomial of f and g.

Calculation of greatest common divisor (gcd) in most computer algebra system for calculating S-polynomial and to convert to a normal form involves only two polynomials at one time. Therefore, it is a time taking and space consuming process to compute more than two polynomials. So, if the leading terms i.e. $LT(f)$ and $LT(g)$ of the polynomials f and g have no common elements then S-poly(f,g) can be treated as zero with respect to $\{f,g\}$. Therefore, in Buchberger Algorithm such kind of computation could be avoided.

I. Theorem(Hilbert Basis Theorem):

Let K be a field. Then every ideal of $K[x_1, x_2, \ldots, x_n]$ is finitely generated (Cox, D., et al., 2007).

J. Theorem(Buchberger Criterion):

A subset $G \subseteq K[x]$ is a Groebner basis of the Ideal I it generates, iff for every $f, g \in G$ we have $S(f,g) \xrightarrow[G]{} 0$ i.e. the remainder of division of $S(f,g)$ by G is 0.

K. Buchberger Algorithm [2]:

Input: A polynomial set $f = (f_1, f_2, \ldots, f_s)$ that generates an ideal I.

Output: A Groebner basis $G = (g_1, g_2, \ldots, g_r)$ that generates the same ideal I with $f \subset G$.

$G := f$

$M := \{\{f_i, f_j\} | f_i, f_j \in G \text{ and } f_i \neq f_j\}$

Repeat
$\{p, q\}$:=a pair in M

$M := M - \{\{p, q\}\}$

$S :=$ S-poly(p, q)

$h :=$NormalForm(S, G)

IF $h \neq 0$ **THEN**

$M := M \cup \{\{g, h\} \forall g \in G\}$

$G := G \cup \{h\}$

Until $M := \emptyset$.

In many areas of mathematics and engineering problems we encounter the systems of equations of the type

$f_1(x_1, x_{2,} \dots, x_n = 0,\ f_2(x_1, x_{2,} \dots, x_n = 0, \dots,$

$f_m(x_1, x_{2,} \dots, x_n = 0$

Such type of system of equation can be computed and is solvable if and only if the Groebner basis of the equations $f_1, f_2, \dots, f_m$ is not one.

L. Example: Let us assume that $\{x + xy^2 = 1, x^2y + y = 1, x^2 + y^2 = 1\}$ be the system of equations. To see whether it is solvable or not we just use MAPLE to compute the Groebner basis:

$> L := [x + xy^2 - 1, x^2y + y - 1, x^2 + y^2 - 1]$

$> G1 := Groebner[Basis](L, plex(x, y, z));$

$G1 := [1]$

So the given system of equations is not solvable.

M. Example: Consider the following systems of equations:

$$x^2 + y^2 + z^2 = 1$$

$$x^2 + y^2 + z^2 = 2x$$

$$2x - 3y - z = 0$$

Let $J = \langle x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z \rangle$, we can compute Groebner basis for J with respect to the lex ordering using maple:

$> Ideal(J) := [x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z]$

$> G2 := Groebner[Basis](Ideal(J), plex(x, y, z));$

$G2 := [40z^2 - 8z - 23, -1 + 3y + z, -1 + 2x]$

So the Groebner basis $G2 = (g_1, g_2, g_3)$ is given by:

$$g_1 = 40z^2 - 8z - 23$$

$$g_2 = 3y + z - 1$$

$$g_3 = 2x - 1$$

By examining the generators in $G2$, we have one generator, g_1, in the variable $x_n = z$ alone. The other variables have been eliminated during the course of finding the Groebner basis. This equation has a finite number of roots that could be solved by single variable method. So, there is exactly one generator in the variables $x_{n-1} = y$ and $x_n = z$. Because we have all possible roots of z we can solve for y. Generator g_3 is in x alone so roots of x could be easily determine.

III. APPLICATIONS ON GROEBNER BASIS

In qualitative analysis of systems of ordinary differential equations, Groebner basis is used to determine the cyclicity problems, critical period perturbations, center-focus problem, finding linearizability and isochronicity conditions for a given group of polynomials [4]. It is also applied in steady state detection of chemical reaction network (CRN), using CRN as a model of system of ODE, which is nonlinear equations containing several variables. The qualitative conduct of the network can be found after solving the ODE. Finding the solutions of such type of problem is hard. In [13], the authors used Groebner basis to analyze CRNs on biochemical examples.

We see that in the design and investigation of robotics, Groebner basis is used to determine kinematics equations [31]. Additionally, it has been utilized in robotics to decide the unique solutions for the forward kinematic issue uncommonly connected to possessing space and planar parallel manipulator in mechanical technology [12, 23, 24]. Applications of Groebner basis in robotics goes back to 1990's. Many researchers worked on 6R robot inverse problem using quaternion matrix and Groebner basis. To solve the problem in [20], authors applied double quaternion and Groebner basis which encounters 8 irrelevant roots. So, they extracted four $1 + t^2$ common factors in Dixon resultant to eliminate the irrelevant roots and hence a 16 degree equation with single variable is obtained. X.G. Huang and Q.Z. Liao in [11], worked on the same algorithm and they transformed the sine and cosine of angle rotation into plural form instead of extracting common factors resulting in single variable equation involving numerical calculation without rigorous proof. Z.S. Ni, and R.K. Wu in [19] introduced quaternion matrix modeling to solve inverse problems in 6R robots for the first time in three-dimensional space. Also, they have introduced a new algorithm based on quaternion and dual quaternion in matrix form, eliminating five variables using Groebner basis after transforming into matrix form. Thus, in this algorithm they could determine the degree of the equation with single variable without any extraneous roots.

So far, many researchers, Gelernter, H., Wu Wen-Tsun and so on in [29, 10, 7, 22, 28], had studied Automated Geometric Theorem proving. Automatic Geometric Theorem proving is the process of proving mathematical theorems with the help of computer program and generates automatically complementary condition that is true for the theorem in [9]. Related works have been found on many papers in [6,16, 21]. In the paper [5], the authors proposed a method by using parametric Groebner basis for proving geometric theorem automatically. Yao Sun, DingKang Wang and Jie Zhou; introduced a new method for proving and discovering geometric theorems automatically in [26]. They extended Rabinovitch's trick to show that a polynomial is radical membership, zero divisors or invertible about an ideal. Applying Rabinovitch's trick and the properties of Comprehensive Groebner System in automatic geometric theorem proving, they have shown whether a geometric statement is true, true on component, generic false or complete false on non-degenerate case in [26].

Uses of Groebner basis could be found in vast area in circuits and systems, for example, the algebraic representation of error bounds for depicting function applying to nonlinear circuit frameworks and the advancement of productive representative methodology for testability measures and ambiguity groups for resolving simple linear circuits in [4]. Additionally, application can be found at solving the load-flow problem as the progressions associated with an electrical network shift [17].

IV. OPEN PROBLEM

If G_1 is a square matrix or a unimodular matrix and the determinant is a non-singular constant in K of an n-dimensional polynomial matrix F then it is very difficult to determine the factorization $F = G_1F_1$ by Groebner basis or by conventional methods. The authors in [32] have pointed out that this problem is very significant in n-dimensional systems theory.

V. CONCLUSION

Here we have shown some of the applications of Groebner basis and provided some of the information about this important technique of Groebner basis. We see that using the properties of Groebner basis the solutions of systems of equations could be easily determined. We can use Computer Algebra Systems like Maple, Singular, Mathematica, Reduce, CoCoCA, Macauley2, etc., to find this technique.

REFERENCES

1. B. Buchberger, An Algorithm for finding a Basis for a Residue Class Ring of a Zero-Dimensional Polynomial Ideal, (Thesis), University of Innsbruck (Austria), 1965.
2. B. Buchberger, Groebner-basis: An Algorithmic Method in Polynomial Ideal Theory, Reidel Publishing Company, Dodrecht Boston – Lancaster, 1985.
3. B. Buchberger, and K. Manuel, Groebner Basis, from http: // www.scholarpedia.org /article/Groebner basis, 2010.
4. B.Cannas, A.Fanni, & A. Montissci, Testability evaluation for analog linear circuits via transfer function analysis, In Proc. ISCAS, Kobe, Japan 992-995, 2005.
5. X.F. Chen, P. Li, L.Lin, & D.K. Wang, Proving Geometric Theorems by Partitioned-parametric Groebner basis, In Hong, H. Wang, D(eds.) (ADG): LNAIS, Heidelberg, vol. 3763, 33-44, 2004.
6. S.C. Chou, Mechanical Geometry Theorem Proving, Mathematics and its Applications, D. Reidel Publ. Comp. ,1988.
7. S.C. Chou, & X.S. Gao, Mechanical formula derivation of elementary geometries, In: *ISSAC*,265–270, 1990.
8. D. Cox, J. Little, & D. O'Shea, Groebner basis: Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Undergraduate Texts in Mathematics. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.
9. G. Dalzotto and T. Recio, On protocols for the automated discovery of theorems in elementary geometry, J. Automated Reasoning, 3, 203–236, 2009.
10. H. Gelernter, Realization of a geometry theorem proving machine, In: PICIP, *Processing*, *Paris*, 273–282, 1959.
11. X.G. Huang, and Q.Z. Liao, New algorithm for inverse kinematics of 6R serial robot mechanism. *Journal of Beijing University of Aeronautics and Astronautics. 36*, 295-293, 2010.
12. C.M. Kalker-Kalkman, An implementation of Buchbergers' algorithm with applications to robotics, *Mechanism Mach.Theory*, *28*(4), 523-537, 1993.
13. I. Martinez-Forero, A., Pelaez-Lopez, & P. Villoslada,, Steady State Detection of Chemical Reaction Networks Using a Simplified Analytical Method, *PLOS ONE*, *5* (6), 1-6, 2010.
14. M. Matej, On Groebner Basis and their use in solving some practical problems, Universal *Journal of Computational Mathematics*, *1*(1), 5-14, 2013.
15. D. Mirandola, Some basic ideas about Groebner basis and their applications to Euclidean geometry, from http://math.sun.ac.za/ wp-content/ uploads /2011/04/ Diego-Mirandola-Groebner-bases, 2011.
16. A. Montes, and T. Recio, Automatic discovery of geometry theorems using minimal canonical comprehensive Groebner systems, In: *Proceeding of (ADG) 2006: Lecture Notes in Artificial Intelligence, Springer, Berlin, Heidelberg*, vol. 4869, 113-138, 2007.
17. A. Montes, Algebraic solution of the load-flow problem for a 4-nodes electrical network, *Math. Computation Simulation*, *45*(**1-2**), 163-174, 1998.
18. Mvngu. Polynomials and affine space, from https://mvngu. wordpress.com /2009/03/27/polynomials-and-affine-space, 2009.
19. Z.S. Ni, & R.K. Wu, 6R Robot Inverse Solution Algorithm Based on Quaternion Matrix and Groebner Bases, *Advances in Linear Algebra and Matrix Theory*, *8***,** 33-40, 2018.
20. S. Qiao, Q. Liao, S. Wei, and H.J. Su, Inverse kinematic analysis of the general 6R serial manipulators based on double quaternions. *Mechanism and Machine Theory*. *45*, 193-197, 2010.
21. T. Recio, & M. Velez, Automatic Discovery of Theorems in Elementary Geometry, *J. Automat. Reason*, *23*, 63-82, 1999.
22. J. Robu, Automated Proof of Geometry Theorems Involving Order Relation in the Frame of the Theorem. Project., In: Horia F. Pop, editor, Knowledge Engineering: Principles and Techniques, number Special Issue in Studia Universitatis "Babes-Bolyai", Series Informatica, 307-315, 2007.
23. L. Rolland, Certified solving of the forward kinematics problem with an exact algebraic method for the general parallel manipulator, J. Adv. Robot, 20(9), 1035-1065, 2005.
24. L. Rolland, Synthesis on forward kinematics problem algebraic modeling for the planar parallel manipulator: Displacement based equation systems, *J. Adv. Robot*, *19*(9), 995-1025, 2006.
25. M. Rosenblum, Generalized Hermite polynomials and the Bose-like oscillator calculus, In: *Operator Theory: Advances and Applications, Birkhauser, Basel*, 369-396, 1994.
26. Y. Sun, D. Wang, and J. Zhou, A new method of automatic geometric theorem proving and discovery by comprehensive Groebner systems. In: *Proc. ADG 2012* , *http: // dream. infed.ac.uk /events /adg2012 /uploads / proceeding s/ADG2012-proceedings.pdf#page=163, 2012*.
27. M. Torrente, *Application of Algebra in the oil Industry*, Anno Academico, 2008-2009.
28. D. Wang, Geometry machines: From ai to smc., In: Jacques Calmet, John Campbell, and JochenPfalzgraf, editors, In: AISMC*(LNCS), Springer Berlin / Heidelberg*, *1138*, 213-239, 1996.
29. Wu Wen-Tsun, Basic principles of mechanical theorem proving in elementary geometries, *Journal of Automated Reasoning*, *2*, 221–252, 1986.

30. M. Yagi, T. Hisakado, & K. Okumura, Algebraic representation of error bounds for describing function using Groebner base, In: *Proc. ISCAS, Kobe, Japan*, 2831-2834, 2005.
31. L.Zhiping, X.Li, & K. B. Nirmal A Tutorial on GrÖbner Bases With Applications in Signals and Systems, *IEEE Transactions on Circuits and Systems I*, 2008.
32. D.C. Youla. and G. Gnavi, Notes on n-dimensional system theory, *IEEE Trans. Circuits Syst.*, vol. CAS-26, no.2, pp. 105-111, Feb. 1979.

AUTHORS PROFILE

Dr. Yengkhom Satyendra Singh, Assistant Professor, School of Applied Sciences, Reva University, Bangalore, India, earned his Ph.D. degree in Mathematics in the year 2011 and M.Sc. degree (Mathematics) in the year 2004 from Jamia Millia Islamia (Central University), New Delhi. His areas of interests are Commutative and non-commutative algebra and its applications in allied fields.

Dr. Benaki Lairenjam is working as an Assistant Professor in the Department of Mathematics, School of Applied Sciences, Reva University Bangalore India. She completed her PhD from Jamia Millia Islamia (Central University), New Delhi. During her research work she has developed classification models using artificial neural Network, Bayes Theorem, Naïve Bayes classifier and Associative Classifiers for the classification of breast cancer mammography data.