International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:5, No:5, 2011

Some Applications of Gröbner bases

Hassan Noori, Abdolali Basiri, and Sajjad Rahmany

Abstract—In this paper we will introduce a brief introduction to theory of Gröbner bases and some applications of Gröbner bases to graph coloring problem, automatic geometric theorem proving and cryptography.

Keywords—Gröbner bases, Application of Gröbner bases, Automatic Geometric Theorem Proving, Graph Coloring, Cryptography.

I. Introduction

We know from the Hilbert Basis Theorem that any ideal $\mathfrak{I}$ in a polynomial ring over a field is finitely generated. However, through of all generators for $\mathfrak{I}$, we try to find the best generators to describe the ideal. More precisely we are looking for a generator G for $\mathfrak{I}$ in order to answer the following questions [2], [8]:

1) Equality of ideals:
   Reduced Gröbner bases are unique for any given ideal and monomial ordering, and also often computable in practice. Thus one can determine if two ideals $\mathfrak{I}, \mathfrak{J}$ are equal by looking at their reduced Gröbner bases.
2) Ideal membership problem:
   Let $\mathbf{R} = \mathbb{K}[x_1, \ldots, x_n]$ be a polynomial ring, given an ideal $\mathfrak{I} \in \mathbf{R}$ where $\mathfrak{I} = \langle f_1, \ldots, f_s \rangle$, and given $f \in \mathbf{R}$, determine whether $f \in \mathfrak{I}$? If so, can we compute $h_1, \ldots, h_s \in \mathbf{R}$ such that $f = h_1 f_1 + \cdots + h_s f_s$?
   To do this, we compute a Gröbner basis G for $\mathfrak{I}$, then $f \in \mathfrak{I}$ if and only if the reminder of the dividing f by G is 0.
3) Solving a system of polynomial equations:
   One of the most important applications of Gröbner basis is the solving of a system of polynomial equations

$$\begin{cases} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ \quad\vdots & \\ f_m(x_1, \ldots, x_n) &= 0 \end{cases} \tag{1}$$

   To do this, at the first we compute a Gröbner basis $G = \{g_1, g_{2,1}, g_{2,2}, \ldots, g_{2,r_2}, \ldots, g_{n,1}, g_{n,2}, \ldots, g_{n,r_n}\}$ for the ideal generated by $f_1, f_2, \ldots, f_m$ with respect to lexicographical order. In general we obtain the following form for our equations:

$$\begin{cases} g_1(x_1) = 0 \\ g_{2,1}(x_1, x_2) = 0, \ldots, g_{2,r_2}(x_1, x_2) = 0 \\ \vdots \\ g_{n,1}(x_1, \ldots, x_s) = 0, \ldots, g_{n,r_n}(x_1, \ldots, x_s) = 0 \end{cases} \tag{2}$$

   It is often easy to compute the solutions of the later system of polynomial equations.
4) Existence of solutions:
   The system of polynomial equations 1 has a solution if and only if the Gröbner basis of $\{f_1, \ldots, f_m\}$ is not equal to $\{1\}$.
5) Number of solutions:
   The system of polynomial equations 1 has a finite number of solutions if and only if any Gröbner basis of $\{f_1, \ldots, f_m\}$ has the following property: For every variable x_i, there exists a polynomial such that its leading term with respect to the chosen term ordering is a power of x_i.

To compute a Gröbner basis we need a division algorithm in $\mathbb{K}[x_1, \ldots, x_n]$, like the division algorithm in $\mathbb{K}[x]$. Unfortunately since there are multiple variables and multiple divisors, the remainder of this division is not unique. Hence if the remainder of the division of f by $f_1, \ldots, f_m$ is equal to zero then f is in the ideal generated by $f_1, \ldots, f_m$, but if the remainder is not equal to zero we don't know whether f is in the ideal generated by $f_1, \ldots, f_m$?

However, if we choose a good divisor, then the remainder is unique regardless of the order of the divisors. These divisors are called a **Gröbner basis**.

In order to define a Gröbner basis, we first need to introduce some notations. If we fix a term order $\succ$, then every polynomial f has a unique **leading monomial** denoted by $LM(f) = x^\alpha$, this is the largest monomial x^α with respect to the term order $\succ$ which occurs with nonzero coefficient in the expansion of f. The coefficient of the leading monomial x^α is called the **leading coefficient** of f and denoted by $LC(f)$, finally the **leading term** of f is defined by $LT(f) = LC(f)LM(f)$ [8].

Definition 1 (Gröbner basis) *A Gröbner basis for an ideal $\mathfrak{I}$ in $\mathbb{K}[x_1, \ldots, x_n]$ is a generating set $G = \{g_1, \ldots, g_m\}$ such that the set $\{LT(g_i) : 1 \leq i \leq n\}$ is a generator set for the ideal generated by $LT(I) = \{LT(f) : f \in \mathfrak{I}\}$ [8].*

If the monomial order $\succ$ is fixed, then every ideal $\mathfrak{I}$ in $\mathbb{K}[x_1, \ldots, x_n]$ has a unique reduced Gröbner basis.

There is some algorithms to compute the Gröbner bases, B. Buchberger presented a such algorithm in his PhD thesis [7]. Later, Faugere presented the $F4$ and $F5$ algorithms, which are improved versions of the principal Buchberger algorithm [9], [10].

II. The 3-Colorable Problem

There is a well-known problem in graph theory called the 3-color problem. Given a graph, we would like to know that if it can be three colored. Specifically, let $\mathcal{G}$ be a graph with n

School of Mathematics and Computer Science, Damghan University
nouri.hasan@gmail.com, {basiri,s_rahmany}@du.ac.ir
Research supported by the Research Affairs of Damghan University

vertices, and suppose that any two vertices share at most one edge. Can each vertex be colored with 3 colors in such a way that adjacent vertices do not have the same color?

Problem: Given a graph $\mathcal{G}$, find an assignment of 3 colors to the vertices of $\mathcal{G}$ such that two vertices connected by an edge have different colors.

The Gröbner basis technique can be applied to solve this problem([1], [2]).

Gröbner bases can be used to determine whether or not a system of equations has a solution, and thus are a simple way to solve the system of equations associated with graph colorings.

Let $\mathcal{G}(V, E)$ be a graph with vertices $V = \{1, \ldots, n\}$.

Definition 2 (k-coloring) *A k-coloring of $\mathcal{G}$ is a function from V to a set of k colors such that adjacent vertices have distinct colors.*

Given a graph $\mathcal{G}$, find an assignment of 3 colors to the vertices of $\mathcal{G}$ such that two vertices connected by an edge have different colors.

Let $\zeta = e^{\frac{2\pi i}{3}}$ and assign to each vertex one of 1, ζ, ζ^2 (representing the 3 colors), where ζ is a cube root of unity. Recall that a cube root of unity satisfies $\zeta^3 = 1$. Notice that 1 and ζ^2 are the other two cube roots of unity. Also recall Euler's formula, $\zeta = e^{\frac{2\pi i}{3}} = \cos\frac{2\pi i}{3} + i\sin\frac{2\pi i}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. For the n vertices of k labeled by the variables $x_1, \ldots, x_n$ therefore the condition that we assign to each vertex a cube root of unity means we must have:

$$x_i^3 - 1 = 0 \tag{3}$$

for $i = 1, \ldots, n$. Now the condition that adjacent vertices i, j have assigned a different root of unity is characterized by the equation

$$x_i^2 + x_i x_j + x_j^2 = 0. \tag{4}$$

Recall that each vertex will have a color, hence

$$x_i^3 = x_j^3 = 1.$$

Then for adjacent vertices

$$x_i^3 - x_j^3 = (x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0 \tag{5}$$

Since we want x_i and x_j to have different colors, the only way to satisfy equation 5 is

$$x_i^2 + x_i x_j + x_j^2 = 0. \tag{6}$$

Consider each pair of adjacent vertices in the above graph. Let $\mathfrak{I}$ be the ideal in $\mathbb{K}[x_1, \ldots, x_n]$ generated by these polynomials.

Theorem 3 *A graph is 3-colorable if and only if the set of polynomials associated with our graph have a common solution in the complex numbers.*

Now suppose that the polynomials associated with adjacent vertices have a common solution. This means that there exists x_i, x_j such that $x_i^2 + x_i x_j + x_j^2 = 0$ for all pairs of adjacent vertices. Notice that $x_i \neq x_j$ for this to be true. Then $x_i^3 - x_j^3 = 0$ and we know from above that x_i and x_j will be assigned different colors. Hence the graph is 3-colorable.

Therefore, $\mathcal{G}$ is 3-colorable if and only if $V(\mathfrak{I}) \neq \emptyset$ if and only if $\mathfrak{I} \neq \langle 1 \rangle$, this is true if and only if, B, the corresponded Gröbner basis of $\mathfrak{I}$, is not equal to $\{1\}$. In this case we can solve the equations to get a specific coloring.

III. Application in Cryptography

There are several general purpose algorithms for Jacobian arithmetic, specially for superelliptic and C_{ab} curves, some efficient algorithms are described in [3], [12], [14] and [6]. The closely related arithmetic of cubic curves with several points at infinity is treated in [17]. The algorithms use the representation of Jacobian elements by polynomials and rely on rather heavy techniques of symbolic computation like **LLL**, Hermite normal form and Gröbner basis computation. On a high level, to compute the addition of two ideals $\mathfrak{I}_1$ and $\mathfrak{I}_2$ a unifying description can be obtained as follow:

Algorithm 1

1) Compute a Gröbner basis for $\mathfrak{I} := \mathfrak{I}_1\mathfrak{I}_2$
2) Select some $u \in \mathfrak{I}$ and an integral ideal $\mathfrak{J}$ in the class of $\mathfrak{I}^{-1}$, such that $\mathfrak{J} = u\mathfrak{I}^{-1}$.
3) Put $e := \min_{C_{ab}}\{h \mid h \in \mathfrak{J}\}$.
4) Put $\mathrm{RED}(\mathfrak{I}) := e\mathfrak{J}^{-1} = \frac{e}{u}\mathfrak{I}$.

Arita represents ideals of $K[C]$ by their Gröbner bases with respect to the C_{ab} order, and chooses u as the C_{ab} minimum of $\mathfrak{I}$. His approach relies on Buchberger's algorithm, whose complexity in the C_{ab} setting is not quite clear.

In [12] and [14], ideals are represented by their Hermite normal forms as $K[X]$-modules, or equivalently by their Gröbner bases with respect to the lexicographic order. The natural choice for u is then the minimum with respect to this order. The minimum for the C_{ab} order can be computed via a variant of **LLL** for function fields due to Paulus ([16]).

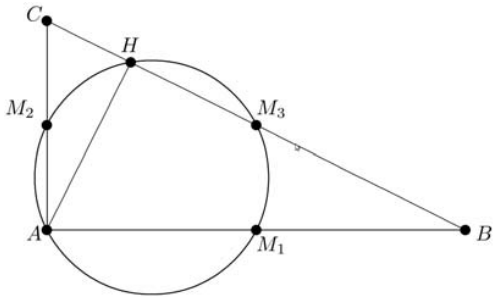
In [4], a new algorithms for realizing the arithmetic in the Jacobians of superelliptic cubics is described. This approach follows the framework of Algorithm general reduction . Representing ideals by their lexicographic Gröbner bases, one can use the FGLM algorithm ([11]) to find the C_{ab} minimum. In [5], closed formula for the reduced ideal in the case of C_{34} is obtained.

IV. Automatic Geometric Theorem Proving

One surprising application of Gröbner bases is "Automatic Geometric Theorem Proving", which use the method of Gröbner bases to prove some problems arising from geometry.

The main key is to translate the hypothesis and conclusions of a theorem to the polynomials language. Then determine whether the thesis lay in hypothesis condition or not. If the conclusion polynomials all belong to the ideal generated by the hypothesis polynomials, then they are true, as are all geometric statements corresponding to polynomials in the ideal.

We introduce this, by an example from [8].



Theorem 4 (The Circle Theorem of Appolonius)
Consider a right triangle spanned by A, B, and C, with the right angle at A. The midpoints of the three sides of the triangle, and the foot of the altitude drawn from A to the edge $\vec{BC}$, all lie on one circle.

The coordinates of the triangle are as follows: we place A at $(0,0)$, B at $(u_1,0)$, and C at $(0,u_2)$, where u_1 and u_2 are arbitrary. The three midpoints at the sides M_1, M_2, and M_3 have their coordinates respectively at $(x_1,0)$, $(0,x_2)$, and (x_3,x_4). Expressing that M_1 is the midpoint of the edge spanned by A and B imposes the condition $h_1 = 2x_1 - u_1 = 0$. The second condition $h_2 = 2x_2 - u_2 = 0$ is imposed by stating that M_2 is the midpoint of the edge spanned by A and C. For M_3 we have two conditions: $h_3 = 2x_3 - u_1 = 0$ and $h4 = 2x_4 - u_2 = 0$.

For the foot of the altitude H we choose coordinates (x_5,x_6). Then we formulate two hypotheses. First: $h_5 = x_5u_1 - x_6u_2 = 0$ expresses that the line segment AH is perpendicular to the edge BC. Second: $h_6 = x_5u_2 + x_6u_1 - u_1u_2 = 0$ means that the points B, H, and C are collinear. To formulate these conditions we use the slopes defined by the segments.

Finally, we consider the statement that the three midpoints and H lie on a circle by saying that the circle through the three midpoints must also contain H. Let (x_7,x_8) be the coordinates of the center O of the circle. We have two more conditions: $M_1O = M_2O$ and $M_1 = M_3O$, given respectively by $h_7 = (x_1-x_7)^2 + x_8^2 - x_7^2 - (x_8-x_2)^2 = 0$ and $h_8 = (x_1-x_7)^2 + x_8^2 - (x_3-x_7)^2 - (x_4-x_8)^2 = 0$.

The eight hypothesis form the following system

$$f(\mathbf{u},\mathbf{x}) = \begin{cases} 2x_1 - u_1 = 0 \\ 2x_2 - u_2 = 0 \\ 2x_3 - u_3 = 0 \\ 2x_4 - u_4 = 0 \\ x_5u_1 - x_6u_2 = 0 \\ x_5u_2 + x_6u_1 - u_1u_2 = 0 \\ (x_1-x_7)^2 + x_8^2 - x_7^2 - (x_8-x_2)^2 = 0 \\ (x_1-x_7)^2 + x_8^2 - (x_3-x_7)^2 - (x_4-x_8)^2 = 0 \end{cases}$$

With respect to these eight hypotheses, the conclusion must then be that $HO = M_1O$, expressed by

$$g = (x_5-x_7)^2 + (x_6-x_8)^2 - (x_1-x_7)^2 - x_8^2 = 0.$$

The theorem is true if g belongs to the ideal spanned by the polynomials which vanish over the zero set of the hypotheses.

APPENDIX A
APPENDIX

As a proof of our work, the following maple code attached, it determines a given graph is 3-colorable or not?

```
>restart:
>#Create the system of equations
x[i]^3-1=0 for i=1,...,n
>#  that n is number of variable (number of
graph vertex);
>crit1:=proc(L)
>local F:
>F:=x->x^3-1:
>#L:={seq(x[i],i=1..n)}:
>map(F,L):
>end:
>##############
>crit1({x[1], x[2], x[3], x[4]}):
>#Create the system of equations
x[i]^2+x[i]*x[j]+x[j]^2=0 for i=/=j
>#  that x[i] and x[j] are vertices that
connected by an edge;
>##############
>crit2:=proc(L)
>local F,k,sys,n:
>n:=nops(L):
>F:=(i,j)->x[i]^2+x[i]*x[j]+x[j]^2:
>sys:={}:
>for k to n do
>sys:=sys union {map(F,op(L[k]))}:
>od:
>sys,indets(sys):
>end:
>##############
>crit2({[1,2],[2,3],[4,3],[2,4]}):
>#This procedure return true if a graph is
3-colorable or false in otherwise;
>#  the input L is a representation of a
graph, which
>#  any pair (i,j) in L means that x[i] is
connected to x[j]
>#  by an edge;
>##############
>colorable:=proc(L)
>local sys,vars:
>sys,vars:=crit2(L):
>sys:=sys union crit1(vars):
>Groebner[Basis](sys,plex(op(vars))):
>if member(1,%) then RETURN(false) else
RETURN(true) fi:
>end:
>##############
>colorable({[1,2],[2,3],[4,3],[2,4]});
>                                    true
>exam1:=[[1,2],[1,5],[1,6],[2,3],[2,4],[2,8],[3,4]
        ,[3,8],[4,5],[4,7],[5,6],[5,7],[6,7],[7,8]
>colorable(exam1);
>                true
```

REFERENCES

[1] W. Adams, *"Minicourse, Second Lecture Applications of Gröbner Bases"*. University of Maryland, March, 2005.
[2] W. Adams, and P. Loustaunau, *"An Introduction to Gröbner Bases"*. AMS, Providence, Rhode Island, 1994.
[3] S. Arita, *"Algorithms for computations in Jacobian group of Cab curve and their application to discrete-log based public key cryptosystems"*. IEICE Transactions, J82-A(8):12911299, 1999. In Japanese. English translation in the proceedings of the Conference on The Mathematics of Public Key Cryptography, Toronto 1999.
[4] A. Basiri, A. Enge, J.-C. Faugere, and N. Gurel. *"Fast arithmetic for superelliptic cubics"*.
[5] A. Basiri, A. Enge, J.-C. Faugere, and N. Gurel. *"Implementing the arithmetic of C34 curves"*. In Proceedings of ANTS-VI, Lecture Notes in Computer Science, pages 87101. Springer-Verlag, June 2004.
[6] M.-L. Bauer. *The arithmetic of certain cubic function fields.* Preprint, 2001.
[7] B. Buchberger, *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (German).* PhD thesis, University of Innsbruck, Austria, 1965.
[8] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms.* Springer: New York, 1997.
[9] J.-C. Faugere, *A new efficient algorithm for computing Gröbner bases (F4)*, Effective methods in algebraic geometry (Saint-Malo, 1998), J. Pure Appl. Algebra 139 no. 1-3 (1999) 6188.
[10] J.-C. Faugere, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, 7583 (electronic), ACM, New York, 2002.
[11] J.-C. Faugere, P. Gianni, D. Lazard, and T. Mora. *Efficient computation of zero-dimensional Gröbner bases by change of ordering.* Journal of Symbolic Computation, 16:329344, 1993.
[12] S.-D. Galbraith, S. Paulus, and N.-P. Smart. *Arithmetic on superelliptic curves.* Mathematics of Computation, 71(237):393405, 2002.
[13] A. Heck, *A Bird's-Eye View of Gröbner Bases*, CAN Expertise Center, 1996.
[14] R. Harasawa and J. Suzuki. *Fast Jacobian group arithmetic on Cab curves.* In Wieb Bosma, editor, Algorithmic Number Theory ANTS-IV, volume 1838 of Lecture Notes in Computer Science, pages 359376, Berlin, 2000. Springer-Verlag.
[15] J. Verschelde, *Lecture Note in Analytic Symbolic Computation*, UIC, Dept. of Math, Stat & CS, spring 2009.
[16] S. Paulus. *Lattice basis reduction in function fields.* In J. P. Buhler, editor, Algorithmic Number Theory ANTS-III, volume 1423 of Lecture Notes in Computer Science, pages 567575, Berlin, 1998. Springer-Verlag.
[17] R. Scheidler, *Ideal arithmetic and infrastructure in purely cubic function fields.* Journal de Theorie des Nombres de Bordeaux, 13:609631, 2001.