STUDIA UNIV. "BABEŞ-BOLYAI", INFORMATICA, Volume II, Number 1, 1997

GRÖBNER BASES FOR THEOREM PROVING IN EUCLIDEAN GEOMETRY

ALIN BLAGA

Abstract. It is known that the three dreams of Descartes in november 1619 become the first theoretical bases of the analytic geometry, but one of them will never come to light until 370 years later. This paper will briefly discuss about this last dream of Descartes: proving a theorem of plane geometry is a matter of reducing it to a statement saying that a polynomial identity is a consequence of other known polynomial identities ([Lev93]). This last part, although is not new at all, has been automatised due to the Gröbner bases

1. Introduction

The problem of theorem proving is older than someone can imagine. Its roots seems to be linked with Euclid's Stoicheia, arround 330 b.C. One might find there theorems from number theory with its famous Euclid's algorithm, or some theorems from plane geometry. Euclid tried to find methods to give algorithms for theorems proving, starting from the idea that a theorem is proved via logical deductions, making use of a set of axioms or other already proved theorems.

For many years the theorem proving in plane geometry had an empiric character. Later, Reneé Descartes (1596-1650) had three dreams, from which he imagined the vaste opera Le Monde. In 1637 he published his fundamental opera Un discours de la Méthode pour conduire correctement la Raison et chercher la Vérité dans le Sciences; En outre essais de cette Méthode en Diôptrique, Météores, Géométrie, where he put the first bases of what we know as analytic geometry. Thus, his last dream came to life, but the problem never been automatised until the Gröbner Bases Theory appeared.

This paper tries to be as accesible as possible, in order to put in touch the reader with this new view of theorem proving, where Gröbner bases are very much involved ([Dav92]).

Received by the editors: December 15, 1997.

¹⁹⁹¹ Mathematics Subject Classification. 01A45, 68Q40.

¹⁹⁹¹ CR Categories and Descriptors. I.1.2 [Algebraic Manipulation]: Algorithms -^{algebraic} algorithms.

2. Ideal membership problem

As we already know the Euclidean n-space

$$\mathbb{R}^n = \{(x_1, \ldots, x_m) | x_i \in \mathbb{R}, i = \overline{1, n}\}$$

is an affine n-space ([DC92], [AL92], [Coh93]). One defines here a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$ which determines a function $\mathbb{R}^n \to \mathbb{R}$, defined by

$$(x_1,\ldots,x_n)\mapsto f(x_1,\ldots,x_n)$$

for all $(x_1, \ldots, x_n) \in \mathbb{R}^n$, called *evaluation*.

Thus we throw a light between geometry and algebra. This light is still too weak to enlight the bridge and we have to go further and give an explicitly and complete algebraic model for Tarski's result ([Bot96]). As a first step we are going to identify the set of multivariate polynomials assigned to the set of axioms needed to prove an existing theorem by the corresponding system of polynomial equations. So, given $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$, the set of all solutions for the system

(1)
$$f_1 = 0, \ldots, f_m = 0$$

is called *variety* defined by f_1, \ldots, f_m :

(2) $V(f_1,\ldots,f_m) = \{(x_1,\ldots,x_n) \in \mathbb{R}^n | f_1 = 0,\ldots,f_m = 0\}.$

Why we need this? In fact, a variety gives an algebraic landscape of a geometrical object. See for instance that $V(x^2 + y^2 - 1) \subseteq \mathbb{R}^2$ is nothing else but the circle in the xy plane with the center being the origin and the radius equal to 1.

In the world of numerical analysis there are many methods to find a variety, more precisely, some of its elements. Unfortunately these methods doesn't show us the geometric properties of the solution space. Besides, the computation speed can be improved by changing the system with an equivalent one, as in Gauss-Jordan elimination, so the last system obtained is easier to solve, but this method applies only for a class of systems of polynomial equations. One might think that we are going to stray from the subject of this paper. Actually we are not. We are not even interested in obtaining the solutions, but only to give an algebraic and geometric information about a system of type (1). This will be fulfilled by starting to take into consideration the ideal generated by a set of polynomials f_1, \ldots, f_m :

(3)
$$I = \langle f_1, \dots, f_m \rangle = \\ = \{a_1 f_1 + \dots + a_m f_m | a_i \in \mathbb{R}[x_1, \dots, x_n], i = \overline{1, m}\}.$$

Can be very easily verified that I is an ideal indeed ([DC92], [Coh93], [WWA95]). Given $f \in \mathbb{R}[x_1, \ldots, x_n]$ and $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ a non-zero ideal, Gröbner bases theory gives an algorithm¹ to check whether $f \in I$ or not, which is the ideal

¹Called *Buchberger*'s algorithm, following the name of Gröbner bases inventor. Wolfgang Gröbner was the advisor of Bruno Buchberger's thesis.

GRÖBNER BASES IN GEOMETRY

membership problem. To solve it we have to find a "nicer" representation of the ideal I and that it will be a Gröbner basis for I.

3. Gröbner bases

Most of the books appeared in this field ([WWA95], [Lev93], [CD92]) gives a quite nice and interesting presentation of what Gröbner basis means. We are going to define it from another the point of view, for our purposes, related to the goal of this paper. Moreover, this brief presentation is concieved in a manner that will lead the reader to the impression that Gröbner bases theory is not a difficult subject and it will be easier for him later, to read some high level stuff about this beautiful subject ([Dav92], [JHD93], [Coh93]).

In order to do this, lets study an easy to follow example, for the univariate polynomials case. Take $f = x^4 + x^3 - 2x^2 + 8x$, $f_1 = x^2 + 2x - 1$, $f_2 = x$ and the ideal $I = \langle f_1, f_2 \rangle \subseteq \mathbb{R}[x]$. If one tries to divide f by $x^2 + 2x - 1$ will get $f = (x^2 - x + 1)(x^2 + 2x - 1) + 5x$, which means that $f \in I$. Following the notation $f \xrightarrow{g} h$, where h is the remainder of the division of f by g, our result looks like $f \xrightarrow{f_1} 5x \xrightarrow{f_2} 0$. Or much shorter $f \xrightarrow{f_1, f_2} 0$.

Thus, in the univariate polynomials case, the ideal membership problem looks like the Euclidean algorithm.

In general, given $I \subseteq \mathbb{R}[x]$ a non-zero ideal

$$(4) f \in I \Leftrightarrow f \xrightarrow{I} 0.$$

Is it true that problem (4) can always be solved? What happens if the generating set of I is infinite? As far as we know up to now there is no information that might enlighten us. Anyway, there is a crucial result that led to all the results in Gröbner bases theory, the so called *Hilbert Basis Theorem*. For the univariate ^{case this} will be:

Theorem 3.1. In the ring $\mathbb{R}[x]$ we have the following:

- (i) If $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$ is an ascending chain of ideals of $\mathbb{R}[x]$, then there exists n_0 such that $I_{n_0} = I_{n_0+1} = I_{n_0+2} = \dots$
- (ii) If I is an ideal of $\mathbb{R}[x]$ then there exists a finite set of polynomials $f_1, \ldots, f_m \in \mathbb{R}[x]$ $\mathbb{R}[x]$ such that $I = \langle f_1, \ldots f_m \rangle$.

It is now clear if an algorithm for (4) exists, it will always terminates and ^{We} got some answers for the questions posed above ([WWA95], [CD93]).

There is only one more step before to define a Gröbner basis and that is There is only one more step before to define a Grobner otal $g_{e_{nerating}}$ with the ideal's structure. So, what happens if an element of the meriting with the ideal's structure. $g_{enerating set}$ of a non-zero ideal *I* can be expressed as a linear combination of h_{e} others? G the others? Can be done something about it? In fact nothing happens, but one $\frac{1}{100}$ be done something about it? In fact nothing set and that it will $\frac{1}{10}$ $\frac{1}{10}$ ^{be a} Gröbner basis.

We discussed in this section only about the univariate polynomials over \mathbb{R} and the real problems about Gröbner bases are posed for $\mathbb{R}[x_1, \ldots, x_n]$. The extension to the multivariate polynomials case can be done easily by defining a term ordering ([CD92], [WWA95]). Afterwards Hilbert's Basis Theorem will be still on its feet and the division algorithm will become a little more complicated. Why an ordering? Only then we can make the division work algorithmically ([KOG92]).

Theorem 3.2. Hilbert Basis Theorem. In the ring $\mathbb{R}[x_1, \ldots, x_n]$ we have the following:

- (i) If $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$ is an ascending chain of ideals of $\mathbb{R}[x_1, \ldots, x_n]$, then there exists n_0 such that $I_{n_0} = I_{n_0+1} = I_{n_0+2} = \ldots$
- (ii) If I is an ideal of $\mathbb{R}[x_1, \ldots, x_n]$ then there exists a finite set of polynomials $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_m \rangle$.

Definition 3.3. Now let $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$ a non-zero ideal and $G \subseteq I$. Then G is a Gröbner basis for I if and only if

(5)
$$f \in I \Leftrightarrow f \xrightarrow{G} + 0, \text{ where } f \in \mathbb{R}[x_1, \dots, x_n].$$

Implementation of Buchberger algorithm, the method to find a Gröbner basis for a generating set of a multivariate polynomials, implies to define the Spolynomials ([WWA95]) and on this way to present a strategy of how to obtain a Gröbner basis. Because the purpose of this paper is to give a challenge for the theorem proving in the Euclidean geometry, we are not going to insist on this theory, we already done what we wanted to do in order to link it with our goal. Moreover, up to now we hope that this presentation was a good arouser for your interest in this part of Computer Algebra.

4. Examples of theorem proving

As we have seen up to now, in order to prove a theorem we have to express the hypotesis and the conclusion as a system of polynomial equations. After this is done, to prove that the theorem is valid means to prove that the polynomial from the conclusion is a linear combination of the hypotesis polynomials. In other words, the conclusion's polynomial normal form is zero with respect to the Gröbner basis of the hypotesis polynomials.

4.1. Carnot's Theorem.

Theorem 4.1. Given a triangle, the circumscript circle is equal to the circumscript circles determined by each of the two of triangle's vertices and the orthocenter.

The first step to do in order to prove this theorem is to choose a proper coordinate system. As we can see from the picture, a good start is to take the

94

GRÖBNER BASES IN GEOMETRY C(0,c) H(0,h) O0(x0 Y0) O(0,0) A(a,0) B(b/0) $O_1(x_1, y_1)$

FIGURE 1. Carnot's Theorem

points like A(a, 0), B(b, 0), C(0, c). Then the orthocenter is H(h, 0), the $\triangle ABC$'s circumcenter is $O_0(x_0, y_0)$ and the $\triangle ABH$'s circumcenter is $O_1(x_1, y_1)$.

An important remark to make here is that the orthocenter's and circumcenters' coordinates are parametric, we don't know their exact expressions, but they can be computed. According to this, the variables needed to compute the ^{corresponding} Gröbner basis will be only the undeterminates x_0 , y_0 , x_1 , y_1 , h. But this is the nice part of theorem prooving, you don't have to express every point, just to give relations that will figure out what their position means. For example, to say that $O_0(x_0, y_0)$ is $\triangle ABC$'s circumcenter we write $|O_0A| = |O_0B| = |O_0B|$. From this relations we extract the first polynomial identities we will need, saying

(6)
$$SquareLine(M, N) = (x_M - x_N)^2 + (y_M - y_N)^2 =$$

(7)
$$f_1 = SquareLine(O_0A) - SquareLine(O_0B) = 0$$

(9)

$$f_2 = SquareLine(O_0A) - SquareLine(O_0C) = 0$$

Analogous, to say that $O_1(x_1, y_1)$ is $\triangle ABH$'s circumcenter we write $|O_1A| = |O_1H| =$ Analogous, to say that $O_1(x_1, y_1)$ is $\triangle ABH$ is circumcented identities: $|O_1B| = |O_1H|$, from which we come up with another polynomial identities:

$$f_{3} = SquareLine(O_{1}A) - SquareLine(O_{1}B) = 0$$

$$f_{4} = SquareLine(O_{1}A) - SquareLine(O_{1}H) = 0$$

Well, we have to describe in some polynomial identities the orthogonal P_{0} we already know that $CH \perp AB$, but it is not enough, we have to say in a polynomial identities that $CH \perp AB$, but it is not enough the formula We have to describe in some polynomial identities the orthocenter, too. $P_{e_{n}}^{(n)}$ we already know that $CH \perp AB$, but it is not enough, we have $P_{e_{n}}^{(n)}$ identity that $BH \perp AC$, too. For this let introduce the formula $P_{e_{n}}^{(n)}$

$$memar(M, N, P, Q) = (x_N - x_M)(x_Q - x_P) + (y_N - y_M)(y_Q - y_P).$$

95

This means that

(10) $f_5 = Perpendicular(B, H, A, C) = 0.$

Finally, our conclusion, as a polynomial identity should be

(11) $f = SquareLine(O_0C) - SquareLine(O_1H) = 0.$

And that will be all we have to do so far, Maple whil handle the Gröbner computation to show that f = 0.

```
A short program in Maple will demonstrate that the normal form of f
with respect to the Gröbner basis<sup>2</sup> of polynomials f_1 up to f_5 will be zero.
SquareLine := proc (M,N)
                             (M[1]-N[1])<sup>2</sup> + (M[2]-N[2])<sup>2</sup>; end:
Perpendicular := proc (M,N,P,Q)
  (N[2]-M[2])*(Q[2]-P[2]) + (N[1]-M[1])*(Q[1]-P[1]);
end:
A := [a,0]: B := [b,0]: C := [0,c]: H := [0,h]:
D_0 := [x_0, y_0]: D_1 := [x_1, y_1]:
f_1 := expand(SquareLine(O_0, A) - SquareLine(O_0, B)):
f_2 := expand( SquareLine(0_0,A) - SquareLine(0_0,C) ):
f_3 := expand( SquareLine(0_1,A) - SquareLine(0_1,B) ):
f_4 := expand( SquareLine(0_1,A) - SquareLine(0_1,H) ):
f_5 := expand( Perpendicular(B,H,A,C) ):
f_6 := expand( SquareLine(0_0,C) - SquareLine(0_1,H) ):
with(grobner):
X := [x_0, y_0, x_1, y_1, h];
F := [f_1, f_2, f_3, f_4, f_5];
G := gbasis(F,X);
normalf(f_6,G,X);
```

4.2. Desargues' Theorem.

Theorem 4.2. If two triangles has the vertices, two by two, on three concurent straight lines, then their edges are crossing out in three collinear points.

Again, let choose the coordinate system to have the origin identical to the crossing point of the three straight lines d_1 , d_2 , d_3 and consider that d_1 is Oy axis. This means that the fascicle has the equation:

(12)
$$\begin{cases} d_1: & x = 0\\ d_2: & \alpha_2 & x + \beta_2 y = 0\\ d_3: & \alpha_3 & x + \beta_3 y = 0 \end{cases}$$

²The Gröbner basis of f_1 up to f_5 with respect to (x_0, y_0, x_1, y_1, h) , arranged in the lexicographic order, is

 $G = \langle hc + ba, -a - b + 2x_0, -a - b + 2x_1, -c^2 - ba + 2y_0c, c^2 + ba + 2cy_1 \rangle.$

GRÖBNER BASES IN GEOMETRY

Let define the points and their coordinates: $A_1(0, y_{a_1}), B_1(x_{b_1}, y_{b_1})$ and $C_1(x_{c_1}, y_{c_1})$ will be the vertices for the first triangle, $A_2(0, y_{a_1})$, $B_1(x_{b_1}, y_{b_1})$ and will be the second triangle's vertices and c_{a_1} . $C_1(x_{c_1}, y_{c_1})$ will be the second triangle's vertices and finally, the points that we should prove they are collinear, denoted by $M(x_M, y_M)$, $N(x_N, y_N)$ and $P(x_P, y_P)$

The fact that $A_1 \in d_1$ and $A_2 \in d_1$ is already specified, so there remains the other points for which we can get their polynomial identities:

- (13) $= \alpha_2 x_{b_1} + \beta_2 y_{b_1} = 0$ f_1
- (14) $f_2 = \alpha_2 x_{b_2} + \beta_2 y_{b_2} = 0$
- $f_3 = \alpha_3 x_{c_1} + \beta_3 y_{c_1} = 0$ (15)(16)
- $= \alpha_3 x_{c_2} + \beta_3 y_{c_2} = 0$ f_4

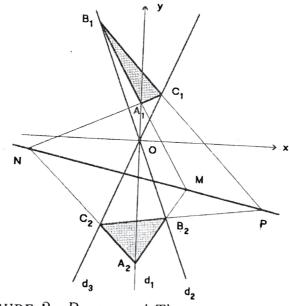


FIGURE 2. Desargues' Theorem

Writing the equation of A_1B_1 and A_2B_2 respectively, the fact that M is placed on the point $A_1B_1 \cap A_2B_2$ can be expressed in two polynomial identities, saving the point $A_1B_1 \cap A_2B_2$ can be expressed in two polynomial identities, saying that $M \in A_1B_1$ and $M \in A_2B_2$ respectively. The same rules applies for N and D. (17)

One may ask what happened with the condition that d_1 , d_2 , d_3 have only one crossing point, say the rank of corresponding matrix from (12) is equal to 2. In fact this condition is true, since we chose and wrote the corresponding equations for the point O(0,0) to be the crossing point.

Now, the hypotesis is completely specified. The last thing we have to do is to write the polynomial f, describing the conclusion and then to verify if its normal form with respect to Gröbner basis of f_1 up to f_{11} vanishes. M, N, P are collinear iff

(23)
$$f = \begin{vmatrix} 1 & 1 & 1 \\ x_M & x_N & x_P \\ y_M & y_N & y_P \end{vmatrix} = 0.$$

A short code in Maple will verify the collinearity imediately³.

5. Hints about writing a code in Maple

A Maple session known as a *worksheet* is based on two main regions, one is where you write the code, called *the input* and the other one is where the results are printed out, called *the output*.

First of all Maple is like a pocket scientific calculator as shown in the following commands

> 34+85;

119

> 5^4;

> cos(Pi);

As far as wee see from these commands Maple is able to handle among ordinary operations, several functions (if you are a little bit experienced you may find even some more complex functions) and some constants. One might see that all commands end-up with a semicolon. This tells Maple to compute and print

625

-1

$$G = \langle (-y_{b_1}y_{a_2} + y_{b_2}y_{a_1})x_m\alpha_2 + (y_{b_1}y_{a_1}y_{b_2} - y_{b_2}y_{b_1}y_{a_2})\beta_2,$$

 $y_{b_1}y_{a_1}y_{a_2} - y_{b_1}y_{a_1}y_{b_2} - y_{b_2}y_{a_2}y_{a_1} + y_{b_2}y_{b_1}y_{a_2} + (-y_{b_1}y_{a_2} + y_{b_2}y_{a_1})y_m,$

$$(y_{c_2}y_{a_1} - y_{c_1}y_{a_2})x_n\alpha_3 + (-y_{c_2}y_{a_2}y_{c_1} + y_{c_1}y_{c_2}y_{a_1})\beta_3,$$

 $-y_{c_2}y_{a_2}y_{a_1}+y_{c_2}y_{a_2}y_{c_1}+y_{c_1}y_{a_2}y_{a_1}-y_{c_1}y_{c_2}y_{a_1}+(y_{c_2}y_{a_1}-y_{c_1}y_{a_2})y_{a_1},$

 $((y_{c_2}y_{b_1} - y_{c_1}y_{b_2})x_p\alpha_3 + (y_{b_1}y_{c_1}y_{c_2} - y_{c_2}y_{c_1}y_{b_2})\beta_3)\alpha_2 + (y_{c_2}y_{b_1}y_{b_2} - y_{b_1}y_{c_1}y_{b_2})\alpha_3\beta_2,$

 $(y_{c_2}y_{b_1} - y_{c_1}y_{b_2})y_p + y_{b_1}y_{c_1}y_{b_2} - y_{b_1}y_{c_1}y_{c_2} - y_{c_2}y_{b_1}y_{b_2} + y_{c_2}y_{c_1}y_{b_2},$

 $\alpha_2 x_{b_1} + \beta_2 y_{b_1}, \alpha_3 x_{c_1} + \beta_3 y_{c_1}, \alpha_2 x_{b_2} + \beta_2 y_{b_2}, \alpha_3 x_{c_2} + \beta_3 y_{c_2} \rangle.$

³Suppose that the parameters are $\alpha_1, \beta_1, \alpha_2, \beta_2, y_{a_1}, y_{b_1}, y_{c_1}, y_{a_2}, y_{b_2}, y_{c_2}$ and the indeterminates are $x_{b_1}, x_{c_1}, x_{b_2}, x_{c_2}, x_M, y_M, x_N, y_N, x_P, y_P$. Then the Gröbner basis of f_1 up to f_{10} with respect to the corresponding basis of indetermintes in the lexicographic order is

out the corresponding result. If you don't want the result to be printed out on the screen, replace the semicolon by a colon. Then Maple will process the command

To see something more powerful than a pocket calculator cannot do, type these lines and see what happens:

100!; >

evalf(Pi,500); >

If you need more informations you should read some good articles about using Maple, like [Mat95], [Moh95], [Mon94], [Dav92].

You can create and use your own variables from the assignment command ":=". For example:

> Alpha := sin(Pi/3);

$$Alpha := \frac{1}{2}\sqrt{3}$$

> i := Alpha;

$$i := \frac{1}{2}\sqrt{3}$$

Variables in Maple, among those from other languages, are bounded. This means that once you have assigned a value to a variable, you will not be able to change it until you assign another value. Take the previous $example^4$ and see what happens if we assign the variable i to itself: > i;

>	i := 'i';	$\frac{1}{2}\sqrt{3}$
>	i;	i := i

i

Maple has several libraries you can load explicitely in your session. Few of them are already loaded when you start a session and those are also known to be a part of the kernel. For our purposes, I will show how to load the Gröbner with(grobner):

If you need more help you may type on the input region the question mark If you need more help you may type on the input region the queet followed : A semicolon is not followed immediately⁵ by a word representing your search. A semicolon is not important in this case, meaning that ^{?grobner[normalf]}

⁴This example shows you how to unbound a variable, too. ⁵ without tabs or blank spaces

or

> ?grobner[normalf];

is one and the same thing, showing a help window for the **normalf** function within the **grobner** package.

References

- [Bot96] N. Both. Istoria Matematicii. Universitatea "Babeş-Bolyai", Facultatea de Matematică și Informatică, Cluj-Napoca, 1996. lito.
- [Coh93] H. Cohen. A course in Computational Algebraic Number Theory. Springer-Verlag, 1993.
- [Dav92] J. H. Davenport. Computer algebra past, present and future. School of Mathematical Sciences, University of Bath, University of Bath BA2 7AY, England, 1992.
- [DC92] D. O'Shea D. Cox, J. Little. Ideals, Varieties and Algorithms. Springer-Verlag, 1992.
- [JHD93] E. Tournier J. H. Davenport, Y. Siret. Computer Algebra. Academic Press, second edition, 1993.
- [Knu81] D. E. Knuth. Seminumerical Algorithms, volume 2 of The Art of Computer Programming. Addison-Wesley, Reading, Massachusetts, second edition, 1981.
- [KOG92] G. Labahn K. O. Geddes, S.R. Czapor. Algorithms for Computer Algebra. Kluwer Academic Publisher, Kluwer Boston, 1992.
- [Lev93] A. H. M. Levelt. Application of the gröbner basis algorithm. University of Nijmegen, Department of Mathematics, Nijmegen, The Netherlands, October 1993.
- [Mat95] J. V. Matthews. The Maple Dictionary with examples, 1995.
- [Moh95] P. Mohseni. Maple in action. Iowa State University, Iowa, 1995.
- [Mon94] M. Monagan. New features in Maple V Release 3. Institute for Scientific Computation, ETH Zentrum, Zürich, Switzerland, 1994.
- [WWA95] P. Loustanau W. W. Adams. An Introduction to Gröbner Bases, volume 3 of Graduate Studies in Mathematics. American Mathematical Society, 1995.

"BABEŞ-BOLYAI" UNIVERSITY, FACULTY OF MATHEMATICS AND COMPUTER SCIENCE RO-3400 Cluj-Napoca, Romania

E-mail address: blaga@cs.ubbcluj.ro