A BRIEF INTRODUCTION TO COMPUTATIONAL COMMUTATIVE ALGEBRA

CIMPA/TUBITAK/GSU SUMMER SCHOOL ON ALGEBRAIC GEOMETRY AND NUMBER THEORY
2-10 JUNE 2014 GALATASARAY UNIVERSITY, ISTANBUL, TURKEY
IN COLLABORATION WITH IPM (IRAN) AND CAMS (LIBAN)

RAHIM ZAARE NAHANDI
UNIVERSITY OF TEHRAN

1. A historic-cultural note - the battle on constructive and non-constructive methods

Leopold Kronecker: *Mathematical notions must be decidable in finitely many steps.*

Hermann Weyl: *Mathematics is the science of infinity.*

Algebra was traditionally based on constructive methods. Division algorithm, Gaussian elimination method for solving a system of linear equations, and the general elimination methods practiced in 19th century, are just a few examples of this approach. Throughout more than the first half of the 20th century, while the mission of the leading experts in algebraic geometry was towards a solid foundation for the subject, the common mentality was against constructive methods.

The story of "elimination of elimination theory" is well-known. D. Eisenbud [Eisenbud 1998, p. 306] points out that, A. Weil in his influential book [Weil 1946, p. 31], says " The device that follows ..., it may be hoped finally eliminates from algebraic geometry the last traces of Elimination Theory...". This statement is actually due to Claude Chevalley from his Princeton lectures [Weil 1946, p. 31, The footnote]. It is therefore not surprising that, contrary to the earlier editions [Van der Waerden 1953], in the preface of the fourth edition of his book Algebra [Van der Waerden 1959], B. L. van der Waerden, influenced by other masters like A. Weil, and C. Chevalley, writes "By omitting some material I have tried to keep the size of the book within reasonable bound. Thus, the chapter "Elimination Theory" has been omitted. The theorem on the existence of resultant system for homogeneous equations, which was formerly proved by means of elimination theory, now appears in Section 121 as a Corollary to Hilbert's Nullstellensatz."

Algebraic geometry is basically the study of the solutions of polynomial equations. Polynomial equations have been studied for a very long time, both theoretically and with a view to solving them. Until recently, manual computation was the only solution method and the theory was developed to accommodate it. With the advent of computers, the situation changed dramatically; many classical results

can be more usefully recast within a different framework which in turn lends itself to further theoretical development tuned to computation.

The proof of the four color map theorem was the first major result to be proven using a computer. The four color map theorem, states that, given any separation of a plane into contiguous regions, producing a figure called a map, no more than four colors are required to color the regions of the map so that no two adjacent regions have the same color.

The four color theorem was proven in 1976 by Kenneth Appel and Wolfgang Haken. Appel and Haken's approach started by showing that there is a particular set of 1,936 maps, each of which cannot be part of a smallest-sized counter-example to the four color theorem. (If they did appear, you could make a smaller counter-example.) Appel and Haken used a special-purpose computer program to confirm that each of these maps had this property. Additionally, any map that could potentially be a counter-example must have a portion that looks like one of these 1,936 maps. Showing this required hundreds of pages of hand analysis. Appel and Haken concluded that no smallest counterexamples existed because any must contain, yet not contain, one of these 1,936 maps. This contradiction means there are no counterexamples at all and that the theorem is therefore true. Initially, their proof was not accepted by all mathematicians because the computer-assisted proof was infeasible for a human to check by hand (Swart 1980). Since then the proof has gained wider acceptance, although doubts remain (Wilson 2002, 216222). To dispel remaining doubt about the proof by Appel and Haken, a simpler proof using the same ideas and still relying on computers was published in 1997 by Robertson, Sanders, Seymour, and Thomas. Additionally in 2005, the theorem was proven by Georges Gonthier with general purpose theorem proving software. For the full story please see: http://en.wikipedia.org/wiki/Four-color-theorem.

Recent achievements on the proof of the *Weak Goldbach Conjecture* and progress on infinity of primes with certain finite gap (the latest small gap being around 6000 but the goal is towards a gap of 2; the *Twin Primes Conjecture*) makes it very difficult to resist opposing the striking impact of computers on mathematics. This is not only on the achievements but also on highly non-trivial theory-machine approach in the proofs. In fact, confrontation between constructive and non-constructive approaches has emerged to an advanced co-ordination reaching to the point of the "state of the art".

2. The first spark on computational methods in commutative algebra

During his research seminar in the Spring of 1964, Wolfgang Gröbner, a professor of Leopold-Franzens University, Innsbruck, proposed a problem which became a Ph.D. thesis for Bruno Buchberger. The title of this thesis was: An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal. A modified version of the abstract of this thesis is:

Let k be a field, and let $I \subset k[x_1, \ldots, x_n]$ be an ideal of height n so that the residue class ring $k[x_1, \ldots, x_n]/I$ is a finite dimensional vector space. We find an algorithm to compute a basis for this vector space from the generating polynomials

of I. We find a termination criterion for this algorithm, and systematize it so that it is suitable for implementation on an electronic computer. Certain inherent properties will also be presented, which suggest an application to the calculation of the Hilbert function of an arbitrary polynomial ideal.

Buchberger's thesis was the major step in establishing the foundation of computational methods in commutative algebra and algebraic geometry. In fact, in his thesis, Buchberger formulated the concept of Gröbner bases, found an algorithm to compute them, and proved the fundamental theorem on which the correctness and termination of the algorithm hinges.

For many years the importance of Buchberger's work was not fully appreciated. Only in the eighties did researchers in mathematics and computer science start a deep investigation of the new theory. Many generalities and a wide variety of applications were developed. It has now become clear that the theory of Gröbner bases can be widely used in many areas of science. The simplicity of its fundamental ideas stands in stark contrast to its power and the breadth of its applications. Simplicity and power: two ingredients which combine perfectly to ensure the continued success of this theory. Gröbner Bases Theory, descends the study of polynomial ideals to the study of monomial ideals. The structure of monomial ideals have combinatorial nature and, in most cases, the original question on polynomial ideals, is much easier to handle for monomial ideals.

Gröbner bases theory provides the foundation for many algorithms in algebraic geometry and commutative algebra, with the Buchberger algorithm acting as the engine that drives the computation. In view of ubiquity of scientific problems modeled by polynomials, this subject is of interest not only to mathematics, but also to an increasing number of scientists and engineers.

Buchberger's thesis brought the revival of constructive methods in commutative algebra and algebraic geometry. In fact, theoretically, the idea in a more general setting, is due to Macaulay. To state Macaulay's theorem, we first need to define monomial orders and some related concepts.

Definition 2.1. *Let $R = k[x_1, \ldots, x_n]$ be the polynomial ring over a field k. A monomial order on R is a total order $>$ on the monomials of R such that if m_1, m_2 and $m \neq 1$ are monomials in R, then*

$$m_1 > m_2 \quad \textit{implies} \quad mm_1 > mm_2 > m_2.$$

A simple but fundamental property of monomial orders is their *Artinian property*:

Lemma 2.2. *(Artinian property of monomial orders) Let $>$ be a monomial order on $R = k[x_1, \cdots, x_n]$. Every non-empty set of monomials has a least element with respect to $>$.*

Recall that by a *term* in R we mean a monomial in R multiplied by an scalar. For $f \in R$ a monomial in a term of f will be called a *monomial* of f.

Definition 2.3. *Let $>$ be a monomial order on $R = k[x_1, \cdots, x_n]$ and let $f \in R$. The initial term of f, denoted by $\text{in}_>(f)$, is the greatest term of f with respect to $>$. If I is an ideal in R, then $\text{in}_>(I)$ is the ideal generated by $\text{in}_>(f)$ for all $f \in I$.*

We will discuss monomial orders further. But, for the time being, let us recall a typical monomial order on R; the lexicographic order:

$$x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n}$$

if and only if $a_i > b_i$ for the first index i with $a_i \neq b_i$.

Theorem 2.4. *(Macaulay). Let $I \subset R = k[x_1, \cdots, x_n]$ be an ideal. For any monomial order $>$ on R, the set B of all monomials not in $\text{in}_>(I)$ forms a basis for the (finite or infinite dimensional) vector space R/I.*

It is not difficult to justify that a merely total order is not sufficient to produce a basis, and it is necessary to use a monomial order.

Observe that in his thesis, Buchberger finds an algorithm to construct such a basis when R/I is a finite dimensional vector space.

Here the concept of Gröbner basis shows up. The point is that if I is generated by $f_1, \cdots, f_t$, then $\text{in}_>(I)$ is not necessarily generated by $\text{in}_>(f_1), \cdots, \text{in}_>(f_t)$!! If a generating set of I satisfies this property, it is called a Gröbner basis. More precisely:

Definition 2.5. *Let $I \subset R = k[x_1, \cdots, x_n]$ be an ideal and let $>$ be a monomial order on R. A set of polynomials $g_1, \cdots, g_t$ in R is said to be a Gröbner basis for I if $\text{in}_>(g_1), \cdots, \text{in}_>(g_t)$ generate $\text{in}_>(I)$.*

It follows that if $g_1, \cdots, g_t$ is a Gröbner basis for I, then $\{g_1, \cdots, g_t\}$ is also a generating set for I. This is immediate from the following simple but important lemma.

Lemma 2.6. *Let $>$ be a monomial order on $R = k[x_1, \cdots, x_n]$ and let $I \subset J \subset R$ be two ideals in R such that $\text{in}_>(I) = \text{in}_>(J)$. Then $I = J$.*

A Gröbner basis $g_1, \cdots, g_t$ for an ideal I is called *minimal* if $\text{in}_>(g_1), \cdots, \text{in}_>(g_t)$ is a minimal generating set for $\text{in}_>(I)$.

Observe that this does not mean that $g_1, \cdots, g_t$ is a minimal generating set for I. In fact, in general, a Gröbner basis is not a minimal generating set for the ideal.

A Gröbner basis $g_1, \cdots, g_t$ for an ideal I is called *reduced* if

(i) $\text{in}_>(g_i)$ does not divide any term of g_j for $i \neq j$.

(ii) $\text{in}_>(g_i)$ is a monomial (that is, the coefficient from k is 1).

Theorem 2.7. *Reduced Gröbner basis exists and is unique.*

Let's give a simple example to show that if I is generated by $f_1, \cdots, f_t$, then $\text{in}_>(I)$ is not necessarily generated by $\text{in}_>(f_1), \cdots, \text{in}_>(f_t)$.

Example 2.8. *Let I be the ideal generated by $f_1 = x^2, f_2 = xy + y^2$ in $R = k[x, y]$. Let $>$ be the lexicographic order on R with $x > y$. Then $\text{in}_>(f_1) = x^2$ and $\text{in}_>(f_2) = xy$. However, $yf_1 - xf_2 = -xy^2 \in I$ and hence, $yf_2 - xy^2 = y^3 \in I$. Consequently, $y^3 \in \text{in}_> I$ but y^3 does not belong to the ideal generated by $\text{in}_>(f_1) = x^2$ and $\text{in}_>(f_2) = xy$. In fact, as we will see later, here $f_1, f_2, f_3 = y^3$ is a Gröbner basis for I.*

3. Division Algorithm, Buchberger Criterion and Buchberger algorithm

We now review the main items for construction of a Gröbner basis.

Theorem 3.1. *(Division Algorithm). Let $R = k[x_1, \cdots, x_n]$ and let $g_1, \cdots, g_t$ be some nonzero polynomials in R. Fix a monomial order $>$ on R. Then given $0 \neq f \in R$, there exist polynomials $f_1, \cdots, f_t$ and f' in R with*

$$f = f_1 g_1 + \cdots + f_t g_t + f' \tag{1}$$

such that

(i) if $f' \neq 0$, then no monomial of f' is in the ideal $(\text{in}_>(g_1), \cdots, \text{in}_>(g_t))$,

and

(ii) $\text{in}_>(f) \geq \text{in}_>(f_i g_i)$ for every i.

Any such f' is called a remainder of f with respect to $g_1, \cdots, g_t$. The expression (1) is called a standard expression of f in terms of $g_1, \cdots, g_t$. One also says that f reduces to f' with respect to $g_1, \cdots, g_t$.

This is indeed a useful generalization of the usual division algorithm of polynomials in one variable using the monomial order induced by degree.

Obviously, either a remainder nor a standard expression are unique. However, if $g_1, \cdots, g_t$ is a Gröbner basis for $I = (g_1, \cdots, g_t)$ then the remainder is unique. See [Herzog-Hibi 2011, Lemma 2.2.3].

Corollary 3.2. *(Membership problem). If $\mathbb{G} = \{g_1, \cdots, g_t\}$ is a Gröbner basis of $I = (g_1, \cdots, g_t)$, then a nonzero polynomial f of R belongs to I if and only if the unique remainder of f with respect to $g_1, \cdots, g_t$ is 0.*

Proof. In fact, if f reduces to $f' \neq 0$, then $f' \in I$, and consequently, $\text{in}_>(f') \in \text{in}_> I = (\text{in}_>(g_1), \cdots, \text{in}_>(g_t))$ which contradicts the conditions on the standard expression. □

Recall that the membership problem is trivial in the case of monomial ideals. This is in fact a basic property of monomial ideals: A polynomial f belongs to a monomial ideal I if each term of f belongs I.

Definition 3.3. *(S-polynomials). Let $>$ be a monomial order on R. For $f \in S$ let c_f denote the coefficient of $\text{in}_>(f)$ in f. For $f_1, f_2 \in R$ the expression*

$$\text{S}(f_1, f_2) = \frac{lcm(\text{in}_>(f_1), \text{in}_>(f_2))}{c_{f_1}\text{in}_>(f_1)} f_1 - \frac{lcm(\text{in}_>(f_1), \text{in}_>(f_2))}{c_{f_2}\text{in}_>(f_2)} f_2$$

is called the S*-polynomial of f_1 and f_2.*

For $f_i, f_j \in R$, we will use the notation

$$m_{ij} = \frac{lcm(\text{in}_>(f_i), \text{in}_>(f_j))}{c_{f_i}\text{in}_>(f_i)}.$$

Now we state the *Buchberger criterion* which is considered the most important theorem on Gröbner bases.

Theorem 3.4. *(Buchberger Criterion). Let I be a none-zero ideal of R, and let $\{g_1, \cdots, g_t\}$ be a system of generators of I. Then $\{g_1, \cdots, g_t\}$ is a Gröbner basis of I if and only if $\text{S}(g_i, g_j)$ reduces to zero with respect to $g_1, \cdots, g_t$ for all $i \neq j$.*

In light of the Buchberger criterion, it is easy to forecast what *Buchberger Algorithm* for constructing a Gröbner basis should be.

Theorem 3.5. *(Buchberger Algorithm). Let I be a none-zero ideal of R, and let $g_1, \cdots, g_t$ be a system of generators of I. Compute the remainder h_{ij}. If all the $h_{ij} = 0$, then the g_i's form a Gröbner basis for I. If some $h_{ij} \neq 0$, then replace $g_1, \cdots, g_t$ with $g_1, \cdots, g_t, h_{ij}$ and repeat the process. As the ideal generated by $g_1, \cdots, g_t, h_{ij}$ is strictly larger than that generated by $g_1, \cdots, g_t$, the process must terminate after finitely many steps (since $k[x_1, \ldots, x_n]$ is a Noeterian ring!).*

The following is immediate from the Buchberger algorithm.

Corollary 3.6. *Let I be an ideal in R and let $>$ be a monomial order on R. Then*

(i) If I is homogenous then the reduced Gröbner basis of I with respect to $>$ consists of homogenous polynomials.

(i) If I is a binomial ideal then the reduced Gröbner basis of I with respect to $>$ consists of binomials.

Now we check the previous example using the Buchberger algorithm.

Example 3.7. *Let I be the ideal generated by $f_1 = x^2, f_2 = xy + y^2$ in $R = k[x, y]$ as discussed before. Let $>$ be the lexicographic order on R with $x > y$. Then $\text{in}_>(f_1) = x^2$ and $\text{in}_>(f_2) = xy$.*

$$\text{S}(f_1, f_2) = \frac{lcm(\text{in}_>(f_1), \text{in}_>(f_2))}{c_{f_1}\text{in}_>(f_1)} f_1 - \frac{lcm(\text{in}_>(f_1), \text{in}_>(f_2))}{c_{f_2}\text{in}_>(f_2)} f_2$$

$$= \frac{x^2y}{x^2}x^2 - \frac{x^2y}{xy}(xy + y^2) = -xy^2 = -yf_2 + y^3.$$

Since y^3 is not a multiple of either initial forms, it is a remainder. Since it is non-zero, f_1, f_2 is not a Gröbner basis. Thus we add $g_3 = y^3$ to the set of generators. We get

$$\mathrm{S}(f_1, f_3) = \frac{lcm(\mathrm{in}_>(f_1), \mathrm{in}_>(f_3))}{c_{f_1}\mathrm{in}_>(f_1)} f_1 - \frac{lcm(\mathrm{in}_>(f_1), \mathrm{in}_>(f_3))}{c_{f_3}\mathrm{in}_>(f_3)} f_3 = \frac{x^2y^3}{x^2}x^2 - \frac{x^2y^3}{y^3}y^3$$
$$= 0.$$
$$\mathrm{S}(f_2, f_3) = \frac{lcm(\mathrm{in}_>(f_2), \mathrm{in}_>(f_3))}{c_{f_2}\mathrm{in}_>(f_2)} f_2 - \frac{lcm(\mathrm{in}_>(f_2), \mathrm{in}_>(f_3))}{c_{f_3}\mathrm{in}_>(f_3)} f_3$$
$$= \frac{xy^3}{xy}(xy + y^2) - \frac{xy^3}{y^3}y^3 = y^4 = yf_3.$$

Therefore, $S(f_i, f_j)$ reduces to zero with respect to f_1, f_2, f_3 , and hence, f_1, f_2, f_3 is Gröbner basis for I.

S-polynomials enjoy another distinguished property on the syzygy modules of a Gröbner basis. In fact the initial letter S stands for syzygy a Turkish word meaning YOKE.

Let $g_1, \cdots, g_t$ be a Gröbner basis for an ideal $I \subset R = k[x_1, \cdots, x_n]$ with respect to some monomial order $>$. Let

$$\mathrm{S}(g_i, g_j) = m_{ij}g_i - m_{ji}g_j - \sum_u f_u^{(ij)} g_u$$

be the S-polynomial of g_i, g_j with respect to $g_1, \cdots, g_t$. Let $F = R^t$ be the free R-modules with basis elements $\epsilon_1, \cdots, \epsilon_t$. Consider the R-linear map

$$\varphi : F \longrightarrow I$$

defined by $\varphi(\epsilon_i) = g_i$. Then, $\mathrm{Ker}(\varphi)$ is the module of syzygies of $g_1, \cdots, g_t$.

Theorem 3.8. *(Schreyer) Let*

$$\tau_{ij} = m_{ij}\epsilon_i - m_{ji}\epsilon_j - \sum_u f_u^{(ij)} \epsilon_u.$$

Then, τ_{ij}'s generate the module of syzygies of $g_1, \cdots, g_t$.
In fact, with a suitable "monomial order" on F, τ_{ij}'s form a Gröbner basis for the module of syzygies. (see [Eisenbud 1998, 15.5]*).*

In the example above, τ_{12}, τ_{13} and τ_{23} form a Gröbner basis for the module of syzygies of f_1, f_2, f_3.

4. Monomial orders, comparison of an ideal with its initial ideal, and applications

Let $R = k[x_1, \cdots, x_n]$. Recall that a monomial order on R is a total order $>$ on the monomials of R such that if m_1, m_2 and $n \neq 1$ are monomials in R, then

$$m_1 > m_2 \quad implies \quad nm_1 > nm_2 > m_2.$$

We already saw the lexicographic order as a typical monomial order on R: Let $m = x_1^{a_1} \cdots x_n^{a_n}$ and $n = x_1^{b_1} \cdots x_n^{b_n}$. Then $m >_{lex} n$ if and only if $a_i > b_i$ for the

first index i with $a_i \neq b_i$.

Although there exist more general monomial orders, besides lexicographic order, there are two other important monomial orders on R which are essential for Gröbner bases computations: Homogenous lexicographic order and reverse lexicographic order:

Definition 4.1. *(Homogenous lexicographic order,* or, *degree lex order) Let* $m_1 = x_1^{a_1} \cdots x_n^{a_n}$ *and* $m_2 = x_1^{b_1} \cdots x_n^{b_n}$. *Then* $m_1 >_{hlex} m_2$ *if and only if* $\deg\, m_1 > \deg\, m_2$ *or* $\deg\, m_1 = \deg\, m_2$ *and* $a_i > b_i$ *for the first index* i *with* $a_i \neq b_i$.

Definition 4.2. *(Reverse lexicographic order) Let* $m_1 = x_1^{a_1} \cdots x_n^{a_n}$ *and* $m_2 = x_1^{b_1} \cdots x_n^{b_n}$. *Then* $m_1 >_{rlex} m_2$ *if and only if* $\deg\, m_1 > \deg\, m_2$ *or* $\deg\, m_1 = \deg\, m_2$ *and* $a_i < b_i$ *for the* ***last*** *index* i *with* $a_i \neq b_i$.

Assume that if m_1 and m_2 are of the same degree. If we reverse the order on variables to $x_n > x_{n-1} > \cdots > x_1$ and use the lexicographic order *induced* by this order of variables for m_1 and m_2, then $x_n^{b_n} \cdots x_1^{b_1} >_{lex} x_n^{a_n} \cdots x_1^{a_1}$ if and only if $b_i > a_i$ for the first i (from the left) with $a_i \neq b_i$. The reverse lexicographic order on m_1 and m_2 is the opposite of this order, and this is the reason for the name .

The two orders $>_{lex}$ and $>_{hlex}$ are different for monomials in more than one variables. For example

$$x_1 x_3 >_{hlex} x_2^2$$

while

$$x_2^2 >_{rlex} x_1 x_3.$$

Proposition 4.3. *(Characterization of the properties of monomial orders) Let* $f \in k[x_1, \cdots, x_n]$. *Then*

a. If $\mathrm{in}_{>_{lex}}(f) \in k[x_s, \cdots, x_n]$ *for some* s, *then* $f \in k[x_s, \cdots, x_n]$.

b. If f *is homogenous and* $\mathrm{in}_{>_{hlex}}(f) \in k[x_s, \cdots, x_n]$ *for some* s, *then* $f \in k[x_s, \cdots, x_n]$.

c. If f *is homogenous and* $\mathrm{in}_{>_{rlex}}(f) \in (x_s, \cdots, x_n)$ *for some* s, *then* $f \in (x_s, \cdots, x_n)$.

One of the main advantages of Gröbner bases is reduction of several properties of polynomial ideals to similar properties on monomial ideals, which are much simpler in general. For example, computation of the Hilbert polynomial of a monomial ideal, determining the intersection of two monomial ideals, are much simpler compared to handling the same problems of polynomial ideals. This is done by comparing an ideal I with its initial ideal $\mathrm{in}_>(I)$. However, dealing with different properties of ideals it may be necessary to use suitable monomial orders.

Before comparing some properties of I and $\mathrm{in}_>(I)$, we need to recall some definitions.

Let M be a finitely generated graded R-module. A *minimal free resolution* of M is an exact graded complex

$$0 \longrightarrow F_p \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

where $F_i = \oplus_j R(-j)^{\beta_{ij}}$ have the minimal possible rank and $R(-j)$ is the ring R considered as a graded module with degree shift by j. The numbers β_{ij} are called *Betti numbers* of M. We now recall some important numerical invariants of modules which can be easily computed for polynomial ideals and t heir quotients using Gröbner bases.

Definition 4.4. *(i) The projective dimension of M is*

$$\text{proj dim } M = \max \{i : \beta_{ij}(M) \neq 0 \text{ for some } j\}.$$

(ii) The regularity of M is

$$\text{reg } M = \max \{j - i : \beta_{ij}(M) \neq 0 \text{ for some } i\}.$$

We will use these concepts when I is a homogenous ideal in R, hence I and R/I may be considered as graded R-modules.

Theorem 4.5. *Let $I \subset R = k[x_1, \cdots, x_n]$ be a homogenous ideal and let $>$ be a monomial order. Then*

(i) The Hilbert function and the Hilbert polynomial of R/I and $R/\text{in}_>(I)$ are equal.

(ii) dim $R/I =$ dim $R/\text{in}_>(I)$ *(*dim *is the Krull dimension).*

(iii) proj dim $R/I \leq$ proj dim $R/\text{in}_>(I)$.

(iv) reg $R/I \leq$ reg $R/\text{in}_>(I)$.

(v) depth $R/I \geq$ depth $R/\text{in}_>(I)$.

Statements (ii) and (v) are also valid for non-homogenous ideals.

Also recall that a ring is *Cohen-Macaulay* if its depth is equal to its Krull dimension. A ring is *Gorenstein* if it is Cohen-Macaulay and the last nonzero Betti number in its minimal free resolution is 1. The above theorem has very important consequences regarding these tow type of rings.

Corollary 4.6. *The ring R/I is Cohen-Macaulay (respectively Gorenstein) if $R/\text{in}_>(I)$ has the corresponding property (see* [Herzog-Hibi 2011, Corollary 3.3.5]*).*

We now review some important application of Gröbner bases. We begin with elimination theory.

Recall that if $R = k[x_1, \cdots, x_n$ and $I \subset T = R[y_1, \cdots, y_s] = k[x_1, \cdots, x_n, y_1, \cdots, y_s]$ is an ideal, then $I \cap R$ is called the *the elimination* ideal (with respect to $y_1, \cdots, y_s$). In the case I is a monomial ideal generated by monomials $m_1, \ldots, m_r$ the $I \cap R$ is simply generated by those monomials among $m_1, \ldots, m_r$ which do not involve

$y_1, \ldots, y_s$. Gröbner bases theory reduces computation of elimination for polynomial ideals to the case of elimination for monomial ideals.

1. Elimination. Given an ideal $I \subset T = R[y_1, \cdots, y_s] = k[x_1, \cdots, x_n, y_1, \cdots, y_s]$, we proceed to compute the elimination ideal $I \cap R$. It is enough to use a monomial order on T satisfying

If $f \in T$ and $\text{in}_>(f) \in R$, then $f \in R$.

This is called an *elimination order* (with respect to $y_1, \cdots, y_s$). For example, the lexicographic order induced by $y_1 > \cdots > y_s > x_1 > \cdots > x_n$ has this property.

Theorem 4.7. *(Elimination) Let $>$ be an elimination order on $T = k[x_1, \cdots, x_n, y_1, \cdots, y_s]$ with respect to $y_1, \cdots, y_s$. If $I \subset T$ is an ideal, then with respect to $>$ on T and its restriction on R,*

$$\text{in}_>(I \cap R) = \text{in}_>(I) \cap R.$$

Further, if $g_1, \cdots, g_t$ is a Gröbner basis for I and $g_1, \cdots, g_u$ are those g_i's that do not involve the variables $y_1, \cdots, y_s$, then $g_1, \cdots, g_u$ form a Gröbner basis for $I \cap R$.

Let us see further nice applications of elimination ideals.

2. Intersection of two ideals. Let $I, J \subset R$ be two ideals. One way to find $I \cap J$ is by elimination of new variable as follows. Let $K = (y.I + (1-y)J)$ considered as an ideal in $R[y]$. Then it is immediate that

$$I \cap J = K \cap R.$$

3. Kernel of a homomorphism between two polynomial rings. Let $R = k[x_1, \cdots, x_n]$ and $Q = k[y_1, \cdots, y_s]$ be two polynomial rings. Let $\varphi : R \longrightarrow Q$ be a homomorphism defined by $\varphi(x_i) = f_i \in Q$. Let $T = k[x_1, \cdots, x_n, y_1, \cdots, y_s]$ and consider the ideal $(f_1 - x_1, \cdots, f_n - x_n) \subset T$. Then it follows that, Ker φ is the elimination ideal

$$\text{Ker } \varphi = (f_1 - x_1, \cdots, f_n - x_n) \cap Q.$$

4. Equations of the image of an algebraic set under a morphism. Let $X \subset \mathbb{A}^s$ be an affine algebraic set defined by an ideal $J \subset k[y_1, \cdots, y_s]$, and let $h : X \longrightarrow \mathbb{A}^n$ be a morphism given by

$$a = (a_1, \cdots, a_s) \mapsto (f_1(a), \cdots, f_n(a))$$

where $f_1, \cdots, f_n \in S = k[y_1, \cdots, y_s]/J$. Find the defining ideal of the Zariski closure of the image of X under h.

Observe that if $\varphi : R = k[x_1, \cdots, x_n] \longrightarrow S = k[y_1, \cdots, y_s]/J$ with $\varphi(x_i) = f_i$, is the corresponding homomorphism, then Ker φ is the defining ideal of the Zariski closure of $h(X)$.

Let's first assume that $X = \mathbb{A}^s$, i.e., $J = 0$ and hence, $f_i \in S$. Set $T = k[x_1, \cdots, x_n, y_1, \cdots, y_s]$ and consider the ideal $(f_1 - x_1, \cdots, f_n - x_n) \subset T$. Then

we have the same situation as the previous example. Hence,

$$\text{Ker } \varphi = (f_1 - x_1, \cdots, f_n - x_n) \cap S.$$

To settle the general case, set $Q = k[y_1, \cdots, y_s]$, and let $F_i \in Q$ be the polynomial that maps to $f_i \in S$. Regarding F_i in T, let $I \subset T$ be the ideal

$$I = J.T + (F_1 - x_1, \cdots, F_n - x_n).$$

Then,

$$\text{Ker } \varphi = I \cap S.$$

(See [Eisenbud 1998, 15.30] for an easy proof.)

5. Projective closure of an affine set (homogenization of an ideal). Recall that if $I \subset R = k[x_1, \cdots, x_n]$ is an ideal, then the *homogenization* of I in $R[w]$ is the ideal

$$I^h = (\{f^h : f \in I\}) \subset R[w]$$

where

$$f^h = \sum_j w^{\deg\ f-j} f_j,$$

with f_j being the homogenous component of f of degree j. If $X \subset \mathbb{A}^n \subset \mathbb{P}^n$ is the algebraic set defined by I, then I^h is the defining ideal of the projective closure of X in $\mathbb{P}^n$. Recall that this is the smallest projective variety in $\mathbb{P}^n$ which contains X.

If I is generated by $f_1, \cdots, f_t$, then in general, I^h may not be generated by $f_1^h, \cdots, f_t^h$. Using Gröbner basis, it is possible to find a generating set for I^h, in fact even to get a Gröbner basis for I^h.

Let $>$ be a monomial order on R such that for every monomials $m_1, m_2 \in R$, if $\deg m_1 > \deg m_2$ then $m_1 > m_2$ (this is called a *graded order*). There is a natural extension of a graded order $>$ to a monomial order $>'$ on $R[w]$.

$$m_1 w^a >' m_2 w^b \text{ if and only if } m_1 > m_2 \text{ or } m_1 = m_2 \text{ and } a > b.$$

Theorem 4.8. *Let $I \subset R$ be an ideal and let $g_1, \cdots, g_t$ be a Gröbner basis of I with respect to a graded monomial order $>$ on R. Then $g_1^h, \cdots, g_t^h$ is a Gröbner basis for $I^h \subset R[w]$ with respect to $>'$.*

Example 4.9. *(Twisted cubic curve). The affine twisted cubic curve parametrically given as $C = \{(t, t^2, t^3) : t \in k\} \subset \mathbb{A}^3$. Thus its defining ideal is $I = (g_1, g_2) \subset k[x, y, z]$ where $g_1 = x^2 - y, g_2 = xy - z$. The projective twisted cubic curve $\overline{X}$ is given by*

$$I^h = (x^2 - yw, xy - zw, xz - y^2).$$

Hence, $g_1^h = x^2 - yw, g_2^h = xy - zw$ do not generate I^h.

Using homogenous lexicographic order on R induced by $x > y > z$ we compute a Gröbner basis for I. Thus,

$\text{in}_>(g_1) = x^2$, $\text{in}_>(g_2) = xy$ *and*

$S(g_1, g_2) = xz - y^2$.

Thus, we need to add $g_3 = xz - y^2$ *to the generators. Then*

$\text{in}_>(g_3) = xz$, *and we get*

$S(g_1, g_3) = yg_2$ *and*

$S(g_2, g_3) = y^3 - z^2$.

This is also a remainder with respect to g_1, g_2, g_3. *Hence, we add* $g_4 = y^3 - z^2$ *to the generators. Then,*

$\text{in}_>(g_4) = y^3$, *and we get*

$S(g_1, g_4) = z^2 g_1 - yg_4$,

$S(g_2, g_4) = zg_3$,

$S(g_3, g_4) = z^2 g_3 - y^2 g_4$.

Therefore, g_1, g_2, g_3, g_4 *is a (reduced) Gröbner basis for* I *with respect to* $>$ *and hence*

$$\text{in}_>(I) = (x^2, xy, xz, y^3).$$

Now by the above theorem, $\{g_1^h, g_2^h, g_3^h, g_4^h\} = \{x^2 - yw, xy - zw, xz - y^2, y^3 - z^2w\}$ *is a Gröbner basis for* I^h *with respect to* $>'$.

Observe that I^h *is generated by* $\{x^2 - yw, xy - zw, xz - y^2\}$. *However, this is not a Gröbner basis for* I^h *with respect to* $>'$.

With the sprit of the four color problem, a topic we discussed at the beginning, we end these notes with an application of Gröbner basis on "graph coloring", essentially due to Bayer [Bayer 1982].

5. Graph colorings. We now see how one can apply Gröbner bases theory for vertex coloring of a graph. Recall that a k-coloring of vertices of a graph $G = (V = \{x_1, \ldots, x_n\}, E)$, is a map $\varphi : V \longrightarrow \{\xi_1, \xi_2, \ldots, \xi_k\}$ such that for each $\{x_i, x_j\} \in E$, $\varphi(x_i) \neq \varphi(x_j)$.

We limit to the case $k = 3$. The general case is almost similar. Assume that a graph $\mathcal{G} = (V, E)$ is given. We like to color its vertices using 3 colors. This can be seen as coloring a map with three colors. Each vertices of this graph represents a country, and two vertices are connected by an edge if and only if the corresponding countries are neighbors.

Let $\xi \in \mathbb{C}$ be the "primitive" third root of 1. Thus $\xi^3 = 1$, and $1, \xi, \xi^2$ are three distinct cubic roots of unity. To each vertex $x_i \in V$ one of the colors $1, \xi, \xi^2$ will be assigned. Accordingly,

$$x_i^3 - 1 = 0, \quad 1 \leq i \leq n.$$

Hence, $x_i^3 = x_j^3, \quad 1 \leq i, j \leq n$. If $x_i \neq x_j$ are vertices of an edge, they should have different colors. Since $x_i^3 = x_j^3$, we have $(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$. Therefore, x_i, x_j have different colors if and only if $x_i^2 + x_i x_j + x_j^2 = 0$. Let I be the ideal

$$\left\langle x_i^3 - 1, x_i^2 + x_i x_j + x_j^2 \mid 1 \leq i, j \leq n, \{x_i, x_j\} \text{ is an edge of } G \right\rangle,$$

in $\mathbb{C}[x_1, \ldots, x_n]$. Now our problem can be interpreted as follows:

Theorem 4.10. *The graph G is 3-colorable if and only if $V(I) \neq \emptyset$.*

In other words, the above system of equations has a solution if and only if the graph G is 3-colorable. But by the "Nullstellensatz" $V(I) \neq \emptyset$ if and only if any 1 does not belong to I, or equivalently, a Gröbner basis for I does not contain the identity element 1.

To illustrate the procedure, let G be the following graph. Then the polynomials corresponding to G are $x_i^3 - 1 = 0,\ 1 \leq i \leq n$, and

$$\{x_i^2 + x_i x_j + x_j^2 : (i, j) \in G\}.$$

Thus

$$I = \langle x_i^3 - 1, x_i^2 + x_i x_j + x_j^2 \mid \begin{array}{l} 1 \leq i \leq 8,\ (i,j) \in \{(1,2),(1,5),(1,6),(2,3),(2,4),\\ (2,8),(3,4),(3,8),(4,5),(4,7),(5,6),(5,7),\\ (6,7),(7,8)\}\rangle. \end{array}$$

A Gröbner basis for I in the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$with respect to the lex order, with $x_1 > \cdots > x_n$, is

$$\mathcal{G} = \{x_8^3 - 1, x_7^2 - x_7 x_8 + x_8^2, x_1 - x_7, x_2 + x_7 + x_8, x_5 + x_7 + x_8, x_3 - x_7, x_4 - x_8, x_6 - x_8\}.$$

As it can bee seen, $\mathcal{G}$ does not contain 1, hence $V(I) \neq \emptyset$. Hence by above theorem, G is 3-colorable. The system of equations given by the above Gröner bases, can be easily solved and any of its solutions gives an explicit coloring.

Now let $1, \xi, \xi^2$ receive colors blue, green and red, respectively.

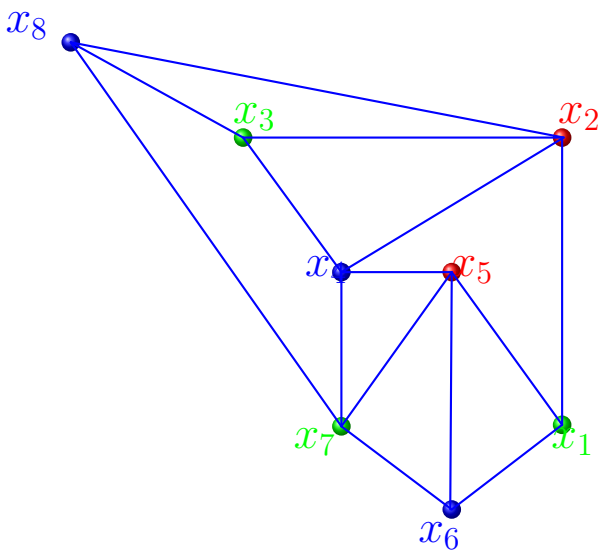
(1) Since $x_8^3 - 1 \in G$, hence any one of the above colors will be the roots of this polynomial. Let assign to x_8 the color BLUE.

(2) Since $x_8^2 + x_7 x_8 + x_7^2$ has two distinct roots, and since x_8 and x_7 are adjacent hence we can assign the color GREEN to x_7.

(3) Since $x_1 - x_7 \in G$, hence x_1 has the same color as x_7, i.e., GREEN.

(4) Since $x_3 - x_7 \in G$, hence x_3 has the same color as x_7, i.e., the color of x_3 is GREEN.

(5) Since $x_2 + x_7 + x_8 \in G$, x_7, x_8 are adjacent, x_2, x_8 also are adjacent, hence the color of x_2 would be RED.
(6) Since $x_5 + x_7 + x_8 \in G$, by the same argument as (5), x_5 would be RED.
(7) Since $x_4 - x_8 \in G$, hence x_4 has then same color as x_8, i.e., BLUE.
(7) And finally since $x_6 - x_8 \in G$, hence x_6 has then same color as x_8, i.e., BLUE.



The Graph$G$

For further references, the web site of RISC is a very useful source the participants could visit: http://www.risc.jku.at/Groebner-Bases-Bibliography/.
This web site contains a list of several books and surveys on Gröbner Bases which are certainly beyond this introductory course. However, a few chapters of the following books (or chapters on Gröbner Bases) will be very helpful: [Adams-Loustaunau 1994], [Eisenbud 1998], [Fröberg 1997], [Kreuzer-Robbiano 2000], [Becker-Weispfenning 1993], [Cox-Little-O'Shea 1992], [Cox-Little-O'Shea 1998], [Gruel-Pfister 2002], and [Sturmfels 1995].

For using computer algebra systems for computations, three major computer algebra packages are CoCoA [CoCoA 2014], Macaulay 2 [Macaulay 2 2014] and Singular [Singular 2014].

Acknowledgments

I am grateful to my colleagues Hassan Haghighi, Hossein Sabzrou and Hadi Zare for helping me in these notes.

References

Adams-Loustaunau 1994. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Math. **3**, Amer. Math. Soc., Providence 1994.

Bayer 1982. D. Bayer, *The division algorith and the Hilbert scheme*, Ph.D. Thesis, Harvard University, 1982.

Becker-Weispfenning 1993. T. Becker, V. Weispfenning, *Gröbner Bases*, Springer, New York 1993.

CoCoA 2014. *CoCoA System, Computations in Commutative Algebra*, 2014, http://cocoa.dima.unige.it/

Cox-Little-O'Shea 1992. D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer, New York 1992.

Cox-Little-O'Shea 1998. D. Cox, J. Little and D. O'Shea, *Using algebraic geometry*, Springer, 1998.

Eisenbud 1998. D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, 1998.

Fröberg 1997. R. Fröberg, *An Introduction to Gröbner Bases*, John Wiley & Son, Chichester 1997.

Gröbner 1949. W. Gröbner, Moderne Algebraische Geometrie, Springer-Verlag, Wien and Innsbruck, 1949.

Gruel-Pfister 2002. G. M. Gruel and G. Pfister, *A Short Intoduction to Commutative Algebra*, Springer 2002.

Herzog-Hibi 2011. J. Herzog and T. Hibi, *Monomial Ideals*, Grad. Texts Math. **260**, Springer, New York, 2011.

Kreuzer-Robbiano 2000. M. Kreuzer and L. Robbiano, *Computional Commutative Algebra 1*, Springer, 2000.

Macaulay 2 2014. *Macaulay 2, a software system for research in algebraic geometry*, http://www.math.uiuc.edu/Macaulay2/

Singular 2014. *Singular, a computer algebra system for polynomial computations*, 2014, http://www.singular.uni-kl.de/

Sturmfels 1995. B. Sturmfels, *Gröbner Bases and Convex Polytopes*, Amer. Math. Soc. University Lecture Note Series **8**, 1995.

Van der Waerden 1953. B. L. van der Waerden, *Modern Algebra*, Vol. 2, Fred. Ungar Pub. Co, New York, 1953.

Van der Waerden 1959. B. L. van der Waerden, *Algebra*, Vol. 2, Fred. Ungar Pub. Co, New York, 1959.

Weil 1946. A. Weil, *Foundation of Algebraic Geometry*, Colloquium Publications, Vol. 29, 1946.