FIRST STEPS WITH GRÖBNER BASES*

Abstract

This is a short introduction to Gröbner bases which requires nothing more than an elementary knowledge of algebra. It prepares the ground for the following speakers and at the same time illustrates Gröbner bases as a tool for understanding some basic concepts of algebraic geometry.

In this talk, I intend to give not only an introduction to the subject, but also some evidence for the beauty of this construction arising from the fundamental question of algebraic geometry: "How to solve a system of polynomial equations?"

The idea of using a term ordering in a ring of polynomials can be traced back to the work of Gauß, and everything which follows here would have been easily understandable to him. Maybe it was only the complexity of calculations, which discouraged mathematicians from that time to naturally generalize the algorithm for solving linear equations and to bring polynomials of arbitrary degree to "row echelon form". Thus, the development of modern computer technics is apparently one reason for the popularity, which Gröbner bases enjoy today. Still, it remains something of a mystery, why "pure mathematics" has discovered them as a powerful tool also for proving theorems "just in time". Several highlights of 20th century algebraic and analytic geometry, notably resolution of singularities in characteristic 0 (Hironaka), or the existence proof for versal deformations of isolated singularities in analytic spaces (Grauert), depend heavily on such methods (still in a non-constructive sense). After the fundamental work of Hermann in 1926, the breakthrough in constructive methods came with the thesis of Buchberger 1965, who also introduced the name "Gröbner base".

For more detailed accounts cf. Eisenbud ([E]), Vasconcelos ([V]), Becker, Weispfenning ([BWe]). General information on the state of the art (including applications in other areas of mathematics) can be found in the recent conference volume edited by Buchberger, Winkler ([BW]).

*This lecture was held by Marko Roczen:
Institut für Mathematik, Humboldt-Universität zu Berlin
Ziegelstr. 13 A D - 10099 Berlin, Germany
e-mail: roczen@mathematik.hu-berlin.de

Here the power of Gröbner bases will be illustrated proving some well known theorems from commutative algebra and algebraic geometry. Main references for this presentation are Cox, Little, O'Shea ([CLO]) and Robbiano ([R2]). The text includes calculations "done by hand", but after this introduction it should be easy to use any of the recent computer algebra systems. In the final section, I provide a number of examples. Several systems like CoCoA ([R1]), Macaulay2 ([GS]) or SINGULAR ([GPS]) are freely available on the web. I tried SINGULAR and found it to be very convenient, but this may depend on the problems you are working with.

Notations: k denotes a field (in section 5 sometimes algebraically closed), $R = k[X]$ the polynomial ring in the indeterminates $X = (X_1, \ldots, X_n)$ over k, and $\mathcal{M} := \{X^\nu |\ \nu \in \mathbb{N}^n\}$ the set of monomials in R. We have a grading on R given by the total degree $|\nu| = |(\nu_1, \ldots, \nu_n)| = \nu_1 + \cdots + \nu_n$ and a "logarithm" (multidegree)

$$log : \mathcal{M} \longrightarrow \mathbb{N}^n$$

sending X^ν to ν. Obviously, $log(m \cdot m') = log(m) + log(m')$ for $m, m' \in \mathcal{M}$. For $f \in R$, write $f = \sum_{\nu \in \mathbb{N}^n} a_\nu X^\nu$ where $a_\nu \in k$ and almost all $a_\nu = 0$. The set $supp(f) := \{\nu \in \mathbb{N}^n |\ a_\nu \neq 0\}$ is the support of f, the $a_\nu X^\nu$ are the terms ($\nu \in supp(f)$).

1 Monomial Ideals

Let $I \subseteq R$ be an ideal . I is said to be monomial if it is generated by a subset of $\mathcal{M}$.

1.1. Remark. *Let I be monomial. Then $f \in I$ if and only if all terms of f are in I.*

Proof. Write f as a linear combination of monomial generators. □

The ideal I is uniquely determined by its monomials, and two monomial ideals coincide if and only if they contain the same monomials.

Calculations with monomials are especially simple. This makes plausible the attempt to reduce computations for arbitrary ideals to this case. An easy exercise is the following

1.2. Remark. *Let I_1, I_2, I_3 be monomial ideals.*

(i) The ideals $I_1 + I_2$ and $I_1 \cdot I_2$ are monomial.

(ii) $(I_1 + I_2) \cap I_3 = I_1 \cap I_3 + I_2 \cap I_3$, and for $m_1,\ m_2 \in \mathcal{M}$ we have

$$(m_1) \cap (m_2) = (lcm(m_1, m_2)).$$

(iii) If $I_3 = (m)$ for some $m \in \mathcal{M}$, then $(I_1 + I_2) : I_3 = (I_1 : I_3) + (I_2 : I_3)$, and

$$(m_1) : (m_2) = (\frac{m_1}{gcd(m_1, m_2)}).$$

1.3. Dickson's Lemma. *Any monomial ideal is generated by a finite set of monomials.*

Of course, this is not a surprise knowing Hilbert's basis theorem, but in section 3. it will become apparent why the above lemma immediately implies the basis theorem, thus giving an independent proof.

Proof of 1.3. For $n = 1$ this is obvious. Assuming the assertion to be true for $n-1$ indeterminates, write the monomial ideal $I \subseteq R$ in the form $I = \cup\, b_j \cdot x_n^j$, where $b_j = (I : x_n^j) \cap k[X_1, \ldots, X_{n-1}]$. Then b_j is a monomial ideal in the subring $k[X_1, \ldots, X_{n-1}]$, where (b_i) is a stationary ascending sequence of ideals generated by finite sets S_i of monomials, $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_j = S_{j+1} = \ldots$ for some j. Now $S' = S_0 \cup S_1 \cdot X_n \cup S_2 \cdot x_n^2 \cup \cdots \cup S_j \cdot x_n^j$ generates I. □

1.4. Corollary. *Let $I = (S)$, where $S \subseteq \mathcal{M}$. Then there is a finite subset $S_1 \subseteq S$ generating I.*

Proof. If $T \subseteq \mathcal{M}$ is a finite system of generators, choose $S_1 = \{m \in S |\ \exists m' \in T : m | m'\}$. □

1.5. Corollary. *Each monomial ideal has a unique (finite) minimal system of monomial generators.*

Proof. Take the minimal elements of $I \cap \mathcal{M}$ with respect to the relation "m divides m'". □

Finally, here is a simple way to compute syzygies of monomial ideals.

1.6. Lemma. *Let $m_1, \ldots, m_s \in \mathcal{M}$ be monomials and $S = S(m_1, \ldots, m_s) = \{(f_1, \ldots f_s) \in R^s |\ \sum f_i m_i = 0\}$. Then the R-module S is generated by the "Koszul-relations"*

$$S_{ij} = \frac{lcm(m_i, m_j)}{m_i} \cdot e_i - \frac{lcm(m_i, m_j)}{m_j} \cdot e_j, \qquad 1 \leq i < j \leq s.$$

Proof. Take $g = (g_1, \ldots, g_s) \in S$. Without loss of generality, $g_i = c_i X^{\nu_i}$, $c_i \in k$, $\nu_i \in \mathbb{N}^n$ and $\nu = \nu_i + log(m_i)$ for all i. Now $\sum c_i X^{\nu_i} m_i = 0$, and we show inductively that g is a linear combination of the S_{ij}. Put $t := |\{i |\ g_i \neq 0\}|$. If $t > 0$, then at least two of the coefficients are $\neq 0$, say c_i and c_j. Let $X^\mu := lcm(m_i, m_j)$. Then X^μ divides X^ν, and $g - c_i X^{\nu-\mu} \cdot S_{ij} =: g'$ coincides in all positions $\neq i, j$ with g. Since $g'_i = 0$ we have finished. □

We have seen until now, that monomial ideals are something of combinatorial nature. In the next step, we will associate to any ideal a monomial ideal, hoping that essential properties are preserved under this procedure. The following talks will provide evidence for this (Popescu, [P]).

First I will explain the notion of a monomial order, which is used to assign a monomial "initial ideal" to an arbitrarily given one. The question of dependence on coordinates will be considered in the talk of Ionescu ([I]).

2 Monomial Orderings

We consider orderings on $\mathcal{M}$ which are appropriate for computations with polynomials ("global orerings")[†].

2.1. Definition. *Let $<$ be a total ordering on the set $\mathcal{M}$ of monomials in $k[X]$ (i.e. for $m, m' \in \mathcal{M}$ exactly one of the conditions $m < m'$, $m = m'$, $m' < m$ is satisfied). Then $<$ is said to be monomial if the following conditions are satisfied:*

(i) Let m_1, m_2, m be monomials such that $m_1 < m_2$. Then $m \cdot m_1 < m \cdot m_2$.

(ii) $<$ is a well ordering, i.e. any nonempty subset has a smallest element.

We use the same notation also for $\mathbb{N}^n$, i.e. we define $log(m_1) < log(m_2)$ if and only if $m_1 < m_2$.

2.2. Remark. *Let $<$ be a monomial ordering and $m_1, m_2 \in \mathcal{M}$ such that m_2 is divisible by m_1. Then $m_1 \leq m_2$.*

This is obvious from the following remark.

2.3. Remark. *Let $<$ be an ordering on $\mathcal{M}$ such that (i) in 2.1. is satisfied. Then condition (ii) is equivalent*

(ii)' The monomial 1 is the minimal element in $\mathcal{M}$.

Proof. (ii) implies (ii)' since for $m \in \mathcal{M}$ minimal and $m \neq 1$ we obtain $m < 1$, thus by (i) $m^2 < m$, which is a contradiction.
Now suppose (ii)': Let $\emptyset \neq M \subseteq \mathcal{M}$ be any subset. If I is the ideal generated by M, 1.4. gives us finitely many elements $m_1 < \cdots < m_s$ in M which generate I, i.e. for any $m \in M$ we obtain $m_1 \leq m$ since m is divisible by some m_i. □

[†]Note that there is a more general notion, appropriate also for the case of power series, where a similar construction is possible ("standard bases").

2.4. Examples of monomials orderings.

(i) **lex (the "lexicographic ordering"):** *For $\mu, \nu \in \mathbb{N}^n$ define $\nu <_{lex} \mu$ if and only if there exists some $j \in \{1, \ldots, n\}$ such that $\nu_j < \mu_j$ and for all $i < j$: $\nu_i = \mu_i$.*

(ii) **deglex (the "graded lexicographic ordering"):** *$\nu <_{deglex} \mu$ if and only if $|\nu| < |\mu|$ or $|\nu| = |\mu|$ and $\nu <_{lex} \mu$.*

(iii) **degrevlex (the "graded reverse lexicographic ordering"):** *$\nu <_{degrevlex} \mu$ if and only if $|\nu| < |\mu|$ or $|\nu| = |\mu|$ and there exists some $j \in \{1, \ldots, n\}$ such that $\nu_j > \mu_j$ and for all $i > j$: $\nu_i = \mu_i$.*

(iv) **block orderings ("product orderings"):** *Let $<_1$ be an ordering for $\mathbb{N}^{n_1}$ and $<_2$ be an ordering for $\mathbb{N}^{n_2}$. The corresponding block ordering on $\mathbb{N}^{n_1+n_2}$ is defined by the condition:*

$(\nu_1, \nu_2) < (\mu_1, \mu_2)$ if and only if $\nu_1 <_1 \mu_1$ or $\nu_1 = \mu_1$ and $\nu_2 <_2 \mu_2$.

(v) **matrix orderings:** *Let $A \in Gl_{\mathbb{R}}(n)$ be an invertible matrix. We define a relation $<_A$ on $\mathbb{N}^n$ by the condition*

$$\nu <_A \mu \iff A \cdot \begin{pmatrix} \nu_1 \\ \vdots \\ \nu_n \end{pmatrix} <_{lex} A \cdot \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}.$$

This is a total ordering since A is invertible. It is monomial if and only if for all $\nu \in \mathbb{N}^n - \{0\}$ the first nonzero term of $A \cdot \begin{pmatrix} \nu_1 \\ \vdots \\ \nu_n \end{pmatrix}$ is positive (corresponding to condition (ii)' in 2.3.). If this is satisfied, $<_A$ is said to be the matrix ordering defined by A. Note that the above condition is automatically satisfied if the first row of A has all entries > 0.

Here are some special cases of *(v)*: **lex** is the **matrix** ordering defined by the unit matrix, **degrevlex** is given by

$$\begin{pmatrix} 1 & \cdots & 1 & 1 \\ 0 & \cdots & 0 & -1 \\ 0 & \cdots & -1 & 0 \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix}.$$

If $<_1$, $<_2$ are defined by matrices A_1, A_2, then the corresponding block ordering is definded by $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$.

Take the above list as a hint as to how useful it may be to attack the same problem with different monomial orderings (cf. exercise 6.1. below)[†].

3 Division Algorithm and Gröbner Bases

Let us fix a monomial ordering $<$ on $\mathcal{M}$. In the examples (if not otherwise specified) this will be $<_{lex}$. Define for $0 \neq f \in k[X]$ the leading multi-index $\mu = log(f) := max_<(Supp(f))$, and write $lm(f) := X^\mu \in \mathcal{M}$ for the leading monomial, $lc(f) := a_\mu \in k$ for the leading coefficient of f. The leading term is $lt(f) = lc(f) \cdot lm(f)$.

3.1. Proposition. *Let $F = (f_1, \ldots, f_s)$ be nonzero elements of $k[X]$ and $f \in k[X]$ arbitrary. Then there exist $a_1, \ldots, a_s, r \in k[X]$ such that*

(*) $f = a_1 f_1 + \cdots + a_s f_s + r$ and

(i) r equals 0 or is a k-linear combination of monomials none of which is divisible by any $lm(f_i)$, $i = 1, \ldots, s$.

(ii) For any i we have $a_i f_i = 0$ or $log(f) \geq log(a_i f_i)$.

Further, there is an algorithm to bring an arbitrary f into the form (*) and such that (i), (ii) are satisfied. r is said to be the remainder of f after division by F in this case.

3.1. is nothing more than a generalization of the classical procedure for $n = s = 1$. Check if $lm(f)$ is divisible by any $lm(f_i)$. Take i minimal with that property and substract a monomial multiple $a_i' f_i$ of f_i from f which has the same leading term. Replace f by $f - a_1' f_1$ (which has a strictly smaller leading term). If $lm(f)$ is not divisible by any $lm(f_i)$, send $lt(f_i)$ to the remainder r and continue with $f - lt(f)$.

3.2. Example. *Use lex ordering with $X < Y < Z$. Take $f_1 = X^2$, $f_2 = XY + Z^2 \in k[X, Y, Z]$.*

(i) Divide $f = X^2Y^2 + XY^2 - 1$ by $F = (f_1, f_2)$. We obtain

$$f = Y^2 \cdot f_1 + Y \cdot f_2 - (YZ^2 + 1),$$

where $-(YZ^2 + 1)$ is the remainder.

(ii) Note that the representation of f in 3.1. (*) is not unique. For the above f we have also $f = (XY + Y - Z^2) \cdot f_2 + (-YZ^2 + Z^4 - 1)$.

[†]For more details on the classification of monomial orderings cf. ([R2]).

Now let I be an ideal $\neq 0$ in $k[X]$.

3.3. Definition. *The ideal $in_<(I)$, generated by all $lm(f)$, $f \in I - \{0\}$, is said to be the **initial ideal of** I **with respect to** $<$.*

Since it is fixed, we usually suppress "$<$" in the notation.

If $I = (f_1, \ldots, f_s)$, then we cannot expect in general $in(I)$ to be generated by $lm(f_1), \ldots lm(f_s)$; e.g. in the above example

$$XZ^3 = -Y \cdot f_1 + X \cdot f_2 \notin (lm(f_1), lm(f_2)).$$

Obviously, $in(I)$ is a monomial ideal, and by Dickson's lemma (1.3.), there is a finite subset $\{f_1, \ldots, f_s\} \subseteq k[X] - \{0\}$ such that $in(I) = (lm(f_1), \ldots, lm(f_s))$.

3.4. Definition. *Let $f_1, \ldots, f_s \in I - \{0\}$ be such that $\{lm(f_i) | 1 \leq i \leq s\}$ generates $in(I)$. Then $(f_1, \ldots, f_s)$ is said to be a **Gröbner base** of I.*

The notation is justified by

3.4. Theorem. *A Gröbner base of I generates I.*

Proof. Fix a Gröbner base $(f_1, \ldots, f_s)$ of I. Choose any $f \in I$. The division algorithm gives $f = a_1 f_1 + \cdots + a_a f_s + r$ with no term of r divisible by any $lm(f_i)$. But $r = f - \sum a_i f_i \in I$. Assume $r \neq 0$. Then $lm(r) \in in(I)$, it therefore has to be a multiple of some $lm(f_i)$, which is impossible. □

(Note that from 3.4. follows Hilbert's basis theorem.)

Another characterization of Gröbner bases is given by the

3.5. Special generation property. *Let $f_1, \ldots, f_s \in I$. Then $(f_1, \ldots, f_s)$ is a Gröbner base of I if and only if any $f \in I$ can be written as $f = \sum a_i f_i$, such that for arbitrary i, $a_i f_i = 0$ or $log(a_i f_i) \leq log(f)$.*

Proof. ($\Rightarrow$) was done before. ($\Leftarrow$): If $f = \sum a_i f_i$, then always

$$log(f) \leq max_<\{log(a_i f_i) | 1 \leq i \leq s\}.$$

Now the condition on the a_i implies equality. Thus $log(f) = log(a_j f_j)$ for some j, i.e. $lm(f)$ is divisible by $lm(f_j)$. □

For a Gröbner base, the remainder is independent of the order of its elements. This is important also from the computational aspect ("*Church-Rosser property*"):

3.6. Theorem. *Let $F = (f_1, \ldots, f_s)$ be a Gröbner base for the ideal $I \neq 0$ and $f \in k[X]$. Then there exists exactly one $r \in k[X]$ such that*

(i) No term of r is divisible by any $lm(f_i)$.

(ii) $f - r \in I$.

Proof. The existence of r is obvious: Divide f by F to obtain r. To show uniqueness, take some r' with properties (i), (ii). Then $g = f - r \in I$ and $g' = f - r' \in I$, thus $r - r' = g' - g \in I$ and if $r - r' \neq 0$ we obtain: $lm(r - r')$ is divisible by some $lm(f_i)$ which is impossible. □

Note that the remainder of f is zero if and only if $f \in I$, and we obtain an isomorphism

$$k[X]/I \longrightarrow k[X]/in(I)$$

of k-vector spaces, sending $\overline{f}$ to the class of the remainder of f. This gives us a monomial basis for the quotient ring $k[X]/I$ ("*Macaulay's theorem*").

In the next section, we prove a theorem that implies

3.7. Buchberger's criterion. *For $g, h \in k[X] - \{0\}$, let*

$$S(g,h) := \frac{X^\nu}{lt(f)} \cdot g - \frac{X^\nu}{lt(h)} \cdot h,$$

where X^ν is the least common multiple of $lm(f)$ and $lm(g)$ ("S-polynomial of f and g"). If an ideal $I \neq 0$ is generated by $f_1, \ldots, f_s \in k[X]$, then $F = (f_1, \ldots, f_s)$ is a Gröbner base for I if and only if for all i, j the remainder of $S(f_i, f_j)$ after division by F is 0.

This gives an obvious possibility to construct a Gröbner base from a given finite set of generators ("*Buchberger algorithm*").

3.8. Example. *We find a Gröbner base for the ideal $I = (f_1, f_2)$, f_i taken from 3.2., computing S-polynomials and (if necessary) adding them to the list:*

$$S(f_1, f_2) = Y \cdot f_1 - X \cdot f_2 = -XZ^2 =: -f_3$$

$$S(f_1, f_3) = 0$$

$$S(f_2, f_3) = Z^4 =: f_4$$

$$S(f_1, f_4) = 0$$

$$S(f_2, f_4) = Z^6 \text{ (has remainder } 0 \text{ after division by } (f_1, \ldots, f_4))$$

$$S(f_3, f_4) = 0$$

Thus, $(f_1, \ldots, f_4)$ *is a Gröbner base for the ideal* I*, and*

$$in(I) = (X^2, XY, XZ^2, Z^4)$$

is generated by the leading monomials.

What about uniqueness? Obviously, there are infinitely many Gröbner bases for an ideal $\neq 0$, but we already know that monomial ideals have essentially unique minimal monomial bases. If $\{f_1, \ldots, f_s\}$ gives a Gröbner base for I and $lm(f_1)$ divides any $lm(f_j)$, $j > 1$, then obviously $\{f_2, \ldots, f_s\}$ is a Gröbner base for I as well. Thus we may always restrict our attention to a subset without divisibility relations between the initial terms. We obtain a so called "*minimal Gröbner base*" and the leading monomials give at the same time the minimal system of monomial generators for the initial ideal $in(I)$.

3.9. Definition. *Let* $(f_1, \ldots, f_s) = F$ *be a Gröbner base for the ideal* I*. Then* F *is said to be a reduced Gröbner base if*

(i) $lc(f_i) = 1$ *for all* i*;*

(ii) No term of f_i *is divisible by any* $lm(f_j)$*,* $j \neq i$*.*

Thus all terms of f_i (except the initial ones) are equal to their remainder.

It is not difficult to obtain a reduced Gröbner base from a given minimal Gröbner base: Take for example f_1, and replace $f_1 - lt(f_1)$ by its remainder after division by $(f_2, \ldots, f_s)$, ... The procedure eventually terminates, and the initial ideal remains unchanged in each step.

3.10. Theorem. *Any ideal* $I \neq 0$ *has a unique reduced Gröbner base.*

Proof. Let $(f_1, \ldots, f_s)$ and $(f'_1, \ldots, f'_{s'})$ be reduced Gröbner bases. Then $s = s'$, and without loss of generality $lm(f_i) = lm(f'_i)$ for all i. Let $g_i := f_i - f'_i$, then no term of g_i is divisible by any $lm(f_i)$, and $g_i \in I$ has remainder $0 = g_i$. Thus $f_i = f'_i$. □

As a result, we obtain a constructive procedure to decide whether or not two ideals (given by any generators) are the same: Their reduced Gröbner bases (for any fixed monomial ordering) have to coincide.

4 Buchberger's Criterion and syzygies of the Initial Terms

As before, we preserve any nonzero polynomials $f_1, \ldots, f_s$ and a monomial ordering $<$. I is the ideal generated by all f_i. Write $F = (f_1, \ldots, f_s) \in k[X]^s$.

This section will improve the method for computing Gröbner bases and at the same time attempt to give an explanation as to why it works. For simplicity, assume $lc(f_i) = 1$ for all i.

4.1. Definition. *$f \in k[X]$ **reduces to** 0, written $f \overset{F}{\rightsquigarrow} 0$, if there exist $a_i \in k[X]$ such that $f = \sum a_i f_i$ with $a_i f_i = 0$ or $log(a_i f_i) \leq log(f)$, $1 \leq i \leq s$.*

In fact this condition is weaker than the condition on the remainder to be 0. We know already if it is satisfied for all $f \in I$, then F is a Gröbner base. We will see in a moment that F is Gröbner if and only if all S-polynomials $S(f_i, f_j)$ reduce to 0, which generalizes 3.7. Also, calculations become easier if we use the following

4.2. Remark. *Let f_i, f_j be such that the g.c.d of their leading monomials is 1. Then $S(f_i, f_j) \overset{F}{\rightsquigarrow} 0$.*

Proof. Let $f_i = X^\mu + p$, $f_j = X^\nu + q$, $log(p) < \mu$, $log(q) < \nu$. Then $S(f_i, f_j) = pf_j - qf_i$, and $log(S(f_i, f_j)) = max_<\{log(pf_j), log(qf_i)\}$ ($\leq$ is always true, and the initial terms in the above expression for $S(f_i, f_j)$ cannot cancel, this would imply $lm(pf_j) = lm(qf_i)$, i.e. $lm(f_j)|lm(q)$ which is impossible). □

Compare e.g. the calculation in 3.8.: There is no need to compute the remainder of $S(f_2, f_4)$. Also it is possible to give examples in which $f \overset{F}{\rightsquigarrow} 0$ does not imply f has remainder 0.

Now consider the module $S(F)$ of syzygies of the initial terms of F:

$$S(F) := \{(h_1, \ldots, h_s) \in k[X]^s \mid \sum_{i=1}^{s} h_i \cdot lm(f_i) = 0\}$$

Of course it is homogeneous in the following sense: Let $\mu \in \mathbb{N}^n$. The μ-th homogeneous part $S(F)_\mu$ of $S(F)$ consists of all $(h_1, \ldots, h_s) \in k[X]^s$ such that (for $h_i \neq 0$) $log(h_i) + log(f_i) = \mu$. Now $S(F)$ is the sum of its homogeneous parts. Also, we write $log(h_1, \ldots, h_s) := max_<\{log(h_i f_i) \mid 1 \leq i \leq s\}$ for arbitrary $(h_1, \ldots, h_s) \in R^s - \{(0, \ldots, 0)\}$.

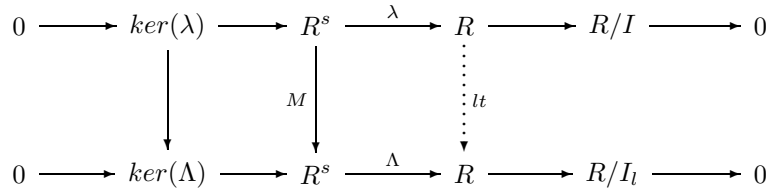
From 1.6. we already know, $S(F)$ is generated by the homogeneous "Koszul-relations" $S_{ij} = \frac{X^{\nu_{ij}}}{lt(f_i)} \cdot e_i - \frac{x^{\nu_{ij}}}{lt(f_j)} \cdot e_j$, where $X^{\nu_{ij}} = lcm(lm(f_i), lm(f_j))$.

Here is a generalization of both announced versions of Buchberger's criterion.

4.3. Theorem. *Fix any homogeneous system $S_1, \ldots, S_t$ of generators for $S(F)$, $S_i = (S_{i1}, \ldots, S_{is})$. Then F is a Gröbner base for the ideal I if and only if for all i*

$$S_i \cdot^t F = \sum_{i=1}^{s} S_{ij} f_j \overset{F}{\rightsquigarrow} 0.$$

The **proof** is done in several steps. Consider the diagram of maps



with exact rows and the left hand square commutative, λ given by $(f_1, \ldots, f_s)$, Λ by $(lt(f_1), \ldots, lt(f_s))$, $I_l = (lt(f_1), \ldots, lt(f_s))$ and $M(h)$ defined for $h = (h_1, \ldots, h_s)$ by $M(h) = (\overline{h_1}, \ldots, \overline{h_s})$ with $\overline{h_i} = 0$ if $log(h_i f_i) < log(h)$ and $\overline{h_i} = lt(h_i)$ if $log(h_i f_i) = log(h)$, $M(0) = 0$.

4.4. Remark. *If $S_i \in ker(\lambda)$ and $\{M(S_1), \ldots, M(S_t)\}$ is a homogeneous system of generators of $ker(\Lambda)$, then $\{S_1, \ldots, S_t\}$ generates $ker(\lambda)$.*

Proof. For $h \in ker(\lambda)$, choose $h^{(1)} := h - \sum m_i S_i$ with m_i constant multiples of monomials such that $M(h) = \sum m_i M(S_i)$. Then $log(h^{(1)}) < log(h)$ and $h^{(1)} \in ker(\lambda)$. Continue by induction. □

4.5. Lemma. *$\{f_1, \ldots, f_s\}$ is a Gröbner base of I if and only if every homogeneous element of $ker(\Lambda)$ lifts to $ker(\lambda)$ via M.*

Proof. ($\Leftarrow$): Let $f := \sum h_i f_i \in I$ and put $(h_1, \ldots, h_s) =: h$. Now $log(h) \geq log(f)$, and equality means special generation of f (3.5.); suppose now $log(h) > log(f)$. Then $M(h) \in ker(\Lambda)$ (leading terms cancel). By hypothesis, maximal terms of h lift to some $g \in ker(\lambda)$, and $h^{(1)} := h - g$ has $log(h^{(1)}) < log(h)$, $\lambda(h^{(1)}) = \lambda(h)$. Continue by induction.

($\Rightarrow$): Let $\{f_1, \ldots, f_s\}$ be a Gröbner base for I, $0 \neq h = (h_1, \ldots, h_s) \in ker(\Lambda)$ homogeneous. For $f := \lambda(h)$ we have special generation, i.e. there exists $g = (g_1, \ldots, g_s)$ such that $f = \sum g_i f_i$, $log(f) = max_<\{log(g_i f_i) |\ 1 \leq i \leq s\}$ and thus $log(g) = log(\lambda(h)) < log(h)$, i.e. $M(h - g) = M(h) = h$ and $h - g \in ker(\lambda)$. □

We are ready to prove 4.3.: We have only to show that the condition is sufficient. To see that $\{f_1, \ldots, f_s\}$ is a Gröbner base for I, it is sufficient to check that each element of a fixed homogeneous system of generators for $ker(\Lambda)$ lifts to $ker(\lambda)$. Let $S_j = S = (g_1, \ldots, g_s)$. Now $\sum g_i \cdot lt(f_i) \rightsquigarrow 0$, thus there exists $h = (h_1, \ldots, h_s)$ such that $log(f) = max_<\{log(h_i f_i) |\ 1 \leq i \leq s\}$ for $f = \sum h_i f_i$. We obtain $S' := S - (h_1, \ldots, h_s) \in ker(\lambda)$ and $M(S') = M(S)$ since terms of top multidegree in $\sum g_i f_i$ cancel. □

5 Gröbner Bases and Elimination Theory

A theorem of algebraic geometry states that over an algebraically closed field k, the projection $V \times \mathbb{P}^n_k \to V$ is (Zariski-) closed for any variety V over k. Here we consider the "affine part" of this statement in a constructive sense. For $k[X_1, \ldots, X_n]$, we fix lex ordering on the set $\mathcal{M}$ of monomials.

5.1. Definition. *For an ideal $I \subseteq k[X_1, \ldots, X_n]$, the intersection ideal $I_r := I \cap k[X_{r+1}, \ldots, X_n]$ in the subring $k[X_{r+1}, \ldots, X_n]$ is said to be the* ***r-th elimination ideal of I.***

A Gröbner base is considered as a set here as far as convenient.

5.2. Elimination Theorem. *Let F be a Gröbner base for the ideal I (with respect to lex). Then the intersection $F_r := F \cap k[X_{r+1}, \ldots, X_n]$ is a Gröbner base for the elimination ideal I_r.*

Proof. $F_r \subseteq I_r$, and we have to show: The initial terms of elements of F_r generate $in(I_r)$. Take any $f \in I_r$, then there exists $g \in F$ such that $lm(g)|lm(f)$. Thus $lm(g) \in k[X_{r+1}, \ldots, X_n]$. Since we have lex ordering, any monomial smaller than $lm(g)$ is not divisible by X_i, $i \leq r$. □

Note that there exist other orderings on $\mathcal{M}$ which allow for such a conclusion ("elimination orderings").

The geometric interpretation is obvious: Let $\pi : k^n \to k^{n-r}$ be the projection map $(\alpha_1, \ldots, \alpha_n) \mapsto (\alpha_{n-r+1}, \ldots, \alpha_n)$. If $V(I)$ and $V(I_r)$ in k^n, k^{n-r} respectively are the sets of zeroes of the corresponding ideals, then $\pi_r(V(I)) \subseteq V(I_r)$. In fact, $V(I_r)$ can be shown to be the (Zariski-) closure of $\pi_r(V(I))$.

Thus, the construction of the elimination ideal gives a candidate for the solution of an implicitization problem: Let $M \subseteq k^n$ be a subset given by polynomials $f_i \in k[T_1, \ldots, T_m]$, $1 \leq i \leq n$, such that

$$M = \{(f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m))|\ (t_1, \ldots, t_m) \in k^m\}.$$

Using lex ordering with $T_1 > \cdots > T_m > X_1 > \cdots > X_n$, we obtain for the elimination ideal J_m of $J = (X_1 - f_1, \ldots, X_n - f_n)$ an ideal in $k[X_1, \ldots, X_n]$ such that M is contained in $V(J_m)$. To check equality we can use the following

5.3. Extension Theorem. *Let k be algebraically closed and $I = (f_1, \ldots, f_s)$ an ideal in $k[X_1, \ldots, X_n]$ with first elimination ideal $I_1 \subseteq k[X_2, \ldots, X_n]$. Write f_i as polynomials in X_1 over $k[X_2, \ldots, X_n]$:*

$$f_i = g_i(X_2, \ldots, X_n) \cdot X_1^{N_i} + (\textit{terms of degree } < N_i \textit{ in } X_1)\,,$$

such that $N_i \geq 0$, $g_i \in k[X_2, \ldots, X_n] - \{0\}$. *Then for any "partial solution"* $(\alpha_2, \ldots, \alpha_n) \in V(I_1)$ *which is not a common zero of* $g_1, \ldots, g_s$, *there exists* $\alpha_1 \in k$ *such that* $(\alpha_1, \ldots, \alpha_n) \in V(I)$.

Obviously this implies

5.4. Remark. *With the above notations, if any* g_i *is a constant, we obtain* $\pi_1(V(I)) = V(I_1)$.

An elementary proof of the extension theorem (using resultants) can be found in ([CLO], ch. 3, §6).

As a conclusion, we obtain a short proof of Hilbert's

5.5. Nullstellensatz. *Let* k *be algebraically closed and* $I \subseteq k[X_1, \ldots, X_n]$ *be an ideal. Then the set* $V(I)$ *of zeroes of* I *is empty if and only if* $I = (1)$.

Proof. We have to show ($\Rightarrow$): Since there is nothing to prove for $n = 1$, suppose $n > 1$, $I = (f_1, \ldots, f_s)$, $V(I) = \emptyset$ and $I \neq 0, (1)$. After a linear change of indeterminates, we may assume $f_1 = X_1^N + (\textit{terms of degree } < N \textit{ in } X_1)$. Thus by 5.4. above, $\pi_1 : k^n \to k^{n-1}$ maps $V(I)$ onto $V(I_1)$, i.e. $V(I_1) = \emptyset$. By induction, we may suppose $I_1 = (1)$, thus $1 \in I_1 \subseteq I$. □

Together with the results of 3., we obtain an algorithmic solution of the consistency problem for polynomial equations. This is generalizing the familiar criterion for linear equations.

5.6. Corollary. *Let* $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ *be polynomials over an algebraically closed field* k. *Then there exists no common zero of* $f_1, \ldots, f_s$ *if and only if the reduced Gröbner base*† *of the ideal* $(f_1, \ldots, f_s)$ *is* $\{1\}$.

6 Using Computer Algebra

Here are examples how to use SINGULAR [GPS] for calculations with Gröbner bases. I do not attempt to rewrite the manual but rather to encourage further study. Thus, I perform a single calculation instead of giving theoretical explanations; this will be a repetition of what we have done "by hand".

Start SINGULAR on your system and enter

```
ring r=0,(x,y,z),lp;
```

to define a polynomial ring over a field of characteristic 0 (in our case $\mathbb{Q}$) in the indeterminates x, y, z with ordering lex†. Define an ideal i with the command

†with respect to an arbitrarily fixed monomial ordering

†lp denotes lex, dp denotes degrevlex, Dp denotes deglex, ...

```
ideal i=x2,xy+z2;
```

and say

```
option(redSB);
```

to obtain always reduced Gröbner bases in the output. Now replace the generators of i by a (reduced) Gröbner base

```
i=std(i);
```

and ask for the result:

```
i;
```

The output is a list of the 4 generators which we have computed in 3.8. already. Further compute the remainder of the polynomial $xy^7 - xyz$ with respect to this Gröbner base: Type

```
reduce(xy7-xyz,i);
```

to obtain the remainder $-y^6z^2 + z^3$.

Here are some examples which are more difficult without technical tools.

6.1. Exercise. *Compare how much the result may depend on the monomial ordering. Compute Gröbner bases in lex and in degrevlex for the ideal* $I = (X^5 + Y^5 - Z^5, X^7 + Y^7 - Z^7)$. *Which ordering do you prefer? Also, find out whether or not* $X^9 + Y^9 - Z^9 \in I$.

6.2. Exercise. *Choose a system of polynomials in* $\mathbb{Q}[X, Y, \dots]$. *Use SINGULAR to decide whether or not there exists a solution over* $\mathbb{C}$.

6.3. Exercise. *Let* $C = \{(s, s^3, s^4) |\ s \in \mathbb{C}\}$ *be the twisted quartic curve in the affine 3-space. The tangent surface* T *has a parametrization*

$$T = \{(s + t, s^3 + 3s^2t, s^4 + 4s^3t) |\ s, t \in \mathbb{C}\}.$$

Use the implicitization method from 5. to find an equation in $\mathbb{C}[X, Y, Z]$ *which defines* T.

References

[BWe] Becker, T., Weispfenning, V., *Gröbner Bases*, Springer Berlin Heidelberg New York, 1995.

[BW] Buchberger, B., Winkler, F. (ed's), *Gröbnerbases and Applications*, London Mathematical Society Lecture Note Series **251**, Cambridge University Press, 1988.

[CLO] Cox, D., Little, J., O'Shea, D., *Ideals, Varieties and Algorithms*, Springer Berlin Heidelberg New York, 1992.

[E] Eisenbud, D., *Commutative Algebra with a View towards Algebraic Geometry*, Springer New York, 1995.

[F] Fröberg, R., *An introduction to Gröbner bases*, Pure and Applied Mathematics, Wiley-Interscience Series of Texts, Monographs, and Tracts. Chichester: John Wiley & Sons, 1997.

[GS] Grayson, D., Stillman, M., *Macaulay2*, available in the web from http://www.math.uiuc.edu/Macaulay2.

[GPS] Greuel, G.-M., Pfister, G., Schönemann, H., *Singular, a System for Computation in Algebraic Geometry and Singularity Theory*, available from http://www.mathematik.uni-kl.de/ftp/pub/Math/Singular.

[I] Ionescu, C., *Theorems of Green, Macaulay and Gotzmann (Estimating the Hilbert function)*, this volume.

[P] Popescu, D., *Bounds for Betti numbers*, this volume.

[R1] Robbiano, L., et al., CoCoA 3.5., available in the web from http://ideal.dima.unige.it/download.html.

[R2] Robbiano, L., *Introduction to the theory of Groebner bases*, Curves Semin. at Queen's, Vol. 5, Kingston/Ont. 1987, Queen's Pap. Pure Appl. Math. **80** (1988), Expose B, 29 p.

[V] Vasconcelos, W. V., *Computational methods of commutative algebra and algebraic geometry*, with chapters by D. Eisenbud, D. R. Grayson, J. Herzog and M. Stillman, Springer Berlin, 1998.