Gröbner Bases: An Introduction

Craig Huneke

Notes by Ananthnarayan H.

University of Kansas

Fall 2004

Setup: Let k be a field and $S := \mathsf{k}[X_1, \ldots, X_n]$ be a polynomial ring over k in n variables.
A *monomial* in S is an element of the form $X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$ with $a_i \geq 0$.
A *term* is an element of the form $\lambda X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$ with $a_i \geq 0$ and $\lambda \in \mathsf{k}$.

Note that these definitions depend on the choice of variables. If $S = \mathsf{k}[X_1, X_2]$, then S is also the same as $\mathsf{k}[X_1 + X_2, X_2]$. But $(X_1 + X_2)X_2$ is a monomial in the second representation of S but not in the first.

As a vector space over k, the monomials are a k-basis of S. In some sense, Gröbner bases are a way to choose a monomial k-basis of S/I, where I is an ideal in S.

Two examples:

Example 1 Let $S = \mathsf{k}[X]$, $I = (f) = X^n + a_1 X^{n-1} + \cdots + a_n$, $a_i \in \mathsf{k}$. Then, S/I has a k-basis $\{1, X, X^2, \ldots X^{n-1}\}$.

This statement is equivalent to the Division Algorithm.

Example 2 Let $S = \mathsf{k}[X, Y, Z]$ and $I = (X - Y + Z, X + Y - Z)$. Note that $I = (X, Y - Z)$. Thus, $S/I \simeq \mathsf{k}[Z]$.
Notice that the generating set $\{X - Y + Z, X + Y - Z\}$ of I corresponds to the matrix $\begin{bmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix}$ while the generating set $\{X, Y - Z\}$ corresponds to $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \end{bmatrix}$, the reduced row echelon form of the first one.

Both of these are examples of Gröbner bases as we will see later.

Definition 1
1) A term ordering τ (or $>_\tau$) is a partial ordering on the monomials of $S = \mathsf{k}[X_1, \ldots, X_n]$ such that
a) for any monomial $m \neq 1$, we have $m >_\tau 1$ and
b) if m, n and m' are monomials such that $m >_\tau n$, then $mm' >_\tau nm'$.

2) A monomial ordering τ (or $>_\tau$) is a total ordering on the monomials of $S = \mathsf{k}[X_1, \ldots, X_n]$ such that

a) for any monomial $m \neq 1$, we have $m >_\tau 1$ and
b) if m, n and m' are monomials such that $m >_\tau n$, then $mm' >_\tau nm'$.

We say that a monomial ordering τ is a *degree-wise monomial ordering* if it recognizes the degrees, i.e. a monomial of higher degree is greater under τ.

Examples:

1) Let S be $\mathsf{k}[X]$ and τ be any monomial ordering. Then by (a), $X >_\tau 1$. Moreover, by repeated application of (b), we get $\cdots >_\tau X^3 >_\tau X^2 >_\tau X >_\tau 1$.

2) Let S be $\mathsf{k}[X,Y]$ and τ be a monomial ordering such that $X >_\tau Y$. Fix a degree d. Then we have

$$X^d >_\tau X^{d-1}Y >_\tau \cdots >_\tau Y^d.$$

Let us see this in degree 2. Since $X >_\tau Y$, we have $X^2 >_\tau XY$ and $XY >_\tau Y^2$. This gives us $X^2 >_\tau XY >_\tau Y^2$.
Thus, there is only one degree-wise monomial ordering in the 2-variable case.

3) Let $S = \mathsf{k}[X,Y,Z]$ and τ be a monomial ordering such that $X >_\tau Y >_\tau Z$. Consider the degree 2 monomials. Multiplying by X, Y and Z we get the respective inequalities:

$$X^2 >_\tau XY >_\tau XZ; XY >_\tau Y^2 >_\tau YZ \text{ and } XZ >_\tau YZ >_\tau Z^2. \text{ Hence}$$

$$X^2 >_\tau XY >_\tau \begin{array}{c} XZ \\ \\ Y^2 \end{array} >_\tau YZ >_\tau Z^2.$$

Thus, to define a degree-wise monomial ordering in the 3-variable case, we need to make a choice in degree 2, namely $XZ >_\tau Y^2$ or $Y^2 >_\tau XZ$.

Something to ponder at this juncture is whether these choices uniquely determine the degree-wise monomial orderings in the 3-variable case, i.e. are there only two possible degree-wise monomial orderings, one determined by $XZ >_\tau Y^2$ and the other by $Y^2 >_\tau XZ$? The answer is no, as we see in the exercises.

Definition 2 *Let τ be a monomial ordering. If $f \in S = \mathsf{k}[X_1, \ldots, X_n]$, we set*

$$\mathrm{in}_\tau(f) := \text{ the largest monomial occuring in a non-zero term of } f$$

and the leading term of f with respect to τ

$$\mathrm{lt}_\tau(f) := \text{ the term which has } \mathrm{in}_\tau(f).$$

If I is an ideal in S, then we define

$$\mathrm{in}_\tau(I) \quad := \quad < \mathrm{in}_\tau(f) : f \in I >$$

Example 3
1) Let $S = \mathsf{k}[X]$, f be a polynomial of degree n in S. Then $\mathrm{in}_\tau(f) = X^n$.

2) In $\mathsf{k}[X,Y]$, with $X >_\tau Y$, we have $\mathrm{in}_\tau(X^2+Y^2+2XY) = X^2$ and $\mathrm{in}_\tau(Y^2-2XY) = XY$.

3) Let $S = \mathsf{k}[X,Y,Z]$, $I = (Y^2 - XZ, XY - Z^2)$ and τ be a degree-wise monomial ordering such that $X >_\tau Y >_\tau Z$. Set $f_1 = Y^2 - XZ$ and $f_2 = XY - Z^2$. Recall that we can choose $XZ >_\tau Y^2$ or $Y^2 >_\tau XZ$.

Case (a): $XZ >_\tau Y^2$.
In this case, $\mathrm{in}_\tau(f_1) = XZ$ and $\mathrm{in}_\tau(f_2) = XY$.
Question: Is $\mathrm{in}_\tau(I) =< \mathrm{in}_\tau(f_1), \mathrm{in}_\tau(f_2) >$?
The answer is no. Let $f_3 = Yf_1 + Zf_2 = Y^3 - Z^3 \in I$. Then $\mathrm{in}_\tau(f_3) = Y^3$. Clearly $\mathrm{in}_\tau(f_3)$ is not in $< XY, XZ >=< \mathrm{in}_\tau(f_1), \mathrm{in}_\tau(f_2) >$. In fact, as we will prove later $\mathrm{in}_\tau(I) = (XY, XZ, Y^3)$.

Case (b): $Y^2 >_\tau XZ$.
In this case, $\mathrm{in}_\tau(f_1) = Y^2$ and $\mathrm{in}_\tau(f_2) = XY$. If we set $f_4 = Xf_1 - Yf_2 = -X^2Z + YZ^2$, then $\mathrm{in}_\tau(f_4) = X^2Z \notin (Y^2, XY) =< \mathrm{in}_\tau(f_1), \mathrm{in}_\tau(f_2) >$. We will show later that in this case $\mathrm{in}_\tau(I) = (Y^2, XY, X^2Z)$.

Thus in general, if $I =< f_1, \ldots, f_r >$, then $\mathrm{in}_\tau(I)$ need not be the equal to the ideal $< \mathrm{in}_\tau(f_1), \ldots, \mathrm{in}_\tau(f_r) >$. This gives a motivation for defining the notion of a Gröbner basis of I.

Definition 3 *A Gröbner basis of an ideal I in S with respect to a monomial ordering τ is a set $\{f_i\}_i \subseteq I$, such that* $\mathrm{in}_\tau(I) =< \mathrm{in}_\tau(f_i) >$.

Thus in example 3.3 above, we claimed that in case (a), $\{f_1, f_2, f_3\}$ is a Gröbner basis of I with respect to τ and in case (b), $\{f_1, f_2, f_4\}$ is a Gröbner basis of I with respect to τ.

Example 4 Let $S = \mathsf{k}[X,Y,Z]$, $I = (X + Y - Z, X - Y + Z)$ and τ be a monomial ordering on S such that $X >_\tau Y >_\tau Z$. We want to find a Gröbner basis for I with respect to τ.

Let $l_1 = X + Y - Z$ and $l_2 = X - Y + Z$. Then $\mathrm{in}_\tau(l_1) = \mathrm{in}_\tau(l_2) = X$ and $\mathrm{in}_\tau(l_1 - l_2) = Y$ (assuming that char $\mathsf{k} \neq 2$. In the characteristic 2 case, $I = (X+Y+Z)$ and $\{X+Y+Z\}$ is a Gröbner basis for I with respect to τ). We claim that $\mathrm{in}_\tau(I) = (X,Y)$. Suppose some power of Z is in $\mathrm{in}_\tau(I)$, then since $X >_\tau Y >_\tau Z$, the same power of Z is in I. Hence $Z \in \mathrm{rad}(I)$. Since $Y - Z$ and X are in I, this forces $Y \in \mathrm{rad}(I)$ and therefore $\mathrm{rad}(I) = (X,Y,Z)$. This implies that $\mathrm{ht}(I) = 3$, which

contradicts the fact that I is generated by two elements (using Krull's Principal Ideal Theorem).
This shows that $\mathrm{in}_\tau(I) = (X, Y)$.

Hence a Gröbner basis for I with respect to τ is $B_1 = \{l_1, l_1 - l_2\}$. A better Gröbner basis is $B_2 = \{X - Y + Z, Y - Z\}$. Even better is $B_3 = \{X, Y - Z\}$. Observe that the matrices corresponding to B_1 and B_2, namely $\begin{bmatrix} 1 & -1 & 1 \\ 0 & -2 & 2 \end{bmatrix}$ and $\begin{bmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \end{bmatrix}$ respectively, are the matrices obtained in the intermediary steps while reducing the matrix $\begin{bmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix}$ corresponding to $\{l_1, l_2\}$ to its reduced row echelon form $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \end{bmatrix}$ which corresponds to B_3.

Some Applications

The following theorem justifies the comment that Gröbner bases give a way of finding a monomial k-basis for the quotient S/I of the polynomial ring.

Theorem 1 *Let τ be a monomial order on $S = \mathsf{k}[X_1, \ldots, X_n]$. Let I be an ideal in S. If $\mathfrak{B}$ is the set of all monomials not in $\mathrm{in}_\tau(I)$, then $\mathfrak{B}$ is a k-basis of S/I.*

We will use the following lemma in the proof of the theorem.

Lemma 2 (Dickson's Lemma) *Let τ be a term ordering and let $\mathfrak{M}$ be a non-empty set of monomials. Then $\mathfrak{M}$ has a minimal element.*

Proof: Let $J =< \mathfrak{M} >$. By the Hilbert Basis Theorem, J is finitely generated. Suppose $J = (m_1, \ldots, m_r)$, where $m_i's$ are monomials. Without loss of generality we may assume that each $\mathfrak{m}_i \in \mathfrak{M}$. Let n be any monomial in J. We claim that there is an i such that $n >_\tau m_i$.

To prove this write $n = \Sigma f_i m_i$ where $f_i \in S$. Since n is a monomial, this forces $m_i | n$ for some i. Hence $n >_\tau m_i$. There is a minimal one among the m_i's which completes the proof. $\square$

Corollary 3 *Let τ be a monomial ordering and let $\mathfrak{M}$ be a non-empty set of monomials. Then $\mathfrak{M}$ has a least element.*

Remark 1 It is easy to prove Dickson's Lemma without appealing to the Hilbert Basis Theorem. In fact one can prove the Hilbert's Basis Theorem using Dickson's Lemma.

Proof of Theorem 1: First of all, let us prove that $\mathfrak{B}$ is linearly independent. Let $m_1, \ldots, m_r$ be distinct elements in $\mathfrak{B}$. Suppose $\lambda_1 m_1 + \cdots + \lambda_r m_r = 0$ in S/I for $\lambda_i \in \mathsf{k}$. This means that $\lambda_1 m_1 + \cdots + \lambda_r m_r \in I$. We want to show that $\lambda_i = 0$ for each i.

Suppose $\lambda_i \neq 0$ for some i. Then $\mathrm{in}_\tau(\lambda_1 m_1 + \cdots + \lambda_r m_r) = m_j$ for some j, $1 \leq j \leq r$. But $m_j = \mathrm{in}_\tau(\lambda_1 m_1 + \cdots + \lambda_r m_r) \in \mathrm{in}_\tau(I)$. This is not possible since $m_j \in \mathfrak{B} \nsubseteq \mathrm{in}_\tau(I)$. Thus $\lambda_i = 0$ for each i which proves the linear independence of $\mathfrak{B}$.

In order to finish the proof that $\mathfrak{B}$ is a basis of S/I, we will show that $I + \mathsf{k} < \mathfrak{B} >= S$, where $\mathsf{k} < \mathfrak{B} >$ is the k-span of $\mathfrak{B}$.

Suppose not. Let $\mathfrak{M} = \{\mathrm{in}_\tau(g) : g \in S \setminus (I + \mathsf{k} < \mathfrak{B} >)\}$. By assumption, $\mathfrak{M}$ is non-empty and hence by Dickson's Lemma, has a least element say $m = \mathrm{in}_\tau(g)$ for some $g \in S \setminus (I + \mathsf{k} < \mathfrak{B} >)$.

Case(1): $m \notin \mathfrak{B}$.
In this case $m \in \mathrm{in}_\tau(I)$, i.e. $m = \mathrm{in}_\tau(f)$ for some $f \in I$. Then there is a $\lambda \in \mathsf{k}$ such that $m >_\tau \mathrm{in}_\tau(g - \lambda f)$. By the choice of m, this forces $g - \lambda f \in I + \mathsf{k} < \mathfrak{B} >$, which implies that $g \in I + \mathsf{k} < \mathfrak{B} >$, a contradiction.

Case(2): $m \in \mathfrak{B}$.
There is a $\lambda \in \mathsf{k}$ such that $m >_\tau \mathrm{in}_\tau(g - \lambda m)$. This implies that $g - \lambda m \in I + \mathsf{k} < \mathfrak{B} >$. But $m \in \mathfrak{B}$ forces $g \in I + \mathsf{k} < \mathfrak{B} >$, again a contradiction. $\square$

Discussion: Recall that if $R = S/I$, I a homogeneous ideal in S, then $R = \mathsf{k} \oplus R_1 \oplus R_2 \oplus \cdots$ is graded and the Hilbert function

$$H_R(d) := \dim_{\mathsf{k}}(R_d) \leq \dim_{\mathsf{k}}(S_d) = \begin{pmatrix} n+d-1 \\ n-1 \end{pmatrix}.$$

For $d >> 0$, $H_R(d) = P_R(d)$, where $P_R(d)$ is a polynomial in d with rational coefficients such that $\deg(P_R) = \dim(R) - 1$.

With this notation, we now prove a corollary of theorem 1.

Corollary 4 *If I is a homogeneous ideal in S, then*

$$H_{S/I}(d) = H_{S/\mathrm{in}_\tau(I)}(d).$$

Proof: Let $\mathfrak{B}$ is the set of all monomials not in $\mathrm{in}_\tau(I)$. Then by theorem 1, $\dim_{\mathsf{k}}((S/\mathrm{in}_\tau(I))_d) =$ number of distinct elements of $\mathfrak{B}$ of degree $d = \dim_{\mathsf{k}}((S/I)_d) = H_{S/I}(d)$. $\square$

Corollary 5 *If I is a homogeneous ideal in S, then*

$$\dim(S/I) = \dim(S/\mathrm{in}_\tau(I)).$$

Remark 2 *Suppose I and J are two homogeneous ideals in S such that $I \subseteq J$. If $H_{S/I}(d) = H_{S/J}(d)$ for $d \geq 0$, then $I = J$.*

Example 5 As in example 3.3, let $f_1 = Y^2 - XZ$, $f_2 = XY - Z^2$ and $I = (f_1, f_2)$. We further assume that $XZ >_\tau Y^2$. Then $\mathrm{in}_\tau(f_1) = XZ$, $\mathrm{in}_\tau(f_2) = XY$. If $f_3 = Zf_2 + Yf_1 = Y^3 - Z^3$, then $\mathrm{in}_\tau(f_3) = Y^3 \notin (\mathrm{in}_\tau(f_1), \mathrm{in}_\tau(f_2))$.
We claim that $\mathrm{in}_\tau(I) = (XY, XZ, Y^2)$.
Let $R := \mathsf{k}[X, Y, Z]/I$. Then

degree d	0	1	2	3	...	d
$H_R(d)$	1	3	4	4	...	4
Basis	1	x, y, z	x^2, xy, xz, yz	x^3, xyz, x^2y, x^2z	...	$x^d, x^{d-2}yz, x^{d-1}y, x^{d-1}z$

Thus $H_R(d) = 1, 3, 4, 4, 4, \ldots$. Hence by Cor.4, $H_{S/\mathrm{in}_\tau(I)}(d) = 1, 3, 4, 4, 4, \ldots$. Since $J := (XY, XZ, Y^3) \subseteq \mathrm{in}_\tau(I)$, to prove the equality, it suffices to prove that $H_{S/J}(d) = 1, 3, 4, 4, 4, \ldots$.
We have

degree d	0	1	2	3	...	d
$H_{S/I}(d)$	1	3	4	4	...	4
Basis	1	x, y, z	x^2, y^2, z^2, yz	x^3, y^2z, z^3, yz^2	...	$x^d, yz^{d-1}, z^d, y^2z^{d-2}$

This proves that $J = \mathrm{in}_\tau(I)$.