DG Algebra Gröbner

March 7, 2020

1 Preliminary Material

Throughout this note, let K be a field and let S denote the polynomial ring $K[x_1, \ldots, x_n]$.

1.1 Monomial orderings on S

Definition 1.1. A **monomial** in S is a product of the form

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

where all of the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers. Here we view α as the ordered n-tuple $\alpha = (\alpha_1, \ldots, \alpha_n)$. We denote by $\mathcal{M}$ to be the set of all monomials in S. A **monomial ordering** on S is a total ordering $>$ on $\mathcal{M}$ which satisfies the following property:

$$x^\alpha > x^\beta \text{ implies } x^\gamma x^\alpha > x^\gamma x^\beta,$$

for all $x^\alpha, x^\beta, x^\gamma \in \mathcal{M}$. We say $>$ is a **global** if $x^\alpha > 1$ for all $x^\alpha \in \mathcal{M}$.

1.1.1 Multidegree, Leading Coefficients, Leading Monomials, and Leading Terms

Definition 1.2. Let $f = \sum_\alpha c_\alpha x^\alpha$ be a nonzero polynomial in S and let $>$ be a monomial ordering on S.

1. The **multidegree** of f is
$$\operatorname{multdeg} f = \max\{x^\alpha \in \mathcal{M} \mid c_\alpha \neq 0\}.$$
2. The **leading coefficient** of f is
$$\operatorname{LC}(f) = c_{\operatorname{multdeg} f} \in K.$$
3. The **leading monomial** of f is
$$\operatorname{LM}(f) = x^{\operatorname{multdeg} f}.$$
4. The **leading term** of f is
$$\operatorname{LT}(f) = \operatorname{LC}(f) \cdot \operatorname{LM}(f).$$

1.2 Gröbner Bases

Definition 1.3. Let I be a nonzero ideal in S and let $>$ be a monomial ordering on S. We denote by $\operatorname{LT}(I)$ the set of leading terms of nonzero elements of I, that is,

$$\operatorname{LT}(I) = \{cx^\alpha \mid \text{there exists } f \in I \setminus \{0\} \text{ with } \operatorname{LT}(f) = cx^\alpha\}.$$

A finite subset $G = \{g_1, \ldots, g_r\}$ is said to be a **reduced Gröbner basis** if

1. $\langle \operatorname{LT}(g_1), \ldots, \operatorname{LT}(g_r) \rangle = \langle \operatorname{LT}(I) \rangle$
2. $\operatorname{LC}(g) = 1$ for all $g \in G$.
3. For all $g \in G$, no monomial of g lies in $\langle \operatorname{LT}(G \setminus \{g\} \rangle$.

1.2.1 Algorithmic computations in the K-algebra S/I using Gröbner bases

Let I be an ideal in S, let $>$ be a global monomial ordering on S, and let $G = \{g_1, \ldots, g_r\}$ be the reduced Gröbner basis for I with respect to this monomial ordering. Given a polynomial f in S, there are unique polynomials

$\pi(f)$ and f^G in S such that

$$f = \pi(f) + f^G$$

and such that no term of f^G is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r)$. We call f^G the **normal form of f with respect to G**. It follows from uniqueness of f^G and $\pi(f)$ that taking the normal form of a polynomial is a K-linear map:

$$c_1 f_1^G + c_2 f_2^G = (c_1 f_1 + c_2 f_2)^G \tag{1}$$

for all $c_1, c_2 \in K$ and $f_1, f_2 \in S$. We will denote this map by $-^G \colon S \to S_I$.

Another important property of $-^G$ is that it preserves homogeneity. In particular, assume that I is a homogeneous ideal. Then S/I is a graded K-algebra, where the ith homogeneous component S_i is the K-vector space of all homogeneous polynomials $f \in S$ of degree i. Define

$$S_I := \mathrm{span}_K\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I) \rangle\}$$

There is an obvious decompostion of S_I into K-vector spaces $(S_I)_i$, where

$$(S_I)_i = \mathrm{span}_K\{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I) \rangle \text{ and } \deg x^\alpha = i\}.$$

In fact, S/I and S_I are isomorphic as graded K-modules. The isomorphism is given by mapping $\overline{f} \in S/I$ to $f^G \in S_I$. Indeed, well-definedness of this map follows from the fact that $f^G = 0$ for all $f \in I$. Also K-linearity follows from (1), and the grading is preserved since $-^G$ preserves homogeneity. This makes S/I isomorphic to S_I as graded K-modules. Using this isomorphism, we can carry multiplication from S/I over to S_I to turn S_I into a graded K-algebra: multiplication in S_I is defined by

$$f_1 \cdot f_2 = (f_1 f_2)^G. \tag{2}$$

for all $f_1, f_2 \in S_I$. Defining multilpication in this way makes S_I isomorphic to S/I as graded K-algebras.

Example 1.1. Consider $S = \mathbb{F}_2[x,y]$ and $I = \langle xy^2 + y^3, x^3 + x^2 y \rangle$. Then $G = \{xy^2 + y^3, x^3 + x^2 y\}$ is the reduced Gröbner basis with respect to graded reverse lexicographical order. Thus $\mathrm{LT}(I) = \langle xy^2, x^3 \rangle$. Let's do some computations in S_I. First, let's write the first few homogeneous terms of S_I:

$$\begin{aligned}
(S_I)_0 &= \mathbb{F}_2 \\
(S_I)_1 &= \mathbb{F}_2 x + \mathbb{F}_2 y \\
(S_I)_2 &= \mathbb{F}_2 x^2 + \mathbb{F}_2 xy + \mathbb{F}_2 y^2 \\
(S_I)_3 &= \mathbb{F}_2 x^2 y + \mathbb{F}_2 y^3 \\
(S_I)_4 &= \mathbb{F}_2 y^4 \\
(S_I)_5 &= \mathbb{F}_2 y^5 \\
&\vdots
\end{aligned}$$

Next, we multiply some elements together in S_I in the multiplication table below

$\cdot$	x	y	y^3
x^2y	y^4	y^4	y^6
x^2	x^2y	x^2y	y^5
x	x^2	xy	y^4

2 Setup

Let A be an n-dimensional graded K-vector space and let $\star \colon A \otimes_K A \to A$ be a graded K-linear map. So $(A, \star)$ is a (not necessarily associative) graded K-algebra. Suppose $\{e_1, \ldots, e_n\}$ is a basis for A as graded K-vector space. Then for each $1 \leq i, j \leq n$, we have

$$e_i \star e_j = \sum_{1 \leq k \leq n} c_{i,j}^k e_k$$

where $c_{i,j}^k \in K$ for all $1 \leq k \leq n$ and $c_{i,j}^k = 0$ if $|e_i| + |e_j| \neq |e_k|$. Let I be the homogeneous ideal in S generated by the set

$$\left\{ x_i x_j - \sum_k c_{i,j}^k x_k \mid 1 \leq i, j \leq n \right\} \cup \left\{ x_i^2 \mid 1 \leq i \leq n \right\} \tag{3}$$

We give S a weighted lexicographical ordering where x_i is assigned the weight $n + 1 - |e_i|$[1] as follows: we say $x^\alpha >_{\mathrm{Wp}} x^\beta$ if either

[1]the reason we assign x_i the weight $n + 1 - |e_i|$ and not $|e_i|$ is so that this becomes a global ordering.

1. $|\alpha| > |\beta|$ where $|\alpha| = \sum_{i=1}^{n} \alpha_i |e_i|$ and $|\beta| = \sum_{i=1}^{n} \beta_i |e_i|$ or;

2. $|\alpha| = |\beta|$ and there exists $1 \le i \le n$ such that $\alpha_i = \beta_i$ and

$$\begin{aligned} \alpha_1 &= \beta_1 \\ &\vdots \\ \alpha_{i-1} &= \beta_{i-1} \\ \beta_{i-1} &= \beta_i \end{aligned}$$

Let $G = \{g_1, \dots, g_r\}$ be the reduced Gröbner basis for I with respect to this monomial ordering. Observe that for each $1 \le i, j \le n$, we have

$$\mathrm{LT}\left(x_i x_j - \sum_k c_{i,j}^k x_k \right) = x_i x_j.$$

In particular, the set of monomials which do not belong to $\mathrm{LT}(I)$ will form a subset of $\{x_1, \dots, x_n\}$. Let us denote this subset by $\mathcal{M}_I$.

Finally, let $\varphi\colon A \to S/I$ be the unique graded K-linear map defined by

$$\varphi(e_i) = \overline{x}_i$$

for $1 \le i \le n$. Observe that $\varphi\colon A \to S/I$ is a K-algebra homomorphism. Indeed, for all $1 \le i, j \le n$, we have

$$\begin{aligned} \varphi(e_i \star e_j) &= \varphi\left(\sum_k c_{i,j}^k e_k \right) \\ &= \sum_k c_{i,j}^k \varphi(e_k) \\ &= \sum_k c_{i,j}^k \overline{x}_k \\ &= \overline{\sum_k c_{i,j}^k x_k} \\ &= \overline{x_i x_j} \\ &= \overline{x}_i \overline{x}_j \\ &= \varphi(e_i)\varphi(e_j). \end{aligned}$$

We are now ready to state and prove the main theorem.

2.1 Theorem

Theorem 2.1. *The multiplication map $\star$ is associative if and only if $\mathcal{M}_I = \{x_1, \dots, x_n\}$.*

Proof. Suppose $\star$ is associative. To show that $\mathcal{M}_I = \{x_1, \dots, x_n\}$, it suffices to show that $\mathrm{S}(f_{i,j}, f_{i',j'})^G = 0$ for all $1 \le i, j, i', j' \le n$, where

$$f_{i,j} = x_i x_j - \sum_k c_{i,j}^k x_k.$$

It follows from the the fact that A is associative and φ is an K-algebra homomorphism that

$$\begin{aligned} 0 &= (-^G \circ \varphi)(0) \\ &= (-^G \circ \varphi)((e_{i'} \star e_{j'}) \star (e_i \star e_j) - (e_i \star e_j) \star (e_{i'} \star e_{j'})) \\ &= (-^G \circ \varphi)\left((e_{i'} \star e_{j'}) \star \left(\sum_k c_{i,j}^k e_k \right) - (e_i \star e_j) \star \left(\sum_k c_{i',j'}^k e_k \right) \right) \\ &= \left(x_{i'} x_{j'} \left(\sum_k c_{i,j}^k x_k \right) - x_i x_j \left(\sum_k c_{i',j'}^k x_k \right) \right)^G \\ &= \mathrm{S}(f_{i,j}, f_{i',j'})^G. \end{aligned}$$

Conversely, suppose $\mathcal{M}_I = \{x_1, \dots, x_n\}$. Let $\psi\colon S_I \to A$ be the unique graded K-linear map defined by

$$\psi(x_i) = e_i$$

for all $1 \leq i \leq n$. Since $\mathcal{M}_I = \{x_1, \ldots, x_n\}$, we see that ψ and $-^G \circ \varphi$ are inverses to each other. Thus for any $1 \leq i, j, \leq n$ we have

$$\begin{aligned}
\psi(x_i) \star \psi(x_j) &= e_i \star e_j \\
&= (\psi \circ -^G \circ \varphi)(e_i \star e_j) \\
&= (\psi \circ -^G)(\overline{x_i x_j}) \\
&= \psi((x_i x_j)^G) \\
&= \psi(x_i \cdot x_j).
\end{aligned}$$

In particular, for all $1 \leq i, j, k \leq n$, we have

$$\begin{aligned}
e_i \star (e_j \star e_k) &= \psi(x_i) \star (\psi(x_j) \star \psi(x_k)) \\
&= \psi(x_i) \star \psi(x_j \cdot x_k) \\
&= \psi(x_i \cdot (x_j \cdot x_k)) \\
&= \psi((x_i \cdot x_j) \cdot x_k) \\
&= \psi(x_i \cdot x_j) \star \psi(x_k) \\
&= (\psi(x_i) \star \psi(x_j)) \star \psi(x_k) \\
&= (e_i \star e_j) \star e_k.
\end{aligned}$$

It follows that $\star$ is associative. $\square$