GRÖBNER BASES

Sam Weinrott, May 2010

Faced with the overwhelming abstraction of, predictably, abstract algebra, it is hard to know what application the topics have for real world problems. I picked up the book *Algorithmic Algebra* by Bhubaneswar Mishra for a more concrete, nay, *constructive* point of view. This write-up provides some basic definitions and theorems on the way to an algorithm for constructing Gröbner bases for a finitely generated ideal. In order to develop constructive methods to compute a Gröbner basis of an ideal, the underlying ring must be a *strongly computable ring*, i.e. it must be:

- detachable
- syzygy-solvable
- computable, and
- Noetherian.

Syzygy-solvability is outside the scope of this paper, so we will focus on definitions and theorems about the *Noetherian* characteristic and direct the reader to Mishra's text for further study. *Detachibility* and *computability* are somewhat simple, so we will define them after taking a moment to introduce notation for the ideal generated by a set $\{a_1, ..., a_k\} \subseteq R$, where R is a ring (using normal parentheses to differentiate from a group generator, denoted $\langle x \rangle$):

$$(a_1, ..., a_k) = \left\{ \sum_{i=1}^{k} r_i a_i : r_i \in R \right\}.$$

Definition 0.1 (**Computability).** *A ring S is said to be computable if for given $r, s \in S$, there are algorithmic procedures to compute $-r$, $r + s$, and $r \cdot s$. If S is a field, then we assume that for a given nonzero field element $r \in S$ $(r \neq 0)$, there is an algorithmic procedure to compute r^{-1}.*

Definition 0.2 (**Detachability).** *Let S be a ring, $s \in S$ and $\{s_1, ..., s_q\} \subseteq S$. S is said to be detachable if there is an algorithm to decide whether $s \in (s_1, ..., s_q)$. If so, the algorithm produces a set $\{t_1, ..., t_q\} \in S$, such that*

$$s = t_1 s_1 + \cdots + t_q s_q.$$

1. Polynomial Rings

Definition 1.1 (**Power Products).** *A power product is an element from a multivariate polynomial ring of the form $p = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$, $e_i \geq 0$. We refer to the set of all power products over a finite number of variables as $PP(x_1, ..., x_n)$.*

Lemma 1.2 (**Dickson's Lemma).** *Every set $X \subseteq PP(x_1, ..., x_n)$ contains a finite subset $Y \subseteq X$ such that each $p \in X$ is a multiple of some power product in Y.*

Proof sketch:
This theorem can be made more obvious by thinking of each indeterminate x_i as a prime number and each power product $p \in \mathrm{PP}(x_1, ..., x_n)$ is a composite number. Then, because we have a finite number of primes, x_i's and each power product is either composite or among the finite number of primes, there will clearly always be a subset Y of a subset X such that all elements of X can be expressed as a multiple of an element of Y by elements of the set X.

Proof:
We use proof by induction on the number of variables, n. For the base case, $n = 1$, we let $Y = X$. So, assuming $n > 1$, pick any $p_0 \in X$,

$$p_0 = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}.$$

Then every $p \in X$ that is not divisible by p_0 belongs to at least one of $\sum_{i=1}^{n} e_i$ different sets $X_{i,j}$ $(1 \leq i \leq n,\ 0 \leq j \leq e_i - 1)$ which contain power products $p \in X$ for which $\deg_{x_i}(p) = j$. Let $X'_{i,j}$ be the set of power products constructed by removing the factor x_i^j from the power products in $X_{i,j}$. By the inductive hypothesis, there exist finite subsets $Y'_{i,j} \subseteq X'_{i,j}$ such that each power product $p \in X'_{i,j}$ can be obtained by multiplying some power product $q \in Y'_{i,j}$ by a power product $x \in X$. Define $Y_{i,j}$ as:

$$Y_{i,j} = \{p \cdot x_i^j : p \in Y'_{i,j}\}.$$

We now adjoin p_0 to the union of these sets $Y_{i,j}$, so that every power product in X is a multiple of some power product in the finite set:

$$Y = \left(\{p_0\} \cup \bigcup_{i,j} Y_{i,j} \right) \subseteq X.$$

Theorem 1.3. *Let K be a field, and $I \subseteq K[x_1, ..., x_n]$ be a monomial ideal. Then I is finitely generated.*
Proof: Let G be a set of monomial generators of I, $(G) = I$. Let

$$X = \{p \in \mathrm{PP}(x_1, ..., x_n) : ap \in G,\ \text{for some } a \in K\}.$$

Note that $(X) = (G) = I$.

- $m = ap \in G \Rightarrow m \in (X)$
- $p \in X \Rightarrow \exists\, m = ap \in G$ such that $p = a^{-1}m \in (G)$

By Dickson's Lemma, X contains a finite subset $Y \subseteq X$ such that each $p \in X$ is a mutliple of a power product $q \in Y$. Clearly, $Y \subseteq X \Rightarrow (Y) \subseteq (X)$. Furthermore,

$$p \in X \Rightarrow \exists\, q \in Y \text{ such that } q \,|\, p, \text{ which implies } p \in (Y).$$

As a result, $(X) = (Y) = I$, and Y is a finite basis of I.

Definition 1.4 (**Admissible Ordering).** *A total ordering $\underset{A}{\leq}$ on the set of power products $PP(x_1, ..., x_n)$ is called admissible if for all power products p, p', and $q \in PP(x_1, ..., x_n)$,*

(1) $1 \underset{A}{\leq} p$

(2) $p \underset{A}{\leq} p' \Rightarrow pq \underset{A}{\leq} p'q$

The total ordering $\underset{A}{\leq}$ *is called semiadmissible if it satisfies the second condition but not necessarily the first.*

Lemma 1.5. *Every admissible ordering* $\underset{A}{\leq}$ *on PP is a well-ordering.*

Proof: To derive a contradiction, suppose we have an infinite descending sequence of power products:

$$p_1 \underset{A}{>} p_2 \underset{A}{>} \cdots \underset{A}{>} p_i \underset{A}{>} \cdots$$

Let $X = \{p_1, p_2, ..., p_i, ...\}$ and $Y \subseteq X$ be a finite subset such that every $p \in X$ is a multiple of some power product in Y (by Dickson's Lemma). Let p' be the power product that is smallest in Y under the ordering $\underset{A}{\leq}$:

$$p' = \min_{\underset{A}{\leq}} Y$$

The power products in X form an infinite descending sequence, so $\exists\, q \in X$ such that $q \underset{A}{<} p'$. However,

$\exists\, p \in Y$ such that $p \,|\, q$ (by defn. of Y) and therefore $\exists\, p \in Y$ such that $p \underset{A}{\leq} q \underset{A}{<} p'$,

contradicting the choice of p' as the smallest power product in Y under the ordering $\underset{A}{\leq}$, so we are finished.

Definition 1.6 (Head Monomial). *The head monomial of a polynomial p is the monomial in p whose power product is largest under some admissible ordering* $\underset{A}{\leq}$. *If* $p = m_1 + m_2 + \cdots + m_k$ *is written in decreasing order under* $\underset{A}{\leq}$ *(as is standard), the head monomial of p is* m_1. *We say* $m_1 = Hmono(p) = Hcoef(p) \cdot Hterm(p)$, *where Hcoef(p) is* m_1*'s ring coefficient and Hterm(p) is* m_1*'s power product.*

2. Gröbner Bases

Definition 2.1 (Head Monomial Ideal). *The head monomial ideal of a subset G of a multivariate polynomial ring R is the ideal generated by the head monomials of the elements of G :*

$$Head(G) = (\{Hmono(g) : g \in G\}).$$

By convention, $Hmono(0) = Hcoef(0) = 0$ *and* $Tail(p) = p - Hmono(p)$.

Definition 2.2 (Gröbner Basis). *A subset G of an ideal* $I \subseteq R$ *is called a Gröbner Basis of the ideal if* $Head(G) = Head(I)$.

Theorem 2.3. *Let* $I \subseteq R$ *be an ideal of R, and G a subset of I. Then*

$$Head(G) = Head(I) \Rightarrow (G) = I$$

Proof:
Since $G \subseteq I$, the ideal generated by G lives inside I. If $(G) \neq I$, we can choose

a polynomial $f \in I \backslash (G)$ such that Hmono(f) is minimal with respect to some admissible well-ordering $\underset{A}{\leq}$. Then Hmono$(f) \in$ Head$(I) =$ Head(G):

$$\text{Hmono}(f) = \sum_{g_i \in G} t_i \text{Hmono}(g_i), \quad t_i \in R,$$

and,

$$\begin{aligned} f' &= \text{Tail}(f) - \sum_{g_i \in G} t_i \text{Tail}(g_i) \\ &= f - \text{Hmono}(f) - \sum_{g_i \in G} t_i (g_i - \text{Hmono}(g_i)) \\ &= f - \sum_{g_i \in G} t_i \text{Hmono}(g_i) + \sum_{g_i \in G} t_i \text{Hmono}(g_i) - \sum_{g_i \in G} t_i g_i \\ &= f - \sum_{g_i \in G} t_i g_i \in I. \end{aligned}$$

Now, we know that $f' \in I \backslash (G)$ because, otherwise, $f = f' + \sum_{g_i \in G} t_i g_i$ would be in the ideal generated by G. You may sense a contradiction forming in our choice of f. Hmono$(f') \underset{A}{<}$ Hmono(f) because the monomials in f's tail are clearly smaller than Hmono(f) as well as the monomials in each t_iTail(g_i). As a result we have a contradiction in the choice of f because it is not minimal w.r.t. $\underset{A}{<}$. Contradiction in hand, we can now say that $(G) = I$ and every Gröbner basis of an ideal generates the ideal.

Corollary 2.4.

(1) *Two ideals I and J with the same Gröbner basis G are the same: $I = (G) = J$.*
(2) *If $J \subseteq I$ are ideals of R, and Head$(J) =$ Head(I), then J=I.*

Proposition 2.5. *Let R be a ring. Then the following three statements are equivalent:*

(1) *R is Noetherian*
(2) *The ascending chain condition (ACC) for ideals holds:*
Any ascending chain of ideals of R,
$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$
becomes stationary: there exists an n_0 $(1 \leq n_0)$ such that for all $n > n_0$, $I_{n_0} = I_n$.
(3) *The maximal condition for ideals holds:*
Any nonempty set of ideals of R contains a maximal element (with respect to inclusion).

Theorem 2.6 (Hilbert's Basis Theorem). *If R is a Noetherian ring, so is $R[x]$.*

Proof Sketch:
We derive a contradiction by assuming R is Noetherian but $R[x]$ is not. We use the fact that there is an ideal of $R[x]$ which is not finitely generated (assuming it is not Noetherian) to make a series of k choices of the polynomial of least degree from the ideal without all previous choices of the polynomial of least degree. We

then contradict the $k+1$th choice of a polynomial of least degree by constructing a polynomial of smaller degree out of the $k+1$th polynomial and the k polynomials of lesser degree already removed from the ideal.

Proof:
We assume R is Noetherian but $R[x]$ is not in order to derive a contradiction. If $R[x]$ is not Noetherian, it must contain an Ideal, I, which is not finitely generated. Let $f_1 \in I$ be a polynomial of least degree. Since I is not finitely generated, we can then make a series of choices:
If f_k $(k \geq 1)$ has already been chosen, we can choose f_{k+1}, the polynomial of least degree in $I \setminus (f_1, f_2, ..., f_k)$ because I is not finitely generated.
Let n_k=deg(f_k) and $a_k \in R$ be the leading coefficient of f_k. Note:

- $n_1 \leq n_2 \leq \cdots$
- $(a_1) \subseteq (a_1, a_2) \subseteq \cdots \subseteq (a_1, a_2, ..., a_k) \subseteq (a_1, a_2, ..., a_k, a_{k+1}) \subseteq \cdots$ is a chain of ideals that must become stationary because R is Noetherian, i.e. for some k, $(a_1, a_2, ..., a_k) = (a_1, a_2, ..., a_k, a_{k+1})$, and $a_{k+1} = b_1 a_1 + b_2 a_2 + \cdots + b_k a_k,\ b_i \in R$.

Now construct the polynomial g:

$$g = f_{k+1} - b_1 x^{n_{k+1}-n_1} f_1 - b_2 x^{n_{k+1}-n_2} f_2 - \cdots - b_k x^{n_{k+1}-n_k} f_k.$$

Notice that,

(1) $\deg(g) < \deg(f_{k+1})$
(2) $g \in I$
(3) $g \notin (f_1, f_2, ..., f_k)$

In other words, g, a polynomial of lesser degree than the polynomial f_{k+1} (ostensibly of least degree in $I \setminus (f_1, f_2, ..., f_k)$) is a member of the set, contradiction ensues, and we are finished.

Corollary 2.7.

(1) *If R is a Noetherian ring, so is every polynomial ring $R[x_1, x_2, ..., x_n]$.*
(2) *For any field K, $K[x_1, x_2, ..., x_n]$ is a Noetherian ring.*

Theorem 2.8. *Let S be a Noetherian ring. Then every ideal of $R = S[x_1, x_2, ..., x_n]$ has a finite Gröbner basis.*
Proof:

S is Noetherian, so by Hilbert's basis theorem, $R = S[x_1, x_2, ..., x_n]$ is too. Let $\underset{A}{<}$ be an arbitrary but fixed admissible ordering on PP$(x_1, x_2, ..., x_n)$.
Let I be an ideal in R and choose a polynomial $g_1 \in I$. If $G_1 = \{g_1\} \subseteq I$ is not a Gröbner basis of I, then Head$(G_1) \subsetneq$ Head(I), and $\exists\ g_2 \in I$ such that Hmono$(g_2) \in$ Head$(I)\setminus$ Head(G_1). Then $G_2 = \{g_1, g_2\} \subseteq I$ and Head$(G_1) \subsetneq$ Head(G_2).
In the $(k+1)$th step, assume we have chosen $G_k = \{g_1, g_2, ..., g_k\} \subseteq I$. If G_k is not a Gröbner basis for I, then there is a $g_{k+1} \in I$ such that

$$\text{Hmono}\,(g_{k+1}) \in \text{Head}\,(I) \setminus \text{Head}\,(G_k),$$

and $G_{k+1} = G_k \cup \{g_{k+1}\} \subseteq I$ and Head$(G_k) \subsetneq$ Head(G_{k+1}). However, R cannot have a nonstationary chain of ideals:

$$\text{Head}\,(G_1) \subsetneq \text{Head}\,(G_2) \subsetneq \cdots \subsetneq \text{Head}\,(G_k) \subsetneq \cdots$$

because it is Noetherian. Then there is some $n \geq 1$ such that $\mathrm{Head}\,(G_n) = \mathrm{Head}\,(I)$. G_n is a subset of I, so $G_n = \{g_1, g_2, ..., g_n\}$ is a finite Gröbner basis for I w.r.t. the admissible ordering $\underset{A}{<}$.

3. Epilogue

Some work with syzygies and S-polynomials and an algorithm for head reduction leads to an algorithm for computing Gröbner bases for a finitely generated ideal.

References

Bhubaneswar, Mishra. *Algorithmic Algebra.* Sections 2.1-3.3. New York: Springer-Verlag, 1993.