Gröbner bases for the polynomial ring with infinite variables and their applications

Kei-ichiro Iima and Yuji Yoshino
(Okayama University)

1 Introduction

Recall that a sequence $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ of positive integers is called a partition of a non-negative integer n if the equality $\lambda_1 + \lambda_2 + \cdots + \lambda_r = n$ holds and $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 1$. In such a case we denote it by $\lambda \vdash n$.

We are concerned with the following sets of partitions:

$$\begin{aligned} A(n) &= \{ \ \lambda \vdash n \ \mid \ \lambda_i \equiv \pm 1 \pmod 6 \ \}, \\ B(n) &= \{ \ \lambda \vdash n \ \mid \ \lambda_i \equiv \pm 1 \pmod 3, \quad \lambda_1 > \lambda_2 > \cdots > \lambda_r \ \}, \\ C(n) &= \{ \ \lambda \vdash n \ \mid \ \text{each } \lambda_i \text{ is odd, and} \\ &\qquad\qquad\qquad \text{any number appears in } \lambda_i\text{'s at most two times} \ \}. \end{aligned}$$

It is known by famous Schur's equalities that all these sets $A(n)$, $B(n)$ and $C(n)$ have the same cardinality for all $n \in \mathbb{N}$. It is also known that the one-to-one correspondences among these three sets are realized in some combinatorial way using 2-adic or 3-adic expansions of integers. In this article we reconstruct such one-to-one correspondences by using the theory of Gröbner bases. For this, we need to extend the theory of Gröbner bases to a polynomial ring with infinitely many variables.

2 Gröbner bases

Throughout this article, let k be any field and let $S = k[x_1, x_2, \ldots]$ be a polynomial ring with countably infinite variables. We denote by $\mathbb{Z}_{\geq 0}^{(\infty)}$ the set of all sequences $a = (a_1, a_2, \ldots)$ of integers where $a_i = 0$ for all i but finite number of integers. Also we denote by $\mathrm{Mon}(S)$ the set of all monomials in S. Since any monomial is described uniquely as $x^a = \prod_i x_i^{a_i}$ for some $a = (a_1, a_2, \dots) \in \mathbb{Z}_{\geq 0}^{(\infty)}$, we can identify these sets:

$$\mathrm{Mon}(S) \;\cong\; \mathbb{Z}_{\geq 0}^{(\infty)}.$$

If we attach degree on S by $\deg x_i = d_i$, then a monomial x^a has degree $\deg x^a = \sum_{i=1}^{\infty} a_i d_i$. In the rest of the paper, we assume that the degrees d_i's are chosen in such a way that there are only a finite number of monomials of degree d for each $d \in \mathbb{N}$. For example, the simplest way of attaching degree is that $\deg x_i = i$ for all $i \in \mathbb{N}$.

Definition 2.1. A total order $>$ on $\mathrm{Mon}(S)$ is called a monomial order if $(\mathrm{Mon}(S),\ >)$ is a well-ordered set, and it is compatible with the multiplication of monomials, i.e. $x^a > x^b$ implies $x^c x^a > x^c x^b$ for all $x^a, x^b, x^c \in \mathrm{Mon}(S)$.

Note that the ordering $x_1 > x_2 > x_3 > \cdots$ is not acceptable for monomial order, since it violates the well-ordering condition. On the other hand, if we are given any monomial order $>$, then, renumbering the variables, we may assume that $x_1 < x_2 < x_3 < \cdots$.

The following are examples of monomial orders on $\mathrm{Mon}(S)$.

Example 2.2. Let $a = (a_1, a_2, \dots)$ and $b = (b_1, b_2, \dots)$ be elements in $\mathbb{Z}_{\geq 0}^{(\infty)}$.

(1) The pure lexicographic order $>_{pl}$ is defined in such a way that $x^a >_{pl} x^b$ if and only if $a_i > b_i$ for the last index i with $a_i \neq b_i$.

(2) The degree (resp. anti-) lexicographic order $>_{dl}$ (resp. $>_{dal}$) is defined in such a way that $x^a >_{dl} x^b$ (resp. $x^a >_{dal} x^b$) if and only if either $\deg x^a > \deg x^b$ or $\deg x^a = \deg x^b$ and $a_i > b_i$ for the last (resp. first) index i with $a_i \neq b_i$.

(3) The degree (resp. anti-) reverse lexicographic order $>_{drl}$ (resp. $>_{darl}$) is defined as follows: $x^a >_{drl} x^b$ (resp. $x^a >_{darl} x^b$) if and only if either $\deg x^a > \deg x^b$ or $\deg x^a = \deg x^b$ and $a_i < b_i$ for the first (resp. last) index i with $a_i \neq b_i$.

These monomial orders are all distinct as shown in the following example in which $\deg x_i = i$ for $i \in \mathbb{N}$:

$$\begin{array}{ccccccccc}
x_4 & >_{dl} & x_1x_3 & >_{dl} & x_2^2 & >_{dl} & x_1^2x_2 & >_{dl} & x_1^4, \\
x_1^4 & >_{dal} & x_1^2x_2 & >_{dal} & x_1x_3 & >_{dal} & x_2^2 & >_{dal} & x_4, \\
x_4 & >_{drl} & x_2^2 & >_{drl} & x_1x_3 & >_{drl} & x_1^2x_2 & >_{drl} & x_1^4, \\
x_1^4 & >_{darl} & x_1^2x_2 & >_{darl} & x_2^2 & >_{darl} & x_1x_3 & >_{darl} & x_4.
\end{array}$$

Now suppose that a monomial order $>$ on $\mathrm{Mon}(S)$ is given and we fix it. Then, any non-zero polynomial $f \in S$ is expressed as

$$f = c_1 x^{a(1)} + c_2 x^{a(2)} + \cdots + c_r x^{a(r)},$$

where $c_i \neq 0 \in k$ and $x^{a(1)} > x^{a(2)} > \ldots > x^{a(r)}$. In such a case, the leading term, the leading monomial and the leading coefficient of f are given respectively as $\ell t(f) = c_1 x^{a(1)}$, $\ell m(f) = x^{a(1)}$ and $\ell c(f) = c_1$. For an ideal $I(\neq (0)) \subset S$, the initial ideal $in(I)$ of I is defined to be the ideal generated by all the leading terms $\ell t(f)$ of non-zero polynomials $f \in I$. The Gröbner base of I is defined similarly to the ordinary case.

Definition 2.3. A subset $\mathcal{G}$ of an ideal I is called a Gröbner base for I if $\{\ell t(g) \mid g \in \mathcal{G}\}$ generates the initial ideal $in(I)$.

Since S is not a Noetherian ring, one cannot expect that there always exists a finite Gröbner base $\mathcal{G}$ for a given ideal I. But any argument concerning Gröbner bases for an ideal of S can be reduced to the ordinary case for the polynomial rings with finite variables by the following theorem.

Theorem 2.4. *Let I be an ideal of S. For a positive integer n, we set $S^{\langle n\rangle} = k[x_1, x_2, \ldots, x_n]$ which is a polynomial subring of S and set $I^{\langle n\rangle} = I \cap S^{\langle n\rangle}$. Now let $\mathcal{G}$ be a subset of I.*

(1) *Suppose that each $\mathcal{G} \cap S^{\langle n\rangle}$ is a Gröbner base for $I^{\langle n\rangle}$ for all $n \in \mathbb{N}$, then $\mathcal{G}$ is a Gröbner base for I.*

(2) *The converse holds when the monomial order is the pure lexicographic order.*

The following division algorithm is proved using Theorem 2.4.

Theorem 2.5 (Division algorithm). *Let $\mathcal{G}$ be a subset of S. Then any non-zero polynomial $f \in S$ has an expression*

$$f = f_1 g_1 + f_2 g_2 + \cdots + f_s g_s + f',$$

with $g_i \in \mathcal{G}$ and $f_i, f' \in S$ such that the following conditions hold:

(1) *If we write $f' = \sum_{i=1}^{t} c_i x^{a(i)}$ with $c_i \neq 0 \in k$, then $x^{a(i)} \notin \{in(g) \mid g \in \mathcal{G}\}S$ for each $i = 1, 2, \ldots, t$.*

(2) *If $f_i g_i \neq 0$, then $\ell m(f_i g_i) \leq \ell m(f)$.*

Any such f' is called a remainder of f with respect to $\mathcal{G}$. Note that a remainder is in general not necessarily unique. But if $\mathcal{G}$ is a Gröbner base for $I = \mathcal{G}S$, then a remainder of f with respect to $\mathcal{G}$ is uniquely determined.

3 Applications

Let $S = k[x_1, x_2, \ldots]$ be a polynomial ring with countably infinite variables as before. We regard S as a graded k-algebra by defining $\deg(x_i) = i$ for each $i \in \mathbb{N}$, and denote by S_n the part of degree n of S for $n \in \mathbb{N}$. Note that there is a bijective mapping between the set of partitions of n and the set of monomials of degree n. In fact, the correspondence is given by mapping a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r) \vdash n$ to the monomial $x^\lambda = x_{\lambda_r} \cdots x_{\lambda_2} x_{\lambda_1}$ of degree n.

Let W be any subset of $\mathbb{N}$ satisfying $pW \subset W$ for an integer $p \geq 2$, where $pW = \{pw \mid w \in W\}$. In this case, we consider a polynomial subring $R = k[x_i \mid i \in W]$ of S. We are interested in the following two subsets of partitions of n:

$$\begin{aligned} X(n) &= \{\ \lambda \vdash n \ \mid\ \lambda_i \in W \setminus pW \text{ for each } i\ \}, \\ Y(n) &= \{\ \lambda \vdash n \ \mid\ \lambda_i \in W \text{ for each } i, \text{ and} \\ &\qquad \text{any number appears among } \lambda_i\text{'s at most } p-1 \text{ times}\}. \end{aligned}$$

Theorem 3.1. *Under the circumstances above, consider the set of polynomials $\mathcal{G} = \{x_i^p - x_{pi} \mid i \in W\}$ in R. We adopt the degree anti-reverse lexicographic order on the set of monomials in R. Then $\mathcal{G}$ is a reduced Gröbner base for the ideal $\mathcal{G}S$.*

Furthermore, define a mapping $\varphi : X(n) \to Y(n)$ so that $x^{\varphi(\lambda)}$ is a remainder of x^λ with respect to $\mathcal{G}$ for any $\lambda \in X(n)$. Then φ is a well-defined bijective mapping.

In particular we have that $|X(n)| = |Y(n)|$ in the case above. Therefore, just considering the generating functions of $|X(n)|$ and $|Y(n)|$, we see that the following functional equality holds;

$$\prod_{m \in W \setminus pW} \frac{1}{1 - t^m} = \prod_{m \in W} (1 + t^m + t^{2m} + \cdots + t^{(p-1)m}).$$

Example 3.2. Recall that $A(n)$, $B(n)$ and $C(n)$ are the sets of partitions given in Introduction.

(1) If $W = \{n \in \mathbb{N} \mid n \equiv \pm 1 \pmod 3\}$ and $p = 2$, then $X(n) = A(n)$ and $Y(n) = B(n)$.

(2) If $W = \{n \in \mathbb{N} \mid n \equiv 1 \pmod 2\}$ and $p = 3$, then $X(n) = A(n)$ and $Y(n) = C(n)$.

As a consequence of all the above, we obtain one-to-one correspondences among $A(n)$, $B(n)$ and $C(n)$ by using the theory of Gröbner bases.

For another example, let

$$\begin{aligned} P(n) &= \{ \lambda \vdash n \mid \lambda_i \equiv \pm 1 \pmod 5 \}, \\ Q(n) &= \{ \lambda \vdash n \mid \lambda_i - \lambda_{i+1} \geq 2 \}. \end{aligned}$$

By Rogers-Ramanujan equality, it is known that the sets $P(n)$ and $Q(n)$ have the same cardinality for each $n \in \mathbb{N}$. If we can find an ideal I as in the following question, then we will obtain a one-to-one correspondence between $P(n)$ and $Q(n)$ by using division algorithm.

Question 3.3. *Find an ideal I of S and a monomial order $>$ on* $\mathrm{Mon}(S)$ *satisfying $S/I \cong k[\{x_i \mid i \equiv \pm 1 \pmod 5\}]$ and $in(I) = (x_i^2,\ x_i x_{i+1} \mid i \in \mathbb{N})$.*

References

[1] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer Verlag (1995).

[2] K. Iima and Y. Yoshino, *Gröbner bases for the polynomial rings with infinitely many variables and applications*, in preparation (2008).

Department of Math., Okayama University, 700-8530, Okayama, Japan
`iima@math.okayama-u.ac.jp, yoshino@math.okayama-u.ac.jp`