Introduction to Gröbner basis

Yasuhide NUMATA

2024 年 4 月 23 日

第 1 章

Introduction to Introduction to Gröbner basis

1.1 An algebra defined by systems of generators and relations

First we see some prototypical examples.

1.1.1 Case 1: Complex numbers.

What is a complex number (if you know real numbers)?

For example, let

$$\begin{aligned}\alpha &= 3i^2 + 1,\\ \beta &= -5i^5 + i + 1,\\ \gamma &= i(4i^2 - i).\end{aligned}$$

These are complex numbers. So, calculate them and check whether $\alpha = \beta$, $\beta = \gamma$, and $\gamma = \alpha$. For this question, we can answer as follows:

$$\begin{aligned}\alpha &= 3i^2 + 1 = 3(-1) + 1 = -2\\ \beta &= -5i^5 + i + 1 = -5(-1)^2 i + i + 1 = -4i + 1\\ \gamma &= i(4i^2 - i) = 4i^3 - i^2 = 4(-1)i - (-1) = -4i + 1\end{aligned}$$

So $\alpha \neq \beta = \gamma$.

What do we do now?

1. Continue the following:
   (a) Expand as a polynomial in the indeterminat (i.e., variable) i.
   (b) Substitute $i^2 \underset{=}{\equiv} -1$.
   Every complex number become the form $x + yi$ with some $x, y \in \mathbb{R}$.
2. For $x, x', y, y' \in \mathbb{R}$,
$$x + yi = x' + y'i \iff \begin{cases} x = x' \\ y = y'. \end{cases}$$
   (In the other words, $\mathbb{C}$ is a vetorspace over $\mathbb{R}$ with a basis $\{\, 1, i \,\}$. So $\{\, 1, i \,\}$ is linearly indenepdent over $\mathbb{R}$.)

Hence, if we get this form, then we can check the equality by comparing the coefficients.

Remark 1.1.1. The form $x + yi$ is important. For example,

$$(x, y, z) = (x', y', z') \implies x + yi + zi^2 = x' + y'i + z'i^2$$

is true. The converse is, however, false. The case where $(x, y, z) = (-1, 0, 0)$ and $(x', y', z') = (0, 0, 1)$ is a counter example.

Remark 1.1.2. We call the following problem *the indentification problem*:

Check the equality of given two elements.

1.1.2 Case 2: Square roots.

What is $\sqrt{5}$ (if you know rational numbers)?
For example, let

$$\begin{aligned}\alpha &= 3\sqrt{5}^2 + 1,\\ \beta &= -\sqrt{5}^5 + 24\sqrt{5} + 5,\\ \gamma &= \sqrt{5}(\sqrt{5} - 1).\end{aligned}$$

Calculate them and check whether $\alpha = \beta$, $\beta = \gamma$, and $\gamma = \alpha$. For this question, we can answer as follows:

$$\begin{aligned}\alpha &= 3\sqrt{5}^2 + 1 = 3 \cdot 5 + 1 = 16,\\ \beta &= -\sqrt{5}^5 + 24\sqrt{5} + 5 = -(5)^2\sqrt{5} + 24\sqrt{5} + 5 = -\sqrt{5} + 5,\\ \gamma &= \sqrt{5}(\sqrt{5} - 1) = \sqrt{5}^2 - \sqrt{5} = 5 - \sqrt{5} = -\sqrt{5} + 5.\end{aligned}$$

So $\alpha \neq \beta = \gamma$.

What do we do now?

1. Continue the following:
   (a) Expand as a polynomial in the indeterminat (i.e., variable) $\sqrt{5}$.
   (b) Substitute $\sqrt{5}^2 \equiv 5$.
   Every complex number become the form $x + y\sqrt{5}$ with some $x, y \in \mathbb{Q}$.
2. For $x, x', y, y' \in \mathbb{Q}$,

$$x + y\sqrt{5} = x' + y'\sqrt{5} \iff \begin{cases} x = x' \\ y = y'. \end{cases}$$

   (In the other words, $\{\, 1, \sqrt{5} \,\}$ is linearly indenepdent over $\mathbb{Q}$.)
   Hence, if we get this form, then we can check the equality by comparing the coefficients.

1.1.3 Case 3: Root of unity.

What is $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ (if you know real numbers)?

Note that

$$\begin{aligned}\omega &= -\frac{1}{2} + \frac{\sqrt{3}}{2}i \\ &= \cos(\frac{2\pi}{3}) + \sin(\frac{2\pi}{3})i \\ &= e^{\frac{2\pi}{3}i}.\end{aligned}$$

$x = \omega$ is a solution of the equation

$$x^2 + x + 1 = 0.$$

Hence $x = \omega$ is also a solution of the equation $x^3 = 1$.

For example, let

$$\begin{aligned}\alpha &= \omega^2 + 4\omega + 7, \\ \beta &= -\omega^3 - 2\omega, \\ \gamma &= \omega(\omega - 1).\end{aligned}$$

Calculate them and check whether $\alpha = \beta$, $\beta = \gamma$, and $\gamma = \alpha$. For this question, we can answer as follows:

$\alpha = \omega^2 + 4\omega + 7 = (-\omega - 1) + 4\omega + 7 = 3\omega + 6,$
$\beta = -\omega^3 - 2\omega = -\omega\omega^2 - 2\omega = -\omega(-\omega - 1) - 2\omega = \omega^2 - \omega = (-\omega - 1) - \omega = -2\omega - 1,$
$\gamma = \omega(\omega - 1) = \omega^2 - \omega = (-\omega - 1) - \omega = -2\omega - 1.$

So $\alpha \neq \beta = \gamma$.

What do we do now?

1. Continue the following:
   (a) Expand as a polynomial in the indeterminat (i.e., variable) ω.
   (b) Substitute $\omega^2 \equiv -omega - 1$.
   Every complex number become the form $x + y\omega$ with some $x, y \in \mathbb{R}$.
2. For $x, x', y, y' \in \mathbb{R}$,

$$x + y\omega = x' + y'\omega \iff \begin{cases} x = x' \\ y = y'. \end{cases}$$

   (In the other words, $\{\, 1, \omega \,\}$ is linearly indenepdent over $\mathbb{R}$.)
   Hence, if we get this form, then we can check the equality by comparing the coefficients.

1.1.4 Case 4: Cubic roots.

What is $\left(5^{\frac{1}{3}}\right) = \sqrt[3]{5}$ (if you know rational numbers)?

For example, let

$$\begin{aligned}\alpha &= 3\left(5^{\frac{1}{3}}\right)^3 + 2\left(5^{\frac{1}{3}}\right)^2 + 4\left(5^{\frac{1}{3}}\right) + 7,\\ \beta &= -\left(5^{\frac{1}{3}}\right)^6 - \left(5^{\frac{1}{3}}\right)^2 + 30,\\ \gamma &= \left(5^{\frac{1}{3}}\right)^2 (\left(5^{\frac{1}{3}}\right) - 1).\end{aligned}$$

Calculate them and check whether $\alpha = \beta$, $\beta = \gamma$, and $\gamma = \alpha$. For this question, we can answer as follows:

$$\begin{aligned}\alpha &= \left(5^{\frac{1}{3}}\right)^3 + 2\left(5^{\frac{1}{3}}\right)^2 + 4\left(5^{\frac{1}{3}}\right) + 7\\ &= 5 + 2\left(5^{\frac{1}{3}}\right)^2 + 4\left(5^{\frac{1}{3}}\right) + 7 = 2\left(5^{\frac{1}{3}}\right)^2 + 4\left(5^{\frac{1}{3}}\right) + 12,\\ \beta &= -\left(5^{\frac{1}{3}}\right)^6 - \left(5^{\frac{1}{3}}\right)^2 + 30\\ &= -\left(5^{\frac{1}{3}}\right)^3\left(5^{\frac{1}{3}}\right)^3 - \left(5^{\frac{1}{3}}\right)^2 + 30\\ &= -5\cdot 5 - \left(5^{\frac{1}{3}}\right)^2 + 30 = -\left(5^{\frac{1}{3}}\right)^2 + 5,\\ \gamma &= \left(5^{\frac{1}{3}}\right)^2 (\left(5^{\frac{1}{3}}\right) - 1)\\ &= \left(5^{\frac{1}{3}}\right)^3 - \left(5^{\frac{1}{3}}\right)^2 = 5 - \left(5^{\frac{1}{3}}\right)^2.\end{aligned}$$

So $\alpha \neq \beta = \gamma$.

What do we do now?

1. Continue the following:
   (a) Expand as a polynomial in the indeterminat (i.e., variable) $\left(5^{\frac{1}{3}}\right)$.
   (b) Substitute $\left(5^{\frac{1}{3}}\right)^3 \rightleftharpoons 5$.
   Every complex number become the form $x + y\left(5^{\frac{1}{3}}\right) + z\left(5^{\frac{1}{3}}\right)^2$ with some $x, y, z \in \mathbb{Q}$.
2. For $x, x', y, y', z, z' \in \mathbb{Q}$,
$$x + y\left(5^{\frac{1}{3}}\right) + z\left(5^{\frac{1}{3}}\right)^2 = x' + y'\left(5^{\frac{1}{3}}\right) + z'\left(5^{\frac{1}{3}}\right)^2 \iff \begin{cases} x = x' \\ y = y' \\ z = z'. \end{cases}$$
   (In the other words, $\left\{1, \left(5^{\frac{1}{3}}\right), \left(5^{\frac{1}{3}}\right)^2\right\}$ is linearly indenepdent over $\mathbb{Q}$.)
   Hence, if we get this form, then we can check the equality by comparing the coefficients.

1.2 Summary

We consider four cases. In each case, we caluculate polynomial in an indeterminant with relations. To solve identification problem, we use the same method in these prototypical cases. We will try to generalize these calculations.

Quiz 1.1. Consider the golden number

$$\tau = \frac{1+\sqrt{5}}{2}.$$

Then τ is a root of the irreducible polynomial

$$\tau^2 - \tau - 1.$$

In the other words, $x = \tau$ is a solution of the equation

$$x^2 - x - 1 = 0.$$

Let

$$\begin{aligned}\alpha &= \tau^3,\\ \beta &= \tau^4 - \tau^2 - \tau,\\ \gamma &= \tau(\tau^2 - 1).\end{aligned}$$

Check whether $\alpha = \beta$, $\beta = \gamma$, and $\gamma = \alpha$.

第 2 章

Our problem

2.1 Summary of Chapter 1

We consider the following:

1. A polynomial over $\mathbb{R}$ in the determinat i with the relation $i^2+1=0$.
2. A polynomial over $\mathbb{Q}$ in the determinat $\sqrt{5}$ with the relation $\sqrt{5}^2-5=0$.
3. A polynomial over $\mathbb{R}$ in the determinat ω with the relation $\omega^2+\omega+1=0$.
4. A polynomial over $\mathbb{Q}$ in the determinat $\left(5^{\frac{1}{3}}\right)$ with the relation $\left(5^{\frac{1}{3}}\right)^3-5=0$.
5. A polynomial over $\mathbb{R}$ in the determinat τ with the relation $\tau^2-\tau-1=0$.

In each case, we solve the identification problem by the following strategy:

1. Continue the following:
   (a) Expand as a polynomial
   (b) Substitute the relation as the following form:

$$\underbrace{\text{monomial}}_{\text{(hightest degree)}} \rightleftharpoons \underbrace{\text{polynomial}}_{\text{(lower degree)}}.$$

2. Obtain a linear combination of linearly indepenedent elements.

Remark 2.1.1. The substitution in Item 1b is "one-way". By the substitution the dgree of polynomial decreases strictly. So, to calculate, we do not need any huristics.

In Chapter 2, our motivation is the following question:

> What about polynomials with the other relations?

Remark 2.1.2. In the prototypical cases, we consider the following relations:

1. $i^2+1=0$ (with $\mathbb{R}$ coefficients).
2. $\sqrt{5}^2-5=0$ (with $\mathbb{Q}$ coefficients).
3. $\omega^2+\omega+1=0$ (with $\mathbb{R}$ coefficients).
4. $\left(5^{\frac{1}{3}}\right)^3-5=0$ (with $\mathbb{Q}$ coefficients).
5. $\tau^2-\tau-1=0$ (with $\mathbb{R}$ coefficients).

We have some candidate of the meanings of "the other" in our motivation. For

example, we have the following:

1. In each prototipical cases, the relation is defined by an irreducible polynomial. What about non-irreducible polynomials?
2. In each prototypical cases, we consider the unique relation. What about multiple relations?
3. In each prototypical cases, we consider polynomials in one indeterminant. What about multivariable polynoimals?

2.2 The case of one indeterminant

Here we consider the case of of one indeterminant, and we see that our strategy works.

To see it, we define some notion.

Definition 2.2.1. We call the following proceedure *Division Algorithm*:

1. Continue the following:
   (a) Expand as a polynomial
   (b) Substitute the relation as the following form:

$$\underbrace{\text{monomial}}_{\text{(hightest degree)}} \equiv \underbrace{\text{polynomial}}_{\text{(lower degree)}}.$$

2. Obtain a linear combination of linearly indepenedent elements.

We call the monomial with the highest degree in the relation the *initial monomial* of the relation.

Remark 2.2.2. By each substitution, the degree of the polynoimal decrease strictly. Hence the degree of the polynomial will be less than the degree of the initial term(s) of the relation(s) So, for each starting polynomial (i.e., the input of algorithm), this proceedure will stop in finitely many steps.

Note that an "algorithm" means a proceedure which will stop in finitely many steps for each input.

2.2.1 In the case of a unique relation

First we consider the case of a unique relation. This corresponds to our question Item 1 in Remark 2.1.2.

If our relation is

$$x^n \equiv \sum_{i=0}^{n-1} a_i x^i, \tag{2.1}$$

then $\left\{ 1, x, \ldots, x^{n-1} \right\}$ is linearly independent. In the algebra defined by the indeterminant x with the relation 2.1, If we use the division algorithm, then we obtain a

linear combination of $\left\{ 1, x, \ldots, x^{n-1} \right\}$ from any polynomial by division algorithm.

Remark 2.2.3 (For readers who know algebra). In each prototypical case, we consider a relation defined by an irreducible polynomial. So our algebra defined by the indeterminant with the relation is a field. Hence every nonzero element has its inverse, e.g., i has $i^{-1} = -i$. If a relation is not irreducible, then the algebra is not a field. The indeterminant might not have its iverse. This is, however, no problem. Even in this case, the division algorithm works.

2.2.2 In the case of multiple relations

Next we consider the case where we have some relations. This corresponds to our question Item 2 in Remark 2.1.2.

In this case, at first, we modify our relations by division algorithm. Then we obtain unique relation which implies any other relations. So we can apply the case of unique realtion to the relation.

For example, consider the relations

$$\begin{cases} x^8 - x^2 = 0 \\ x^6 - x^2 = 0. \end{cases}$$

By the following calculation

$$x^8 - x^2 \xrightarrow{x^6 \equiv x^2} x^4 - x^2$$

of substitution, we obtain the relation $x^4 - x^2 = 0$ from $x^8 - x^2 = 0$. So our relations are

$$\begin{cases} x^4 - x^2 = 0 \\ x^6 - x^2 = 0. \end{cases}$$

Moreover, the calculation

$$x^6 - x^2 = x^4x^2 - x^2 \xrightarrow{x^4 \equiv x^2} x^2x^2 - x^2 = x^4 - x^2 \xrightarrow{x^4 \equiv x^2} 0,$$

we obtain the relation $0 = 0$ from $x^6 - x^2$. So our relations become

$$\begin{cases} x^4 - x^2 = 0. \end{cases}$$

Now we obtain unique relation.

Remark 2.2.4. By substitution, the degree of the target relation become less thatn the degree of used relation. Hence, by this modification, all relations except one realtion become 0. Hence we have a unique relation.

Remark 2.2.5. This modification of relations is equivalent to so-called sEuclidian Algorithm. Hence we can obtain a unique relation as the greatest common divisor of the relations.

Remark 2.2.6 (For readers who know algebra). A polynomial ring in one indeterminant over a field is a PID. Hence every ideal has a system of generators consisting of one element. Therefore we can always apply to the case of unique realtion.

2.3 The case of multiple indeterminants

Here we consider the case of of more than one indeterminant. In this case, we have some problems to apply our strategy works. We see problems with examples.

2.3.1 Initial monomial.

In the case of one indeterminant, the degree induces a total order over monomials. Hence we can canonically select the initial term in each polynomial. If we have more than one indeterminant, then we have no canonical way to select.

Example 2.3.1. Which term in $x^5y + xy^5 + x^4y^4$ is initial?

If the degree means the degree of x, then x^5y is initial. If the degree means the degree of y, then xy^5 is initial. If the degree means the sum of degrees, then x^3y^4 is initial.

Example 2.3.2. Which term in $x^2 + xy + y^2$ is initial?

If the degree means the sum of degrees, then all monomials are the same.

Example 2.3.3. Which term in $x + xy$ is initial?

If the degree means the degrees of x, then all monomials are the same.

2.3.2 Order of substitutions

Assume that we can choose the initial monomial for each relation. Even if so, we have some problem if we have more than one relation.

Remark 2.3.4 (For readers who know algebra). A polynomial ring in more than one indeterminant is not a PID. Hence some ideal has a system of generators consisting of more than one element.

Consider the following two relations:

$$x^4y^5 - y = 0 \tag{2.2}$$

$$x^6y^3 - x^2y = 0 \tag{2.3}$$

Assume that x^4y^5 is the initial monomial of eq. (2.2)[*1], and that x^6y^3 is the initial monomial of eq. (2.3)[*2]. Then our relations for substitution are

$$x^4y^5 \rightleftharpoons y, \tag{2.4}$$

$$x^6y^3 \rightleftharpoons x^2y. \tag{2.5}$$

Let us calculate x^7y^5.

If we use Equation (2.4) at first, then we obtatin x^3y by the following substitution:

$$x^7y^5 = x^3 \cdot x^4y^5 \xrightarrow{x^4y^5 \rightleftharpoons y} x^3y.$$

[*1] Note that the degree of x^4y^5 is greater than y in any sense in Example 2.3.1.

[*2] Note that the degree of x^6y^3 is greater than x^2y in any sense in Example 2.3.1.

We can not apply our relations to x^3y. Hence we stop here.

If we use Equation (2.5) at first, then we obtatin x^3y^3 by the following substitution:

$$x^7y^5 = xy^2 \cdot x^6y^3 \xrightarrow{x^6y^3 \equiv x^2y} xy^2 \cdot x^2y = x^3y^3.$$

We can not apply our relations to x^3y^3. Hence we stop here.

We obtain different final forms x^3y and x^3y^3 by substitution. Since we obtain x^3y and x^3y^3 from the same polynomial, these should be the same in our algebra. This means that these form are not useful for identification problem.

2.4 Summary

In the case of one indeterminat, we can calculate, or solve identificationproblem, by the division algorithm and Euclidean Algorithm.

We also want to calculate in the case of multi-indeterminants, but naïve strategy does not work.

Quiz 2.1. Consider $\mathbb{Q}[x]/\left\langle x^{10}+x^4-2, x^9-1, x^6-1\right\rangle$, i.e., the algebra defined by x with the relations

$$\begin{aligned} x^{10}+x^4-2 &= 0,\\ x^9-1 &= 0,\\ x^6-1 &= 0. \end{aligned}$$

Let

$$\begin{aligned} \alpha &= x^5+x^6,\\ \beta &= x^4+x,\\ \gamma &= 2x. \end{aligned}$$

Check whether $\alpha=\beta$, $\beta=\gamma$, and $\gamma=\alpha$.

第 3 章

Gröbner basis

3.1 Summary of Chapter 2

We want to calculate in multiindeterminant case. We have, however, problems:

1. We have no canonical way to select the initial monomial.
2. The results depends on choice of order of substitutions.

In chapter 3, we give solution for them.

3.2 Monomial order — anser for item 1

In chapter 3, we consider polynomials in more than one indeterminant, e.g., $x_1, \ldots, x_n$. We use so-called multiindex notation defined as follows:

Definition 3.2.1. For $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\underline{x} = (x_1, \ldots, x_n)$, we define $\underline{x}^{\underline{\alpha}}$ by

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

In the case of single indeterminant, degree induces a total order over (monic) monomials. The order has nice property, i.e., compatibility with the product operation. Thanks to this property, the substitution is "one-way". We generalize not the degree but this total order.

Definition 3.2.2 (Monomial order)**.** We call $\leq$ a *monomial order* if

1. $\leq$ is a total oder on the set $\{ \underline{x}^{\underline{\alpha}} \mid \underline{\alpha} \in \mathbb{N}^n \}$ of monic monomials.
2. $\underline{x}^{\underline{\alpha}} \leq \underline{x}^{\underline{\beta}} \implies \underline{x}^{\underline{\gamma}}\underline{x}^{\underline{\alpha}} \leq \underline{x}^{\underline{\gamma}}\underline{x}^{\underline{\beta}}$.
3. $\forall \underline{x}^{\underline{\alpha}},\ 1 \leq \underline{x}^{\underline{\alpha}}$

Example 3.2.3 (Lexicographi order). We define $\underline{x}^{\underline{\alpha}} < \underline{x}^{\underline{\beta}}$ if there exists i such that

$$\begin{aligned} &j < i \implies \alpha_j = \beta_j, \\ &\alpha_i < \beta_i. \end{aligned}$$

Then $\leq$ is a monomial order.

Proof. By definition, this is a total order on monomials.

Let $\underline{x}^{\underline{\alpha}} < \underline{x}^{\underline{\beta}}$ and i satisfy

$$\begin{aligned} &j < i \implies \alpha_j = \beta_j, \\ &\alpha_i < \beta_i. \end{aligned}$$

Then

$$\begin{aligned} &j < i \implies \alpha_j + \gamma_j = \beta_j + \gamma_j, \\ &\alpha_i + \gamma_j < \beta_i + \gamma_j. \end{aligned}$$

Hence $\underline{x}^{\underline{\gamma}}\underline{x}^{\underline{\alpha}} < \underline{x}^{\underline{\gamma}}\underline{x}^{\underline{\beta}}$.

Let $\alpha \neq (0, \dots, 0)$ and $i = \min\{\, j \mid \alpha_j \neq 0 \,\}$. Then i satisfies

$$\begin{aligned} &j < i \implies 0 = \alpha_j, \\ &0 < \alpha_i. \end{aligned}$$

Hence $1 = \underline{x}^{(0,\dots,0)} < \underline{x}^{\underline{\alpha}}$. □

Remark 3.2.4. For a monomial order $<$, each subset of $\{\, \underline{x}^{\underline{\alpha}} \mid \underline{\alpha} \in \mathbb{N}^n \,\}$ has the minimum element. Hence, for each weakly increasing sequence

$$\underline{x}^{\underline{\alpha}^{(0)}} \geq \underline{x}^{\underline{\alpha}^{(1)}} \geq \underline{x}^{\underline{\alpha}^{(2)}} \geq \cdots$$

of monomials, there exists N such that

$$\underline{x}^{\underline{\alpha}^{(N)}} = \underline{x}^{\underline{\alpha}^{(N+1)}} = \underline{x}^{\underline{\alpha}^{(N+2)}} = \cdots.$$

3.3　Gröbner basis — anser for item 2

Fix a monomial order $\leq$. For substitution, we only use relations of the form

$$\underbrace{\underline{x}^{\underline{\alpha}}}_{\text{initial monomial}} \eqq \sum_{\underline{\beta}\colon\, \underline{\beta} < \underline{\alpha}} a_{\underline{\beta}} \underline{x}^{\underline{\beta}}.$$

If we use the symbol $\eqq$, then we assume that the left hand side is the initial monomial of the relation. For $c \neq 0$, we can transform a relation

$$c\underline{x}^{\underline{\alpha}} - \sum_{\underline{\beta}\colon\, \underline{\beta} < \underline{\alpha}} a_{\underline{\beta}} \underline{x}^{\underline{\beta}} = 0$$

to our form

$$\underline{x}^{\underline{\alpha}} \eqq \frac{1}{c} \sum_{\underline{\beta}\colon\, \underline{\beta} < \underline{\alpha}} a_{\underline{\beta}} \underline{x}^{\underline{\beta}}.$$

uniquely. Hence we identify a polynomial

$$c \underbrace{\underline{x}^{\underline{\alpha}}}_{\text{initial monomial}} - \sum_{\underline{\beta}\colon\, \underline{\beta} < \underline{\alpha}} a_{\underline{\beta}} \underline{x}^{\underline{\beta}}$$

with the relation

$$\underbrace{\underline{x}^{\underline{\alpha}}}_{\text{initial monomial}} \eqq \frac{1}{c} \sum_{\underline{\beta}\colon\, \underline{\beta} < \underline{\alpha}} a_{\underline{\beta}} \underline{x}^{\underline{\beta}}.$$

Definition 3.3.1 (S-polynomial)**.** Consider two realtions

$$\underline{x}^{\underline{\alpha}} \equiv \sum_{\underline{\beta}\,:\,\underline{\beta}<\underline{\alpha}} a_{\underline{\beta}}\underline{x}^{\underline{\beta}},$$
$$\underline{x}^{\underline{\alpha}'} \equiv \sum_{\underline{\beta}'\,:\,\underline{\beta}'<\underline{\alpha}'} a_{\underline{\beta}'}\underline{x}^{\underline{\beta}'}.$$

Let

$$r = \underline{x}^{\underline{\alpha}} - \sum_{\underline{\beta}\,:\,\underline{\beta}<\underline{\alpha}} a_{\underline{\beta}}\underline{x}^{\underline{\beta}},$$
$$r' = \underline{x}^{\underline{\alpha}'} - \sum_{\underline{\beta}'\,:\,\underline{\beta}'<\underline{\alpha}'} a_{\underline{\beta}'}\underline{x}^{\underline{\beta}'}.$$

Let $\underline{x}^{\underline{\alpha}+\underline{\gamma}} = \underline{x}^{\underline{\alpha}'+\underline{\gamma}'}$ be the least common multiplier for $\underline{x}^{\underline{\alpha}}$ and $\underline{x}^{\underline{\alpha}'}$. In other words,

$$\gamma_i = \max\{\,0, \alpha_i' - \alpha_i\,\},$$
$$\gamma_i' = \max\{\,0, \alpha_i' - \alpha_i\,\}.$$

We define the S-polynomial $S_{\leq}(r, r')$ of r and r' by

$$\begin{aligned} S_{\leq}(r,r') &= -\underline{x}^{\underline{\gamma}} \sum_{\underline{\beta}\,:\,\underline{\beta}<\underline{\alpha}} a_{\underline{\beta}}\underline{x}^{\underline{\beta}} + \underline{x}^{\underline{\gamma}'} \sum_{\underline{\beta}'\,:\,\underline{\beta}'<\underline{\alpha}'} a_{\underline{\beta}'}\underline{x}^{\underline{\beta}'} \\ &= \underline{x}^{\underline{\gamma}} r - \underline{x}^{\underline{\gamma}'} r'. \end{aligned}$$

Let R be a set of relations, i.e., polynomials. For a polynomial f, we write

$$f \,\%\, R \rightsquigarrow f'$$

to denote that we obtain f' from f by conituuing substitution unless impossible.

Remark 3.3.2. If

$$f \,\%\, R \rightsquigarrow f',$$

then we can not apply division algorithm to f'. Hence

$$f \,\%\, R \rightsquigarrow f$$

means we can not apply division algorithm to f'.

Remark 3.3.3. As see in Section 2.3.2, the following conditions dot not imply $f' = f''$:

$$f \,\%\, R \rightsquigarrow f',$$
$$f \,\%\, R \rightsquigarrow f''.$$

Definition 3.3.4. Let $R = \{\, r_1, \ldots, r_l \,\}$ be a set of relations. We call R a *Gröbner basis* if

$$S(r_i, r_j) \,\%\, R \rightsquigarrow 0$$

for any i, j.

Theorem 3.3.5. *Let $R = \{\, r_1, \ldots, r_l \,\}$ be a Gröbner basis. Let B be the set of monomials $\underline{x}^{\underline{\alpha}}$ such that any initial monomial r_i does not divide $\underline{x}^{\underline{\alpha}}$.*

1. *For each polynomial f, there uniquely exsists f' such that*

$$f \,\%\, R \rightsquigarrow f'.$$

2. *If*

$$f \,\%\, R \rightsquigarrow f',$$

   then f' is a linear combination of B.
3. *B is linearly independent.*

Remark 3.3.6. If R is a Gröbner basis, then the algebra with relations R is a vector space with the basis B. Each element in B is called a standard monomial.

This is a solution for item 2. We, however, have another problem: How do we obtain Gröbner basis?

Theorem 3.3.7 (Buchberger Algorithm)**.** *Let G be a set of relations. We can obtain a Gröbner basis by continuing the following: If there exist r and $r' \in G$ such that $S_{\leq}(r, r') \,\%\, G \rightsquigarrow c\underline{x}^{\underline{\alpha}} - \sum_{\underline{\beta}:\ \underline{\beta}<\underline{\alpha}} a_{\underline{\beta}}\underline{x}^{\underline{\beta}}$ with $c \neq 0$, then append $\underline{x}^{\underline{\alpha}} \equiv \frac{1}{c}\sum_{\underline{\beta}:\ \underline{\beta}<\underline{\alpha}} a_{\underline{\beta}}\underline{x}^{\underline{\beta}}$ to G.*

The algebra defined by indeterminants with original relations is the same as the algebra defined by indeterminants with resulting Gröbner basis.

Remark 3.3.8. Buchberger Algorithm is Euclidian Algorithm in the case of single indeterminant. Buchberger Algorithm is Gaussian Elimination in the case where the relations are polynoimals of degree one.

Example 3.3.9. Consider $\mathbb{Q}[x, y]/\left\langle x^4y^5 - y, x^6y^3 - x^2y\right\rangle$. Calculate Gröbner basis with respect to the lexicographic order by Buchberger Algorithm. Let $G = \left\{\ f_1 = x^6y^3 - x^2y, f_2 = x^4y^5 - y\ \right\}$. The S-polynomial is

$$S_{\leq}(f_2, f_1) = x^2(x^4y^5 - y) - y^2(x^6y^3 - x^2y) = -x^2y + x^2y^3.$$

We can not substitute our relations to $x^2y^3 - x^2y$. We append the polynomial and now we have $G = \left\{\ f_1, f_2, f_3 = x^2y^3 - x^2y\ \right\}$. Now $S_{\leq}(f_1, f_2) \,\%\, G \rightsquigarrow 0$. For f_2, f_3, we have

$$S_{\leq}(f_2, f_3) = (x^4y^5 - y) - x^2y^2(x^2y^3 - x^2y) = -y + x^4y^3 \xrightarrow{x^2y^3 \equiv x^2y} -y + x^4y.$$

We append the polynomial and now we have $G = \left\{\ f_1, f_2, f_3, f_4 = x^4y - y\ \right\}$. Now $S_{\leq}(f_2, f_3) \,\%\, G \rightsquigarrow 0$. For f_3, f_4, we have

$$S_{\leq}(f_3, f_4) = x^2(x^2y^3 - x^2y) - y^2(x^4y - y) = -x^4y + y^3 \xrightarrow{x^4y \equiv y} -y + y^3.$$

We append the polynomial and now we have $G = \left\{\ f_1, f_2, f_3, f_4, f_5 = y^3 - y\ \right\}$. Now $S_{\leq}(f_3, f_4) \,\%\, G \rightsquigarrow 0$. For f_4, f_5, we have

$$S_{\leq}(f_4, f_5) = y^2(x^4y - y) - x^4(y^3 - y) = -y^3 + x^4y \xrightarrow{x^4y \equiv y} -y^3 + y \xrightarrow{y^3 \equiv y} 0.$$

For f_1, f_3, we have

$$S_{\leq}(f_1, f_3) = (x^6y^3 - x^2y) - x^4(x^2y^3 - x^2y) = -x^2y + x^6y \xrightarrow{x^4y \equiv y} -x^2y + x^2y = 0.$$

For f_2, f_4, we have

$$S_{\leq}(f_2, f_4) = (x^4y^5 - y) - y^4(x^4y - y) = -y + y^5 \xrightarrow{y^3 \equiv y} -y + y^3 \xrightarrow{y^3 \equiv y} -y + y = 0.$$

For f_3, f_5, we have

$$S_{\leq}(f_3, f_5) = (x^2y^3 - x^2y) - x^2(y^3 - y) = -x^2y + x^2y = 0.$$

For f_1, f_4, we have

$$S_{\leq}(f_1, f_4) = (x^6y^3 - x^2y) - x^2y^2(x^4y - y) = -x^2y + x^2y^3 \xrightarrow{y^3 \equiv y} -x^2y + x^2y = 0.$$

For f_2, f_5, we have

$$S_{\leq}(f_2, f_5) = (x^4y^5 - y) - x^4y^2(y^3 - y) = -y + x^4y^3 \xrightarrow{y^3 \equiv y} -y + x^4y \xrightarrow{x^4y \equiv y} -y + y = 0.$$

For f_1, f_5, we have

$$S_{\leq}(f_2, f_5) = (x^6y^3 - x^2y) - x^6(y^3 - y) = -x^2y + x^6y \xrightarrow{x^4y \equiv y} -x^2y + x^2y = 0.$$

Hence

$$G = \left\{ \begin{array}{l} f_1 = x^6y^3 - x^2y, \\ f_2 = x^4y^5 - y, \\ f_3 = x^2y^3 - x^2y, \\ f_4 = x^4y - y, \\ f_5 = y^3 - y \end{array} \right\}$$

is a Gröbner basis.

Quiz 3.1. Consider $\mathbb{Q}[x, y]/\left\langle x^4y^5 - y, x^6y^3 - x^2y \right\rangle$. Let

$$\begin{aligned} \alpha &= x^5y^5, \\ \beta &= x^7y, \\ \gamma &= x^3y^3. \end{aligned}$$

Check whether $\alpha = \beta$, $\beta = \gamma$, and $\gamma = \alpha$.

第 4 章

Some remarks

4.1 Remarks for calculation of Gröbner basis

4.1.1 Remarks on S-polynomials

The following is usefull to calculate Gröbner basis.

Lemma 4.1.1. *Let $\leq$ be a monomial order. Let*

$$r_1 = \underline{x}^{\underline{\alpha}} + \sum_{\underline{\beta}:\ \underline{\beta}<\underline{\alpha}} a_{\underline{\beta}} \underline{x}^{\underline{\beta}}$$
$$r_2 = \underline{x}^{\underline{\alpha}'} + \sum_{\underline{\beta}:\ \underline{\beta}<\underline{\alpha}'} a'_{\underline{\beta}} \underline{x}^{\underline{\beta}}.$$

If $\underline{x}^{\underline{\alpha}}$ and $\underline{x}^{\underline{\alpha}'}$ are coprime, then $S_<(r_1, r_2) \,\%\, \{ r_1, r_2 \} \rightsquigarrow 0$.

Proof. Let $\underline{x}^{\underline{\alpha}}$ and $\underline{x}^{\underline{\alpha}'}$ be coprime. Then the least commom multiplier of them is $\underline{x}^{\underline{\alpha}+\underline{\alpha}'}$. Let

$$f = \sum_{\underline{\beta}:\ \underline{\beta}<\underline{\alpha}} a_{\underline{\beta}} \underline{x}^{\underline{\beta}} = r_1 - x^{\underline{\alpha}},$$
$$f' = \sum_{\underline{\beta}:\ \underline{\beta}<\underline{\alpha}'} a'_{\underline{\beta}} \underline{x}^{\underline{\beta}} = r_2 - x^{\underline{\alpha}'}.$$

Then

$$\begin{aligned} S_<(r_1, r_2) &= \underline{x}^{\underline{\alpha}'} r_1 - \underline{x}^{\underline{\alpha}} r_2 = \underline{x}^{\underline{\alpha}'} f - \underline{x}^{\underline{\alpha}} f' \\ &\xrightarrow{x^{\underline{\alpha}} \equiv f} \underline{x}^{\underline{\alpha}'} f - f f' \\ &\xrightarrow{x^{\underline{\alpha}'} \equiv f'} f' f - f f' = 0. \end{aligned}$$

□

4.1.2 Examples of monomial orders

Example 4.1.2 (Lexicographic order). We define $\underline{x}^{\underline{\alpha}} < \underline{x}^{\underline{\beta}}$ if there exists i such that

$$\begin{aligned} &j < i \implies \alpha_j = \beta_j, \\ &\alpha_i < \beta_i. \end{aligned}$$

Then $\leq$ is a monomial order. This monomial order is called the lexicographic order.

Nonexample 4.1.3 (Reverse lexicographic order). We define $\underline{x}^{\underline{\alpha}} < \underline{x}^{\underline{\beta}}$ if there exists i such that

$$\begin{aligned} &j < i \implies \alpha_j = \beta_j, \\ &\alpha_i > \beta_i. \end{aligned}$$

Then $\leq$ is a total order over (monic) monomials. It follows, however, that $1 > \underline{x}^{\underline{\alpha}}$ for $\underline{\alpha} \neq (0, \ldots, 0)$. Hence $\leq$ is not a monomial order.

Example 4.1.4 (Graded lexicographic order). For $\underline{\alpha} \in \mathbb{N}^n$, we define $|\underline{\alpha}|$ to be $\alpha_1 + \cdots + \alpha_n$. We define $\underline{x}^{\underline{\alpha}} < \underline{x}^{\underline{\beta}}$ if $|\alpha| < |\beta|$; or $|\alpha| = |\beta|$ and there exists i such that

$$\begin{aligned} &j < i \implies \alpha_j = \beta_j, \\ &\alpha_i < \beta_i. \end{aligned}$$

Then $\leq$ is a monomial order. This monomial order is called the graded lexicographic order.

Example 4.1.5 (Graded reverse lexicographic order). For $\underline{\alpha} \in \mathbb{N}^n$, we define $|\underline{\alpha}|$ to be $\alpha_1 + \cdots + \alpha_n$. We define $\underline{x}^{\underline{\alpha}} < \underline{x}^{\underline{\beta}}$ if $|\alpha| < |\beta|$; or $|\alpha| = |\beta|$ and there exists i such that

$$\begin{aligned} &j < i \implies \alpha_j = \beta_j, \\ &\alpha_i > \beta_i. \end{aligned}$$

Then $\leq$ is a monomial order. This monomial order is called the graded reverse lexicographic order.

We have many monomial orders. Gröbner bases depend on the choice of monomial oeders.

Example 4.1.6. Consider

$$\begin{aligned} r_1 &= x^2 - z^5, \\ r_2 &= y^2 - z^5. \end{aligned}$$

If $<$ is the lexicographic order, then the $x^2 > z^5$ and $y^2 > z^5$. Hence $S_<(r_1, r_2) \,\%\, \{ r_1, r_2 \} \rightsquigarrow 0$. Therefore $\{ r_1, r_2 \}$ is a Gröbner basis with respect to the lexicographic order $<$.

If $<$ is the graded lexicographic order, then $x^2 < z^5$ and $y^2 < z^5$. Hence $S_<(r_1, r_2) = x^2 - y2 \,\%\, \{ r_1, r_2 \} \rightsquigarrow x^2 - y^2$. Therefore $\{ r_1, r_2 \}$ is not a Gröbner basis with respect to the graded lexicographic order $<$.

4.2 Yet another definition of Gröbner basis

Let $<$ be a monomial order.

Definition 4.2.1. For a set S of a polynomials, define

$$\langle S \rangle = \left\{ \sum_{i=1}^{n} f_i r_i \;\middle|\; n = 1, 2, \ldots; f_i \text{ is a polynomial; } r_i \in S \right\}.$$

We call $\langle S \rangle$ the ideal generated by S.

Definition 4.2.2. For a polynomial $f = \sum_{\underline{\alpha}} a_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}$, define

$$\mathrm{in}_<(f) = \max_< \left\{ \underline{x}^{\underline{\alpha}} \;\middle|\; a_{\underline{\alpha}} \neq 0 \right\}.$$

We call $\mathrm{in}_<(f)$ the initial monomial of f with respect to $<$.

Theorem 4.2.3. *Let S be a finite set of polynomials. The set S is a Gröbner basis if and only if*

$$\langle \{ \mathrm{in}_<(r) \mid r \in S \} \rangle = \langle \{ \mathrm{in}_<(f) \mid f \in \langle S \rangle \} \rangle$$

4.3 Reduced Gröbner basis

Lemma 4.3.1. *Let S be a Gröbner basis. Let $r \in S$ satisfy*

$$r \,\%\, (S \setminus \{ r \}) \rightsquigarrow r'.$$

Let $S' = (S \setminus \{ r \}) \cup \{ r' \}$. Then S' is also Gröbner basis, and $\langle S \rangle = \langle S' \rangle$. Hence the algbra with realtion S is the same as one with S'.

Lemma 4.3.2. *Let S be a Gröbner basis. Let $S' = S \setminus \{ 0 \}$. Then S' is also Gröbner basis, and $\langle S \rangle = \langle S' \rangle$. Hence the algbra with realtion S is the same as one with S'.*

Definition 4.3.3. We call S a reduced Gröbner basis if S is a Gröbner basis satisfying

$$f \,\%\, (S \setminus \{ f \}) \rightsquigarrow f$$

for each $f \in S$.

Theorem 4.3.4. *Let S be a set of polynomials. For each monomial order $\leq$, there uniquely exists a reduced Gröbner basis S' with respect to $\leq$ such that $\langle S \rangle = \langle S' \rangle$.*

Example 4.3.5. Let

$$G = \left\{ \begin{array}{l} f_1 = x^6y^3 - x^2y, \\ f_2 = x^4y^5 - y, \\ f_3 = x^2y^3 - x^2y, \\ f_4 = x^4y - y, \\ f_5 = y^3 - y \end{array} \right\}.$$

Then G is a Gröbner basis with respect to the lexicographic order. Since

$$f_1 = x^6y^3 - x^2y \xrightarrow{y^3 \overline{=} y} x^6y - x^2y \xrightarrow{x^4y \overline{=} y} x^2y - x^2y = 0,$$

$G' = \{ f_2, \ldots, f_5 \}$ is a Gröbner basis such that $\langle G' \rangle = \langle G \rangle$. Since

$$f_2 = x^4y^5 - y \xrightarrow{y^3 \overline{=} y} x^4y^3 - y \xrightarrow{y^3 \overline{=} y} x^4y - y \xrightarrow{x^4y \overline{=} y} y - y = 0,$$

$G'' = \{ f_3, f_4, f_5 \}$ is a Gröbner basis such that $\langle G'' \rangle = \langle G \rangle$. Since

$$f_3 = x^2y^3 - x^2y \xrightarrow{y^3 \overline{=} y} x^2y - x^2y = 0,$$

$G''' = \{ f_4, f_5 \}$ is a Gröbner basis such that $\langle G''' \rangle = \langle G \rangle$. Hence

$$\left\{ \begin{array}{l} f_4 = x^4 y - y, \\ f_5 = y^3 - y \end{array} \right\}.$$

is a reduced Gröbner basis with respect to the lecicographic order.

4.4 Application

4.4.1 Computer algebras

If we use Gröbner bases, then we can calculate in algebra defined by generators with relations. In this calculation, we can clculate without heuristics. Hence this calculation can be implement as computer programs. Many authors develops algorithms to colve algebraic problems via Gröbner bases.

4.4.2 Algebraic equations

For a set S of polynomials, we consider the solutions of the system of equations

$$X_S = \left\{ (a_1, \ldots, a_n) \in \mathbb{C}^n \;\middle|\; \forall f \in S, f|_{\underline{x}=(a_1,\ldots,a_n)} = 0 \right\}.$$

If $\langle S \rangle = \langle S' \rangle$, then $X_S = X_{S'}$. Hence, to solve the system of equations, we want to find a "nice" system of generators of the ideal $\langle S \rangle$.

Lemma 4.4.1. *Let G be a set of polynomials in indeterminants $x_1, \ldots, x_n$. Assume that G is a reduced Gröbner basis with respect to the lexicographic order $<$. Let $I = \langle G \rangle$. For each $k = 1, \ldots, n$, define*

$$I_k = \{ f \in I \mid f \text{ is a polynomial in } x_k, x_{k+1}, \ldots, x_n \}$$
$$G_k = \{ f \in G \mid f \text{ is a polynomial in } x_k, x_{k+1}, \ldots, x_n \}.$$

Then G_k is a a reduced Gröbner basis with respect to the lexicographic order $<$, and

$$\langle G_k \rangle = I_k.$$

Remark 4.4.2. A general monomial order does not satisfy Lemma 4.4.1. We call sometimes a monomial order satisfying Lemma 4.4.1 an elimination order.

If we have a reduced Gröbner basis with respect to the lexicographic order $<$, then we can solve the system of equation as follows: An element in G_n is a polynomial in a single indeterminat x_n. Hence we can solve the system of equations for x_n and obtain X_{G_n}. Now we consider G_{n-1}. If x_n is given, then each elemet in G_{n-1} is a polynomial in a sigle indeterminant x_{n-1}. Hence we can solve the system of equations for x_{n-1} and obtain $X_{G_{n-1}}$. Now we consider G_{n-2}. If x_{n-1}, x_n is given, then each elemet in G_{n-2} is a polynomial in a sigle indeterminant x_{n-2}. Hence we can solve the system of equations for x_{n-2} and obtain $X_{G_{n-1}}$. Repeating this process, we obtain X_G.

Quiz 4.1. Solve the system of equations

$$\begin{cases} x^4y^5 - y = 0 \\ x^6y^3 - x^2y = 0. \end{cases}$$

参考文献