Computational Algebraic Statistics and its Applications

Satoshi Aoki (Kobe Univ.)

RIKEN iTHEMS

26 June, 2018

Contents

- References

1. Cox, D., Little, J. and O'Shea, D. (2000). *Ideals, Varieties, and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra*. 3rd ed. Springer.
   ··· An introduction of Gröbner basis theory.
2. Hibi, T. (ed). (2013). *Gröbner Bases, Statistics and Software Systems*. Springer.
   ··· Translation of [3]. Chap 1 by Hibi: An introduction of Gröbner basis theory. Chap 4 by Aoki and Takemura: An application to the analysis of contingency tables.
3. JST CREST 日比チーム (編). (2011). グレブナー道場. 共立出版.
4. 青木敏. 計算代数統計 — グレブナー基底と実験計画法 —. 統計学 One Point 第 9 巻. 2018 年 8 月刊行予定.
   ··· The slides 1 and 2 today are partially based on this book.

5. Pistone, G. and Wynn, H. P. (1996). Generalized confounding with Gröbner bases. *Biometrika*, **83**, 653–666.
   · · · An application to the design of experiments. (One of the two origins of computational algebraic statistics.)
6. Pistone, G., Riccomagno, E. and Wynn, H. P. (2001). *Algebraic statistics: Computational commutative algebra in statistics.* Chapman & Hall Ltd, Boca Raton.
   · · · The first textbook of computational algebraic statistics.
7. Diaconis, P. and Sturmfels, B. (1998). Algebraic algorithms for sampling from conditional distributions. *Annals of Statistics.* **26**, 363–397.
   · · · Application to the analysis of contingency tables. (One of the two origins of computational algebraic statistics.)
8. Aoki, S., Hara, H. and Takemura, A. (2012). *Markov bases in statistics.* Springer Series in Statistics.
   · · · Application to the analysis of contingency tables.

1. An introduction of Gröbner bases of polynomial rings

1. Gröbner bases and algebraic equations

- The stage of the Gröbner bases is an ideal of a polynomial ring. Prof. Takayama says, "Ideal is an algebraic equation."
- Prob. 1 Solve the simultaneous linear equations:

$$\begin{cases} x + 2y - z = 2 \\ x + y - 4z = 3 \\ x + 3y + 3z = 0 \end{cases}$$

- Easy. (Linear algebra)

$$\begin{cases} x + 2y - z &= 2 \\ y + 3z &= -1 \\ z &= -1 \end{cases}$$

- Prob. 2 Solve the simultaneous algebraic equations:

$$\begin{cases} x^2 + y^2 + 4z^2 = 81 \\ x - y + z^2 = 13 \\ xz - 2y = 18 \end{cases}$$

- Answer:

$$\begin{cases} x^2 + y^2 + 4z^2 = 81 \\ x - y + z^2 = 13 \qquad (1) \\ xz - 2y = 18 \qquad (2) \end{cases}$$

From $(2) - 2 \times (1)$, we can eliminate y as

$$xz - 2x - 2z^2 = -8.$$

The answer is given from the factorization

$$(z - 2)(x - 2z - 4) = 0.$$

- **Prob. 3** Solve the simultaneous algebraic equations:

$$\begin{cases} x^2 + y^2 + 4z^2 = 90 \\ x - y + z = 12 \\ xz - 3y = 28 \end{cases}$$

- Similarly to Prob. 2, we can eliminate y as

$$xz - 3x - 3z + 8 = 0,$$

  however, we cannot factorize this.

- It is quite difficult to solve Prob. 3 by hand, though it seems to be similar to Prob. 2.
- Prob. 2 is easy to solve because we can use the factorization of the equation.

> What is a general method to obtain an equation of one variable from algebraic simultaneous equations, by not using factorization?

- The calculation of the Gröbner bases is an effective answer.

- "Gröbner bases like" solution of Prob. 3

$$\begin{cases} f_1 = x^2 + y^2 + 4z^2 - 90 = 0 \\ f_2 = x - y + z - 12 = 0 \\ f_3 = xz - 3y - 28 = 0 \end{cases}$$

  - Aim: eliminate x, y and obtain the equation of z.
  - From $f_2 = 0$, substitute $x = y - z + 12$ into f_3, we have

$$f_3 = z(y - z + 12) - 3y - 28 = yz - 3y - z^2 + 12z - 28.$$

We have

$$f_4 = yz - 3y - z^2 + 12z - 28.$$

$$\boxed{\begin{aligned} f_1 &= x^2 + y^2 + 4z^2 - 90 = 0 \\ f_2 &= x - y + z - 12 = 0 \\ f_4 &= yz - 3y - z^2 + 12z - 28 = 0 \end{aligned}}$$

- Similarly, substitute $x = y - z + 12$ into f_1, we have

$$\begin{aligned} f_1 &= (y - z + 12)^2 + y^2 + 4z^2 - 90 \\ &= 2y^2 - 2yz + 24y + 5z^2 - 24z + 54. \quad (*) \end{aligned}$$

We already have $f_4 = 0$. Substitute $yz = 3y + z^2 - 12z + 28$ as

$$\begin{aligned} (*) &= 2y^2 - 2(3y + z^2 - 12z + 28) + 24y + 5z^2 - 24z + 54 \\ &= 2y^2 + 18y + 3z^2 - 2. \end{aligned}$$

We have

$$f_5 = y^2 + 9y + 3z^2/2 - 1.$$

- Now we have the equivalent simultaneous equation

$$\begin{cases} f_2 = x - y + z - 12 = 0 \\ f_4 = yz - 3y - z^2 + 12z - 28 = 0 \\ f_5 = y^2 + 9y + 3z^2/2 - 1 = 0. \end{cases}$$

- Next we want to eliminate y from $f_4 = f_5 = 0$. But we do not use rational expression

$$y = \frac{z^2 - 12z + 28}{z - 3}.$$

We only consider polynomials.

Eliminate yz and y^2, the leading terms of f_4, f_5.

◦ Calculate $yf_4 - zf_5$:

$$\begin{aligned} & yf_4 - zf_5 \\ = \quad & y(yz - 3y - z^2 + 12z - 28) - z(y^2 + 9y + 3z^2/2 - 1) \\ = \quad & -3y^2 - yz^2 + 3yz - 28y - 3z^3/2 + z. \qquad (**) \end{aligned}$$

yz and y^2 can be replaced from $f_4 = f_5 = 0$ as

$$\begin{aligned} (**) \quad = \quad & -3(-9y - 3z^2/2 + 1) - (z - 3)(3y + z^2 - 12z + 28) \\ & \qquad\qquad -28y - 3z^3/2 + z \\ = \quad & -3yz + 8y - 5z^3/2 + 39z^2/2 - 63z + 81 \\ = \quad & -3(3y + z^2 - 12z + 28) + 8y - 5z^3/2 + 39z^2/2 - 63z + 81 \\ = \quad & -y - 5z^3/2 + 33z^2/2 - 27z - 3. \end{aligned}$$

We have $f_6 = y + 5z^3/2 - 33z^2/2 + 27z + 3$.

◦ Now we have the equivalent simultaneous equations

$$\begin{cases} f_2 = x - y + z - 12 = 0 \\ f_4 = yz - 3y - z^2 + 12z - 28 = 0 \\ f_6 = y + 5z^3/2 - 33z^2/2 + 27z + 3 = 0. \end{cases}$$

◦ Now it is easy to obtain

$$\begin{cases} x + 5z^3/2 - 33z^2/2 + 28z - 9 = 0 \\ y + 5z^3/2 - 33z^2/2 + 27z + 3 = 0 \\ z^4 - 48z^3/5 + 31z^2 - 36z + 38/5 = 0. \end{cases}$$

The last one is an equation of z.

◦ Note: The third equation can be factorized as

$$(z^2 - 4z + 1)(z^2 - 28z/5 + 38/5) = 0.$$

The solution of Prob. 3 is

$$(x, y, z) = \left\{ \left(\frac{7 \pm \sqrt{3}}{2}, \frac{-13 \pm 3\sqrt{3}}{2}, 2 \pm \sqrt{3} \right), \right.$$
$$\left. \left(4 \pm \sqrt{6}, \frac{-26 \pm 6\sqrt{6}}{5}, \frac{14 \pm \sqrt{6}}{5} \right) \right\}.$$

- The set of the polynomials we have

$$x + 5z^3/2 - 33z^2/2 + 28z - 9,$$
$$y + 5z^3/2 - 33z^2/2 + 27z + 3,$$
$$z^4 - 48z^3/5 + 31z^2 - 36z + 38/5$$

  is a Gröbner basis.

- The polynomial deformation we done is a Buchberger algorithm.
- For general simultaneous algebraic equations, we can obtain the polynomial of z in similar way, if x, y can be eliminated.
- Prof. Hibi says, "Gröbner basis is a powerful technique for solving simultaneous equations".

2. Ideals of polynomial rings

The stage of the Gröbner bases: polynomial rings in n variables.

- Monomial of the variables $x_1, \ldots, x_n$:

$$\prod_{i=1}^{n} x_i^{a_i} = x_1^{a_1} \cdots x_n^{a_n}, \quad a_1, \ldots, a_n \in \mathbb{Z}_{\geq 0}. \qquad \sum_{i=1}^{n} a_i : \text{ degree}$$

  - Term: monomial with a nonzero coefficient
  - Polynomial: finite sum of terms
  - Example: $f = -5x_1^2x_2x_3^2 + \dfrac{2}{3}x_2x_4^3x_5^2 - x_3^3 - 7$ is a polynomial with 4 terms $-5x_1^2x_2x_3^2,\ \dfrac{2}{3}x_2x_4^3x_5^2,\ -x_3^3,\ -7$.
    The monomials appearing in f are $x_1^2x_2x_3^2,\ x_2x_4^3x_5^2,\ x_3^3,\ 1$.

- K: field. (Example: $K = \mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$.)
- $K[x_1, \ldots, x_n]$: the set of all polynomials in the variables $x_1, \ldots, x_n$ with coefficients in K.
  - Example:

$$x_1^2 - \sqrt{2}x_2x_3 \in \mathbb{R}[x_1, x_2, x_3],$$
$$2x_1^2x_2 - \frac{2}{3}x_2x_3^4 + 1 \in \mathbb{Q}[x_1, x_2, x_3](\subset \mathbb{R}[x_1, x_2, x_3])$$

- $K[x_1, \ldots, x_n]$ has the structure of a ring (i.e., sum and product), and is called a polynomial ring in n variables over K.

- To introduce an ideal of $K[x_1, \ldots, x_n]$, consider Prof. Takayama's words: "Ideal is an algebraic equations".
  - For $f_1(x_1, \ldots, x_n),\ \ldots,\ f_r(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, consider the simultaneous equation

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \qquad\qquad \vdots \\ f_r(x_1, \ldots, x_n) = 0. \end{cases}$$

  - Affine variety of $f_1, \ldots, f_r$:

$$\mathbf{V}(f_1, \ldots, f_r) = \{(a_1, \ldots, a_n) \in K^n \mid \forall i,\ f_i(a_1, \ldots, a_n) = 0\}.$$

  - Solve the equation $f_1 = \cdots = f_r = 0$
    $\Leftrightarrow$ Derive the affine variety $\mathbf{V}(f_1, \ldots, f_r)$.

◦ In Prob. 3, we have

$$\mathbf{V}(f_1, f_2, f_3) = \left\{ \left(\frac{7 \pm \sqrt{3}}{2}, \frac{-13 \pm 3\sqrt{3}}{2}, 2 \pm \sqrt{3} \right), \left(4 \pm \sqrt{6}, \frac{-26 \pm 6\sqrt{6}}{5}, \frac{14 \pm \sqrt{6}}{5} \right) \right\}$$

for $K = \mathbb{R}$ and

$f_1 = x^2 + y^2 + 4z^2 - 90,\ f_2 = x - y + z - 12,\ f_3 = xz - 3y - 28.$

How did we get it?

$$\boxed{\begin{aligned} f_1 &= x^2 + y^2 + 4z^2 - 90 = 0 \\ f_2 &= x - y + z - 12 = 0 \\ f_3 &= xz - 3y - 28 = 0 \end{aligned}}$$

- From $f_1 = f_2 = f_3 = 0$, "solve $f_2 = 0$ for x and substitute it into f_3", we have

$$\begin{cases} f_1 = x^2 + y^2 + 4z^2 - 90 = 0 \\ f_2 = x - y + z - 12 = 0 \\ f_4 = yz - 3y - z^2 + 12z - 28 = 0. \end{cases}$$

  Note that $f_3 - zf_2 = f_4$.

$$\boxed{\begin{aligned} f_1 &= x^2 + y^2 + 4z^2 - 90 = 0 \\ f_2 &= x - y + z - 12 = 0 \\ f_4 &= yz - 3y - z^2 + 12z - 28 = 0 \end{aligned}}$$

- Next, "solve $f_2 = 0$ for x and substitute it into f_1", and into this, substitute the result of "solve $f_4 = 0$ for yz", and multiply the result by $1/2$, we have

$$\begin{cases} f_2 = x - y + z - 12 = 0 \\ f_4 = yz - 3y - z^2 + 12z - 28 = 0 \\ f_5 = y^2 + 9y + 3z^2/2 - 1 = 0. \end{cases}$$

Note that

$$\frac{1}{2} f_1 - \frac{x + y - z + 12}{2} f_2 + f_4 = f_5.$$

- Next, to eliminate yz of f_4 and y^2 of f_5, consider $yf_4 - zf_5$, and substitute $yz = \cdots$ from $f_4 = 0$ and $y^2 = \cdots$ from $f_5 = 0$ into it. Then multiply it by -1, we have

$$\begin{cases} f_2 = x - y + z - 12 = 0 \\ f_4 = yz - 3y - z^2 + 12z - 28 = 0 \\ f_6 = y + 5z^3/2 - 33z^2/2 + 27z + 3 = 0. \end{cases}$$

  Note that

$$\begin{aligned} & -1 \times (yf_4 - zf_5 + 3f_5 + (z-3)f_4 + 3f_4) \\ = \quad & (-y - z)f_4 + (z-3)f_5 = f_6. \end{aligned}$$

- Finally we have $f_6 = f_7 = f_8 = 0$ as

$$\begin{aligned} f_7 &= f_2 + f_6 = x + 5z^3/2 - 33z^2/2 + 28z - 9 \\ f_8 &= -\frac{2}{5}f_4 + \frac{2z-6}{5}f_6 = z^4 - \frac{48}{5}z^3 + 31z^2 - 36z + \frac{38}{5}. \end{aligned}$$

- Point: The deformations of polynomials above are expressed as "multiplied by polynomials" and "addition" of polynomials.

- Now we define the set

$$\langle f_1, \ldots, f_r \rangle = \{h_1 f_1 + \cdots + h_r f_r \mid h_1, \ldots, h_r \in K[x_1, \ldots, x_r]\},$$

  i.e., the set of polynomials that can be obtained from $f_1, \ldots, f_r$ by "multiplied by polynomials" and "addition".

- In other words, $\langle f_1, \ldots, f_r \rangle$ is the set of all polynomials that can appear to solve the equation $f_1 = \cdots = f_r = 0$.

- $\langle f_1, \ldots, f_r \rangle$ is an important example of an ideal.

Definition A nonempty subset I of $K[x_1, \ldots, x_n]$ is called an ideal of $K[x_1, \ldots, x_n]$ if the following conditions are satisfied.

- If $f \in I, g \in I$, then $f + g \in I$;
- If $f \in I, h \in K[x_1, \ldots, x_n]$, then $hf \in I$.

Proposition $I = \langle f_1, \ldots, f_r \rangle$ is an ideal of $K[x_1, \ldots, x_n]$.

- $\langle f_1, \ldots, f_r \rangle$ is the ideal generated by $\{f_1, \ldots, f_r\}$, i.e., finitely generated ideal.
  - In general, let $\{f_\lambda \mid \lambda \in \Lambda\}$ be a nonempty subset of $K[x_1, \ldots, x_n]$, then we can show that

    $$\langle \{f_\lambda \mid \lambda \in \Lambda\} \rangle = \left\{ \text{finite sum } \sum_{\lambda \in \Lambda} h_\lambda f_\lambda,\ h_\lambda \in K[x_1, \ldots, x_n] \right\}$$

    is an ideal of $K[x_1, \ldots, x_n]$.
  - Conversely, for an ideal $I \subset K[x_1, \ldots, x_n]$, there exists $\{f_\lambda \mid \lambda \in \Lambda\} \subset K[x_1, \ldots, x_n]$ satisfying $I = \langle \{f_\lambda \mid \lambda \in \Lambda\} \rangle$. The subset $\{f_\lambda \mid \lambda \in \Lambda\}$ is called a system of generators of I.

- Fundamental problems for ideal:
  1. Ideal description problem
     Can every ideal $I \subset K[x_1, \ldots, x_n]$ be written as
     $$I = \langle f_1, \ldots, f_r \rangle$$
     for some finite set $\{f_1, \ldots, f_r\} \subset K[x_1, \ldots, x_n]$?
  2. Ideal membership problem
     For an ideal $I \subset K[x_1, \ldots, x_n]$, is there an algorithm to decide whether a given $f \in K[x_1, \ldots, x_n]$ lies in I?
- The answers for both are "YES".
- For the case of one variable polynomial ring $K[x]$, both problems can be solved by high school mathematics.

  A key is a division algorithm.

Prob. 4

Divide $f(x) = x^4 + 2x^3 - x^2 + 4x - 1$ by $g(x) = x^2 - 3x + 1$.

Answer:

$$
\begin{array}{r}
x^2+5x+\ 13 \\
\hline
x^2-3x+1 \ \big| \ x^4+2x^3-\ x^2\ +4x-1 \\
\underline{x^4-3x^3+\ x^2} \\
5x^3-\ 2x^2+4x-1 \\
\underline{5x^3-15x^2+5x} \\
13x^2-\ x\ -1 \\
\underline{13x^2-39x+13} \\
38x-14
\end{array}
$$

The quotient is $x^2 + 5x + 13$ and the remainder is $38x - 14$.

- The expression we have is

$$f(x) = (x^2 + 5x + 13)g(x) + 38x - 14.$$

- A division of $f \in K[x]$ by $g \in K[x]$ is to express f in the form

$$f(x) = q(x)g(x) + r(x),$$

where $q(x)$ is the quotient and $r(x)$ is the remainder satisfying

$$r(x) = 0 \quad \text{or} \quad \deg(r(x)) < \deg(g(x)).$$

$q(x)$ and $r(x)$ are decided uniquely.

- Point: "Divide by $g(x) = x^2 - 3x + 1$" means "replace x^2 by $g(x) + 3x - 1$ as many times as possible".

$$
\begin{array}{rrcl}
 & x^2+5x+13 & & \\
x^2-3x+1 \;\big|\; & x^4+2x^3-x^2+4x-1 & & x^4+2x^3-x^2+4x-1 \\
 & x^4-3x^3+x^2 & = & x^2(g+3x-1)+2x^3-x^2+4x-1 \\
\hline
 & 5x^3-2x^2+4x-1 & = & x^2g+5x^3-2x^2+4x-1 \\
 & 5x^3-15x^2+5x & = & x^2g+5x(g+3x-1)-2x^2+4x-1 \\
\hline
 & 13x^2-x-1 & = & (x^2+5x)g+13x^2-x-1 \\
 & 13x^2-39x+13 & = & (x^2+5x)g+13(g+3x-1)-x-1 \\
\hline
 & 38x-14 & = & (x^2+5x+13)g+38x-14
\end{array}
$$

- Ideal description problem for $K[x]$
  - $I \subset K[x]$: ideal.
  - $g \in I$: an element of I with a minimum degree.
  - For each $f \in I$, we have the expression

$$f = qg + r,$$
$$\text{where } r = 0 \text{ or } \deg(r) < \deg(g).$$

    $q \in K[x]$ and $r \in K[x]$ are decided uniquely.
  - From $f, g \in I$, we have $r = f - qg \in I$. Because g is an element of I with a minimum degree, $r = 0$. Therefore each $f \in I$ can be expressed as $f = qg$, i.e., I is generated by g:

$$I = \{qg \mid q \in K[x]\} = \langle g \rangle .$$

- Each ideal $I \subset K[x]$ is a principal ideal.

- Ideal membership problem for $K[x]$

  To judge whether $f \in K[x]$ is in $\langle g \rangle \subset K[x]$ or not, divide f by g, and we have the expression

$$f = qg + r, \quad q, r \in K[x],$$
$$\text{where } r = 0 \text{ or } \deg(r) < \deg(g).$$

  Then we have

$$r = 0 \quad \Leftrightarrow \quad f \in \langle g \rangle .$$

3. Monomial order and division algorithm

- To solve the ideal membership problem for n variables, consider the division algorithm for $K[x_1, \ldots, x_n]$.
- Recall that "divide $g = x^2 - 3x + 1$" means "replace x^2 by $g + 3x - 1$" for one variable case.
- How it can be generalized to n variable cases?
  - "Divide f by $h = x^2 - yz$" means "replace x^2 in f with $h + yz$"? or "replace yz in f with $-h + x^2$"?
  - Anyway, $\deg(f)$ cannot be reduced. Also, we must define a stopping rule.
- To generalize the division algorithm for $K[x_1, \ldots, x_n]$, we need "order" on the set of monomials.

- Definition Let M_n be the set of monomials in the variables $x_1, \ldots, x_n$. A monomial order on $K[x_1, \ldots, x_n]$ is a total order $\prec$ on M_n such that

  (i) $1 \prec u$ for all $1 \neq u \in M_n$;

  (ii) If $u, v \in M_n$ and $u \prec v$, then $uw \prec vw$ for all $w \in M_n$.

  - Example: An order by the degree

$$1 \prec x \prec x^2 \prec x^3 \prec \cdots$$

    is a monomial order on M_1.

- Examples of monomial orders:

  Definition Let $u = x_1^{a_1} \cdots x_n^{a_n}, v = x_1^{b_1} \cdots x_n^{b_n} \in M_n$.

  (i) We define $u \prec_{\text{purelex}} v$ if the leftmost nonzero element of $(b_1 - a_1, \ldots, b_n - a_n)$ is positive. It follows $\prec_{\text{purelex}}$ is a monomial order on $K[x_1, \ldots, x_n]$, called the pure lexicographic order.

  (ii) We define $u \prec_{\text{lex}} v$ if either (i) $\deg(v) > \deg(u)$ or (ii) $\deg(v) = \deg(u)$ and the leftmost nonzero element of $(b_1 - a_1, \ldots, b_n - a_n)$ is positive. It follows $\prec_{\text{lex}}$ is a monomial order on $K[x_1, \ldots, x_n]$, called the lexicographic order.

  (iii) We define $u \prec_{\text{rev}} v$ if either (i) $\deg(v) > \deg(u)$ or (ii) $\deg(v) = \deg(u)$ and the rightmost nonzero element of $(b_1 - a_1, \ldots, b_n - a_n)$ is negative. It follows $\prec_{\text{rev}}$ is a monomial order on $K[x_1, \ldots, x_n]$, called the reverse lexicographic order.

- Prob. 5 Let $n = 3$ and $x_1 = x, x_2 = y, x_3 = z$. List the monomials of degree less than 5 with respect to $\prec_{\text{purelex}}, \prec_{\text{lex}}, \prec_{\text{rev}}$ induced by $x \succ y \succ z$, respectively.

  Answer

  - The pure lexicographic order:

$$x^4,\ x^3y,\ x^3z,\ x^3,\ x^2y^2,\ x^2yz,\ x^2y,\ x^2z^2,\ x^2z,\ x^2,$$
$$xy^3,\ xy^2z,\ xy^2,\ xyz^2,\ xyz,\ xy,\ xz^3,\ xz^2,\ xz,\ x,$$
$$y^4,\ y^3z,\ y^3,\ y^2z^2,\ y^2z,\ y^2,\ yz^3,\ yz^2,\ yz,\ y,$$
$$z^4,\ z^3,\ z^2,\ z,\ 1$$

- The lexicographic order:

$$x^4,\ x^3y,\ x^3z,\ x^2y^2,\ x^2yz,\ x^2z^2,\ xy^3,\ xy^2z,\ xyz^2,\ xz^3,$$
$$y^4,\ y^3z,\ y^2z^2,\ yz^3,\ z^4,$$
$$x^3,\ x^2y,\ x^2z,\ xy^2,\ xyz,\ xz^2,\ y^3,\ y^2z,\ yz^2,\ z^3,$$
$$x^2,\ xy,\ xz,\ y^2,\ yz,\ z^2,\ x,\ y,\ z,\ 1$$

- The reverse lexicographic order:

$$x^4,\ x^3y,\ x^2y^2,\ xy^3,\ y^4,\ x^3z,\ x^2yz,\ xy^2z,\ y^3z,$$
$$x^2z^2,\ xyz^2,\ y^2z^2,\ xz^3,\ yz^3,\ z^4,$$
$$x^3,\ x^2y,\ xy^2,\ y^3,\ x^2z,\ xyz,\ y^2z,\ xz^2,\ yz^2,\ z^3,$$
$$x^2,\ xy,\ y^2,\ xz,\ yz,\ z^2,\ x,\ y,\ z,\ 1$$

- We fix a monomial order $\prec$ on $K[x_1, \ldots, x_n]$.
- For each $f \in K[x_1, \ldots, x_n]$, we can define the initial monomial of f with respect to $\prec$, $\text{in}_\prec(f)$, as the largest monomial belonging to f.
- We also write c_f as the coefficient of $\text{in}_\prec(f)$. The term $c_f \cdot \text{in}_\prec(f)$ is the initial term of f.
- Example: $f = 2xy^4 - x^3z + 5x^2y^2z + 1 \in K[x, y, z]$
  - For $\prec_{\text{purelex}}$, $\text{in}_{\prec_{\text{purelex}}}(f) = x^3z$ and the initial term is $-x^3z$.
  - For $\prec_{\text{lex}}$, $\text{in}_{\prec_{\text{lex}}}(f) = x^2y^2z$ and the initial term is $5x^2y^2z$.
  - For $\prec_{\text{rev}}$, $\text{in}_{\prec_{\text{rev}}}(f) = xy^4$ and the initial term is $2xy^4$.

- Division algorithm for $K[x_1, \ldots, x_n]$

  Let $f, g_1, \ldots, g_s \in K[x_1, \ldots, x_n]$. Divide f by $g_1, \ldots, g_s$ as follows.

  - Fix a monomial order $\prec$ on M_n.
  - Suppose a monomial in f is divided by some $\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_s)$. Then replace $\mathrm{in}_\prec(g_i)$ in f with

    $$\frac{1}{c_{g_i}} g_i - \left(\frac{1}{c_{g_i}} g_i - \mathrm{in}_\prec(g_i) \right).$$

  - Replace similarly as possible as we can.

- **Theorem (Division algorithm)** Fix a monomial order $\prec$ on M_n. Let $g_1, \ldots, g_s$ and f are nonzero polynomials in $K[x_1, \ldots, x_n]$. Then there exists a standard form of f with respect to $g_1, \ldots, g_s$,

$$f = q_1 g_1 + \cdots + q_s g_s + r$$

for some $q_1, \ldots, q_s, r \in K[x_1, \ldots, x_n]$, satisfying

(i) If $r \neq 0$, then any monomial of r cannot be divided by any $\mathrm{in}_\prec(g_i)$.

(ii) If $q_i \neq 0$, then $\mathrm{in}_\prec(q_i g_i) \preceq \mathrm{in}_\prec(f)$ holds.

r is called a remainder of f with respect to $g_1, \ldots, g_s$.

- Prob. 6 For $\prec_{\mathrm{lex}}$ on M_3, derive a standard form of $f = xyz + xz^2 - y^2 - 1$ with respect to $g_1 = yz - x,\ g_2 = xz - y^2$.

  Answer. For the lexicographic order, the initial monomials of g_1, g_2 are

  $$\mathrm{in}_{\prec_{\mathrm{lex}}}(g_1) = yz, \quad \mathrm{in}_{\prec_{\mathrm{lex}}}(g_2) = xz.$$

  Then, we "replace yz in f with $g_1 + x$" or "replace xz in f with $g_2 + y^2$" as possible as we can.

$$\boxed{g_1 = \underline{yz} - x,\ g_2 = \underline{xz} - y^2}$$

$$\begin{aligned}
f &= xyz + xz^2 - y^2 - 1 \\
&= x(g_1 + x) + xz^2 - y^2 - 1 \\
&= xg_1 + x^2 + xz^2 - y^2 - 1 \\
&= xg_1 + x^2 + z(g_2 + y^2) - y^2 - 1 \\
&= xg_1 + zg_2 + x^2 + y^2 z - y^2 - 1 \\
&= xg_1 + zg_2 + x^2 + y(g_1 + x) - y^2 - 1 \\
&= (x + y)g_1 + zg_2 + x^2 + xy - y^2 - 1
\end{aligned}$$

This is a standard form of f with respect to g_1, g_2 for $\prec_{\text{lex}}$.

Another answer. Replace by g_2 first, we have

$$\begin{aligned} f &= xyz + xz^2 - y^2 - 1 \\ &= y(g_2 + y^2) + xz^2 - y^2 - 1 \\ &= yg_2 + y^3 + xz^2 - y^2 - 1 \\ &= yg_2 + y^3 + z(g_2 + y^2) - y^2 - 1 \\ &= (y+z)g_2 + y^3 + y^2z - y^2 - 1 \\ &= (y+z)g_2 + y^3 + y(g_1 + x) - y^2 - 1 \\ &= yg_1 + (y+z)g_2 + y^3 + xy - y^2 - 1. \end{aligned}$$

This is also a standard form of f with respect to g_1, g_2 for $\prec_{\mathrm{lex}}$.

For n variable cases, a standard form is not unique.

4. Gröbner bases and ideal membership problems

- Consider the ideal membership problem for $K[x_1, \ldots, x_n]$.
- For an ideal $I = \langle g_1, \ldots, g_s \rangle \subset K[x_1, \ldots, x_n]$ and $f \in K[x_1, \ldots, x_n]$, if we fix a monomial order $\prec$ on M_n, we have a standard form of f with respect to $g_1, \ldots, g_s$ by the division algorithm,

$$f = q_1 g_1 + \cdots + q_s g_s + r.$$

- If $r = 0$, then we know $f \in I$. However, $r = 0$ is not necessary condition for $f \in I$.

- Example. For $\prec_{\mathrm{lex}}$ on M_3,

$$\begin{aligned} f &= (x+y)g_1 + zg_2 \\ &= yg_1 + (y+z)g_2 + y^3 - x^2 \end{aligned}$$

  are standard forms of $f = xyz + xz^2 - x^2 - xy$ with respect to $g_1 = yz - x, g_2 = xz - y^2$.

- Here, write $g_3 = y^3 - x^2$ and express $I = \langle g_1, g_2 \rangle$ as $I = \langle g_1, g_2, g_3 \rangle$. Then we have standard forms of f with zero remainder with respect to g_1, g_2, g_3,

$$\begin{aligned} f &= (x+y)g_1 + zg_2 \\ &= yg_1 + (y+z)g_2 + g_3. \end{aligned}$$

- This $\{g_1, g_2, g_3\}$ is a Gröbner basis of I.

- Consider the case that $f \in I = \langle g_1, \ldots, g_s \rangle$ has a standard form

$$f = q_1 g_1 + \cdots + q_s g_s + r,$$

where $r \neq 0$.

- Here, $r = f - q_1 g_1 - \cdots - q_s g_s \in I$. Each monomial of r cannot be divided by any of $\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_s)$. In particular, $\mathrm{in}_\prec(r)$ cannot be divided by any of $\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_s)$, i.e.,

$$\mathrm{in}_\prec(r) \notin \langle \mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_s) \rangle .$$

- Conversely, for a monomial order $\prec$, if the set $\{g_1, \ldots, g_s\}$ satisfies the condition

$$f \in \langle g_1, \ldots, g_s \rangle \;\Rightarrow\; \mathrm{in}_\prec(f) \in \langle \mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_s) \rangle ,$$

then it follows, for each $f \in K[x_1, \ldots, x_n]$, the remainder of f with respect to $g_1, \ldots, g_s$ is unique.

- The above consideration leads to the definition of the Gröbner basis.
- Write the (monomial) ideal generated by $\{\mathrm{in}_\prec(f) \mid f \in I\}$ as

$$\mathrm{in}_\prec(I) = \langle \{\mathrm{in}_\prec(f) \mid f \in I\} \rangle .$$

  This is called an initial ideal of f with respect to $\prec$.
- Definition Fix a monomial order $\prec$ on M_n. Let I be an ideal of $K[x_1, \ldots, x_n]$. Then a Gröbner basis of I with respect to $\prec$ is a finite set $\{g_1, \ldots, g_s\}$ of polynomials in I satisfying

$$\mathrm{in}_\prec(I) = \langle \mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_s) \rangle .$$

- For $I = \langle g_1, \ldots, g_s \rangle$, $\mathrm{in}_\prec(I) \supset \langle \mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_s) \rangle$ in general.
- The converse does not necessary hold.

  Example.

  For $\prec_{\mathrm{lex}}$ on M_3, consider $g_1 = yz - x,\ g_2 = xz - y^2$, $I = \langle g_1, g_2 \rangle$.
  From $y^3 - x^2 = xg_1 - yg_2 \in I$, $\mathrm{in}_{\prec_{\mathrm{lex}}}(y^3 - x^2) = y^3 \in \mathrm{in}_{\prec_{\mathrm{lex}}}(I)$ holds. However, $y^3 \notin \langle yz, xz \rangle = \langle \mathrm{in}_{\prec_{\mathrm{lex}}}(g_1), \mathrm{in}_{\prec_{\mathrm{lex}}}(g_2) \rangle$, i.e., $\mathrm{in}_{\prec_{\mathrm{lex}}}(I) \neq \langle \mathrm{in}_{\prec_{\mathrm{lex}}}(g_1), \mathrm{in}_{\prec_{\mathrm{lex}}}(g_2) \rangle$.

- A finite Gröbner basis always exists.

  (From Dickson's lemma saying that "The set of minimal elements of a nonempty subset of M_n is at most finite".)

- A Gröbner basis of I is a system of generators of I.

  (This yields the so-called Hilbert Basis Theorem. Therefore the ideal description problem reduces to a calculation of Gröbner basis for arbitrary fixed $\prec$.)

- The remainder of the standard form with respect to the Gröbner basis is unique.

  (Therefore the ideal membership problem is solved by the division algorithm with respect to the Gröbner basis.)

5. Buchberger criterion and Buchberger algorithm

- Given a system of generators of an ideal, how can we decide whether they form its Gröbner basis or not?
- The answer is Buchberger criterion.
- Recall that $\{g_1, g_2\} = \{yz - x, xz - y^2\}$ is not a Gröbner basis of $I = \langle g_1, g_2 \rangle$ with respect to $\prec_{\mathrm{lex}}$ because the initial monomial of $g_3 = xg_1 - yg_2 \in I$ is not included in $\langle \mathrm{in}_{\prec_{\mathrm{lex}}}(g_1), \mathrm{in}_{\prec_{\mathrm{lex}}}(g_2) \rangle = \langle yz, xz \rangle$.
- Idea: check the element of I that can be produced from g_1, g_2 by "cancelling the initial monomials $\mathrm{in}_{\prec}(g_1), \mathrm{in}_{\prec}(g_2)$ each other".

- Write the least common multiple $\mathrm{lcm}(u, v)$ of two monomials $u = x_1^{a_1} \cdots x_n^{a_n}$ and $v = x_1^{b_1} \cdots x_n^{b_n}$ as

$$\mathrm{lcm}(u, v) = x_1^{c_1} \cdots x_n^{c_n}, \quad c_i = \max\{a_i, b_i\}, \ i = 1, \ldots, n.$$

- **Definition** The polynomial

$$S(f, g) = \frac{\mathrm{lcm}(\mathrm{in}_\prec(f), \mathrm{in}_\prec(g))}{c_f \cdot \mathrm{in}_\prec(f)} f - \frac{\mathrm{lcm}(\mathrm{in}_\prec(f), \mathrm{in}_\prec(g))}{c_g \cdot \mathrm{in}_\prec(g)} g$$

is called the S-polynomial of f and g with respect to $\prec$, where c_f, c_g are the coefficients of $\mathrm{in}_\prec(f), \mathrm{in}_\prec(g)$ in f, g, respectively.

- The S-polynomial of f and g is obtained by cancelling the initial monomials of f and g.
- Example: $g_1 = yz - x, g_2 = xz - y^2$

  Lexicographic order:

$$\mathrm{in}_{\prec_{\mathrm{lex}}}(g_1) = yz,\ \mathrm{in}_{\prec_{\mathrm{lex}}}(g_2) = xz,$$
$$S(g_1, g_2) = xg_1 - yg_2 = -x^2 + y^3$$

  Reverse lexicographic order:

$$\mathrm{in}_{\prec_{\mathrm{lex}}}(g_1) = yz,\ \mathrm{in}_{\prec_{\mathrm{lex}}}(g_2) = y^2,$$
$$S(g_1, g_2) = yg_1 + zg_2 = -xy + xz^2$$

  Pure lexicographic order:

$$\mathrm{in}_{\prec_{\mathrm{lex}}}(g_1) = x,\ \mathrm{in}_{\prec_{\mathrm{lex}}}(g_2) = xz,$$
$$S(g_1, g_2) = -zg_1 - g_2 = -yz^2 + y^2$$

- **Theorem (Buchberger criterion)**

  Fix a monomial order $\prec$ on M_n. Let I be an ideal of $K[x_1, \ldots, x_n]$ and $G = \{g_1, \ldots, g_s\}$ is a system of generators of I. Then G is a Gröber basis of I if and only if the following condition is satisfied:

  "For all $i \neq j$, the remainder of the standard form of $S(g_i, g_j)$ with respect to $g_1, \ldots, g_s$ is 0."

- Example:
  $g_1 = yz - x,\ g_2 = xz - y^2,\ I = \langle G \rangle \subset K[x, y, z], G = \{g_1, g_2\}$
  - Lexicographic order $\prec_{\text{lex}}$
    $S(g_1, g_2) = y^3 - x^2$ is a standard form w.r.t. G and is a remainder itself. Therefore G is not a Gröbner basis of I.
    Write $g_3 = y^3 - x^2$ and $G' = G \cup \{g_3\}$, then

$$S(g_1, g_3) = x^2 z - xy^2 = xg_2$$
$$S(g_2, g_3) = -y^2 g_3 + x^2 g_2 \qquad (*)$$

    are standard forms w.r.t. G' with 0 remainder. Therefore G' is a Gröbner basis of I w.r.t. $\prec_{\text{lex}}$.

- Reverse lexicographic order $\prec_{\text{rev}}$

  $S(g_1, g_2) = xz^2 - xy$ is a standard form w.r.t. G and is a remainder itself. Therefore G is not a Gröbner basis of I. Write $g_3 = xz^2 - xy$ and $G' = G \cup \{g_3\}$, then

$$S(g_1, g_3) = xy^2 - x^2z = -xg_2$$
$$S(g_2, g_3) = -xzg_3 - xyg_2 \qquad (*)$$

  are standard forms w.r.t. G' with 0 remainder. Therefore G' is a Gröbner basis of I w.r.t. $\prec_{\text{rev}}$.

- Pure lexicographic order $\prec_{\text{purelex}}$

  $S(g_1, g_2) = y^2 - yz^2$ is a standard form w.r.t. G and is a remainder itself. Therefore G is not a Gröbner basis of I. Write $g_3 = y^2 - yz^2$ and $G' = G \cup \{g_3\}$, then

$$S(g_1, g_3) = -y^3 z + xyz^2 = -yzg_3 - yz^2 g_1 \qquad (*)$$
$$S(g_2, g_3) = xyz^3 - y^4 = -y^2 g_3 + yz^2 g_2 \qquad (*)$$

  are standard forms w.r.t. G' with 0 remainder. Therefore G' is a Gröbner basis of I w.r.t. $\prec_{\text{purelex}}$.

- As we have seen, Buchberger criterion is not only a criterion, but supplies an element that is needed to be a Gröbner basis.

  Buchberger algorithm

  Fix a monomial order $\prec$. Let $I = \langle G \rangle = \langle g_1, \ldots, g_s \rangle$. If each S-polynomial $S(g_i, g_j)$ has a standard form with 0 remainder w.r.t. G, G is a Grb̈ner basis of I. Otherwise, if $S(g_i, g_j)$ has a standard form with nonzero remainder r_{s+1}, add r_{s+1} to G. Repeating this procedure, we can obtain a Gröbner basis after finite number of steps.

$$\left(\begin{array}{l} \text{The ``finiteness'' is important. This is from the fact} \\ \text{that the polynomial ring is Noetherian ring.} \end{array} \right)$$

- To perform the Buchberger algorithm, the following lemma is useful.

  Lemma

  Fix a monomial order $\prec$ on M_n. For $f, g \in K[x_1, \ldots, x_n]$, suppose $\mathrm{in}_\prec(f)$ and $\mathrm{in}_\prec(g)$ are relatively prime, i.e., $\mathrm{lcm}(\mathrm{in}_\prec(f), \mathrm{in}_\prec(g)) = \mathrm{in}_\prec(f) \cdot \mathrm{in}_\prec(g)$. Then there exists a standard form of $S(f, g)$ with 0 remainder w.r.t. f, g.

  (Therefore the calculation of S-polynomials $(*)$ are not needed in the previous Example in pages 56-58.)

- Now we back to Prob. 3.

  By the Buchberger algorithm, calculate the Gröbner basis of the ideal $I = \langle f_1, f_2, f_3 \rangle \subset K[x, y, z]$ for $\prec_{\text{purelex}}$, where

  $$f_1 = \underline{x^2} + y^2 + 4z^2 - 90,\ f_2 = \underline{x} - y + z - 12,\ f_3 = \underline{xz} - 3y - 2.$$

- Let $F = \{f_1, f_2, f_3\}$. Check $S(f_1, f_2), S(f_1, f_3), S(f_2, f_3)$.

$$\begin{aligned} S(f_2, f_3) &= zf_2 - f_3 \\ &= -yz + 3y + z^2 - 12z + 28. \end{aligned}$$

This is a standard form w.r.t. F and is a remainder itself. We add

$$f_4 = \underline{yz} - 3y - z^2 + 12z - 28$$

to F. We have $F = \{f_1, f_2, f_3, f_4\}$.

$$\begin{aligned} S(f_1, f_2) &= f_1 - xf_2 \\ &= xy - xz + 12x + y^2 + 4z^2 - 90 \\ &= (y - z + 12)f_2 - 2f_4 + 2y^2 + 18y + 3z^2 - 2. \end{aligned}$$

This is a standard form w.r.t. F. We add the remainder

$$f_5 = \underline{y^2} + 9y + \frac{3}{2}z^2 - 1$$

to F. We have $F = \{f_1, f_2, f_3, f_4, f_5\}$.

$$\begin{aligned} S(f_1, f_3) &= zf_1 - xf_3 \\ &= 3xy + 28x + y^2z + 4z^3 - 90z \\ &= (3y + 28)f_2 - 12f_4 + (z + 3)f_5 + y + 5z^3/2 \\ &\quad -33z^2/2 + 27z + 3. \end{aligned}$$

This is a standard form w.r.t. F. We add the remainder

$$f_6 = \underline{y} + \frac{5}{2}z^3 - \frac{33}{2}z^2 + 27z + 3$$

to F. We have $F = \{f_1, f_2, f_3, f_4, f_5, f_6\}$.

- Now we have

$$
\begin{aligned}
f_1 &= \underline{x^2} + y^2 + 4z^2 - 90, \\
f_2 &= \underline{x} - y + z - 12, \\
f_3 &= \underline{xz} - 3y - 2, \\
f_4 &= \underline{yz} - 3y - z^2 + 12z - 28, \\
f_5 &= \underline{y^2} + 9y + \tfrac{3}{2}z^2 - 1, \\
f_6 &= \underline{y} + \tfrac{5}{2}z^3 - \tfrac{33}{2}z^2 + 27z + 3.
\end{aligned}
$$

Checked: $S(f_1, f_2),\ S(f_1, f_3),\ S(f_2, f_3)$.

Check needed: $S(f_3, f_4),\ S(f_4, f_5),\ S(f_4, f_6),\ S(f_5, f_6)$.

$$\begin{aligned} S(f_3, f_4) &= yf_3 - zf_4 \\ &= xyz - 3y^2 - yz^2 + 3yz - 28y + z^3 - 12z^2 + 28z \\ &= (3y + 28)f_2 + (z - 12)f_3 + (x - z)f_4, \end{aligned}$$

$$\begin{aligned} S(f_4, f_5) &= yf_4 - zf_5 \\ &= -3y^2 - yz^2 + 3yz - 28y - 3z^3/2 + z \\ &= -zf_4 - 3f_5 - f_6. \end{aligned}$$

These are standard forms w.r.t. F with 0 remainder.

$$\begin{aligned} S(f_4, f_6) &= f_4 - zf_6 \\ &= -3y - 5z^4/2 + 33z^3/2 - 28z^2 + 9z - 28 \\ &= -3f_6 - 5z^4/2 + 24z^3 - 155z^2/2 + 90z - 19 \end{aligned}$$

This is a standard forms w.r.t. F. We add the remainder

$$f_8 = \underline{z^4} - \frac{48}{5}z^3 + 31z^2 - 36z + \frac{38}{5}$$

to F. We have $F = \{f_1, f_2, f_3, f_4, f_5, f_6, f_8\}$.

$$\begin{aligned} S(f_5, f_6) &= f_5 - y f_6 \\ &= -5yz^3/2 + 33yz^2/2 - 27yz + 6y + 3z^2/2 - 1 \\ &= (-5z^2/2 + 9z) f_4 + 6 f_6 - (5/2) f_8. \end{aligned}$$

This is a standard form w.r.t. F with 0 remainder.

- Now we have

$$
\begin{aligned}
f_1 &= \underline{x^2} + y^2 + 4z^2 - 90, \\
f_2 &= \underline{x} - y + z - 12, \\
f_3 &= \underline{xz} - 3y - 2, \\
f_4 &= \underline{yz} - 3y - z^2 + 12z - 28, \\
f_5 &= \underline{y^2} + 9y + \tfrac{3}{2}z^2 - 1, \\
f_6 &= \underline{y} + \tfrac{5}{2}z^3 - \tfrac{33}{2}z^2 + 27z + 3., \\
f_8 &= \underline{z^4} - \tfrac{48}{5}z^3 + 31z^2 - 36z + \tfrac{38}{5}
\end{aligned}
$$

Checked: $S(f_1, f_2),\ S(f_1, f_3),\ S(f_2, f_3),\ S(f_3, f_4),$
$S(f_4, f_5),\ S(f_4, f_6),\ S(f_5, f_6).$

Check needed: $S(f_3, f_8), S(f_4, f_8).$

$$
\begin{aligned}
S(f_3, f_8) &= z^3 f_3 - x f_8 \\
&= 48xz^3/5 - 31xz^2 + 36xz - 38x/5 - 3yz^3 - 28z^3 \\
&= -(38/5) f_2 + (48z^2/5 - 31z + 36) f_3 \\
&\quad + (-3z^2 + 99z/5 - 168/5) f_4 - (2/5) f_6 - 3 f_8.
\end{aligned}
$$

$$
\begin{aligned}
S(f_4, f_8) &= z^3 f_4 - y f_8 \\
&= 33yz^3/5 - 31yz^2 + 36yz - 38y/5 - z^5 + 12z^4 - 28z^3 \\
&= (33z^2/5 - 31z + 99z/5 - 57 + 297/5) f_4 \\
&\quad - (2/5) f_6 - (z - 9) f_8.
\end{aligned}
$$

These are standard forms w.r.t. F with 0 remainder.

Therefore $F = \{f_1, f_2, f_3, f_4, f_5, f_6, f_8\}$ is a Gröbner basis of I w.r.t. $\prec_{\text{purelex}}$ from the Buchberger criterion.

6. Elimination theory and solving simultaneous equations

- Prof. Hibi says, "Gröbner basis is a powerful technique for solving simultaneous equations".
- This is due to the elimination theory. It is a fascinating result which demonstrates the power of Gröbner bases.

- Recall that the Gröbner basis w.r.t. $\prec_{\mathrm{purelex}}$ of $I = \langle f_1, f_2, f_3 \rangle \subset \mathbb{Q}[x, y, z]$, where

  $$f_1 = x^2 + y^2 + 4z^2 - 90,\ f_2 = x - y + z - 12,\ f_3 = xz - 3y - 28$$

  includes a polynomial of z,

  $$5z^4 - 48z^3 + 155z^2 - 180z + 38,$$

  as an element.

- In fact, the Gröbner basis w.r.t. the pure lexicographic order is effective for solving simultaneous equations.

Proposition Let $I = \langle f_1, \ldots, f_r \rangle$ is an ideal of $K[x, y, z]$. If $I \cap K[z] \neq \langle 0 \rangle$, there is only one polynomial of $K[z]$ in the reduced Gröbner basis of I w.r.t. $\prec_{\text{purelex}}$ satisfying $x \succ_{\text{purelex}} y \succ_{\text{purelex}} z$, and is unique. Write this element be $g^* \in G \cap K[z]$, then $I \cap K[z] = \langle g^* \rangle$ holds.

- Note that $I \cap K[z]$ is the set of elements in I with the variable z. In other words, $I \cap K[z]$ is the set of polynomials that is derived from the simultaneous equation $f_1(x, y, z) = \cdots = f_r(x, y, z) = 0$ by eliminating x, y.
- $I \cap K[z]$ is an ideal of $K[z]$.

- We have seen that each ideal of one variable polynomial ring is a principal ideal, and the unique generator is the element with the minimum degree. (see page 32)
- Therefore this Proposition means that $g^* \in G \cap K[z]$ is the element of $I \cap K[z]$ with the minimum degree.
- In the previous example, we have

$$I \cap \mathbb{Q}[z] = \left\langle 5z^4 - 48z^3 + 155z^2 - 180z + 38 \right\rangle .$$

- Extending Proposition.
- Let $K[x_{i_1}, x_{i_2}, \ldots, x_{i_m}]$ be the set of the polynomials in $K[x_1, \ldots, x_n]$ with the variables $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$ $(1 \leq i_1 < i_2 < \cdots < i_m \leq n)$. This is a polynomial ring.
- A monomial order $\prec$ on $K[x_1, \ldots, x_n]$ naturally induce the monomial order $\prec'$ on $K[x_{i_1}, x_{i_2}, \ldots, x_{i_m}]$.

- **Theorem (The Elimination Theorem)**
  Let $\prec$ be a monomials order on $K[x_1, \ldots, x_n]$ and G a Gröbner basis of an ideal $I \subset K[x_1, \ldots, x_n]$ w.r.t. $\prec$. Suppose that

  $$g \in G,\ \mathrm{in}_{\prec}(g) \in K[x_{i_1}, x_{i_2}, \ldots, x_{i_m}] \ \Rightarrow\ g \in K[x_{i_1}, x_{i_2}, \ldots, x_{i_m}]$$

  holds. Then $G \cap K[x_{i_1}, x_{i_2}, \ldots, x_{i_m}]$ is a Gröbner basis of $I \cap K[x_{i_1}, x_{i_2}, \ldots, x_{i_m}]$ w.r.t. $\prec'$.

- The pure lexicographic order satisfies this condition.

- In the previous example, we have the Gröbner basis $G = \{g_1, g_2, g_3\}$,

$$\begin{aligned} g_1 &= 5z^4 - 48z^3 + 155z^2 - 180z + 38, \\ g_2 &= 2y + 5z^3 - 33z^2 + 54z + 6, \\ g_3 &= 2x + 5z^3 - 33z^2 + 56z - 18, \end{aligned}$$

  of $I = \langle g_1, g_2, g_3 \rangle$ w.r.t. $\prec_{\text{purelex}}$.

  From the elimination theorem,

  - $\{g_1\}$ is a Gröbner basis of $I \cap K[z]$,
  - $\{g_1, g_2\}$ is a Gröbner basis of $I \cap K[y, z]$ w.r.t. $y \succ_{\text{purelex}} z$.

- Solving equation $f_1 = \cdots = f_r = 0$ by the elimination theorem

  1. Calculate the reduced Gröbner basis G of $I = \langle f_1, \ldots, f_r \rangle$ w.r.t. $x_1 \succ_{\text{purelex}} x_2 \succ_{\text{purelex}} \cdots \succ_{\text{purelex}} x_n$.
  2. If $G \cap K[x_n] \neq \emptyset$, this is the reduced Gröbner basis of $I \cap K[x_n]$. Solve it for x_n.
  3. If $G \cap K[x_{n-1}, x_n] \neq \emptyset$, this is the reduced Gröbner basis of $I \cap K[x_{n-1}, x_n]$. Substitute x_n and solve it for x_{n-1}.
  4. Similarly, obtain $x_{n-2}, x_{n-3}, \ldots, x_1$ in order.