Innovationinfo Journal of Multidisciplinary Research and Reviews

J Multidis Res Rev 2019
Volume 1: 2

Computational Algebraic Geometry and Quantum Mechanics: An Initiative toward Post Contemporary Quantum Chemistry

Akihito Kikuchi*
Ichio Kikuchi

Independent Researcher, Member of International Research Center for Quantum Technology, Tokyo, Japan

Abstract

A new framework in quantum chemistry has been proposed recently ("An approach to first principles electronic structure calculation by symbolic-numeric computation" by A. Kikuchi). It is based on the modern technique of computational algebraic geometry, viz. the symbolic computation of polynomial systems. Although this framework belongs to molecular orbital theory, it fully adopts the symbolic method. The analytic integrals in the secular equations are approximated by the polynomials. The indeterminate variables of polynomials represent the wave-functions and other parameters for the optimization, such as atomic positions and contraction coefficients of atomic orbitals. Then the symbolic computation digests and decomposes the polynomials into a tame form of the set of equations, to which numerical computations are easily applied. The key technique is Gröbner basis theory, by which one can investigate the electronic structure by unraveling the entangled relations of the involved variables. In this article, at first, we demonstrate the featured result of this new theory. Next, we expound the mathematical basics concerning computational algebraic geometry, which are necessitated in our study. We will see how highly abstract ideas of polynomial algebra would be applied to the solution of the definite problems in quantum mechanics. We solve simple problems in "quantum chemistry in algebraic variety" by means of algebraic approach. Finally, we review several topics related to polynomial computation, whereby we shall have an outlook for the future direction of the research.

Keywords: Quantum mechanics, Algebraic geometry, Commutative algebra, Grönber basis, Primary ideal decomposition, Eigenvalue problem in quantum mechanics, Molecular orbital theory; Quantum chemistry, Quantum chemistry in algebraic variety, First principles electronic structure calculation, Symbolic computation, symbolic-numeric solving, Hartree-Fock theory, Taylor series, Polynomial approximation, Algebraic molecular orbital theory.

Introduction

Dear Readers,

If you are researchers or students with the expertise of physics or chemistry, you might have heard of "algebraic geometry" or "commutative algebra". Maybe you might have heard only of these words, and you might not have definite ideas about them, because these topics are taught in the department of mathematics, not in those of physics and chemistry. You might have heard of advanced regions of theoretical physics, such as super-string theory, matrix model, etc., where the researchers are seeking the secret of the universe by means of esoteric theories of mathematics with the motto *algebraic geometry and quantum mechanics*. And you might be desperate in imagining the required endurance to arrive at the foremost front of the study... However, algebraic geometry is originated from rather a primitive region of mathematics. In fact, it is an extension

Article Information

Article Type: Review
Article Number: JMRR118
Received Date: 30 September, 2019
Accepted Date: 18 October, 2019
Published Date: 25 October, 2019

***Corresponding Author:** Akihito Kikuchi, Independent Researcher, Member of International Research Center for Quantum Technology, 2-17-7 Yaguchi, Ota-ku, Tokyo, Japan. Tel: +81-3-3759-6810; Email: akihito_kikuchi(at)gakushikai.jp

Citation: Kikuchi A, Kikuchi I (2019) Computational Algebraic Geometry and Quantum Mechanics: An Initiative toward Post Contemporary Quantum Chemistry. J Multidis Res Rev Vol: 1, Issu: 2 (47-79).

of analytic geometry which you must have learned in high-schools. According to Encyclopedia Britannica, the definition of the word goes as follows:

algebraic geometry, study of the geometric properties of solutions of polynomial equations, including solutions in three dimensions beyond three...

It simply asserts that algebraic geometry is the study of polynomial systems. And polynomial is ubiquitous in every branch of physics. If you attend the lecture of elementary quantum mechanics, or you study quantum chemistry, you always encounter secular equations in order to compute the energy spectrum. Such equations are actually given by the polynomial systems, although you solve them through linear algebra. Indeed, linear algebra is so powerful that you have almost forgotten that you are laboring with polynomial algebraic equations.

Be courageous! Let us have a small tour in the sea of QUANTUM MECHANICS with the chart of ALGEBRAIC GEOMETRY. Your voyage shall never be in stormy and misty *mare incognitum*. Having chartered a cruise ship, the "COMMUTATIVE ALGEBRA", we sail from a celebrated seaport named "MOLECULAR ORBITAL THEORY".

The molecular orbital theory [1] in the electronic structure computation of quantum chemistry is computed by the solution of the secular equation, if one adopts the localized atomic orbital basis $\{\phi_i\}$ defined on the set of atoms at the positions $\{R_i\}$ with other optimizable variables $\{\zeta_i\}$:

$$\mathrm{H}\left(\{R_i\},\{\zeta_j\}\right)\cdot\Psi = E\,\mathrm{S}\left(\{R_i\},\{\zeta_j\}\right)\cdot\Psi,$$

in which the matrix elements are defined by

$$\mathrm{S}_{ij} = \int dr\,\phi_i\,\phi_j.$$

and

$$\mathrm{S}_{ij} = \int dr\,\phi_i\,\phi_j.$$

In these expressions, $\mathcal{H}$ is the Hamiltonian; the vector Ψ represents the coefficients in LCAO wave-function $\Psi = \sum \chi_i \phi_i$; E is the energy spectrum. The Fock matrix H and the overlap matrix S are, in theory, computed symbolically and represented by the analytic formulas with respect to the atomic coordinates and other parameters included in the Gaussian- or Slater- type localized atomic basis; they are, in practice, given numerically and the equation is solved by means of linear algebra. In contrast to this practice, it is demonstrated by Kikuchi [2] that there is a possibility of symbolic-numeric computation of molecular orbital theory, which can go without linear algebra: the secular equation is given by the analytic form and approximated by the polynomial system, which is processed by the computational algebraic geometry. The symbolic computation reconstructs and decomposes the polynomial equations into a more tractable and simpler form, by which the numerical solution of the polynomial equation is applied for the purpose of obtaining the quantum eigenstates. The key technique is the Gröbner basis theory and triangulation of polynomial set. Let us review the exemplary computation of hydrogen molecule in [2].

Let ϕ_i, Z_a, R_a be the wavefunctions, the atomic charges, and the atomic positions. The total energy functional of Hartree-Fock theory is given by

$$\Omega = \sum_i \int dr\,\phi_i(r)\left(-\frac{\Delta^2}{2} + \sum_a \frac{Z_a}{|r-R_a|}\right)\phi_i(r)$$

$$+\frac{1}{2}\sum_{i,j}\int dr\,dr'\,\frac{\phi_i(r)\phi_i(r)\phi_j(\mathrm{r}')\phi_j(\mathrm{r}')}{|r-r'|}$$

$$-\frac{1}{2}\sum_{i,j}\int dr\,dr'\,\frac{\phi_i(r)\phi_j(r)\phi_j(\mathrm{r}')\phi_i(\mathrm{r}')}{|r-r'|}$$

$$+\sum_{a,b}\frac{Z_a Z_b}{|R_a - R_b|}$$

$$-\sum_{i,j}\lambda_{i,j}\left(\int dr\,\phi_i(r)\phi_j(r) - \delta_{i,j}\right)$$

The secular equation is derived from the stationary condition with respect to the wave-function

$$\frac{\delta\Omega}{\delta\phi_i} = 0.$$

The energy minimum with respect to the atomic coordinate gives the stable structure:

$$\frac{\delta\Omega}{\delta R_j} = 0.$$

Let us consider the simple hydrogen, as in Figure 1.

Assume that the two hydrogen atoms are placed at R_A and R_B. By the simplest model, we can choose the trial wave-functions for up-and down-spin at the point $z \in \mathbb{R}^3$ as follows:

$$\phi_{\mathrm{up}}(z) = \frac{1}{\sqrt{\pi}}\left(a\exp(-z_A) + b\exp(-z_B)\right)$$

$$\phi_{\mathrm{down}}(z) = \frac{1}{\sqrt{\pi}}\left(c\exp(-z_A) + d\exp(-z_B)\right)$$

Where

$$z_{A/B} = |z - R_{A/B}|$$

and a,b,c,d are the real variables to be determined. Let *ev* and *ew* to be Lagrange multipliers λ_{ij} for ϕ_{up} and ϕ_{down}. Since these two wave-functions are orthogonal in nature, due to

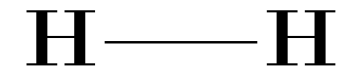

Figure 1: The image of a hydrogen molecule, composed of two atoms.

the difference of spin, we assume that the multipliers are diagonal: $\lambda_{ij}=0$ for $i\neq j$.

From these expressions, all of the integrals involved in the energy functional are analytically computed. (As for the analytic forms of the integrals, see the supplement of [2].) Then, with respect to inter-atomic distance R_{AB}, Taylor expansion of the energy functional is computed up to degree four, at the center of $R_{AB}=7/5$. The polynomial approximation is given by

OMEGA = (3571 - 1580*a^2 - 3075*a*b - 1580*b^2 - 1580*c^2

+ 625*a^2*c^2 + 1243*a*b*c^2 + 620*b^2*c^2 - 3075*c*d

+ 1243*a^2*c*d + 2506*a*b*c*d + 1243*b^2*c*d - 1580*d^2

.....

.....

.....

- 86*a*b*c*d*r^4 - 17*b^2*c*d*r^4 + 12*d^2*r^4 - 4*a^2*d^2*r^4

-17*a*b*d^2*r^4+13*a*b*ev*r^4+13*c*d*ew*r^4)/1000

where the inter-atomic distance R_{AB} is represented by r (for the convenience of polynomial processing).

The equations used in the study are quite lengthy, so we only show the part of them. We give the exact ones in the appendix (supplementary material): the energy functional in Appendix A; the secular equations in Appendix B; the Gröbner bases in Appendix C; the triangulation in Appendix D.

In order to reduce the computational cost, the numerical coefficients are represented by the fraction, by the truncation of decimal numbers. We make the change of variables from a,b,c,d to s,t,u,v in the following way:

$$a=t+s, b=t-s, c=u+v, d=u-v$$

Consequently, the wave-functions are represented by the sum of symmetric and anti-symmetric parts:

$$\phi_{\text{up}}(z)=\frac{t}{\sqrt{\pi}}\left(\exp(-z_A)+\exp(-z_B)\right)$$

$$+\frac{s}{\sqrt{\pi}}\left(\exp(-z_A)-\exp(-z_B)\right)$$

$$\phi_{\text{down}}(z)=\frac{u}{\sqrt{\pi}}\left(\exp(-z_A)+\exp(-z_B)\right)$$

$$+\frac{v}{\sqrt{\pi}}\left(\exp(-z_A)-\exp(-z_B)\right)$$

The stationary conditions $\frac{\delta\Omega}{\delta a}$, $\frac{\delta\Omega}{\delta c}$, $\frac{\delta\Omega}{\delta c}$, $\frac{\delta\Omega}{\delta d}$, with respect to *t, s, u, v*, yields those equations:

S[1]32*s*u*v*r^4-336*s*u*v*r^3+992*s*u*v*r^2-160*s*u*v*r

.....

+126*t*r^4-882*t*r^3+1748*t*r^2+1896*t*r-12470*t=0

S[2]156*s*u^2*r^4-1068*s*u^2*r^3+2248*s*u^2*r^2-80*s*u^2*r

.....

+992*t*u*v*r^2-160*t*u*v*r+40*t*u*v=0

S[3]156*s^2*u*r^4-1068*s^2*u*r^3+2248*s^2*u*r^2-80*s^2*u*r

.....

+126*u*r^4-882*u*r^3+1748*u*r^2+1896*u*r-12470*u=0

S[4]-52*s^2*v*r^4+236*s^2*v*r^3-32*s^2*v*r^2-104*s^2*v*r

.....

-30*v*r^4+330*v*r^3-1148*v*r^2+760*v*r-170*v=0

The stationary conditions $\frac{\delta\Omega}{\delta ev}$, $\frac{\delta\Omega}{\delta ew}$, with respect to ev, ew, are the normalization condition for the wave-functions. They yield two equations:

S[5]-13*s^2*r^4+139*s^2*r^3-458*s^2*r^2+63*s^2*r

.....

-63*t^2*r-3986*t^2+1000=0

S[6]13*u^2*r^4-139*u^2*r^3+458*u^2*r^2-63*u^2*r

.....

+63*v^2*r-14*v^2+1000=0

The stable condition for the molecular geometry $\frac{\delta\Omega}{\delta r}$ yields this:

312*s^2*u^2*r^3-1602*s^2*u^2*r^2+2248*s^2*u^2*r

.....

.....

+380*v^2+740*r^3-3903*r^2+7288*r-5102=0

For simplicity, however, we replace the last equation with a simple one (of the fixed inter-atomic distance) as follows:

S[7] 5*r-7=0.

It fixes the inter-atomic distance at 1.4.

By processing polynomials S[1],...,S[7], We obtain 18 polynomials in the Grönber basis J[1],...,J[18]. We only show the skeletons of them, because the coefficients are too lengthy. The exact form is given in the appendix.

J[1]=r-1.4

J[2]=(...)*ew^6+(...)*ew^5+(...)*ew^4

+(...)*ew^3+(...)*ew^2+(...)*ew+(...)

J[3]=(...)*ev+(...)*ew^5+(...)*ew^4+(...)*ew^3

-(...)*ew^2-(...)*ew+(...)

J[4]=(...)*v*ew^4+(...)*v*ew^3+(...)*v*ew^2

-(...)*v*ew-(...)*v

J[5]=(...)*v^2-(...)*ew^5-(...)*ew^4-(...)*ew^3
-(...)*ew^2+(...)*ew-(...)
J[6]=(...)*u*ew^4+(...)*u*ew^3+(...)*u*ew^2
+(...)*u*ew+(...)*u
J[7]=(...)*u*v*ew^2+(...)*u*v*ew+(...)*u*v
J[8]=(...)*u^2+(...)*ew^5+(...)*ew^4+(...)*ew^3
+(...)*ew^2-(...)*ew-(...)
J[9]=(...)*t*ew^4+(...)*t*ew^3+(...)*t*ew^2
+(...)*t*ew+(...)*t
J[10]=(...)*t*v*ew^3+(...)*t*v*ew^2+(...)*t*v*ew+(...)*t*v
J[11]=(...)*t*u*ew^3+(...)*t*u*ew^2+(...)*t*u*ew+(...)*t*u
J[12]=(...)*t^2-(...)*ew^5-(...)*ew^4-(...)*ew^3
+(...)*ew^2+(...)*ew-(...)
J[13]=(...)*s*ew^2+(...)*s*ew-(...)
*s-(...)*t*u*v*ew-(...)*t*u*v
J[14]=(...)*s*v*ew-(...)*s*v-t*u*ew^2-(...)*t*u*ew-(...)*t*u
J[15]=(...)*s*u*ew+(...)*s*u+(...)*t*v*ew^2
+(...)*t*v*ew+(...)*t*v
J[16]=(...)*s*u*v+(...)*t*ew^3+(...)*t*ew^2
+(...)*t*ew+(...)*t
J[17]=(...)*s*t-(...)*u*v*ew-(...)*u*v
J[18]=(...)*s^2+(...)*ew^5+(...)*ew^4+(...)*ew^3
-(...)*ew^2-(...)*ew-(...)

The triangular decomposition to the Gröbner basis is computed, which contains five decomposed sets of equations T[1],..., T[5]. Here the only the skeleton is presented, while the details are given in the appendix. Observe that one decomposed set includes seven entries; from the first entry to the last, the seven variables are added one by one, with the order of r, ew, ev, v, u, t, s, in the arrangement of a triangle. Now we can solve the equation by determining the unknown variables one by one. As a result, the triangular decomposition yields four subsets of the solutions of equations: the possible electronic configurations are exhausted, as is shown in Table 1.

T[1]:
_[1]=r-1.4
_[2]=(...)*ew+(...)
_[3]=(...)*ev+(...)
_[4]=v
_[5]=(...)*u^2-(...)
_[6]=t
_[7]=(...)*s^2-(...)
T[2]:
_[1]=r-1.4
_[2]=ew-(...)
_[3]=ev-(...)
_[4]=v^2-(...)
_[5]=u
_[6]=t
_[7]=(...)*s^2-(...)
T[3]:
_[1]=r-1.4
_[2]=ew^2+(...)*ew+(...)
_[3]=ev-ew
_[4]=v^2-(...)*ew-(...)
_[5]=u^2+(...)*ew+(...)
_[6]=t^2+(...)*ew+(...)
_[7]=s+(...)*t*u*v*ew+(...)*t*u*v
T[4]:
_[1]=r-1.4
_[2]=ew+(...)
_[3]=ev+(...)
_[4]=v
_[5]=u^2-(...)
_[6]=t^2-(...)
_[7]=s
T[5]:
_[1]=r-1.4
_[2]=ew+(...)
_[3]=ev+(...)
_[4]=v^2-(...)
_[5]=u
_[6]=t^2-(...)
_[7]=s

Table 1: This table shows the solutions for the secular equation after the triangulation. The electron 1 and 2 lie in the up- and down- spin respectively; and the result exhausts the possible four congurations of the ground and the excited states.

	Solution 1	Solution 2	Solution 3	Solution 4
t	-0.53391	0.00000	-0.53391	0.00000
s	0.00000	-1.42566	0.00000	-1.42566
u	-0.53391	-0.53391	0.00000	0.00000
v	0.00000	0.00000	-1.42566	-1.42566
ev	-0.62075	-0.01567	-0.62734	0.01884
ew	-0.62075	-0.62734	-0.01567	0.01884
r	1.40000	1.40000	1.40000	1.40000
The total energy	-1.09624	-0.49115	-0.49115	0.15503
electron 1	symmetric	asymmetric	symmetric	asymmetric
electron 2	symmetric	symmetric	asymmetric	asymmetric

This is one of the featured results in [2]. The author of that work had demonstrated the procedure of the computation in a factual way, but he had not explained the underlying mathematical theory so minutely. Consequently, it is beneficial for us to grasp some prerequisites of commutative algebra and algebraic geometry because these theories are still strange to a greater part of physicists and chemists. In the following sections, we review concepts of commutative algebra and algebraic geometry, which are utilized in this sort of computation. Next, we learn about Grönbner bases. We will find that the "primary ideal decomposition" in commutative algebra surrogate the eigenvalue problem of linear algebra. Then we apply our knowledge to solve simple problems of molecular orbital theory from the standpoint of polynomial algebra. In the end, we take a look at the related topics which shall enrich the molecular orbital theory with a taste of polynomial algebra, such as "polynomial optimization" and "quantifier elimination". The employment of these methods will show the course of future studies.

Basics of Commutative Algebra and Algebraic Geometry

Our handy tool is polynomial and our chief concern is how to solve the set of polynomial equations. Such topics are the themes of commutative algebra. If we would like to do with geometrical view, the task lies also in algebraic geometry. From this reason, in this section, we shall review mathematical definitions and examples related to the theory of polynomials.

N. B.: The readers should keep in mind that the chosen topics are mere "thumbnails" to the concepts of profound mathematics. As for proofs, the readers should study from more rigorous sources; for instance, for commutative algebra, the book by Eisenbud [3] or the Book by Reid [4]; for algebraic geometry, the book by Perrin [5], for Gröbner bases, the works by Cox, Little, and O'Shea [6,7], the book by Becker and Weispfenning [8], or the book by Ene and and Herzog [9].

Polynomial and ring

A polynomial should be defined in a ring. A ring is composed by the coefficie (in some field) and the indeterminate variables. Let K be the coefficient field. The polynomial ring $S = K[x_1, x_2, ..., x_n]$ is the K-vector space, with the basis elements (monomials) of the form

$$x_1^{c_1} x_2^{c_2} ....x_n^{c_n} (= \mathrm{X}^c)$$

with $c_i \in \mathbb{N}$. The polynomial is represented by $f = \sum C_a X^a$ and we use the notation sup $(f) = \{X^a C_a \neq 0\}$. We define the degree of a monomial $\mathrm{X}^C = x_1^{c_1} x_2^{c_2} ....x_n^{c_n}$ by

$$\left|\mathrm{X}^C\right| = \sum_{i=1}^{n} c_i$$

The degree of polynomial is given by

$$\deg(f) = \max\{\left|\mathrm{X}^C\right| : \mathrm{X}^c \in \mathrm{supp}(f)\}$$

A homogeneous polynomial is a polynomial, in which every non-zero monomial has the same degree.

Example 4.1

$x^3 + x^2 y + x y^2 + y^3$ is a homogeneous polynomial of degree 3.

$x^3 + x^2 y + z^2$ is not homogeneous.

Example 4.2 (Homogenization) A non-homogeneous polynomial $P(x_1, ..., x_n)$ is homogenized by means of an additional variable x_0.

For $P(x, y, z) = x^3 + x^2 y + z^2$,

Ideal

Definition 4.1 An ideal I in the polynomial ring S is the set of polynomials, which is closed under these operation:

$i_1 \in I$ and $i_2 \in I$ then $i_1 + i_2 \in I$

$i_1 \in I$ and $\alpha \in S$ then $\alpha \cdot i \in I$.

We usually denote an ideal by the generators, such as $I = (x, y)$ or $J = (x^2 + y^2, xy)$.

The sum and the product of the ideals are defined by

$$I + J = \{f + g : f \in I \text{ and } g \in J\}$$

$$IJ = \{f.g : f \in I \text{ and } g \in J\}$$

The ideal quotient is defined to be the ideal

$$I : J = \{f \in S : f : g \in I \text{ for all } g \in J\}$$

For two ideals *I* and *m*, the saturation is defined by

$$I : m^{\infty} = \sum_{i=1}^{\infty} I : m^i \cdot$$

(Observe that $I : m^i \subset I : m$ for $I < j$. In many cases, we do not have to consider the union of infinite number of ideal quotients, as the extension by union with $I : m^i$ shall "saturates" and stop to grow at some finite *i*, if the ring is Noetherian, as will be discussed later.)

The radical of an ideal *I* is defined by

$$\sqrt{I} = \{f \in S : f^k \in I \text{ for some integer k} > 0\}$$

Affine algebraic set (Affine algebraic variety)

Definition 4.2. Let *S* be the subset of a ring $k[x_1, ..., x_n]$. We denote the common zeros of polynomials $P(x, ... x)$ in *S* by

$$V(S) = \{x \in k^n \mid \forall P(x_1, ..., x_n) \in S \text{ such that } P(x) = 0\}$$

We call $V(S)$ the affine algebraic set (or affine variety) defined by *S*

Example 4.3 In $\mathbb{C}[X, Y]$, $V(X^2 + Y^2) = \{X = \pm\sqrt{-1}\, Y\}$.

Example 4.4 In $\mathbb{R}[X, Y]$, $V(X^2 + Y^2) = X = Y = 0$.

Example 4.5 In $k[x_1, x_2, ..., x_n]$, $V(\{1\}) = \varnothing$.

Example 4.6 In $k[x_1, x_2, ..., x_n]$, $V(\{0\}) = k^n$.

Also, these properties of the affine algebraic set are notable.

If $A \subset B$, $V(B) \subset V(A)$.

A point $a = (a_1, ..., a_n)$ is an affine algebraic set: $V(a) = (x - a_1, ..., x - a_n)$

If then $I = (f_1, f_2, ..., f_n)$

$V(I) = V(f_1) \cap ... \cap V(f_n)$

- The intersection of affine algebraic sets is also an affine algebraic set:

$\bigcap_j V(S_j) = V\left(\bigcap_i S_j\right)$

Or

$V(I) \cup V(J) = V(IJ) = V(I \cap J)$.

- The finite union of affine algebraic sets is also an affine algebraic set:

$V(I) \cup V(J) = V(IJ) = V(I \cap J)$.

The interpretation of the saturation $I : J^\infty$ in algebraic geometry is this: the saturation is the closure (in the sense of topology) of the complement of $V(J)$ in $V(I)$.

Definition 4.3 Let V be a subset of k^n (where *K* is an arbitrary field). The *ideal* of V is defined as

$$I(V) = \{ f \in k[\chi_1, ..., \chi_n] \mid \forall \chi \in V, f(\chi) = 0 \}$$

In other words, $I(V)$ is the set of polynomial functions which vanish on V.

Example 4.7 $I(\varnothing) = k[X_1, ..., X_n]$.

Example 4.8 For the ideal

$$I = \left(\left(x^2 - y^3 \right) x^2 \right),$$

the saturation is given by

$$I : (x)^\infty = \left(x^2 - y^3 \right).$$

$x^2 = y^3$ is the composure of the curve $x^2 = y^3$ and the doubled line $x = 0$. The saturation $I : (x)^\infty$ removes the line $x = 0$ from that composure; the point $(x, y) = (0, 0)$ (which lies on $x = 0$), however, is not removed, because the saturation is the closure.

The ideal of an affine algebraic set of a ideal *I*, denoted by $I(V(J))$, is computable.

Example 4.9 For $J = (Y^2, Y^2) \subset \mathbb{R}[X, Y]$, $V(J) = \{(0,0)\}$ and $I(V(J)) = (X, Y)$. Observe that the $I(V(J)) \neq J$. This is the consequence of the famous theorem of Hilbert (Nullstellensatz), which we will learn later.

Residue class ring or quotient ring

We can define "residue class rings". Let $I \subset R$ be an ideal in a ring *R*, and f is an element in *R*. The set $f + I = \{ f + h : h \in I \}$ is "the residue class of *f* modulo *I*"; *f* is a representative of the residue class $f + I$. We denote the set of residue classes modulo I by R / I. It also has the ring structure through addition and multiplication.

Several resources use the term "quotient ring" or "factor ring" for the same mathematical object.

In general, an ideal depicts geometric objects, which might be discrete points or might be connected and lie in several dimensions. They are represented by the residue class ring:

$$k[x_1, x_2, ..., x_n] / I .$$

Let us see several examples.

$$\mathbb{Q}[x] / \left(x^2 - 2 \right).$$

Example 4.10 The elements in the ring $R[x]$ are the polynomial $f(x) = a_0 + a_1 x + \cdots a_n x^n$. We divide $f(x)$ by $x^2 - 2$, so that

$$f(x) = b_0 + b_1 x + g(x) \cdot \left(x^2 - 2 \right)$$

The residue $b_0 + b_1 x$ is the representative of $f(x)$ when it is mapped into the residue class ring. We might assume that $\overline{x}$ (the representative of x in the residue class ring) would not be an undetermined variable, but a certain number α (outside of $\mathbb{Q}$) such that $\alpha^2 = 2$.

Example 4.11 $\mathbb{R}[x, y] / \left(x^2 + y^2 - 1 \right)$.

We assume that the representatives $\overline{x}$ and $\overline{y}$ of x and y in the residue class ring would not be undetermined variables, but a pair of numbers α and β such that $\alpha^2 + \beta^2 = 1$, and that $(\overline{x}, \overline{y})$ depicts a unit circle, as a one-dimensional geometric object in $\mathbb{R}^2$.

Example 4.12

$$\mathbb{R}[x, y] / \left(x^2 + y^2 - 1, x - y \right)$$

The representative $\overline{x}$ and $\overline{y}$ of x and y are considered to the points or $(1/\sqrt{2}, 1/\sqrt{2})$ (which lie in the intersection of $x^2 + y^2 = 1$ and $x = y$). This example is a simplest case of zero-dimensional ideal.

Prime and primary ideal

There are two fundamental types of ideal: prime ideal and primary ideal.

Definition 4.4 An ideal I ($\subset R$) is prime, if $xy \in I$, and, if $xy \in I$, then $x \in I$ or $y \in I$.

Definition 4.5 An ideal I is primary, if $I \neq R$, and, if $xy \in I$, then $x \in I$ or $y^n \in I$ for some $n > 0$; that is to say, every zero divisor of R / I is nil-potent.

Example 2.13 $(x) \subset \mathbb{R}[x]$ is a prime ideal.

Example 4.14 P=$\left(x^2, xy, y^2 \right) \subset \mathbb{R}[x, y]$ is a primary ideal: x and are zero R/P divisors in R / P; $x^2 \in P$ and $y^2 \in p$.

Example 4.15 Every prime ideal p is primary.

In the affine algebraic set, these two properties are equivalent.

Ideal I is a prime ideal.

$V(I)$ is irreducible.

The correspondence between variety and ideal

In order to unify the algebraic and geometric views, let us review the correspondence between varieties and ideals.

There are correspondences:

$\{\text{Ideals of } k[x_1,\ldots,x_n]\} \underline{v} \{\text{Subsets } X \text{ of } k^n\}$ {Ideals of k[x1,...,xn]}

and

$$\{\text{Subsets } X \text{ of } k^n\} \underline{i} \{\text{Ideals of } k[x_1,\ldots,x_n]\}$$

Where, the ideal $I(X)$ and the variety $V(J)$ are defined in the previous sections.

Also there are one-to-one correspondences:

$$\begin{array}{ccc} \{\text{Radical ideals of } k[x_1,\ldots,x_n]\} & \leftrightarrow & \{\text{Varieties } X \subset k^n\} \\ \cup & & \cup \\ \{\text{Prime ideals of } k[x_1,\ldots,x_n]\} & \leftrightarrow & \{\text{Irreducible varieties } X \subset k^n\}. \end{array}$$

Example 4.16 For the ideal $I=(x^2)\subset\mathbb{R}[x]$, $\sqrt{J}=(x)$. We have $V(I)=V(\sqrt{I})$.

Example 4.17 For the non-prime ideal $I=(xy)\subset\mathbb{R}[x]$, $V(I)=V(x)\cup V(y)$.

When we compute or analyze $V(I)$ for an ideal I, it might be convenient for us to work with $V(\sqrt{I})$ or its irreducible component $V(p_i)$ because the defining ideal would be simpler. The principle of "divide and conquer" is equally effective in symbolic computation.

Noetherian ring

Definition 4.6 A ring is Noetherian when it is finitely generated.

This means that there is no infinite ascending sequence of ideals: if there is an ascending sequence of ideals, such that

$$I_1 \subseteq \ldots \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq \ldots$$

it terminates somewhere in the following sense:

$$I_n = I_{n+1} = \cdots.$$

Example 4.18 $\mathbb{R}[x_1,x_2,\ldots,x_n]$ and $\mathbb{C}[x_1,x_2,\ldots,x_n]$ are Noeterian rings. If there is a computational process in these rings which would create the ascending sequence of ideals, it must terminate after finite number of steps.

Example 4.19 If R is a Noetherian ring, then $R[X]$ is Noetherian (as the consequence of the Hilbert basis theorem) [3]. By induction, $R[X_1,\ldots,X_n]$ is also a Noetherian ring.

Example 4.20 The power series ring $R[[x]]$ is a Noetherian ring.

Example 4.21 If R is a Noetherian ring and I is a two-sided ideal (such that for $a\in R$, $aI\subset I$ and $Ia\subset I$), then the residue class ring is R/I also Noetherian. In other words, the image of a surjective ring homomorphism of a Noetherian ring is Noetherian.

Dimension and Krull dimension

Let X be a topological space. The dimension of X is the maximum of the lengths of the chains of irreducible closed subsets of X. The chain is the relation of inclusion as this:

$$X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X_n$$

We have seen that for a prime ideal P, the affine algebraic set $V(P)$ is an irreducible closed subset. Hence we define a kind of dimension related to prime ideals. For a prime ideal p, we can construct the chain of prime ideals with length n of the form

$$p_0 \subsetneq p_1 \subsetneq \ldots \subsetneq p_n = p\,.$$

with prime ideals p_0 ,..., p_n. The chain is not necessarily unique, and we denote the maximum of the length of chains by height (p). The Krull dimension of a ring A is the maximal length of the possible chains of prime ideals in A. We denote it by $\dim_k$(A)

Recall that for two prime ideals such that $p\subset q$, $V(p)\supset V(q)$; the inclusion is reversed.

Example 4.22 We have $\dim_k$ R[x_1,x_2,...,x_n]=n, because the maximal chain of primes ideals is given by

$$(0)\subset(x_1)\subset(x_1,x_2)\subset\ldots\subset(x_1,x_2,\ldots,x_n).$$

One often refers to the Krull dimension of the residue class ring R/I by "dimension of the ideal I". The smallest prime ideal p_0 ideal is I itself (when I is prime) or a minimal p_0 including I (as one might study a non-prime ideal I), and the dimension counting ascends from p_0 as the start-point.

Example 4.23 Consider $I=(xy)$ in $R=\mathbb{R}[x,y]$. This ideal is not prime. In order to count the dimension of the ideal I, the chain of primes is given by $(x)\subset(x,y)$ or $(y)\subset(x,y)$, since (x) and (y) are the minimal prime ideals over (xy). Hence $\mathbb{R}[x_1,x_2,\ldots,x_n]$.

Example 4.24 Let f be a polynomial in the ring S of dimension n, (say, $\mathbb{R}[x_1,x_2,\ldots,x_n]$). We assume that f is not the zero divisor, i.e. there is no element $g\in S$ such that $g\cdot f=0$ and that it is not invertible, namely, there is no element $g\in S$ such that $g\cdot f=1$. Then $R/(f)$ has dimension n-1. A simple example is $\mathbb{R}[x,y]/(x-y)$, which is the line defined by the equation $y=x$.

These examples seem to be trivial but demand us a certain amount of technical proof to show the validity of the statements. (See the argument in [5].)

Zero-dimensional ideal

As we have seen, an ideal I in a ring $R[x_1,x_2,\ldots,x_n]$ is defined by the set of polynomials. The points $(x_1,x_2,\ldots,x_n)\in R$, which are the zero of the generating polynomials, determine the affine algebraic set $V(I)$. If the affine algebraic set $V(I)$ is a discrete set, the ideal I is said to be "zero-dimensional". If we have to solve the set of polynomials, we have to work with the zero-dimensional ideal, where we shall find the solution as the discrete set of points. It is fairly difficult to find the zero-set for general cases. Hence it is important to foresee whether an ideal is zero-dimensional or not. The criterion for an ideal to be zero-dimensional is given by Gröbner basis theory, which we shall see later.

Nullstellensatz

Assume that k is an algebracally closed field.

Theorem 4.1 Weak Nullstellensatz Let $I\subset k[x_1,\ldots x_n]$ be an ideal (different from $k[x_1,\ldots x_n]$ itself), then $V(I)$ is nonempty.

Theorem 4.2 Nullstellensatz Let $I \subset k\ [x_1,...x_n]$, then $I(V(I))=\sqrt{I}$.

Spectrum of ring and Zariski topology

As the set of polynomials define the geometric objects, we can adopt a view of geometry. In this section, we see a bit of it.

We say that a variety is *irreducible* when it is not empty and not the union of two proper sub-varieties, namely,

$X = X_1 \cup X_2$ for X_1 and $X_2 \Rightarrow X = X_1$ or $X = X_2$.

For a prime ideal *P* in a ring *S*, *V*(*P*) is irreducible.

For a ring *A*, we define the ring spectrum by

Spec(*A*) = {prime ideals of A}

For $A=K\ [x_1,...x_n]/J$ there is a one-to-one correspondence between Spec(A) and irreducible sub-varieties of *V*(*J*).

$\mathrm{Spec}(A) \leftrightarrow \{\text{irreducible sub-varities } V(J)$.

Every maximal ideal (hence being prime) in $A=K\ [x_1,...x_n]/I$ with an algebraically closed field *K* (such as $\mathbb{C}$) and an ideal *I* has the form

$$(x-a_1,\ldots,x-a_n)$$

for some point$(a_1,...,a_n) \in V(I)$. (Notice that, in case of $I=(0)$, $V(I)=K^n$. Hence there is a one-to-one correspondence

$V(J) \leftrightarrow$ m-Spec

by means of

$(x-a_1,\ldots,x-a_n) \leftrightarrow (a_1,\ldots,a_n)$.

The Zariski topology of a variety *X* is defined by assuming that the sub-varieties $Y \subset X$ are the closed sets, whereby the union and the intersection of a family of variety are also closed sets. For an algebraically closed field *K*, these two statements are valid.

Any decreasing chain $V_1 \supset V_2 \ldots$ of varieties in K^n eventually terminates.

Hence any non-empty set in K^n has a minimal element.

A variety which satisfies the descending chain condition for closed subsets is called to be Noetherian. Observe that the chain for the Noetherian varieties is descending, while the chain for the ideals is ascending when we have defined the Noetherian ring.

We define another type of topology in Spec(*A*): the Zariski topology of Spec(*A*), in which the closed sets are of the form

$$V(I)=\{P \in \mathrm{Spec}(A) \mid P \supset I\}$$

Two types of Zariski topology for varieties and Spec(*A*) have similar properties. The comparison is given in Chapter 5 of the book of Reid [4].

Unique factorization domain

Definition 4.7 An integral domain is a non-zero commutative ring in which the product of any two non-zero elements is non-zero.

Example 4.25 $\mathbb{R}[x_1,\ldots,x_n]$ and $\mathbb{C}[x_1,\ldots,x_n]$ are integral domains.

Definition 4.8 A unique factorization domain (UFD) is an integral domain in which any nonzero element has a unique factorization by the irreducible elements in the ring.

Example 4.26 $\mathbb{Z}$ is a UFD.

Example 4.27 For a field *F*, *F* [*x*] is a UFD.

Example 4.28 For a UFD *R*, $R[x_1,...,x_n]$ is a UFD. By induction, $R[x_1,\ldots,x_n]$ is a UFD.

By the last example, $\mathbb{R}[x_1,\ldots,x_n]$ and $\mathbb{C}[x_1,\ldots,x_m]$ are UFDs. Hence any polynomial in these rings has unique factorization. However there are a lot of example which is not a unique factorization domain.

Example 4.29 $R[X,Y,Z,W]/(XY-ZW)$ is not a UFD, since it permits two different factorization for one element: $a = XY = ZW$.

Completion: formal description of Taylor expansion

In the computation of molecular orbital theory through computer algebra, as is presented in the introduction, we approximate the energy function by polynomials. We simply replace the transcendental functions in the energy functional (such as $\exp(Ax)$ or $erf(Bx)$ with the corresponding formal power series, and we truncate these series at the certain degree. For this purpose, we execute Taylor expansion for the variable at a certain center point in the atomic distance. If we increase the maximum degree in Taylor expansion toward the infinity, the computation would converge to that by the exact analytic energy functional. Such a circumstance could be represented in a formal language of mathematics.

We need several definitions in order to present the formal description of Taylor expansion.

For a ring *S*, a "filtration" by the powers of a proper ideal *I* would be written as follows:

$$F^0S(:=S) \supset F^1S(:=I) \supset F^2S \supset \cdots \supset F^nS(:=I^n) \supset \cdots$$

The sequence is given by the inclusion relation. The filtration determines the Krull topology of *I*-adic topology.

An "inverse system" is a set of algebraic objects $(A_j)_{j\in J}$, which is directed by the index *J* with an order $\leq$. In the inverse system, we have a family of map (homomorphism),

$f_{ij} : A^j \to A^i$ for all i ≤ j

between two objects, from the larger index j to the smaller i. The map satisfies

$f_{ii} = 1$

and

$f_{ik} = f_{ij}\ o\ f_{jk}$ i ≤ j ≤ k

Let $I = (x_1, x_2, \ldots, x_n)$ and $I = (x_1, x_2, \ldots, x_n)$. The $F^iS(:=I^i)$ is the ideal in *R*, generated by the monomials of degree i in *S*. We also assume that the inclusion is given in the sense of ideal so that ideals generated by monomials of lower degrees

should contain those generated by monomials of higher degrees. We set $A_i = S / F^i S$ by the quotient rings. Hence the entries in $A_i = S / F^i S$ are the finite polynomials, in which the monomials in $F^i S$ are nullified, and A_i are represented by the set of polynomials up to degree $i-1$. The operation of the map from $S / F^j S$ to $S / F^i S$ is to drop the monomials of higher degrees and to shorten polynomials. In case of the polynomial approximation by means of Taylor expansion, the map is the projection from finer to coarser approximations.

The inverse system can be glued together as a mathematical construction, which is called the "inverse limit" (or "projective limit"). The inverse limit is denoted and defined as

$$A = \varprojlim A_i = \{(a_j) j \in J = \prod_{j \in J} A_i \Big| a_i = f_{ij}(a_j) \text{ for all } i \le j\}$$

The inverse limit A has the natural projection $\pi : A \to A_i$ (by which we can extract A_i).

The inverse limit is a "completion" of the ring $S = \mathbb{R}[x_1, x_2, \ldots, x_n]$ with respect to $I = (x_1, x_2, \ldots, x_n)$, when the inverse limit is taken for the quotient rings in the following way:

$$\hat{S}_I = \varprojlim (S / I^n S).$$

$\hat{S}_I$ is the ring of formal power series $R[[x_1, x_2, \ldots, x_n]]$, and we can arbitrarily approximate the formal power series by some finite polynomials through the natural projection.

Example 4.30 Consider $\exp(x)$. Let $S = \mathbb{R}[x]$ and $I = (x)$. FS^j is the set of polynomials of the form $x^j f(x)$. The Taylor expansion $\exp(x)$ up to degree $j-1$, $1 + x + (1/2)x^2 + \cdots (1/(j-1)!)x^{j-1}$, lies in F / FS^j. In the inverse limit of A_i, namely, $\mathbb{R}[[x]]$, the formal power series of $\exp(x)$, $1 + x + (1/2)x^2 + \cdots + (1/n!)x^n + \cdots$ is defined.

We can assume the formal power series in $R[[x_1, x_2, \ldots, x_n]]$ would represent the inverse limit of "glued" Taylor expansions. In the algebraic formulation of molecular orbital theory, by means of inverse limit, we can bundle the different level of polynomial approximation with respect t the maximum polynomial degrees. Hence the natural map π means the model selection.

Such a mathematical formality might appear only to complicate the matter in practice, but it is important to introduce a neat "topology" in theory. The topology is constructed as follows: an object (i.e. a polynomial) s in a ring S has the nested (or concentrated) neighborhoods in S; the open basis of the neighborhoods is generated by the powers of a proper ideal $I \subset S$ and represented as

$$x + I^n S \text{ for } x \in S$$

We say "open basis" in the sense of topology. If the reader is unfamiliar with topology, simply image that polynomials around a polynomial x are sieved into different classes, which are represented by the above form. The powers of the ideal I serve as the indicator of the distance between polynomials. In the terminology of topology, the completion makes a "complete" topological space. If we consider the inverse system for Taylor expansions at a point X, the formal neighborhoods of X should be small enough so that Taylor series should be convergent.

Example 4.31 Consider the map from $\mathbb{R}[x] / x^j \mathbb{R}[x]$ to $\mathbb{R}[x] / x^i \mathbb{R}[x]$ and the corresponding inverse system. Now $S = \mathbb{R}[x]$ and $F^i S = (x^i)\mathbb{R}[x]$. A polynomial f in $\mathbb{R}[x]$ has the open basis of neighborhoods, which is given by the set of the form

$$f + x^n \mathbb{R}[x].$$

The extension to the multivariate case in $\mathbb{R}[x_1, x_2, \ldots, x_n]$ is straightforward.

We interpret the neighborhoods of 0 in the slightly different view. Any polynomial has the image in each of $\mathbb{R}[x] / x^j \mathbb{R}[x]$. Hence there are the different classes of polynomials around 0, which are represented by nil-potent ε as follows,

$$\{0 + a\varepsilon \text{ such that } \varepsilon^2 = 0\}$$

$$\{0 + a_1\varepsilon + a_1\varepsilon^2 \text{such that } \varepsilon^3 = 0\}$$

likewise,

$$\{0 + \sum_{i=1}^{n} a_1 \varepsilon^i \text{such that } \varepsilon^{n+1} = 0\}$$

and so on. In other words, the choice of the neighborhoods of 0 is to choose the tolerable threshold, above which the monomials are admittedly zero.

Localization

Let $R = \mathbb{R}[x_1, \ldots, x_n]$ be a ring of polynomial functions. We can consider the rational function (or the fraction)

$$\frac{f(X)}{g(X)}$$

for $f, g \in R$. This sort of fraction is determined locally on a subset X in $\mathbb{R}^n$, such that $g(X) \neq 0$. For a fixed point $a = (a_1, \ldots, a_n) \in X$, we define the subset S of R such that

$$S = \{ p(a) \in R[x_1, \ldots, x_n] | \, p(a) \neq 0 \}$$

Then, for the pair in (*a*,*s*), denoted (*a*,*s*), the fraction a / s can be well-defined, although it is a "local function". The set of fractions must be closed under multiplication and addition. Moreover the equivalence relation between two pairs in $R \times S$ is given by

$$(a, s) \equiv (a', s') \Leftrightarrow as' - a's = 0.$$

In commutative algebra, "localization" is defined in a more general way.

Definition 4.9 Let R be a ring.

A subset $S \subset R$ is "multiplicatively closed" if $1 \in S$ and $ab \in S$ for all $a, b \in S$.

For R and its multiplicatively closed subset S, the equivalence relation between two elements in RxS is given by

$$(a, s) \sim (a', s') \Leftrightarrow \text{there is an element } u \in S \text{ such that } u(as' - a's) = 0$$

Then the set of equivalence classes

$$S^{-1}R := \left\{ \frac{a}{s} \middle| a \in R, s \in S \right\}$$

is the localization of at *R* the multiplicatively closed *subset S*. It is a ring with addition and multiplication,

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$$

and

$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}.$$

Example 4.32 Let *P* be a prime ideal in a ring *R*. As the set $S = R \setminus P$ is multiplicatively closed, we localize R by *S*. It is usually denoted by R_P and c *P* alled the localization of R at the prime ideal P. This localization has the exactly one maximum ideal PR_P. In particular, for $R = \mathbb{R}[x_1, \ldots, x_n]$ and $P = \{ f \in R | f(a) = 0 \text{ for a point } a \in \mathbb{R}^n \}$, R_P is the set of rational functions well defined around a.

Example 4.33 Let R be a commutative ring and let *f* be a non-nilpotent element in R. A multiplicatively closed subset S is given by $\{ f^n | n = 0,1,\ldots \}$. The localization $S^{-1}R = R[t]/(ft-1) \left(= R\left[f^{-1} \right] \right)$.

Example 4.34 Let $X = V(xy)$ (an affine algebraic set defined by the ideal (xy)). Consider the ring $A(X) = \mathbb{R}[x,y]/(xy)$. For a point $a = (1,0)$ in x-axis, the function y is equal to zero. So $y/1$ and $0/1$ should be equivalent as the elements in $S^{(-1)}R$ with $S = \{ f \in R | f(a) \neq 0 \}$. Indeed $x \in S$ and $x(y \cdot 1 - 0 \cdot 1) = xy = 0$ in $A(X)$, although $(y \cdot 1 - 0 \cdot 1) = y \neq 0$ in $\mathbb{R}[x,y]$. Hence the equivalence between $y/1$ and $0/1$ is proved. (This argument is not valid for $a = (0,0)$, because $x = 0$ at that point and it is not in S.)

Example 4.35 Consider the secular equation

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = e \begin{pmatrix} x \\ y \end{pmatrix}.$$

The roots are given by $(x,y,e) = (t,t,-1),(t,-t,1),(0,0,0)$, and they lie in the affine algebraic set $V(I)$ by the ideal $I = (x+ey, y+ex)$ in $R = \mathbb{R}[x,y]$. Let $P = (x,y,e+1)$ and $S = R \setminus P$. Since I is represented by another basis set (by a Gröbner basis with lexicographic order $x > y > e$) as

$$I = \left(y\left(e^2 - 1\right), x + ey \right)$$

it follows that

$$I \cdot S^{-1}R = \left(y(e+1), x + ey \right)$$

because $e-1$ is not in P and it is an invertible element in $S^{(-1)}R$. The ideal $I \cdot S^{-1}R$ describes "how the affine algebraic set $V(I)$ looks like" locally around the point $(x,y,e) = (0,0,-1)$. Indeed, the eigenvalue e is the root of the determinant $e^2 - 1 = 0$ and the parabola $f = e^2 - 1$ looks like $g = 2(e+1)$ locally around $e = -1$.

Integrality

Consider the extension of quotient ring

$$R = K[x_2, \ldots x_n] / I_1 \subset S = K[x_1, \ldots x_n] / I$$

We say $\overline{x_1} = x_1 + I \in S$ is integral over R when it satisfies the following condition:

Definition 4.10 Let $R \subset S$ be a ring extension. An element $s \in S$ is integral over R if it satisfies a monic polynomial equation

$$s^d + a_1 s^{d-1} + \cdots + a_d = 0$$

with $a_i \in R$ for all $i = 1, \ldots, d$.

If every element in S is integral over R, then S is integral over *R*. We say that S is the integral extension of *R*.

Then these statements hold:

If $s_1, \ldots, s_m \in S$ are integral over R, $R[s_1, \ldots, s_m]$ is integral over R.

The succession of integral extensions makes the integral extension. If S is integral over *R* and *T* is integral over *S*, then is *T* integral over.

Example 4.36 $\mathbb{R}[y] \to \mathbb{R}[x,y]/(xy-1)$ is not an integral extension. From the geometrical viewpoint, the correspondence by this map (by inverting the direction) gives us the projection of the hyperbola $xy = 1$ to -axis. There is no point in $xy = 1$ which is projected to the point $y = 0$ in y-axis, while any other points in y-axis have a preimage in $xy = 1$.

Example 4.37 Apply the change of coordinates to the above example: $x \to t$ and $y \to t + s$. Then we obtain $\mathbb{R}[s] \to \mathbb{R}[t,s]/(t^2 + ts - 1)$, which is an integral extension. From the geometrical viewpoint, the correspondence between two rings gives us the projection to the hyperbola $t(t+s) = 1$ to t-axis. One always finds two points in $t(t+s) = 1$, namely, $\left((1/2)\left(s \pm \sqrt{s^2 + 4} \right), s \right)$, which are projected to an arbitrary point *s* in *s*-axis. The change of coordinates with polynomial maps of this sort (which might be non-linear) enables us to obtain an integral extension of a ring, even if the domain of the map is not an integral extension (Noether-normalization) [2].

Example 4.38 Consider the ideal $I = (x+ey, y+ex) \subset \mathbb{R}[x,y,e]$. I represents a simple secular equation

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = e \begin{pmatrix} x \\ y \end{pmatrix}.$$

$\mathbb{R}[x,y] \to \mathbb{R}[e,x,y]/I$ is not an integral extension. In fact, I can be represented by another basis $\left(-y + ye^2, x + ye \right)$, but there is no monic equation for e. One cannot find the point in $V(I)$ which is projected to the non-zero vector (x,y) unless *e* takes certain particular values (the eigenvalues). This example is an application of integrality check by means of Gröbner basis. (This useful idea will be expounded later.)

Normalization

Let us consider a curve $y^2 = x^3 + x^2$ in $\mathbb{R}[x,y]$, as in Figure 2. The curve has a singularity at $(0,0)$ where two branches intersect. Let $t = y/x$. Then $y = tx$, $y^2 = x^3 + x^2$, and $t^2 = (x+1)$. These equations make an ideal $I = \left(y' x, y^2 - x^3 - x^2, t^2 - x - 1 \right)$ in $\mathbb{R}[x,y,t]$. The affine algebraic variety $y^2 = x^3 + x^2$ has no singularity and it maps to the curve $y^2 = x^3 + x^2$ by the projection to $\mathbb{R}[x,y]$.

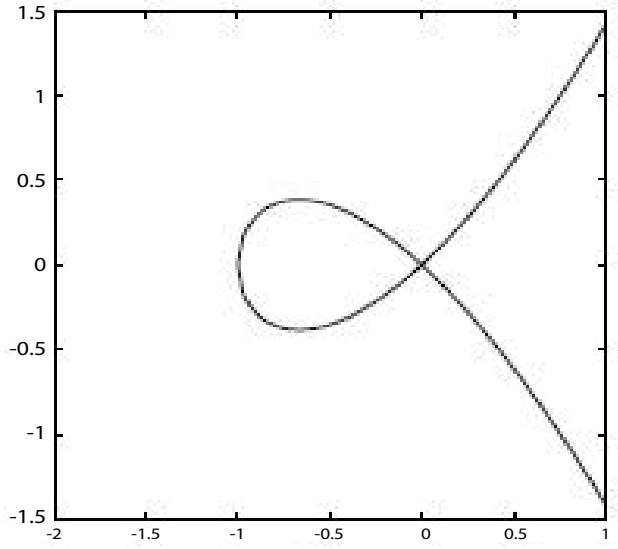

Figure 2: The curve $y^2 = x^3 + x^2$ with the singularity at (0; 0).

The curve $y^2 = x^3 + x^2$ with the singularity at $(0,0)$

The curve $y^2 = x^3 + x^2$ with the singularity at $(0,0)$

This is an example of the resolution of singularity. This sort of procedure lies in a broader concept of "normalization". If *S* is an integral domain, its normalization *S* is the integral closure of *S* in the quotient field (the field of fractions) of *S*.

Definition 4.11 (Normal) Let *S* be an integral domain with the field of fractions *K*. Let *f* be any monic polynomial in $S[x]$. If every root $a/b \in K$ of *f* also lies in *S*, then *S* is normal.

Example 4.39 One can prove that every UFD is normal.

Definition 4.12 (Normalization) Let R be a commutative ring with identity. The normalization of R is the set of elements in the field of fractions of R which satisfy any monic polynomial with coefficients in R.

Example 4.40 Observe that, in the above example, t is in the quotient field of $S = \mathbb{R}[x,y]/(y^2 - x^3 - x^2)$, and observe that the equation $t^2 - x - 1$ is a monic polynomial which guarantees that *t* is integral over *S*. In fact, in order to prove that this resolution of singularity is literally the normalization, it is necessary for us to do the argument in detail. So we omit it now.

Example 4.41 Consider $I = (x^2 - y^3)$ and $V(I)$. By setting $x = t^3$ and $y = t^2$, the coordinate ring $C[x,y]/I \simeq C[t^3, t^2]$. Let us denote $\mathbb{C}[t^3, t^2]$ by $\mathbb{C}(V)$. Then t is a root of polynomial $s^2 - t^2$ in $\mathbb{C}(V)[s]$, and $t \notin \mathbb{C}(V)$. Hence $\mathbb{C}(V)$ is not normal.

Example 4.42 In the above example of the resolution of singularity, t is contained in the normalization of $\mathbb{C}(V)$. As t is the root of $s^2 - t^2 \in \mathbb{C}(V)[s]$, every element of $\mathbb{C}[t]$ is also a root of some monic polynomial in $(V)[s]$. (To prove the validity of this statement, we need some arguments by commutative algebra) Hence, $\mathbb{C}[t]$ in the normalization of $\mathbb{C}(V)$. Besides, $\mathbb{C}[t]$ is a UFD, hence normal. Therefore $\mathbb{C}[t]$ is the normalization of $\mathbb{C}(V)$.

In fact, the procedure to find a normalization of $S = K[x_1,...,x_n]/I$ is to find another ring $\overline{S} = K[y_1,...,y_m]/I'$ with the normalization map $S \hookrightarrow \overline{S}$. The algorithm by Decker et al. enables us to compute such normalization. If $I \subset R = K[x_1, x_2, ...x_n]/I$ is a radical ideal, the normalization by the algorithm shall give the ideal decomposition of I. The computation returns s polynomial rings $R_1,...,R_s$ and s prime ideals $I_1 \subset R_1,..., I_s \subset R_S$ and s maps $\{\pi_i : R \to R_i, i = 1,...s\}$ such that the induced map

$$\pi : K[x_1,...,x_n]/I \to R_1/I_1 \times \cdots \times R_s/I_s,$$

whereby the target of π (the product of quotient rings) is the normalization.

As we shall see in section 6, the primary ideal decomposition is a substitution for the solution of eiganvalue problem. It is not so surprising that we meet again the decomposition of an ideal in the desingularization of the algebraic variety. The secular equation is given as

$$\{ a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = \grave{\alpha} x_i, i = 1,...n \}$$

or

$$\{ 0 = f_i(x_1, x_2, ..., x_n) := a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n - \grave{\alpha} x_i, i = 1,...n \}.$$

Then we have to find $\grave{\alpha}$ which shall give the non-zero solution of the matrix equation

$$\begin{pmatrix} a_{11} - \grave{\alpha} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - \grave{\alpha} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - \grave{\alpha} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Observe that the matrix in the left-hand side is the Jacobian matrix

$$J_{ij} = \frac{\partial f_i}{\partial x_j}$$

The singular locus of the algebraic affine set defined by $\{f_i\}$ is determined by the rank condition of the Jacobian matrix, namely by the condition that the Jacobian matrix is not of full rank. The desingularization is the normalization, and the latter would result in the decomposition of an ideal, by the algorithm of Decker.

It is not so difficult to trace the algorithm of normalization given in [10,11].

We need some definitions. Let $A = K[x_1,...,x_n]/I$. For $I = (f_1,...,f_m)$ The Jacobian ideal $\mathrm{Jac}(I)$ is defined by the $c \times c$ minors of the matrix

$$\begin{pmatrix} \frac{\partial f_1}{x_1} & \cdots & \frac{\partial f_1}{x_1} \\ \vdots & & \vdots \\ \frac{\partial f_s}{x_1} & \cdots & \frac{\partial f_m}{x_1} \end{pmatrix}$$

Where, $c = n - \dim(X)$ with $X = V(I)$. Then the singular locus of A is given by $\mathrm{sloc}(A) = V(\mathrm{Jac}(I) + I)$.

Then we execute the computation by following these steps.

- Compute the singular locus *I*. Let *J* be a radical ideal such that $V(J)$ contains this singular locus.
- Choose a non-zero divisor $g \in J$ and compute $gJ : J$. For a homomorphism from J to J, denoted by $\mathrm{Hom}(J,J)$, and for a non-zero divisor x in J, $x\mathrm{Hom}(J,J) = xJ : J$.
- Let $g_0 (:= g), g_1, ..., g_s$ be the generators of $gJ : J$. There are quadratic relations of the form

$$\frac{g_i}{g}\frac{g_j}{g} = \sum_{k=0}^{s} \zeta_k^{ij} \frac{g_k}{g}, \text{ with } \zeta_k^{ij} \in A.$$

- Also there are linear relations between $g, g_1, ..., g_s$ (the syzygy) of the form

$$\sum_{k=0}^{s} \eta_k \frac{g_k}{g} = 0$$

- Then a surjective map is given by

$$A[T_1, ..., T_s] \twoheadrightarrow \mathrm{Hom}(J,J), \twoheadrightarrow T_i \rightsquigarrow \frac{g_i}{g}$$

- The kernel of this map is an ideal I_1 generated by the quadratic and linear relations of the form

$$T_i T_j - \sum_{k=0}^{s} \zeta_k^{ij} T_k, \sum_{k=0}^{s} \eta_k T_k$$

and it yields the extension of *A* by

$$A_1 = A[T_1, ..., T_s] / I_1$$

- This ring A_1 may be normal. If not, we make the extension of A_1 again. After finite steps of the successive extensions, we arrive at the normalization.
- The criterion of normality: A is normal if and only if $A = \mathrm{Hom}_A(J,J)$. If this criterion is satisfied, we do not have to add extra T_i. Then the algorithm stops.

Consider $I = (x + ey, y + ex)$ in $\mathbb{Q}[x, y, e]$.

Let $A = \mathbb{Q}[x, y, e] / I$. The Jacobian matrix of I is

$$\begin{pmatrix} 1 & e & y \\ e & 1 & x \end{pmatrix}.$$

Then

$\mathrm{Jac}(I) = (1 - e^2, x - ey, xe - y)$, or more simply, and. $\mathrm{sloc}(A) = V(\mathrm{Jac}(I) + I) = V(1 - e^2, x, y)$ (Recall that the Gröbner basis of I is.) Hence we set $J = (1 - e^2, x, y)$ as a radical ideal containing the singular locus. Choose x as the non-zero divisor in J. Then $xJ = (x^2, xy)$, since $x(1 - e^2)$ vanishes as an element in A. Hence, $xJ : J = (x, y)$. Let $T = y / x$. Then there are two linear relations

$$e + T = 0, eT + 1 = 0$$

and a quadratic relation

$$T^2 = \frac{y^2}{x^2} = e^2$$

We have the extended ring

$$A' = A[T] / (e + T, eT + 1, T^2 - e^2)$$
$$= \mathbb{Q}[x, y, e, T] / (x + ey, y + ex, y - Tx, e + T, eT + 1, T^2 - e^2)$$

with the ideal $I' = (x + ey, y + ex, y - Tx, e + T, eT + 1, T^2 - e^2)$. This ring A' is normal. Indeed, after some algebra (in fact, by means of computer algebra), we can check that the singular locus of $V(A')$ is an empty set. (We check the emptiness by the computation of Gröbner basis, which should be generated by (1).) From this reason, for a radical ideal J which contains the singular locus, we have $J = A'$ (the ring itself). Hence $\mathrm{Hom}_{A'}(J,J) = A'$ and the criterion for the normality is satisfied.

As T is integral over A and actually $T = \pm e$ in A, the ideal I' is represented in two ways by the substitution for *T*:

$$I_a = (x + ey, y + ex, y - ex, e, e^2 + 1) = (1)$$

$$I_b = (x + ey, y + ex, 1 - e^2) = (x + ey, 1 - e^2)$$

These two ideal lie in $\mathbb{Q}[x, y, e]$. As I_a is trivial, we adopt I_b for the purpose of normalization. In addition, when we introduce the variable *T*, we implicitly assume that $x \neq 0$. When $x = 0$, the ideal I is given by

$$I_0 = I \cap (x) = (x, y).$$

Then the normalization of A is given by two rings:

$$\mathbb{Q}[x, y, e] / I_0 = \mathbb{Q}[x, y, e] / (x, y)$$

and

$$\mathbb{Q}[x, y, e] / I_b = \mathbb{Q}[x, y, e] / (x + ey, 1 - e^2)$$

Compare this result to the example of primary ideal decomposition with the same ideal *I* which we will compute in section 6. We observe that the normalization has done the decomposition of the ideal imperfectly.

Hensel's lemma

Consider the problem to solve the equation

$$f(x) = x^2 - 7 = 0$$

Let us substitute $a_0 = 1$ in $f(x)$:

$$f(1) = -6 \equiv 0 \bmod 3$$

Let $a_1 = 1 + 3s$. Then

$$f(a_1) \equiv -6 + 6s \bmod 3^2.$$

Hence, if $s = 1$, then

$$f(a_1) \equiv -6 + 6.1 = 0 \bmod 3^2.$$

Let $a_2 = 1 + 3 \cdot 1 + 3^2 s$. Then

$$f(a_2) \equiv 9 + 72s \bmod 3^3.$$

Hence, if $s = 1$, then

$$(a\ ) \equiv 9 + 71.1 \equiv 0 \bmod 3$$

Likewise, by setting $a_n = a_{n-1} + 3^n s$, we can determine *s*

such that $f(a_n) \equiv 0 \bmod 3^{n+1}$. It means that we obtain the 3-adic solution of the equation

$$X = a_0 + 3 \cdot a_1 + 3^2 \cdot a_1 + \cdots$$

Let us consider the polynomial $f(X)$ in $\mathbb{Z}_p[x]$. We have

$$f\left(X + p^n Y_n\right) = f\left(X\right) + p^n Y_n f'\left(X\right) \bmod p^{n+1}$$

Hence if $p^n f'(X) \not\equiv 0 \bmod p^{n+1}$ or, equivalently, if $0 \bmod p \not\equiv 0 \bmod p$, we obtain Y such that $f\left(X + p^n Y\right) \equiv 0 \bmod p^{n+1}$ by the fraction.

$$Y_n = -\frac{f(X)}{f'(X)}$$

Observe the similarity with Newton method in numerical analysis. In other words, the p-adic solution of $f(x) = 0$ as $\sum_{i=0}^{\infty} p^i Y_n$. This is Hensel's lemma, stated as follows.

Theorem 4.3 (Hensel's lemma) If $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ satisfies

$$f\left(a\right) \equiv 0 \bmod p$$

and

$$f'\left(a\right) \not\equiv 0 \bmod$$

then there is a unique $\alpha \in \mathbb{Z}_p$ such that $f\left(\alpha\right) = 0$ and $\alpha \equiv a \bmod p$.

In the lemma, there is a condition $f'(\alpha) \not\equiv 0 \bmod p$, while, from the above example, it seems that we should use $f'(a_n) \equiv f'(a)$ for changeable a_n. In fact, by the construction, $a_n \equiv a_0 = a \bmod p$, it follows that $f'(a_n) \equiv f'(a)$. Hence we assume that condition only for the starting point a.

In commutative ring there is a related idea, called "Linear Hensel Lifting", by the following theorem.

Let *R* be a commutative ring. Let *f*, g_1, h_1 be univariate polynomials in *R*[*x*] and let *m* be a ideal in *R*. If *f* decomposes into the product of g_0 and h_0 in R/m, that is to say,

$$f \equiv g_0 h_0 \bmod m,$$

and if there exist polynomials *s* and *t* in $R[x]$ such that

$$s.g_0 + t.h_0 \equiv 1 \bmod m,$$

then, for every integer l we have polynomials $g^{(l)}$ and $h^{(l)}$ such that

$$f \equiv f^{(l)} g^{(l)} \bmod m^l,$$

and

$$f \equiv f^{(l)}, g \equiv g^{(l)} \bmod m$$

The computation of $g^{(l)}$ and $h^{(l)}$ is done in a constructive way.

Let $g^{(1)} = g_0$ and $h^{(1)} = h_0$. And let

$$g^{(l+1)} = g^{(l)} + m^l q_g$$

and

$$h^{(l+1)} = h^{(l)} + m^l q_h$$

We solve the equation

$$g_0 q_h + h_0 q_g \equiv \frac{f - g^{(l)} h^{(l)}}{m^{(l)}} \bmod m$$

so that we obtain q_g and q_h such that $\deg\left(q_g\right) < \deg\left(g_1\right)$ and $\deg\left(q_h\right) < \deg\left(h_1\right)$.

Example 4.44 $f\left(x\right) = x - \left(+ t\right)$, and $R = \mathbb{C}\left[\left[t\right]\right]$. For $m = \left(t\right) \subset R$, we begin from

$$g_0 = x + 1$$

$$g^{(l)}, h^{(l)}$$

and we obtain $g^{(l)}, h^{(l)}$ in an iterative way. As usual, we simply write the roots of $f(x) = 0$ by $\pm\sqrt{1+t}$. Hensel's lemma implies the existence of a power series in $\mathbb{C}\left[\left[t\right]\right]$.

Real algebraic geometry

The computation of hydrogen molecule, presented in the introduction, is done in the real number, and in the algebraic set defined by the polynomials:

$$A = \{ p_i\left(x_1, x_2, ..x_n\right) = 0 \mid i = 1, ...r \}$$

On the other hand, we can add extra constraint of the form

$$B = \{ q_i\left(x_1, x_2, ..x_n\right) \geq 0 \mid i = 1, ...s \}.$$

Hence it is important to study the existence of solutions of (A) with (B).

We review several results from real algebraic geometry from now on. (As for rigorous theory, see the book by Bochnak et al. [12] or the book by Lassere [13].)

These two statement are equivalent for an affine algebraic variety:

the ideal $I(X)$ has real generators $f_1, ..., f_k \in \mathbb{R}\left[x_1, ..., x_n\right]$.

$X = \overline{X}$, (by complex conjugation)

Then we define real affine algebraic variety and real ideal.

Definition 4.13 The set of real points $V_{\mathbb{R}}\left(f_1, ..., f_k\right)$ with $f_i \in \mathbb{R}\left[x_1, ..., x_n\right]$ is called a real affine algebraic variety.

Definition 4.14 An ideal I is called as a *real ideal*, if it is generated by real generators and satisfies the following property:

$$a_i \in \mathbb{R}\left[x_1, ..., x_n\right] \text{and} \, a_2^2 + ... + a_p^2 \in I \Rightarrow a_i \in I$$

For any real algebraic variety, $I(X)$ is a real ideal. To see the difference between real and non-real ideals, consider $\left(x\right)$, $\left(x^2\right)$, and $\left(1 + x^2\right)$. The last two ideals are not real ideals.

Definition 4.15 Let $p_1, ...p_r \in \mathbb{R}\left[x_1, x_2, ..., x_n\right]$ polynomials. The set

$$W\left(p_1, ..., p_r\right) = \{ a \in \mathbb{R}^n \mid p_1\left(a\right) \geq 0, ...p_1\left(a\right) \geq 0 \}$$

is called as a basic closed semi-algrbraic set. A general semi-algebraic set is the boolean combination of them.

Theorem 4.5 (Real NullStellensatz) Let us define the real radical as follows:

$$\sqrt[\mathbb{R}]{I} = \left\{ p \in \mathbb{R}[x] \middle| \, p^{2m} + \sum_j g_j^2 \in I \text{ for some } q_j \in \mathbb{R}[x], m \in \mathbb{N} \setminus 0 \right\}$$

Then it holds that $\sqrt[\mathbb{R}]{I} = I\left(V_{\mathbb{R}}\left(I\right)\right)$, where $V_{\mathbb{R}}\left(I\right)$ is the real affine algebraic set of *I*. If *J* is a real ideal, $\sqrt{J} = I\left(V_{\mathbb{R}}\left(J\right)\right)$; that is to say, for a real ideal *J*, the radical ideal $\sqrt{J}$ (by the standard

definition of commutative algebra) is equal to the ideal of $V_{\mathbb{R}}(J)$ (the affine algebraic set of J in $\mathbb{R}$).

Example 4.45 For $I=\left(x^2+y^2\right)$, $I\left(V_{\mathbb{R}}(I)\right)=(x,y)$.

Definition 4.16

$$\sum \mathbb{R}[x]^2=\left\{p\in\mathbb{R}[x]\middle| p=\sum_{i=1}^{r} q_i(x)^2 \text{ for some } r\in\mathbb{N}\right\},$$

$$\Sigma^2(g_1,...,g_n)=\left\{\sum_{e\in\{0,1\}^r}\sigma_e g_1^{e_1}...g_1^{e_r}\middle|\sigma_e\in\sum\mathbb{R}[x]^2\right\}$$

$$M(f_1,...,f_m)=\left\{f_1^{e_1}f_2^{e_2}...f_m^{e_m}\middle|e_1,...,e_m\in\mathbb{N}\right\}$$

From these definitions, $\mathbb{R}[x]^2$ are the sums of squares of polynomials; $\Sigma^2(g_1,...g_n)$ is the "quadratic module", which is the set of polynomials generated by $\mathbb{R}[x]^2$ and $g_1,...,g_n$; M is the multiplicative monoid generated by $f_1,...,f_m$.

Theorem 4.6 (Positivestellensatz) Let $\{g_k\,|\,k=1,...,n\}$, $\{f_i|i=1,..m\}$, and $\{h_l|l=1,...t\}$ be the polynomials in $\mathbb{R}[x_1,...,x_n]$. The following properties are equivalent.

$$\left\{x\in\mathbb{R}^n\middle|\begin{matrix}g_k(x)\geq 0,k=1,...,\mathrm{n}\\ f_i(x)\neq 0,i=1,...,m\\ h_l(x)=0,l=1,...,t\end{matrix}\right\}$$

$\exists g\in\Sigma^2\langle g_1,...g_n\rangle$, $\exists f\in \mathrm{M}(f_1,...f_m)$, and $\exists h\in I\left(h_1,...h_l\right)$ such that $g+f^2+h=0$.

From this theorem, one can derive the following theorem, also.

Theorem 4.7 Let $f\,\{g_k\,|i=1,...,n\}$ be polynomials in $\mathbb{R}[x]$ and $K=\{x\in\mathbb{R}\,|\,x\in W(g_1,..,g_n)\}$. Then the following statements hold.

$\forall x\in K f(x)\geq 0$ if and only if $\exists p\in\mathbb{N},\exists g,h\in\Sigma^2\left(g_1,...g_n\right)$ such that $fg=f^{2p}+h$.

$\forall x\in K f(x)>0$ if and only if $\exists p\in\mathbb{N},\exists g,h\in\Sigma^2\left(g_1,...g_n\right)$ such that $fg=1+h$.

Example 4.46

The theorem asserts that

$f>0$

if and only if

$q^2 f=p_1^2+\cdots+p_n^2$,

for some polynomials $q,p_1,...,p_n$. (From the theorem, the set $\{x\in\mathbb{R}\,|-f(x)\geq 0,f(x)\neq 0\}$ is empty if and only if $\exists u=s_1^2+\cdots+s_{n-1}^2-fq^2\in\Sigma^2(-f)$, $\exists p\in\mathbb{N}$, $\exists v=f^p\in\mathrm{M}(f)$, such that $u+v^2=0$. Now we can choose $p_1=s_1,...,p_{n-1}=s_{n-1},p_n=f^p$.) In other words, every non-negative polynomial is a sum of squares of rational functions.

Example 4.47 Consider $x^2+ax+b=0$.

Define D, f, g, h to be

$D=b-a^2/4$,

$g=\left(\frac{1}{\sqrt{D}}\left(x+\frac{a}{2}\right)\right)^2$,

$f=1$

$h=-\frac{1}{D}\left(x^2+ax+b\right)$.

When $D>0$, these polynomials are well defined in $\mathbb{R}[x]$. Then it happens that $g+f^2+h=0$, where $1=f\in\mathrm{Monoid}(\{1\})$, $g\in\sum\mathbb{R}[x]^2\subset\Sigma^2(\{1\})$, and $h\in I\left(x^2+ax+b\right)$. In other words, the quadratic equation has no real root if and only if $D>0$.

Example 4.48 Consider the secular equation (for a molecular orbital model of a simple diatomic molecule):

$$\begin{pmatrix}0&-1\\-1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=e\begin{pmatrix}x\\y\end{pmatrix}.$$

The problem is equivalent to

$$\begin{aligned}h_1=x+e\,y &= 0\\ h_2=y+e\,x &= 0.\end{aligned}$$

Add the constraint:

$$f=x-y\neq 0$$

A Gröbner basis (with respect to the lexicographic order $x>y>e$) of the ideal $I=(h_1,h_2)$ is $H=\left(ye^2-y,x+ye\right)$. After some algebra, f^2 reduces to $2y^2e+2y^2$ with respect to H. Hence we have obtained

$$g+f^2+h=0$$

for $h\in I(h_1,h_2)$ and $g=-2(e+1)y^2$. If $e\leq -1$, $g=\left(\sqrt{-2(e+1)}\,y\right)^2$ and it satisfies the condition of Positivstellensatz. Hence there is no real solution to the problem. (Or we say that the non-symmetric wave function (x,y) such that $x\neq y$ is not the ground state of the molecule at eigenvalue -1.)

Noether normalization

Let $R\subset S$ be a ring extension. Remember how can be an element $s\in S$ integral over R.

Definition 4.17 An element $s\in S$ is integral over R if it satisfies a monic polynomial equation with coefficients $\{r_i\in R\}$

$$s^d+r_1s^{d-1}+\cdots+r_d=0$$

The equation is called an integral equation for S over R. If every element $s\in S$ is integral over R, we say that S is integral over R. We also say that $R\subset S$ is an integral extension.

Definition 4.18 Let S be an affine ring $S=K[x_1,...,x_n]/I$. Then there are elements $y_1,...,y_d\in S$ with the following properties.

$y_1,...,y_d$ are algebraically independent over K.

$K[y_1,...,y_d]\subset S$ is an integral ring extension.

If the elements $y_1,...,y_d$ satisfy these two conditions, the inclusion $K[y_1,...,y_d]\subset S$ is a Noether normalization for S.

Example 4.49 Let $I=(x+ey,y+ex)\subset\mathbb{R}[x,y,e]$, and let $S=\mathbb{R}[x,y,e]/I$. The residuals $\bar{x},\bar{y}(\in S)$ are not integral over $\mathbb{R}[e]$. But the change of the variables

$$x\to x,y\to y'=4x+y,e\to 5x+6y+e$$

makes the change in I as follows:

$$I\to I'=(20x^2+29xy+4xe+x$$

$$+6y^2+ye,5x^2+6xy+xe+4x+y)$$

We can prove the residuals $\overline{x}, \overline{y'} (\in S' = \mathbb{R}[x, y', e'] / I')$ are integral over $\mathbb{R}[e']$. Indeed, after a hard algebra (by means of Gröbner basis theory and the variable elimination as we learn later), we affirm that the ideal I' contains following two polynomials

$$65y^3 + 28y^2e + 2y^2 + 3ye^2 - 3y$$

and

$$325x^3 - 38x^2e - 12x^2 + xe^2 - x$$

Example 4.50 There are several types of the variable change which conduct Noether normalization.

$x_i \to y_i = x_i + \lambda_n x_n$ with λ_i in the coefficient field K, when K is an infinite field.

$x_i \to y_i = x_i - x_i^{r^{i-1}}$ for $2 \le i \le n$. We have to find an integer r.

To do with the latter type is, in fact, the proof of the existence of Noether normalization. Let $f(x_1, ..., x_n)$ be a polynomial defining the ideal I. By the change of variables, we obtain

$$f\left(x_1, y_2 + x_1^r, ..., y_n + x_1^{r^{n-1}}\right).$$

If the monomial of the highest degree with respect to x_1 is originally given by

$$Ax_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

it becomes

$$Ax_1^{a_1} \prod_{i=2}^{n} \left(y_i + x_1^{r^{i-1}}\right).$$

Hence, after the change of the variables, the term of the highest degree with respect to x_1 is given by

$$Ax_1^{a_1 + a_2 r^2 + \cdots + a_n r^{n-1}}$$

If r is large enough, this term has the degree larger than any other monomials. Therefore x_1 is integral over $K[y_2, ..., y_n]$. There is another way to define the dimension of the variety. Let $I \in K[x_1, ..., x_n]$ be a proper ideal. Let $A = V(I)$. If $K[y_1, .., y_d] \in K[x_1, ..., x_n] / I$ is a Noether normalization, the dimension of A is given by the number d, namely,

$$dim(A) = d$$

Differential Galois theory

One of the important ideas concerning algebraic geometry, differential algebra, and quantum mechanics is the differential Galois theory.

Let us solve

$$y' - y = 0$$

We get $C\exp(t)$.

Let us solve

$$y'' + 2ty' = 0$$

We get $C\int dt \exp(-t^2)$. In the first case, we can get the solution in the range of elementary functions; on the other hand, in the second case, we have to do the integration.

Then there arises a question: under what circumstance one can express the solution of a differential equation using exponents, integration, and also by adding algebraic elements? We proceed step by step, by adding more elements which are constructed over the elements already presented in the computation. The analytic solution given by this way is called *Liouvillian solution*, although it is not always possible to construct it. The solvability condition is given by the differential Galois theory [14-16].

In the application of eigenvalue problem in quantum mechanics, we can consider the one-dimensional Schrödinger equation:

$$\psi''(x) = \left(P_{2n}(x) - \lambda\right)\psi(x)$$

with the even-degree monic polynomial potential

$$P_{2n}(z) = z^{2n} + \sum_{i=0}^{2i-1} a_i z^i = \left(z^n + \sum_{i=0}^{i-1} b_i z^i\right)^2 + \sum_{i=0}^{n-1} c_i z^i$$

In the last representation of P_{2n}, the polynomial is given by completing squares. Let us write the solution in the following form:

$$\psi(x) = P_s \exp\left(\pm f(x)\right)$$

as the product of a monic polynomial P_s and

$$f(x) = \frac{x^n}{n+1} + \sum_{k=0}^{n-1} \frac{b_k x^{k+1}}{k+1}$$

Now we can establish the relation among the coefficients $\{b_i\}$ and $\{c_i\}$ in the polynomial potential, the eigenvalue λ and P_s. The relation of this sort is given by a second-order differential equation for P_s. As the consequence of differential Galois theory, the equation has solutions at the particular setting of $\{b_i\}$, $\{c_i\}$ and λ. To solve the problem, one can utilize Gröbner basis theory and the variable elimination, which shall be explained later. If the equation is solvable, we can obtain the analytic solution [16].

Other important concepts of commutative algebra

It is advisable that the readers should consult textbooks and grasp the concepts of more advanced technical terms, such as "module", "free module", "regular local rings", "valuation", "Artinian ring", "affine algebraic variety", or so. Maybe the concepts of homological algebra would be necessary, such as "functor", "exact sequence", "resolution", "projective", "injective", "Betti-number", and so on. Indeed, the research articles are frequented by these concepts.

Gröbner Basis Theory

The Gröbner basis theory is the key technique of commutative algebra and algebraic geometry[17-19]. The idea was first proposed by Bruno Buchberger, and the namesake is his advisor Wolfgang Gröbner.

The monomial orders

In one-variable case, we implicitly use the "monomial order" through the ordering of degrees: $1 < x < x^2 < \cdots$ or $1 > x > x^2 > \ldots$ In the multivariate case, we encounter the monomials of the form $x^i y^j z^k$. What should be the appropriate ordering of the monomials? In fact, there are several ways to set the order .

Let $x^a(=x_1^{a_1}...x_n^{a_n})$ and $x^b(=x_1^{b_1}...x_m^{b_m})$ be the monomials. And let a and b be sequence of superscripts $(a_1,a_2,...,a_n)$ and $(b_1,b_2,...,b_n)$.

Definition 5.1 The lexicographic order.

$$x^a < x^b \Leftrightarrow \exists i(1 \le i \le n) : a_n = b_1,...,a_{i-1} = b_{i-1}, a_i < b_i.$$

This definition is equivalent to the following statement.

$x^a < x^b$, if the left-most component of a-b is negative.

Definition 5.2 The reverse lexicographic order.

$$x^a < x^b \Leftrightarrow \exists i(1 \le i \le n) : a_n = b_n,...,a_{i+1} = b_{i+1}, a_i > b_i$$

This definition is equivalent to the following statement.

$x^a < x^b$, if the right-most component of a-b is positive.

Definition 5.3 The degree reverse lexicographic order:

Let $\deg(x^a) = a_1 + ... + a_n$

$x^a < x^b \Leftrightarrow$

(1) $\deg(x^a) < \deg(x^b)$

or

(2) $\deg(x^a) = \deg(x^b)$ and $\exists i\,(1 \le i \le n)$:

$a_n = b_n,...,a_{i+1} = b_{i+1}, a_i > b_i$. (The right-most component of a-b is positive.)

Example 5.1 Compute $(x+y+z+1)^3$ in $\mathbb{Z}[x,y,z]$. The monomials can be sorted by the different types of monomial order. (Here the degree of a monomial is given by this correspondence: $x > y > z$.

The lexicographic order: $x > y > z$;

$$x^3 + 3x^2y + 3x^2z + 3x^2 + 3xy^2 + 6xyz + 6xy + 3xz^2 + 6xz$$
$$+3x + y^3 + 3y^2z + 3y^2 + 3yz^2 + 6yz + 3y + z^3 + 3z^2 + 3z + 1$$

The reverse lexicographic order: z > y > x;

$z^3 + 3yz^2 + 3xz^2 + 3z^2 + 3y^2z + 6xyz + 6yz + 3xz + 3z + y^3 + 3xy^2 + 3y^2 + 3x^2y + 6xy + 3y + x^3 + 3x^2 + 3x + 1$

The degree reverse lexicographic order: $x > y > z$;

$$x^3 + 3x^2y + 3xy^2 + y^3 + 3x^2z + 6xyz + 3y^2z + 3xz^2 + 3yz^2 + z^3$$
$$+3x^2 + 6xy + 3y^2 + 6xz + 6yz + 3z^2 + 3x + 3y + 3z + 1$$

The difference between the lexicographic order and the reverse lexicographic order is apparent; it is simply a reversal. The difference between lexicographical order and the degree reverse is subtle; it could be understandable by these phrases by Ene and Herzog [9],

...in the lexicographic order, $u > v$ if and only if u has "more from the beginning" than u; in the degree reverse lexicographic order, $u > v$ if and only if u has "less from the end" than u...

Initial ideal

Let $f \neq 0$ be a polynomial in the ring $R = K[x_1, x_2, ..., x_n]$ with the monomial order $<$. The "initial monomial" $\text{in}_<(f)$ is the largest monomial included in f (from which the coefficient is removed). The "initial coefficient" $lc(f)$ is the coefficient of $\text{in}_<(f)$. Hence the "leading term" is given by the product of the initial coefficient and the initial monomial: $lc(f)\text{in}_<(f)$. We use an extra definition: $\text{in}_<(0) = 0$.

The initial ideal $\text{in}_<(I)$ is the monomial ideal, generated by the initial terms of the polynomials in I,

$$\text{in}_<(I) = \{\text{in}_<(f) : f \in I\}.$$

This ideal is a useful tool in the theory of Gröbner bases.

Definition of Gröbner basis

The Gröbner basis is defined now.

Definition 5.4 Let I be the ideal in the polynomial ring R, with the monomial order $<$. The Gröbner basis is the sequence of elements $g_1, g_2, ..., g_m$, such that $\text{in}_<(I) = (\text{in}_<(g_1), ..., \text{in}_<(g_n))$.

We could represent the polynomial f by means of a sequence of polynomials $u_1, u_2, ..., u_m (\in I)$ in the following way (the standard expression)

$$f = p_1u_1 + p_2u_2 + \cdots p_mu_m + r$$

such that

No monomial in the remainder r is contained in the ideal $(\text{in}_<(u_1), ...\text{in}_<(u_n))$.

$$\text{in}_<(f) \ge \text{in}_<(p_iu_i) \text{ for all } i$$

If $r = 0$ we say that f reduces to zero with respect to $u_1, u_2, ..., u_m$. In general case, the standard expression is not unique. From this reason, we have to use Gröbner basis, since the standard expression by Gröbner basis is unique and any polynomial reduces uniquely by this basis. For example, consider the case with $f = xy - y^2$, $g_1 = x - y$, and $g_2 = x$ in the lexicographic order. There are two standard expression: $f = yg_1$ and $f = yg_2 - y^2$. However, the ideal (g_1, g_2) is generated by the Gröbner basis (x, y), by which f reduces to zero and it has the unique standard expression.

Buchburger's algorithm

The Buchberger's algorithm is the standard way to generate Gröbner basis [3,6,7,9,20-22]

Let us define the S-polynomial of two polynomials f and g

$$spoly(f,g) = \frac{\text{lcm}(\text{in}_<(f), \text{in}_<(g))}{c\text{in}_<(f)} f - \frac{\text{lcm}(\text{in}_<(f), \text{in}_<(g))}{d\text{in}_<(f)}$$

where d and d are the leading coefficients of f and g.

One can prove that

$g_1, ..., g_m$ are the Grbner basis of ideal I with respect to a monomial order $<$,

if and only if

$spoly(g_i, g_j)$ reduces to zero with respect to $g_1, ..., g_m$ for $i < j$.

The computational step is as follows.

Step–0 Let G be the generating set of ideal I.

Step–1 For every pair of polynomials p, q in the ideal G, compute $spoly(p,q)$ and its reminder r with respect to G.

Step–2 If all $spoly(p,q)$ reduce to zero with respect to G, we have already obtained the Gröbner basis. If there are non-zero reminders $r \neq 0$, add r to G and repeat again at Step–1.

The computation terminates after finite steps.

Let us see examples.

Example 5.2 Consider $f = x + ye$ and $R = \mathbb{R}[x,y,e]$ in $R = \mathbb{R}[x,y,e]$, with respect to lexicographic order $x > y > e$. In the beginning, $G = \{f,g\}$. As $\text{in}_<(f) = x$ and $\text{in}_<(g) = xe$, $spoly(f,g) = ef - g = -y - ye^2$. The leading monomial $\text{in}_<(spoly(f,g))$ is ye^2. As the monomials in $S(f,g)$ is not included by the monomial module $(\text{in}_<(f), = \text{in}_<(g)) = (x, xe)$, $h := spoly(f,g)$ does not reduce to zero; indeed it is the reminder itself. We add $h := spoly(f,g)$ to G so that $G = \{f,g,h\}$. Then we compute more of s-polynomials : $spoly(h,g) = xy - y^2e = -yf$ and $spoly(h,f) = -xy - y^2e^3 = -yf - yeh$. Since $spoly(h,g)$ and $spoly(f,g)$ reduces to zero with respect to G, we obtain the Gröbner basis G. In fact, the initial term of $g = xe + y$ is divisible that of $f = x + ey$, and $h = ef - g$, g is a redundant term which we can remove from the basis safely.

Example 5.3 Consider $f_1 = x + ey$, $f_2 = y + ex$ $f_3 = x^2 + y^2 - 1$ in $R = [x,y,e]$, with respect to lexicographic orer $x > y > e$. We have $G = \{f_1, f_2, f_3\}$. We compute the s-polynomials: $spoly(f_1, f_2) = ye^2 - y$, $spoly(f_1, f_3) = xye - y^2 + 1$, and $spoly(f_2, f_3) = xy - y^2e + e$. These three polynomials reduce to $f_4 = ye^2 - y$, f_5=-2y^2+1, and $f_6 = -2y^2e + e$. We get $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ and we compute the s-polynomials and the reminders. The only non-zero reminder is $(1/2)(e^2 - 1)$, to which $spoly(f_4, f_5)$ and $spoly(f_4, f_6)$ reduce. We have $G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7 = e^2 - 1\}$. We compute the s-polynomials and ascertain that all of them reduce to zero. Thus $G = \{x + ey, y + ex, x^2 + y^2 - 1, xye - y^2 + 1, -2y^2 + 1, -2y^2e + e, e^2 - 1\}$ is the Gröbner basis. However, $y + ex$, $x^2 + y^2 - 1$, $xye - y^2 + 1$ and $-2y^2e + e$ are redundant: indeed they have the initial monomials divisible by those of other polynomials ($\hat{G} = \{x + ey, -2y^2 + 1, e^2 - 1\}$) and reduce to zero with respect to $\hat{G}$. Thus we can chose $\hat{G}$ as the Gröbner basis, and indeed this ideal satisfies the required property.

Example 5.4 Consider $I = (x+1, 1)$ in $\mathbb{R}[x]$. As $spoly(x+1, x) = 1$, The Gröbner basis is $(x+1, x, 1) = \{1\}$. This Gröbner basis is never to be zero, and the set of equation $x + 1 = 0 \wedge x = 0$ does not have any solution. In other words, the ane algebraic set of this ideal is empty $V(I) = V(\{1\}) = \varnothing$. Likewise, in the more complicated case, by computing the Gröbner bases G, we can check the existence of the solutions of the set of polynomial equations.

In the above algorithm the generated Gröbner basis is not properly "reduced" by the terminology of several contexts. A reduced Gröbner basis $(g_1, ..., g_n)$ should have the following property [23]:

The leading coefficient of each g_i is 1.

for all $i \neq j$, the monomials in g_j are not divisible by $\text{in}_<(g_i)$.

Gröbner basis of zero-dimensional ideal

The following statements are equivalent for a zero-dimensional ideal $I \subset S = K[x_1, x_2, ..., x_n]$ with a monomial order $<$.

I is a zero-dimensional ideal.

The affine algebraic set $V(I)$ is finite.

If G is a Gröbner basis, then, for any $1 \leq i \leq$ n, there exists $g \in G$ such that $\text{in}_<(g) = x_i^{v_j}$ for some $nu_i \geq 0$.

I is contained in finitely many maximal ideals of S.

Let $\text{Mon}(A)$ be the set of monomials in A. The set $\text{Mon}(S) \setminus \text{Mon}(in_<(I))$ is a finite set.

S / I is a K-vector space of finite dimension.

The statement 3) enables us to detect a zero-dimensional ideal from its Gröbner basis, if the latter contains polynomials which have initial terms such that $x_i^{v_i}$ for any $1 \leq i \leq n$.

The feature of zero-dimensional ideal, given by statement 5) and 6), will be useful for solving polynomial equations by Stickelberger's theorem, as is explained in section 5.12.

Example 3.5 For $I = (x^2 + y^2 + z^2 - 1, x + y + z, x) \subset R[x,y,z]$, the Gröbner basis with respect to lexicographic monomial order $x > y > z$ is $(2z^2 - 1, y + z, x)$. This is the example of zero-dimensional ideals and it satisfies the statement 3).

Example 5.6 For $I = (x^2 + y^2 + z^2 - 1, x + y + z) \subset \mathbb{R}[x,y,z]$, the Gröbner basis with respect to lexicographic monomial order $x > y > z$ is $(2y^2 + 2yz + 2z^2 - 1, x + y + z)$. As the ideal depicts the intersection of the unit sphere and a plane surface, it is not zero-dimensional. Although the Gröbner basis has the terms z^2 and z, these terms are not initial terms. Hence this ideal does not satisfy the statement 6).

Example 5.7 For $I = (x^2 + y^2 + z^2 - 1, x + y + z, x) \subset R[x,y,z]$, the Gröbner basis with respect to lexicographic monomial order $x > y > z$ is $(2z^2 - 1, y + z, x)$. This is the example of zero-dimensional ideals and it satisfies the statement 3).

Sygygy

For a Gröbner basis $\{f_1, f_2, ..., f_m\}$, there are relations as follows

$$\sum_{i=1}^{s} s_i f_i = 0$$

by means of the set of polynomials $\{s_1, s_2, ..., s_m\}$. (A trivial example is) $f_i f_j - f_j f_i = 0$ Such a set of polynomials is a "module" (which is actually a vector space), and we call it the first sygyzy and denote it by $Syz(f_1, f_2, ..., f_n)$. The basis set of this module is computed from the Gröbner basis.

When the computation of Gröbner basis is completed, there are relations among the generators of the basis of the form:

$$spoly(f_i, f_j) = q_{ij,1} f_1 + q_{ij,2} f_2 + \cdots + q_{ij,m} f_m .$$

Let us define

$$r_{ij} = spoly(f_i, f_j) - q_{ij,1} f_1 - q_{ij,2} f_2 - \cdots - q_{ij,m} f_m$$

Then $\{r_{ij}\}$ generates $Syz(f_1, f_2, \ldots, f_n)$. Moreover,even if $p_1, p_2, \ldots, p_n$ is not a Gröbner basis, we can compute $Syz(p_1, p_2, \ldots, p_n)$ through its Gröbner basis.

Example 5.8 Let us compute the syzygy of $\{p_1 = tx + ey, p_2 = tx + ey, p_3 = x^2 + y^2 - 1\}$ with the lexicographic monomial order $t > x > y > e$. $Syz(p_1, p_2, \ldots, p_3)$ are generated by three trivial generators

$(-p_3, 0, p_1), (-p_2, p_1, 0), (0, -p_3, p_1)$,

and by the non-trivial one,

$(x^2 ye + y^3 e - ye, -x^2 - y^2 + 1, -y^2 e^2)$.

Observe that the inner product of those generators and (p_1, p_2, p_3) is zero. The generators form a vector space.

Sygyzy is a module, in other words, a kind of vector space generated by the vectors, the entries of which are polynomials. We can compute the second syzygy in the vector generators of the first syzygy and, likewise, the higher syzygy, too. The successive computation of higher syzygy enables us to construct the "resolution" of a module *M* in a Noetherian ring; the computation terminates after a certain step so that we do not find any non-trivial sygyzy in the last step [23].

Church-Rosser property

The reduction is a binary relation from one object to another, like an arrow going in one direction. We often call it the rewriting process.

Definition 5.5 A binary relation (denoted by the symbol $\rightarrow$) has the Church-Rosser property, if, whenever P and Q are connected by a path of arrows, P and Q have a common destination R by the relation.

Hence we can define Gröbner bases in the other way: A basis is a Gröbner basis if and only if the reduction with respect to the bases has the Church-Rosser property, as is illustrated in Figure 3.

Complexity of the Gröbner basis algorithm

The original algorithm by Buchberger, as is presented here, is not so efficient. It produces a lot of useless pairs of polynomials (p, q), since such pairs give birth to s-polynomials $spoly(p, q)$, which immediately reduce to zero or produce redundant polynomials. There are a lot of studies about the upper bound of the complexity of Gröbner bases, such as Hermann bound [24], Dube bound [25], Wiesinger's theorem [26], and so on. Those bounds are determined by several factors: (1) the number of variables, (2) the number of polynomials in the ideal, (3) the number of possible s-polynomials, (4) the maximum degrees of the polynomials, etc. In the worst case, the complexity is doubly exponential in the number of variables [25,27-30]. However, the computation of the Gröbner basis is equivalent to the Gaussian elimination process of a large matrix (by the row reduction of Macauley matrix) [17,29,31,32]. For the case of homogeneous polynomial ideals, the complexity in the Gaussian elimination method is bounded by

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right),$$

where ω is a constant, *m* is the number of polynomials [33], n is the dimension of the ring, and D is the maximum degree of the polynomials . In order to improve efficiency, one can employ more refined methods, such as Faugère's F_4 and F_5. Indeed the efficiency of F_5 [34, 35] outperforms the row reduction computation of Macaulay matrix [33].

In fact, the efficiency of the algorithm is highly dependent on the chosen monomial order. The lexicographic order is convenient for theoretical study, but it consumes a considerable quantity of computational resource. Thus one often has to compute the Gröbner basis by other monomial orders (say, the degree reversible lexicographic order) in order to facilitate the computation, and then, one can remake the computed result in lexicographic order, by means of FGLM (Faugère, Gianni, Lazard, Mora) algorithm [36].

There is another problem in the Gröbner bases generation. which is apparent in practice. The Buchberger's algorithm applies the operation of addition, subtraction, multiplication, and division to the polynomial system. It often causes a great discrepancy in the degrees of the generated polynomials and the numerical scale of coefficients in the final result. In the computation presented in the introduction of this article, one can observe such a tendency. Thus, for the practical purpose, one must utilize several tricks to keep the polynomials as "slim" as one can [37-39].

Gröbner basis for modules

Let us review what is the module. A $R-$module *M* is an abelian group with scalar multiplication $R \times M \rightarrow M$, such as $(a, m) \rightarrow am \in M$. It has the following property.

$1m = m$

$(a+b)m = am + bm$

$(a+b)m = am + bm$

$a(m+n) = am + bm$.

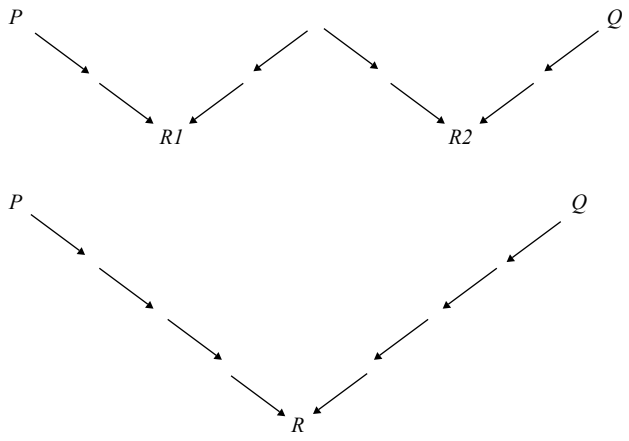

Figure 3: Two types of reductions by binary relations. (Upper) not Church-Rosser type; (Lower) Church-Rosser type. If the basis of an ideal is not Gröbner, the reduction goes in several destinations as in the upper figure. On the other hand, if the basis is Gröbner, the reduction is unique.

A free module is the module with a basis set $\{e_i\}$. We can compute Gröbner bases of free modules. One of the purpose of this sort of computations is to study the linear equation of polynomials:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

for which one might ask for the linear dependence of rows.

We define the monomial order in modules in these ways.

Position over coefficient : $ue_i > ve_j$ if $i < j$ or $i = j$ and $u > v$.

(Example: $x_2e_1 > x_1e_2$).

Coefficient over position $ue_i > ve_j$: if $u > v$ or $v = v$ and $i < j$.

(Example: $x_1e_2 > x_2e_1$).

In the similar way as in the case of polynomial, we chose the leading terms of the elements in a module; we also compute the s-polynomials and the reminders in order that we obtain the Gröbner basis. The slight difference is that when $\mathrm{in}_<(f) = ue_i$ and $\mathrm{in}_<(g) = ve_i$ we use the s-polynomial as follows:

$$spoly(f,g) = \frac{\mathrm{lcm}(u,v)}{\mathrm{lc}(f)u} f - \frac{\mathrm{lcm}(u,v)}{\mathrm{lc}(g)u}$$

(Here we use the notation $\mathrm{lc}(x)$ to represent the coefficient of $\mathrm{in}_<(x)$.)

Application of Gröbner basis

Gröbner basis is a convenient tool to actually compute various mathematical objects in the commutative algebra.

Example 5.9 Elimination of variables: The intersection of ideal $I \subset R$ and the subring $S \subset R[x_1, x_2, ..., x_n]$ is computable. Let $S = R[x_{t+1}, ..., x_n]$ and let G be a Gröbner basis of I. Then $G_t = G \cap S$ is the Gröbner basis of S. If we compute the Gröbner basis by means of lexicographic orders $x_1 > x_2 > ... > x_n$, we obtain the set of polynomials,

$\left\{ f_1^i(x_n), i = 1, ..., i_1 \right\}$,

$\left\{ f_2^i(x_{n-1}, x_n), i = 1, ..., i_2 \right\}$,

...

$\left\{ f_{n-t+1}^i(x_{t+1}, ..., x_{n-1}, x_n), i = 1, ...i_{n-t-1} \right\}$,

...

$\left\{ f_n^i(x_1, x_2, ..., x_n), i = 1, ..., i_n \right\}$.

Thus we can easily get $G_t = G \cap S$.

Example 5.10 Intersection of ideal *I* and *J* in *R*. Let *y* be an extra variable. $I \cap J$ is computable by the relation $I \cap J = (I \cdot Y \cdot R[y] + J \cdot (-1) \cdot R[y]) \cap R$. The intersection of the right-hand side is computed by the elimination of variable y.

Example 5.11 The ideal quotient $I : J$ is computable. If $J = (f_1, ..., f_s)$, then $I : J = \hat{\bigcap}_{j=1}(I : f_j)$. In addition, for a single polynomial *f*, $I \cap (f) = f \cdot (I : f)$. We can compute $I \cap (f)$ and obtain the generators $\{g_1, g_2, ..., g_m\}$. Then $I : f$ is generated by $\{g_1 / f, g_2 / f, ..., g_m / f\}$. Hence $I : f_j$ is computed as the intersection of $I : f_j$.

Example 5.12 Saturation: it is defined for an ideal I and a polynomial f in a ring S as follows.

$$I : f^\infty = \left| \left\{ g \in S : \text{there exists} \, i > 0 \, \text{such that} \, f^i g \in I \right\} \right.$$

Let t be a new variable, and let $\tilde{I}$ be the ideal generated in $S[t]$ by *I* and by the polynomial $1 - ft$. Then the saturation $f \in \sqrt{I} \Leftrightarrow f^i \in I$. [compsat]

Example 5.13 Radical membership: $f \in \sqrt{I} \Leftrightarrow f^i \in I$ for someone $i > 0 \Leftrightarrow$ For all $g \in S$, there exists $i(>0)$ such that $f^i g \in I$. $\Leftrightarrow I : f^\infty = S$. Hence, if the ideal, $\hat{I}$ defined in example 5.12, has the Gröbner basis $\{1\}$, then $f \in \sqrt{I}$.

Gröbner basis algorithm in a different light

The Buchberger's algorithm is actually the elimination in large matrices. It is the way of Faguère to do the row reduction in the large matrix. Let us see how it would work.

Consider the same problem: $f_1 = x + ye$, $f_2 = y + xe$, $f_3 = x^2 + y^2 - 1$. We compute the s-polynomials $ef_1 - f2$ and $xf_1 - f_3$. The coefficients in these polynomials are given in the matrix.

$$\begin{pmatrix} xf_1 \\ ef_1 \\ f_2 \\ f_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} x^2 \\ xye \\ xe \\ ye^2 \\ y^2 \\ y \\ 1 \end{pmatrix}$$

The matrix in the right hand side is the so-called Macaulay matrix of the second order. The row reduction yields:

$$\begin{pmatrix} xf_1 \\ ef_1 \\ f_4 \\ f_5 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} x^2 \\ xye \\ xe \\ ye^2 \\ y^2 \\ y \\ 1 \end{pmatrix}$$

We obtain $f_4 = -ye^2 + y$ and $f_5 = -xye + y^2 - 1$ and now we have the temporary Gröber basis $G = \{f_1, f_4, f_5\}$; f_2 and f_3 can be excluded in the consideration, because they are "top-reducible" by f_1 and easily recovered by the present *G*.

Let us compose the third order Macaulay matrix:

$$\begin{pmatrix} yef_1 \\ f_5 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} xye \\ y^2e^2 \\ y^2 \\ 1 \end{pmatrix}$$

The row reduction yields this:

$$\begin{pmatrix} yef_1 \\ f_6 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} xye \\ y^2e^2 \\ y^2 \\ 1 \end{pmatrix}$$

We obtain $f_6 = y^2 e^2 + y^2 - 1$. Now $G = \{f_1, f_4, f_6\}$

We again compute the third order Macaulay matrix

$$\begin{pmatrix} y f_4 \\ f_6 \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 \\ 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} y^2 e^2 \\ y^2 \\ 1 \end{pmatrix}$$

The row reduction yields:

$$\begin{pmatrix} y f_4 \\ f_7 \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 2 & -1 \end{pmatrix} \begin{pmatrix} y^2 e^2 \\ y^2 \\ 1 \end{pmatrix}$$

We obtain $f_7 = 2y^2 - 1$. Now $G = \{f_1, f_4, f_7\}$.

We compute the fourth order Macaulay matrix:

$$\begin{pmatrix} y f_4 \\ \frac{1}{2} e^2 f_7 \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 1 & 0 & -1/2 & 0 \end{pmatrix} \begin{pmatrix} y^2 e^2 \\ y^2 \\ e^2 \\ 1 \end{pmatrix}$$

We do the row reduction in the fourth order Macaulay matrix:

$$\begin{pmatrix} y f_4 \\ \frac{1}{2} f_8 \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & 1 & -1/2 & 0 \end{pmatrix} \begin{pmatrix} y^2 e^2 \\ y^2 \\ e^2 \\ 1 \end{pmatrix}$$

We obtain $f_8 = 2y^2 - e^2$. Now $G = \{f_1, f_4, f_7, f_8\}$. However, as $f_7 - f_8$ yields $f_9 = e^2 - 1$, and as $f_4 = -y^2 f_9$, G would be $\{f_1, f_7, f_9\} = \{x + ye, 2y^2 - 1, e^2 - 1\}$. The s-polynomials for G are computed now:

$$spoly(f_1, f_7) = \frac{1}{2}x + y^3 e = \frac{1}{2} f_1 + \frac{ye}{2} f_7$$

$$spoly(f_1, f_9) = x + ye^3 = f_1 + yef_9,$$

$$spoly(f_7, f_9) = 2y^2 - e^2 = f_7 - f_9.$$

As those s-polynomials reduce to zero with respect to G, it is proved that G is a Gröbner basis.

In the above example, we process the computation carefully so that the unnecessary polynomials are removed immediately as soon as they appear; we also limit the computation in the Macaulay matrices which would be as small as possible, although these matrices might be embedded into a very large one. Indeed we have done the row reduction numerically, not symbolically, in a very large, but sparse matrix. The algorithms F_4 and F_5 by Faugère adopt these policies in a systematical way so that these algorithms are of the most efficient methods to generate Gröbner bases.

Stickelberger's theorem

In [2], an alternative of the numerical solution, instead of Gröbner basis, is also used. This method is based on Stickelberger's theorem. In general, for a zero-dimensional ideal $I \subset R = k[x_1, \ldots x_n]$, R/I is a -vector space of finite dimension; that is to say, the vector space is spanned by the set of monomials and the result of the multiplication between two monomial is also represented by the linear combination of the monomial basis. Therefore, according to the assertion of the theorem, the operation of a monomial to the monomial basis is thought to be the operation of a matrix in k. And the eigenvalue of the matrix gives the numeral value of the corresponding monomial at $V(I)$.

Consider $I = (x + ye, y + xe, x^2 + y^2 - 1) \subset R = \mathbb{R}[x, y]$. As a Gröbner basis of I is $(x + ye, 2y^2 - 1, e^2 - 1)$, the monomial basis in R/I is given by $\{1, \overline{ye}, \overline{e}, \overline{y}\}$, from which x is dropped.

The transformation by x and e are given as follows.

$$\overline{y} \begin{pmatrix} \overline{1} \\ \overline{ye} \\ \overline{e} \\ \overline{y} \end{pmatrix} = \begin{pmatrix} \overline{y} \\ \overline{y^2 e} \\ \overline{ye} \\ \overline{y^2} \end{pmatrix} = \begin{pmatrix} \overline{y} \\ 1/2\overline{e} \\ \overline{ye} \\ 1/2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1/2 & 0 \\ 0 & 1 & 0 & 0 \\ 1/2 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \overline{1} \\ \overline{ye} \\ \overline{e} \\ \overline{y} \end{pmatrix}.$$

$$\overline{e} \begin{pmatrix} \overline{1} \\ \overline{ye} \\ \overline{e} \\ \overline{y} \end{pmatrix} = \begin{pmatrix} \overline{e} \\ \overline{ye^2} \\ \overline{e^2} \\ \overline{ye} \end{pmatrix} = \begin{pmatrix} \overline{e} \\ \overline{y} \\ 1 \\ \overline{ye} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \overline{1} \\ \overline{ye} \\ \overline{e} \\ \overline{y} \end{pmatrix}.$$

The transformation matrices M_y (by y) and (M_e by e) are those in the right hand side in the both equations. It is easily checked that there are four eigenvectors, common both for M_y and M_h, which lie in R/I:

$$\begin{pmatrix} \overline{1} \\ \overline{ye} \\ \overline{e} \\ \overline{y} \end{pmatrix} = \begin{pmatrix} 1 \\ 1/\sqrt{2} \\ 1 \\ 1/\sqrt{2} \end{pmatrix}, \begin{pmatrix} 1 \\ -1/\sqrt{2} \\ 1 \\ -1/\sqrt{2} \end{pmatrix}, \begin{pmatrix} 1 \\ 1/\sqrt{2} \\ -1 \\ -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ -1/\sqrt{2} \\ -1 \\ 1/\sqrt{2} \end{pmatrix}$$

Now we have obtained the numeral values of e and y at $V(I)$ from $\overline{y}$ and $\overline{y}$. In fact, the eigenvalues M_y and M_h also give us the value of y and e at $V(I)$. As for the value of x, we easily compute it from the polynomial relation by the ideal I.

Algorithm of computing Krull dimension

As we have seen, the zero-dimensional ideal is detected immediately after the computation of its Gröbner ideal. However, it takes a little of algebra to compute the non-zero dimension of an ideal [40].

Let $I \subset R[x_1,...,x_n]$ be an ideal. Then the Krull dimension of $R[x_1,...,x_n]/I$ is given by an integer d, i.e., $\dim_K(R[x_1,...,x_n]/I) = d$, such that d is the maximal cardinality of a subset of variables $u \subset \{x_1,...,x_n\}$ with $I \cap R[u] = (0)$. (*A maximal independent set of variables with respect to* I is a subset u of variables of maximal cardinality, defined as this.)

Let $>$ be any monomial ordering on $R[x_1,...,x_n]$. And let $I \subset R[x_1,...,x_n]$ be an ideal. Then the Krull dimension of the quotient ideal is computed by means of the initial ideal $\mathrm{in}_<(I)$ of I:

$$\dim_K(R[x_1,...,x_n]/I) = \dim_K(R[x]/\mathrm{in}_<(I))$$

Hence we only have to consider the initial ideal $\mathrm{in}_<(I)$, instead of the ideal I itself.

Let $I = (m_1,...,m_k) \subset R[x_1,...,x_n]$ be an ideal with monomial generators m_i. Let denote $\{x_1,...,x_n\}$ by X. Define $d(I, R[x])$ in a recursive way

$$d((0), R[X]) = n,$$

and

$$d(I, R[X]) = \max\{d(I|_{x_i=0}, R[X \setminus x_i]) \text{ for } x_i \text{ such that } x_i \mid m_1\}.$$

Then $d(I, K[x]) = \dim_K(R[x]/I)$.

Example 5.14 Consider $I = (xy) \subset \mathbb{R}[x,y]$.

$$d(I, \mathbb{R}[x,y]) = \max\{d((0), \mathbb{R}[x]), d((0), \mathbb{R}[y])\},$$

as $I|_{x=0} = I|_{y=0} = (0)$. Since $d((0), \mathbb{R}[x]) = d((0), \mathbb{R}[y]) = 1$, $d(I, K[x,y]) = \dim_K \mathbb{R}[x,y]/(xy) = 1$.

Example 5.15 Consider $I = (xy-1) \subset \mathbb{R}[x,y]$. Then we have to consider $\mathrm{in}_<(I) = (xy)$ and the conclusion is the same as the previous example.

Example 5.16 Consider $I = (x+ey, y+ex) \subset \mathbb{R}[x,y,e]$ with lexicographic order $x > y > e$. The Gröbner basis is $\{y - ye^2, x + ey\}$. Hence $\mathrm{in}_<(I) = (y,x)$. Since $u = \{e\}$ is the set of variable of maximal cardinality with

$$(y,x) \cap \mathbb{R}[e] = (0)$$

we have $\dim_K \mathbb{R}[x,y,e]/I = 1$. (We can arrive at the same conclusion by means of the recursive function $d(I, \mathbb{R}[x,y,e]$.)

Algorithm for The Decomposition of The Ideal as Eigenvalue Solver

In the example of the hydrogen molecule in section 3, we have seen that the polynomial secular equation is made into the triangular form, in which the relation of variables is clarified, almost to represent the roots themselves. The mathematical foundation of such computations is the primary ideal decomposition.

Primary ideal decomposition

There are two special sorts of ideal: prime ideal and primary ideal, as we have seen in the previous section. One can comprehend these sorts of ideal with the analogy of elementary number theory. An integer is decomposed as $n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ by the prime factorization. The ideal of the integer n is $n\mathbb{Z}$ (the integer multiple of n); and it is represented by $n\mathbb{Z} = p_1^{a_1}\mathbb{Z} \cap p_2^{a_2}\mathbb{Z} \cap \cdots \cap p_n^{a_n}\mathbb{Z}$ as the intersection of the ideals generated by certain powers of primes.

An ideal in the commutative algebra, likewise, could be decomposed as the intersection of primary ideals [3]:

$$I = \bigcap_i p_i$$

One of the most elementary procedure for primary ideal decomposition is summarized as follows [41]. Let I be the ideal in a Noetherian ring R, and $r, s \in R$ are elements such that $r \notin \sqrt{I}$, $s \notin I$ and $rs \in I$.

Find n such that $I : r^\infty = I : r^n$.

Let $I_1 = I + (r^n)$ and $I_2 = I : (r^n)$.

The ideal I_1 and I_2 are larger than I. The decomposition process must be done for each of them. By choosing some proper r, we can decompose I_1 and I_2, hence I by primary ideals.

Example 6.1 Consider $J = (x+ey, y+ex)$ in $R = [x,y,e]$ with the lexicographic order $x > y > e$.

y is not in the radical $\sqrt{J}$; and $y \cdot (e^2-1) = ey(x+ey) - y(y+ex) \in J$. Thus we set r y and $s = e^2 - 1$

Let $J_1 \equiv (J, y) = (y, x+ye, y+xe)$. This is a primary (in fact, a prime) ideal, and $J : y = J : y^2 = \ldots$ (stabilized).

Let $J_2 \equiv J : y = (e^2-1, x+ye)$: this is because of another representation $J = (y(e^2-1), x+ye)$. The ideal J_2 can be decomposed again.

Now take $r = e-1$, $s = e+1$.

$J_{21} \equiv (J_2, e-1) = (e-1, x+ey) = (e-1, x+y)$. This ideal is primary (in fact, prime).

$J_{22} \equiv (J_2 : e-1) = (e+1, x-y)$ and $J_2 : (e-1) = J_2 : (e-1)^2 = \ldots$ (stabilized). This ideal is primary (in fact, prime).

Now we have done the primary ideal decomposition: $J = J_1 \cap J_{21} \cap J_{22}$.

We should notice that the ideal J is the secular equation of the diatomic system,

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = e \begin{pmatrix} x \\ y \end{pmatrix}$$

The primary ideal decomposition is the operation equivalent to the eigenstate computation by means of linear algebra: the solutions of the secular equation are given by the affine algebraic sets of the computed ideals. We obtain the eigenvalue $e = 1$ and $e = -1$ for which the eigenvectors are (x,x) and $(x,-x)$.

In fact, the above example is one of the simplest cases which we can compute manually. The general algorithm for ideal decomposition is first proposed by Eisenbud [42]; and

practical algorithms are developed by Gianni, Trager and Zacharias [43], by Shimoyama and Yokoyama [44], by Möller [45] and by Lazard . (As for the semi-algebraic set, one can do similar decomposition, as is studied by Chen and Davenport [46].) The comparison of algorithms is given in [10].

Algorithm of gianni, grager, and gacharias

In this section, we review the primary ideal decomposition algorithm of Gianni, Trager, and Zacharias (GTZ algorithm) [18, 40]. In the algorithm which we have seen in the previous section, we have to search a "key polynomial" by trial and error to decompose an ideal. In contrast, GTZ algorithm enables us to find such a key in a more rational way.

Definition 6.1

A maximal ideal $I_M \subset K[x_1,...,x_n]$ is called in general position with respect to the lexicographical ordering $>$ with $x_1 > ... > x_n$, if there exist $g_1,...,g_n \in K[x_n]$ such that $I_M = (x_1 + g_1(x_n),...,x_{n-1} + g_{n-1}(x_n), g_n(x_n))$.

When an ideal is decomposed by primary ideal decomposition $I = Q_1 \cap \cdots \cap Q_s$, the prime ideals $P_i = \sqrt{Q_i}$ are called associated primes of *I*. P_i is a minimal associated prime of I if $P_i \neq P_j$ for all $j \neq i$.

A zero-dimensional ideal $I \in K[x_1,...,x_n]$ is called in general position with respect to the monomial order $>$ with $x_1 > \cdots x_n$), if all associated primes $P_1,...,P_s$ are in general position and $P_i \cap K[x_n] \neq P_j \cap K[x_n]$ for $i \neq j$.

Theorem 6.1 (Zero-dimensional Decomposition) Let $I \in K[x_1,...,x_n]$ be a zero-dimensional ideal. Let $(f) = I \cap K[x_n]$, $f = f_1^{v_1} \cdots f_s^{v_s}$ with $f_i \neq f_j$ for $i \neq j$. Then the decomposition of ideal I is given by

$$I = \bigcap_{i=1}^{s} \left(I, f_i^{v_i}\right).$$

If *I* is in general position with respect to the monomial order $>$ with $x_1 > ... > x_n$, then (I, f^{v_i}) are primary ideals for all i.

Theorem 6.2 (Ideal decomposition in general case) Let $X = (x_1,...,x_n)$. Let $I \subsetneq K[X]$ be an ideal, and let $u \subset X$ be a maximal independent set of variables for I. Then these statements hold.

The ideal $IK(u)[X \setminus u]$ generated by *I* in $K(u)[x \setminus u]$ is zero-dimensional. We denote the field of rational functions on K with variables *u* by $K(u)$.

Let $\{g_1,...g_s\} \subset I$ be a Gröbner basis of $IK(u)[x \setminus u]$. Let $h = \operatorname{lcm}(\operatorname{lc}(g_1),...,\operatorname{lc}(g_s)) \in K[u]$. Then $IK(u)[x \setminus u] \cap K[x] = I : h^{\infty}$. If $I = (I : h^d) \cap (I, h^d)$, then $I = (I : h^d) \cap (I, h^d)$.

If $IK(u)[X \setminus u] = Q_1 \cap ... \cap Q_s$ is an irredundant primary decomposition, then $IK(u)[x \setminus u] \cap K[X] = (Q_1 \cap K[X]) \cap ... \cap (Q_s \cap K[X])$ is also an irredundant primary decomposition.

Example 6.2 Consider $I = x + ey, y + ex$ in $\mathbb{Q}[x,y,e]$ with lexicographic order $x > y > e$. We know a Gröbner basis of *I* is $\{y(e^2-1), x+ey\}$.

Choose $u = \{y\}$ as a maximal independent set of variables.

$I\mathbb{Q}(y)[x,e] = (e^2 - 1, x + ey)$. This ideal us a Gröbner basis in $\mathbb{Q}(y)[x,e]$.

Then $h = \operatorname{lcm}(\operatorname{lc}(g_1), \operatorname{lc}(g_2)) = xe^2$.

$J := I : h = I : h^2 = (e^2 - 1, x + ey)_{\mathbb{Q}[x,y,e]}$. And $(I,h) = (x + ey, y + ex, xe^2) = (x, y)$. We have a decomposition $I = (I : h) \cap (I, h)$.

We decompose J. As J is zero-dimensional in $\mathbb{Q}(y)[x,e]$, we apply the algorithm in zero-dimensional case. Since $e^2 - 1 = (e+1)(e-$, the decomposition of J is given by $J = (J,(e+1)) \cap (J,(e-1)) = (e+1, x-y) \cap (e-1, x+y)$. As the ideal J is in general position with respect to lexicographic order $x > e$ in $\mathbb{Q}(y)[x,e]$, and (*J*, (*e*-1)) are primary ideals. Notice that we are working in $\mathbb{Q}(y)[x,e]$. However, as the decomposition of $J\mathbb{Q}[x,y,e]$ inherits that of $J\mathbb{Q}(y)[x,e]$, we have obtained the required decomposition.

Triangulation of polynomial system

In case of the systems of polynomial equations $\{p_i(x_1, x_2, ...x_n) | i = 1...m\}$ which have only finitely many solutions (i.e. to be zero-dimensional), several methods methods are proposed [45,47] which decompose the solution set into finitely many subset of the triangular form with respect to the variables entries,

$$\left\{ f_1^l(x_1), f_1^l(x_1, x_2), ..., f_n^l(x_1, x_2, ...x_n) \middle| l - 1, ...L \right\}$$

This kind of algorithm is used in the application of algebraic geometry in molecular orbital theory as is demonstrated in section 3, instead of conventional linear algebra.

Let us review the triangular decomposition algorithm by Möller [45]. The algorithm is based upon several lemmas.

Lemma 6.1 (Lemma 2 in [45]) Let A be an ideal in a ring $R = \mathbb{K}[x_1,...,x_n]$ such that Krull dimension of the residue class ring R/A is zero : $dim(R/A) = 0$. If B is an ideal such that $B \subset A$ and if $m \in \mathbb{N}$ is sufficiently large, the affine algebraic set $V(A)$ is the disjoint union: $V(A) = V(A : B^m) \cup V(B)$ with

$$V(B) = \{ y \in V(A) | \forall b \in B : b(y) = 0 \}$$

$$V(A : B^m) = \{ y \in V(A) | \exists b \in B : b(y) \neq 0 \}.$$

(The definition of $V(B)$ of this theorem, given in [45], is slightly different from the conventional one. In this section only, we use this definition.)

Lemma 6.2 (Lemma 3 in [45] Let A is a ideal in a ring R such that Krull-dimension of R/A equals to zero $\dim k(R/A) = 0$ and let B be another ideal in R such that $A \subseteq B = (g_1,...,g_s)$. Then, for sufficiently large $m, m_1,...,m_s \in \mathbb{N}$

$$V(A : B^m) = \bigcup_{i=1}^{s} V((A + (g_1,...,g_{i-1}) : g_i^{m_i}).$$

with $V((A + (g_1,...,g_{i-1}) : g_i^{m_i}) = \{ y \in V(A) | g_1(y) = ... = g_{i-1}(y) = 0 \neq g_i(y) \}$. In addition, if A is a radical ($A = \sqrt{A}$), the above relation holds for all positive $m, m_1,...,m_s$. [lemmasaturation]

Lemma 6.3 (Lemma 5 iii) in [45]). Let $f_i := \sum_{j=0}^{d_i} \tilde{g}_{ij}(x_1,...,x_{n-1}) x_n^{d_i - j}$ with nonzero polynomials $\tilde{g}_{ij}$, $i = 1,...,r$. If $F := \{f_1,...,f_r\}$ is a Gröbner basis with respect to a monomial order <, then

G={g˜_10,...g˜_r0} is a a Gröbner basis with respect to <. [lemmagb]

Lemma 6.4 (Lemma 7 in [45]) Let $G := \{f_1,...,f_r\}$ be a reduced Gröbner basis with respect to a monomial order <, where x_n is lexicographically in front of $\{x_1,..,x_{n-1}\}$, and let

$$f_i := \sum_{j=0}^{d_i} \tilde{g}_{ij}(x_1,...,x_{n-1}) x_n^{d_i-j}$$

with nonzero polynomials $\tilde{g}_{ij}$, $i=1,...,r$, and $lt(f_r) < \cdots < lt(f_1)$. If g_{10} is a constant, then the ideal quotient $(f_2,...,f_r):f_1$ has the Gröbner basis (with respect to <) $\{\tilde{g}_2,...,\tilde{g}_{r0}\}$ and $f_1 \notin (f_2,...f_r)\}$. [lemmadecomposition]

Indeed, if $\{f_1,...,f_r\}$ generates a zero-dimensional ideal, $\tilde{g}_{10}$ is constant by Lemma 6 in .

The algorithm is summarized as follows:

Let $A(\subset R[x_1,...,x_n])$ be a zero-dimensional ideal with a reduced Gröbner basis $\{f_1,...,f_r\}$ with respect to a monomial order <. Let B: $(f_2,...,f_r)$: f_1+(f_1). Then $V(A)$ is the union as $V(A) = V(A:B^m) \cup V(B)$. (It is easily checked that for ideals I, J, the relation $V(I\cap J) = V(I)\cup V(J)$ holds. Hence the decomposition of the affine algebraic set is equivalent to that of ideal: $K = I \cap J$.) The varieties involved in the union have following properties.

For $V(B)$ (which is one of the components of the decomposition), it holds that $V(B)=V(f_1)\cap V(\tilde{f}_2,...,\tilde{f}_r)$ and $\{\tilde{f}_2,...,\tilde{f}_r\}$ is a reduced Gröbner basis.

By lemma 4.4, $V(A:B^m)$ is the disjoint union of the zero-zets,

$$V(A:f_1^{m_1}), V((A+(f_1)):\tilde{f}_2^{m_2}),...,V((A+(f_1,\tilde{f}_2,...,\tilde{f}_{r-1})):\tilde{f}_r^{m_r})$$

These sets are other components of the decomposition of $V(A)$.

$V(A:(f_1)^m)=\varnothing$ (because $f_1 \in A$): this item is removed.

The Gröbner bases are computable for the ideals $A+(f_1):\tilde{f}_2^{m_2}$, ... , $A+(f_1,\tilde{f}_2$, ..., $\tilde{f}_{r-1})):\tilde{f}_r^{m_r}$. These Gröbner bases are in $R[x_1,...,x_{n-1}]$ (where the dimension is exactly dropped by one). Therefore we go down into $R[x_1,...,x_{n-1}]$ and in this ring we have the set of ideals which are to be processed again.

Iteratively we apply the algorithm to the set of ideals and drop the variable one by one; the process shall terminate after finite steps.

Let us consider the problem

$$f_1 = x + y^2 e, f_2 = y + x^2 e, f_3 = x^2 + y^2 - 1$$

The reduced Gröbner basis with respect to the lexicographic order $x > y > e$ is given by

$$p_1 = x + y + e, p_2 = 2y^2 + 2ye + e^2 - 1,$$
$$p_3 = 2ye^2 + 2y + e^3 + e, p_4 = e^4 - e^2 - 2$$

We apply the triangulation to $A_0 = (p_1, p_2, p_3, p_4)$. For variable x, it exists only in g_1. Thus should be added in all components of the decomposition. We only decompose the smaller system $A = (p_2, p_3, p_4)$. For the variable y, $\tilde{p}_3 = 2e^2 + 2$, $\tilde{p}_4 = e^4 - e^2 - 2$. By the removal of the redundant term, the simpler Gröbner basis for $(\tilde{p}_3, \tilde{p}_4)$ is, which is also a Gröbner basis of $(p_3, p_4):p_2$.

As for the decomposition $V(A) = V(B) \cap V(A:(e^2+1)^m)$, the components are given as

$$B = (p_3, p_4):p_2 + (p_2)$$
$$= (e^2+1, 2y^2 + 2ye + e^2 - 1) = (e^2+1, y^2 + ye - 1)$$

and

$$A:(e^2+1) = (e^2 - 2, 2y + e)$$

Indeed, the last statement implies the saturation: since, for $m = 1,2,...$,

$$A:(e^2+1)^m = (e^2 - 2, 2y + e)$$

Thus we obtain the decomposition of (f_1, f_2, f_3, f_4) as the intersection of $(e^2+1, y^2 + ye + 1, p_1)$ and $(e^2 - 2, 2y + e, p_1)$.

Simple Example of The Molecular Orbital Method by Means of Algebraic Geometry

Let us execute molecular orbital computation by means of algebraic geometry. The example is a hexagonal molecule, like benzene, where s-orbital is located at each atom and interacts only with the nearest neighbors. as is depicted in Figure 4.

The secular equation for a hexagonal molecule, like a benzene, could be given by the simplest model:

$$\begin{pmatrix} 0 & T & 0 & 0 & 0 & T \\ T & 0 & T & 0 & 0 & 0 \\ 0 & T & 0 & T & 0 & 0 \\ 0 & 0 & T & 0 & T & 0 \\ 0 & 0 & 0 & T & 0 & T \\ T & 0 & 0 & 0 & T & 0 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \end{pmatrix} = \varepsilon \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \end{pmatrix}$$

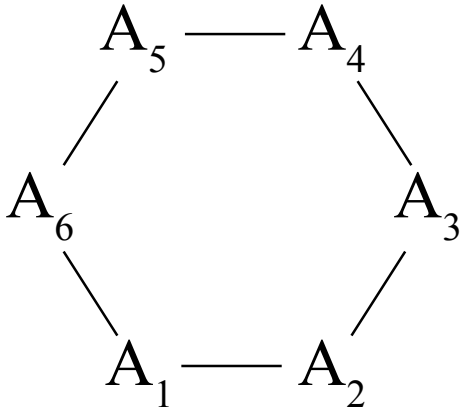

Figure 4: The framework of a hexagonal molecule. The atoms are indexed as $A_1,...,A_6$ and they interact between nearest neighbors, as are indicated by the bonds.

We place one orbital in each of the vertex of the hexagon; we assume the interaction between the nearest neighbors with the hopping parameter *T*; the wavefunction is given by the coefficients $(c_1,...,c_6)$ to six atomic orbitals. (We assume the following model: $|\psi\rangle = \sum_{i=1}^{6} C_i |a_i\rangle$ such that $\langle a_i | a_j \rangle = \delta_{i,j}$; and $H = \sum_{i=1}^{6} |a_i\rangle T \langle a_{i+1}|$ in the hexagonal closed graph with $a_7 = a_1$.)

The corresponding energy functional is given by

$$U = Tc_2(c_1 + c_3) + Tc_3(c_2 + c_4) + Tc_4(c_3 + c_5)$$
$$+Tc_5(c_4 + c_6) + T_6(c_5 + c_1) + Tc_1(c_6 + c_2)$$
$$-e(c_1^2 + c_2^2 + c_3^2 + c_4^2 + c_5^2 + c_6^2 - 1)$$

The ideal from the secular equation is represented as:

I=(-2*c1*e+2*c2*T+2*c6*T,

2*c1*T-2*c2*e+2*c3*T,

2*c2*T-2*c3*e+2*c4*T,

2*c3*T-2*c4*e+2*c5*T,

2*c4*T-2*c5*e+2*c6*T,

2*c1*T+2*c5*T-2*c6*e,

-c1^2-c2^2-c3^2-c4^2-c5^2-c6^2+1).

We assume that

$$I \subset \mathbb{Q}[\, c_1, c_2, c_3, c_4, c_5, c_6, T, e, U \,]$$

with the lexicographic monomial order

$$c_1 > c_2 > c_3 > c_4 > c_5 > c_6 > T > e > U$$

The Gröbner basis is given in Table 2:

The first entry of the list in Table 2 shows the relation between the energy e and the hopping integral T. Then the polynomials including other variables (c_6, c_5,...., c_1) appear in succession. This is the example of variable elimination.

Let us evaluate the energy functional U. For this purpose, we make a new ideal $I + (f)$ with a polynomial f which equates the variable U and the definition of the energy functional at $f = 0$:

$$f = Tc_2(c_1 + c_3) + Tc_3(c_2 + c_4)c_3 + Tc_4(c_3 + c_5)$$
$$+Tc_5(c_4 + c_6) + T_6(c_5 + c_1) + Tc_1(c_6 + c_2)$$
$$-e(c_1^2 + c_2^2 + c_3^2 + c_4^2 + c_5^2 + c_6^2 - 1) -$$

The Gröbner basis of the ideal $I + (f)$ is given in Table 3. The first polynomial gives the relation between the total energy U and the hopping integral, while the other variables are swept into remaining polynomials. Consequently, it follows that, by means of symbolic computation, we have executed the molecular orbital computation and have obtained the observable quantities: if we give T, we determine the total energy U and we have the relations for the variables of the wave-function and the eigenvalue e. As for the wave-function, there is a particular feature in the symbolic computation, which will be discussed later.

Now let us see how the primary ideal decomposition works. The decomposition for ideal $I + (f)$ is given

_[1]=e^4-5*e^2*T^2+4*T^4

_[2]=6*c6^2*e^2-6*c6^2*T^2-e^2+T^2

_[3]=2*c5*e^2*T-2*c5*T^3-c6*e^3+c6*e*T^2

_[4]=c5*e^3-c5*e*T^2-2*c6*e^2*T+2*c6*T^3

_[5]=4*c5^2*T^2-4*c5*c6*e*T-4*c6^2*e^2

+8*c6^2*T^2+e^2-2*T^2

_[6]=4*c5^2*e-4*c5*c6*T+4*c6^2*e-e

_[7]=24*c5^2*c6^2*T-4*c5^2*T-24*c5*c6^3*e

+4*c5*c6*e+24*c6^4*T-10*c6^2*T+T

_[8]=24*c5^4*T-16*c5^3*c6*e+16*c5^2*c6^2*T

-10*c5^2*T+8*c5*c6^3*e+2*c5*c6*e-4*c6^2*T+T

_[9]=c4*T-c5*e+c6*T

_[10]=c4*e+12*c5^3*T-8*c5^2*c6*e+8*c5*c6^2*T

-4*c5*T+4*c6^3*e

_[11]=c3*T-c4*e+c5*T

_[12]=c3*e-4*c4^2*c5*e+12*c4^2*c6*T+4*c4*c5^2*T

-8*c4*c5*c6*e+12*c5^2*c6*T+8*c6^3*T-4*c6*T

_[13]=c2*T-c3*e+c4*T

_[14]=c2*e-c3*T+c5*T-c6*e

_[15]=c1*T+c5*T-c6*e

_[16]=c1*e-c2*T-c6*T

_[17]=c1^2+c2^2+c3^2+c4^2+c5^2+c6^2-1

Table 2: Gröbner basis of the secular equation of the hexagonal molecule.

_[1]=4*T^4-5*T^2*U^2+U^4

_[2]=e-U

_[3]=12*c6^2*T^2-12*c6^2*U^2-e^2+3*e*U-2*T^2

_[4]=c5*T^2*U-c5*U^3+c6*e^2*T-2*c6*T^3+c6*T*U^2

_[5]=2*c5*T^3-2*c5*T*U^2+c6*e^3-2*c6*e*T^2+c6*T^2*U

_[6]=4*c5^2*U-4*c5*c6*T+4*c6^2*e-e

_[7]=4*c5^2*T^2-4*c5*c6*e*T-4*c6^2*e*U+8*c6^2*T^2+e*U-2*T^2

_[8]=24*c5^2*c6^2*T-4*c5^2*T-24*c5*c6^3*e+4*c5*c6*e

+24*c6^4*T-10*c6^2*T+T

_[9]=24*c5^4*T-16*c5^3*c6*e+16*c5^2*c6^2*T

-10*c5^2*T+8*c5*c6^3*e

+2*c5*c6*e-4*c6^2*T+T

_[10]=c4*U+12*c5^3*T-8*c5^2*c6*e+8*c5*c6^2*T-

4*c5*T+4*c6^3*e

_[11]=c4*T-c5*e+c6*T

_[12]=c3*U-4*c4^2*c5*e+12*c4^2*c6*T+4*c4*c5^2*T-8*c4*c5*c6*e

+12*c5^2*c6*T+8*c6^3*T-4*c6*T

_[13]=c3*T-c4*e+c5*T

_[14]=c2*U-c3*T+c5*T-c6*e

_[15]=c2*T-c3*e+c4*T

_[16]=c1*U-c2*T-c6*T

_[17]=c1*T+c5*T-c6*e

_[18]=c1^2+c2^2+c3^2+c4^2+c5^2+c6^2-1

Table 3: The Gröbner basis of the ideal $I + (f)$.

[1]:(p1)
_[1]=T
_[2]=e
_[3]=c1^2+c2^2+c3^2+c4^2+c5^2+c6^2-1
[2]:(p2)
_[1]=e-T
_[2]=4*c5^2-4*c5*c6+4*c6^2-1
_[3]=c4-c5+c6
_[4]=c3+c6
_[5]=c2+c5
_[6]=c1+c5-c6
[3]:(p3)
_[1]=e+T
_[2]=4*c5^2+4*c5*c6+4*c6^2-1
_[3]=c4+c5+c6
_[4]=c3-c6
_[5]=c2-c5
_[6]=c1+c5+c6
[4]:(p4)
_[1]=e+2*T
_[2]=6*c6^2-1
_[3]=c5+c6
_[4]=c4-c6
_[5]=c3+c6
_[6]=c2-c6
_[7]=c1+c6
[5]:(p5)
_[1]=e-2*T
_[2]=6*c6^2-1
_[3]=c5-c6
_[4]=c4-c6
_[5]=c3-c6
_[6]=c2-c6
_[7]=c1-c6

Table 4: Primary ideal decomposition of ideal $I + (f)$. The ideal decomposes into ve primary ideals, each of which is represented by the generators.

in Table 4. Each entry in the list is the primary ideal $\{p_i | i = 1,...,5\}$, the intersection of which shall build the polynomial ideal of secular equation $I = \bigcap_{(i=1)}^{5} p_i)$.

Table 5 gives the Gröbner basis for the ideal $\left(p_i + \left(f\right)\right)$. The first entry gives the linear relation between the total energy U and the hopping parameter T. This is the improvement in the result by the use of primary ideal decomposition; in Table 3 of the Gröbner basis, we have obtained the relation between U and T, but the polynomial is not decomposed yet.

The dimension of the ideals is given in Table 6. (We refer to the Krull dimension of the quotient ring by an ideal by the

[1](p1+(f))
_[1]=U
_[2]=T
_[3]=e
_[4]=c1^2+c2^2+c3^2+c4^2+c5^2+c6^2-1

[2](p2+(f))
_[1]=T-U
_[2]=e-T
_[3]=4*c5^2-4*c5*c6+4*c6^2-1
_[4]=c4-c5+c6
_[5]=c3+c6
_[6]=c2+c5
_[7]=c1+c5-c6

[3](p3+(f))
_[1]=T+U
_[2]=e+T
_[3]=4*c5^2+4*c5*c6+4*c6^2-1
_[4]=c4+c5+c6
_[5]=c3-c6
_[6]=c2-c5
_[7]=c1+c5+c6

[4](p4+(f))
_[1]=2*T+U
_[2]=e+2*T
_[3]=6*c6^2-1
_[4]=c5+c6
_[5]=c4-c6
_[6]=c3+c6
_[7]=c2-c6
_[8]=c1+c6

[5](p5+(f))
_[1]=2*T-U
_[2]=e-2*T
_[3]=6*c6^2-1
_[4]=c5-c6
_[5]=c4-c6
_[6]=c3-c6
_[7]=c2-c6
_[8]=c1-c6

Table 5: Gröbner basis for the ideals $p_i + (f)$.

Ideal	$\dim_k(R/I)$
$p_{} + (f)$	5
$p_2 + (f)$	2
$p_3 + (f)$	2
$p_4 + (f)$	1
$p_5 + (f)$	1

Table 6: The dimension of the ideals $p_i + (f)$.

phrase "dimension of the ideal" according to the custom of computational algebraic geometry.)

As for $U = T = e = 0$, the affine algebraic set is determined by $U = T = e = 0$ and $c_1^2 + \cdots + c_6^2 = 1$; thus there are five degrees of freedom for $(c_1,..,c_6)$. As for $p_4 + (f)$ and $p_5 + (f)$, the only one indeterminate is the hopping integral T, which contribute one to the dimension of the ideal; $(c_1,...,c_6)$is determined up to sign. As for $p_2 + (f)$ and $p_3 + (f)$, the hopping integral T is still an indeterminate and contributes one to the dimension; $(c_1,...,c_6)$is not determined explicitly, unless c_5 or c_6 would be explicitly given in the quadratic equation in the list (which is one-dimensional geometrical object). In this circumstance, the dimension of the ideal rises by one. The increase of the dimension in the cases of $p_2 + (f)$ and $p_3 + (f)$ is, by the familiar phrase of physics, due to the degeneracy in the eigenvalue. For such cases in the numerical computation, the solvers automatically return the ortho-normalized basis vectors. The numerical library determines them by an arbitrary way. However, by summing up the degenerated eigenstates with the equal weights, one can compute the observable quantum mechanical quantity which is free from this sort of ambiguity. In contrast, the symbolic computation processes the equation up to the "minimal" polynomials of the variables of the wave-functions and it does not anymore. The wave-functions are, however, non-observable quantities; one can eliminate them from the polynomial equations by symbolic computation so that one could obtain only observable quantities, such as energy. In fact, it is not always true that the degeneracy of eigenvalues should lead to non-zero-dimensional character of eigenspace: for example, consider the following polynomial as the energy functional:

$$f = -c_1(c_2 + c_3) - c_2(c_1 + c_3) - c_3(c_1 + c2) + \left(c_1^4 c_2^4 + c_2^4 c_3^4 + c_3^4 c_1^4\right) - e\left(c_1^2 + c_2^2 + c_3^2 - 1\right)$$

The local energy minima are represented by discrete points (not continuous) both in real and in complex number. For example, $e = -3/2$ is the eigenvalue with six fold degeneracy and the corresponding eigenvectors are discrete (as zero-dimensional ideal) as follows:

$$(c_1, c_2, c_3) = \pm\left(1/\sqrt{2}, -1/\sqrt{2}, 0\right), \pm\left(1/\sqrt{2}, 0, -\sqrt{2}\right), \pm\left(0, 1/\sqrt{2}, -\sqrt{2}\right)$$

Outlook for Related Topics

We have seen how the computational algebraic geometry could be applied to the molecular orbital theory, in so far as the equations could be represented by polynomials. In this section, we will see the related topics on the symbolic computation by means of polynomials.

Polynomial optimization

Polynomial optimization is a numerical method which solves the optimization problem given by polynomial equations and inequities [47,48-51].

Example 8.1 Consider the cost function $g(x_1, x_2) = x_2$ and the constraints $f_1 = 5 - x_1^2 - x_2^2 \geq 0$, $f_2 = 1 - x_1 x_2 \geq 0$, $f_3 = x1 - x_2 \geq 0$.

The problem is given by:

Maximize the cost multivariate polynomial function $g(x)$

with the constraint of multivariate polynomial function $f_i(x) \geq 0$.

In other words, the cost function g is to be maximized in the semi-algebraic set defined by f_1, f_2 and f_3, as in Figure 5.

The curves $5 - x^2 - y^2 = 0$, $y = x$, $1 - xy = 0$ are depicted. The y-coordinate of the upper-right intersection point between the diagonal line and the hyperbola gives the solution of the optimization problem presented in the main article.

The curves $5 - x^2 - y^2 = 0$, $y = x$, $1 - xy = 0$ are depicted. The y-coordinate of the upper-right intersection point between the diagonal line and the hyperbola gives the solution of the optimization problem presented in the main article.

The key idea is to replace the monomials $x_1^i x_2^j$ with variables y_{ij}. The variables should satisfy relations such as $y_{p,q} y_{r,s} = y_{p+q,r+s}$ and $y_{00} = 1$. Let us define the first-order moment matrix in the following style:

$$M_1(y) = \begin{pmatrix} 1 & y_{10} & y_{01} \\ y_{10} & y_{20} & y_{11} \\ y_{01} & y_{11} & y_{02} \end{pmatrix}$$

By means of the formalism of the polynomial optimization, the problem is restated as follows.

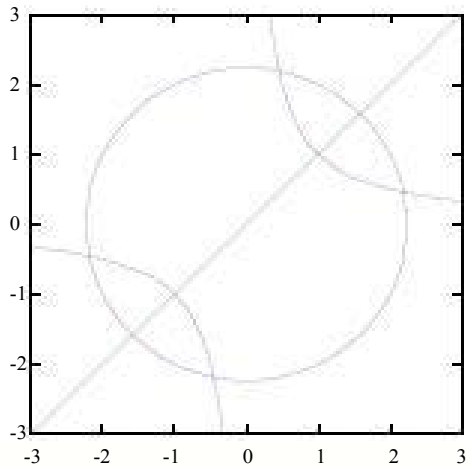

Figure 5: The curves $5\text{-}x^2\text{-}y^2 = 0$, $y = x$, $1 - xy = 0$ are depicted. The y-coordinate of the upper-right intersection point between the diagonal line and the hyperbola gives the solution of the optimization problem presented in the main article.

Maximize the linear cost function y_{01},

With the constraint that the moment matrix $M_1(y)$ is semi-positive definite,

With the constraint of multivariate polynomial functions: $\hat{f}_1 = 5 - y_{20} - y_{02} \geq 0$, $\hat{f}_2 = 1 - y_{11} \geq 0$, $\hat{f}_3 = y_{10} - y_{01} \geq 0$

In the above, the constraint of the moment matrix comes from the semi-positive-definiteness of the quadratic form:

$$0 \leq \left(\sum_{i=1}^{2} c_i x_i \right) \left(\sum_{i=1}^{2} c_i x_i \right) \simeq \sum_{i,j} c_i c_j y_{ij}$$

Hereafter we denote the semi-positive definiteness of a matrix M as $M \succeq 0$.

The optimization problem is solved by the standard way of semi-positive-definite programming. We can formulate the dual problem also. In general, it is not guaranteed that the use of the first-moment matrix would suffice to give the correct answer; indeed the formulation should be given in the matrices of infinite dimension, which include the moments of higher orders up to the infinity. In addition, in the above formulation, there is no constraint for the condition $y_{p,q} y_{r,s} = y_{p+q,r+s}$. We only expect that the moment matrix would be reduced into the one with lower and suitable rank at the optimum. Actually, the above procedure is an approximation and the accuracy is improved by the use of larger matrices.

Let $y = (y_\alpha)_{\alpha \in \mathbb{N}^n}$, where y_α represents $\mathrm{x}^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$. Let denote the degree of ( ) as $|\alpha| = \sum_{i=1}^{n} \alpha_i$. We try to optimize the problem in the limited range of $(y_\alpha)_{\alpha \in \mathbb{N}^n}$, such that $|\alpha| \leq 2r$.

For $y = (y_{\alpha_1}, y_{\alpha_1}, \ldots, y_{\alpha_N})$ (such that $|\alpha_N| \leq 2r$), the *r*-th order moment matrix $M_r(y)$ is constructed as follows:

$$M_r(y)[1,1] = 1,$$
$$M_r(y)[i,1] = y_{\alpha_i},$$
$$M_r(y)[1,i] = y_{\alpha_i},$$
$$M_r(y)[i,j] = y_{\alpha_i + \alpha_j},$$

where the index *i, j* are taken in the range such that $|\alpha_i| \leq r$.

Let $p(x)$ be the polynomial constraint :

$$p(x) = \sum_{beta} c_\beta \mathrm{x}^\beta$$

For $p(x)$, the localizing matrix is defined by:

$$M_s(py)[i,j] = \sum_{\beta} c_\beta y_{\alpha_i + \alpha_j + \beta}$$

where the index i, j are taken in the range such that $|\alpha_i| \leq s$. This matrix should be semi-positive definite, too.

In general, a global polynomial optimization problem is given by

$$p^* = \min_y F(x) = \sum_\alpha f_\alpha \mathrm{x}^\alpha$$

such that $G_i(x) \geq 0$, $i = 1, 2, \ldots$.

Assume that the degree of $g_i(x)$ to be $2d_i - 1$ or $2d_i$. In correspondence to the above global polynomial problem, The relaxation of order *k* is stated in this way:

$$p_k^* = \min_y \sum_\alpha f_\alpha y^\alpha$$

such that $M_k(y) \succeq 0$

and $M_{k-d_i}(G_i y) \succeq 0$, $i = 1, 2, \ldots$

It is guaranteed that, as the degree k increases, the optima p_k^* converges to the global optimum *p.*

Example 8.2 Let us compute these matrices.

The second-order moment matrix is given by

$$M_2(y) = \begin{pmatrix} 1 & y_{10} & y_{01} & y_{20} & y_{11} & y_{02} \\ y_{10} & y_{20} & y_{11} & y_{30} & y_{21} & y_{12} \\ y_{01} & y_{11} & y_{02} & y_{21} & y_{12} & y_{03} \\ y_{20} & y_{30} & y_{21} & y_{40} & y_{31} & y_{22} \\ y_{11} & y_{21} & y_{12} & y_{31} & y_{22} & y_{13} \\ y_{02} & y_{12} & y_{03} & y_{22} & y_{13} & y_{04} \end{pmatrix}$$

The higher-order moment matrices are computed likewise.

The localizing matrices are computed for the polynomials f_1, f_2 and f_3 in the example problem.

For $f_1 = 5 - x_1^2 - x_2^2$,

$$M_1(f_1 y) = \begin{pmatrix} 5 - y_{20} - y_{02} & 5y_{10} - y_{30} - y_{12} & 5y_{01} - y_{21} - y_{03} \\ 5y_{10} - y_{30} - y_{12} & 5y_{20} - y_{40} - y_{22} & 5y_{11} - y_{31} - y_{13} \\ 5y_{10} - y_{21} - y_{02} & 5y_{11} - y_{31} - y_{13} & 5y_{02} - y_{22} - y_{04} \end{pmatrix}$$

For $f_2 = 1 - x_1 x_2$,

$$M_1(f_2 y) = \begin{pmatrix} 1 - y_{11} & y_{10} - y_{21} & y_{01} - y_{12} \\ y_{10} - y_{21} - y_{20} & y_{20} - y_{31} & y_{11} - y_{22} \\ y_{01} - y_{12} & y_{11} - y_{22} & y_{02} - y_{13} \end{pmatrix}$$

For $f_3 = x_1 - x_2$,

$$M_1(f_2 y) = \begin{pmatrix} y_{10} - y_{01} & y_{20} - y_{11} & y_{11} - y_{02} \\ y_{20} - y_{11} & y_{30} - y_{21} & y_{21} - y_{12} \\ y_{11} - y_{02} & y_{21} - y_{12} & y_{12} - y_{03} \end{pmatrix}$$

Observe that these localizing matrices include the entries of the second order moment matrix and do not contain superfluous ones. We can optimize the given problem concisely with the use of $M_2(y), M_1(f_1 y), M_1(f_2 y), M_1(f_3 y)$.

As is demonstrated in [2], once the molecular orbital theory has been built over the polynomial system on the ground of algebraic geometry and commutative algebra, it enables us to joint the equation of conventional quantum mechanics and the extra constraints into a set of polynomial equations. We solve the problem through the collaboration of numerical and symbolical methods. The computational scheme is basically to determine the affine algebraic set described by the set of equations. However, it is somewhat inconvenient that we should use only equations for the general optimization problem. It seems that polynomial optimization could get over such limitations because it could deal with the constraints by inequities in the semi-algebraic set. The mathematical ground is "real algebraic geometry" which contains a various range of interests.

Quantifier elimination

When we deal with equations and inequities of polynomials, we often ask ourselves about the existence of the solutions. For example, under what condition would a quadratic equation have roots? The "quantifier elimination" (QE) is the computational process to answer this sort of questions: when the question is given by $\exists x \in \mathbb{R}.\left(x^2+bx+c=0\right)$, the computer eliminates the quantifier ($\exists$) and returns the simplified form $b^2-4ac \geq 0$ as the answer. In fact, there are general theories for executing such sort of simplifications, proposed by several mathematicians, such as by Fourier, by Motzkin, and by Tarski [52,53], or Presburger arithmetic. But those algorithms are not practical. Afterward, more practical algorithms by Collins and by others have come into use, called "Cylindrical Algebraic Decomposition" (CAD). The theoretical ground of the standard algorithm in Algebraic Cylindrical Decomposition are given in [46,54-58]. There are computer several packages in which this algorithm is implemented, such as QEPCAD [59], Mathematica [60], Maple [61], and Reduce [62].

Since CAD algorithm is apparently related to the theme of this article, let us review the computational procedure in this section. Let us consider the problem through a simpler example of quantifier elimination:

$$\exists a.\left(x^2+ax+1=0\right).$$

We can simplify the above prenex form into the one without quantifier, such as $a^2-4 \geq 0$.

The cylindrical algebraic decomposition analyses the critical point of $f(a,x)=x^2+ax+1=0$ in two-dimensional real $a-x$ plane. The critical points are the solutions of $f(a,x)=x^2+ax+1=0$ and $\frac{\partial f(a,x)}{\partial x}=2x+a$. They are also the solution of $x^2+ax+1=0$, $2x+a=0$ and $x\left(2x+a\right)=0$. Thus we obtain the matrix equation:

$$\begin{pmatrix} 1 & a & 1 \\ 2 & a & 0 \\ 0 & 2 & a \end{pmatrix}\begin{pmatrix} x^2 \\ x \\ 1 \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

The determinant of the matrix in the left-hand side is the discriminant of $f(a,x)$. If it is zero, the matrix equation would permit non-zero vector solution. Hence we project the polynomial in one ring into a polynomial in another ring of lower dimension (Projection step). We now analyse the projected polynomial (the discriminant) in order to inquire after the existence of the root. As the discriminant is $4-a^2$, we can divide the a-axis into five cells: $(-\infty,-2),\{-2\},(-2,2),\{2\},(2,\infty)$ so that each of them gives the distinct sign of the discriminant.

Let us build the set of cylinders in *a*-*x* plane which pass through each cells in *a*-axis. They are given by

$$(a,x) \in (-\infty,-2)\times(-\infty,\infty),$$
$$(a,x) \in (-2,2)\times(-\infty,\infty),$$
$$(a,x) \in (-2,2)\times(-\infty,\infty),$$
$$(a,x) \in \{2\}\times(-\infty,\infty),$$
$$(a,x) \in (2,\infty)\times(-\infty,\infty).$$

In each cylinder, we should check the zeros and the sign condition of $f(a,x)=x^2+ax+1$ in $a-x$ plane. The solutions of $f(a,x)$ are listed as follows.

$a \in (-\infty,-2)$: the solutions are $x_1=\left(-a-\sqrt{a^2-4}\right)/2$ and $x_2=\left(-a+\sqrt{a^2-4}\right)/2$.

$a=-2$: the solution is $x_1=1$.

$a \in (-2,2)$: no solution.

$a=2$: the solution is $x_1=-1$.

$a \in (-2,\infty)$: the solutions are $x_1=\left(-a-\sqrt{a^2-4}\right)/2$ and $x_2=\left(-a+\sqrt{a^2-4}\right)/2$.

(In the actual computation, we do not try to obtain such analytic solutions in uplifting step. Instead, we place one sampling point, say a_s, in each subdivision, and we inspect the sign condition and the solution of univariate polynomial $f(a_s,x)$.)

The cylinders are again divided into cells according to the sign condition of $f(a,x)$. For example, the cylinder $(-\infty,-2)\times(-\infty,\infty)$ is divided by five cells:

$$(-\infty,-2)\times(-\infty,x_1);$$
$$(-\infty,-2)\times\{x_1\};$$
$$(-\infty,-2)\times(x_1,x_2);$$
$$(-\infty,-2)\times\{x_2\};$$
$$(-\infty,-2)\times(x_2,\infty).$$

For other cylinders, we construct the cells likewise, as is illustrated in Figure 6. These cells in *a*-*x* plane are distinguished by the sign conditions of $f(a,x)=x^2+ax+1$ and $\mathrm{dis}(f)=a^2-2$. Then we seek the cells which would satisfy the condition of the first question about the existence of the roots of $x^2+ax+1=0$, and by joining the cells which satisfy the requirement, we find the answer: $a \leq 2$ or $a \geq 2$.

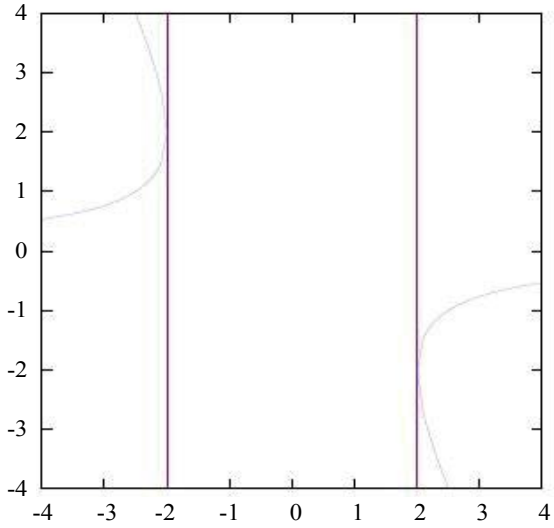

Figure 6: The cylindrical algebraic decomposition for x^2+ax+1. The vertical and horizontal axes represent the variables x and a respectively. The zone is decomposed into cells by the solid lines and curves; each cell is distinguished from others by the sign conditions of two polynomials, x^2+ax+1 and a^2-4.

The cylindrical algebraic decomposition for x^2+ax+1. The vertical and horizontal axes represent the variables *x* and *a* respectively. The zone is decomposed into cells by the solid lines and curves; each cell is distinguished from others by the sign conditions of two polynomials, x^2+ax+1 and a^2-4.

The cylindrical algebraic decomposition for x^2+ax+1. *The vertical and horizontal axes represent the variables* x *and* a *respectively. The zone is decomposed into cells by the solid lines and curves; each cell is distinguished from others by the sign conditions of two polynomials,* $\mathrm{x}^2+\mathrm{ax}+1$ *and* a^2-4.

In general multivariate case of CAD, the algorithm executes the multi-step projection (from n-variables to one-variable) and uplifting (from an axis to the whole space).

There are examples of QE with the taste of molecular orbital theory. Let $e,(x,y)$ be the energy and the wavefunction of the simple diatomic system, such that

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = e\begin{pmatrix} x \\ y \end{pmatrix}$$

Example 8.3 $\exists e : e<0 \wedge x+ey=0 \wedge y+ex=0 \wedge x^2+y^2-1=0 \wedge x+y=0..$

The prenex form inquires if the negative e (the energy) would exists in the diatomic molecule of asymmetric configuration $x+y=0$. The quantifier elimination concludes that the formula is

False

Example 8.4

$$\exists e : e<0 \wedge x+ey=0 \wedge y+ex=0 \wedge x^2+y^2-1=0 \wedge x-y=0$$

The prenex form inquires if the negative e (the energy) would exists in the diatomic molecule of symmetric configuration $x-y=0$. The quantifier elimination concludes that the formula is simplified as

$$x^2+y^2-1=0 \wedge x-y=0$$

This is the process of quantifier elimination. If the prenex form contains several polynomials $\{f_j(x_1,x_2,...,x_n) \mid j=1,...,m\}$, we have to compute the intersection of f_i and f_j for $i \neq j$ as well as the critical point of each f_i. The intersection is computed by projection by means of variable elimination, the tool of which is "resultant". Assume that x_n are the uni-variate polynomials of x_n, in which the coefficients are the polynomials of $\{x_1,..,x_{n-1}\}$. In this assumption, the resultant for two polynomials

$$A = a_0x^d + a_1x^{d-1} + \cdots + a_d$$

and

$$B = b_0x^e + b_1x^{e-1} + \cdots + b_e$$

is the determinant of a square matrix of dimension *d+e*, defined as

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_d & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_{d-1} & a_d & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_0 & a_1 & \cdots & \cdots & a_d \\ b_0 & b_1 & \cdots & b_e & \cdots & \cdots & 0 \\ 0 & b_0 & \cdots & b_{e-1} & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & b_0 & b_1 & \cdots & \cdots & b_e \end{pmatrix}$$

in which the rows are made from the array of coefficients of $\{x^iA \mid i=e-1,.,,,0\}$ and $\{x^jB \mid j=d-1,...,0\}$ so that the product of the matrix and the vector $(x^{d+e},x^{d+e-1},...,x,1)$ should give those set of polynomials. The discriminant of $f(x)$ is a special case as the resultant of $f(x)$ and $\frac{df(x)}{dx}$.

We expect that quantifier elimination would be applicable to the molecular orbital theory when we give the polynomial representation to the problem. If the quantifier elimination goes well, we would obtain the polynomial representation of the solution of the optimization problem; we could render the zone and the boundary in the parameter space which shall satisfy our requirement; we might "reason" for the question of quantum mechanics by means of the rigorous foundation of logic. However, at present, the computer and the algorithm are still powerless; indeed the complexity of the algorithm, in the worst case, is double exponential in the number of variables . (This is because of the enormous number of combinations of polynomials in the process of variable-elimination.) Therefore we must expect some breakthrough both in algorithm and in computer architecture in order that we could apply quantifier elimination for the practical purpose.

Polynomial optimization and wave-geometry

In the above examples, we implicitly assume that all of the required ingredients are polynomials. They are generated by the method of quantum chemistry: by the use of localized atomic basis, the integrodifferential equation is converted into the secular equation of analytic functions, and the latter is furthermore approximated by polynomials. On the other hand, the fundamental equations of quantum mechanics always involve differential operators. Indeed the symbolic computation would be applicable to the algebra generated by variables and differentials (G-algebra); the Gröber basis could be computed by extending the Buchberger's algorithm (Mora's algorithm). However, G-algebra is rather a purely mathematical topic and it seems to be powerless in solving numerical problems.

For this issue, the aforementioned polynomial optimizations would give us some hint. The key idea is to replace the monomials in the equation with the variables of one-degree, and the latter variables are determined by the framework of semi-positive definite programming.

The algorithm of polynomial optimization is based on the measure theory. The variables of degree one, corresponding to the monomials $X^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_1}$, represent the integrals in the moment problem,

$$y_\alpha = \int X^\alpha d\mu$$

by means of some probability measure μ, which satisfies $\int d\mu = 1$. We construct the entry of the moment matrix in the following form

$$y_{\alpha,\beta} = \int X^\alpha X^\beta d\mu$$

Instead of directly determining the measure, however, the algorithm computes the moments $y_{\alpha,\beta}$ by utilizing the constraints among them so that the objective function would be maximized.

This foundation of the algorithm has a great significance: it is plausible that, if we inspect the problem from the analogy of quantum mechanics, the measure $d\mu$ might be replaced by $|\phi(x)|^2 dx$ by a certain "wavefunction" ϕ, and the moments will be given by the expectation value in the sense of quantum mechanics. As the expectation values of the products of coordinate operators and the differential operators can be computed, we can extend the idea of the moment matrix. For the univarite case, the typical integrals are given by

$$y_{ij} = \left(\phi \middle| x^i x^j \middle| \phi\right)$$

or

$$y_{i;j} = \left(\phi \middle| x^i \left(\frac{\partial}{\partial x}\right)^j \middle| \phi\right).$$

Let us consider the simplest problem: the harmonic oscillator.

The total energy of the harmonic oscillator is given by the sum of squares of the kinetic-momentum operator p and the coordinate operator $x : H = p^2 + x^2$, with the relation:

$$= -\sqrt{-1}h$$

In order to avoid the argument in the complex number, we make use of $u = hd/dx$, instead of p.

We define the extended moment matrix as

$$M\left[x^i u^j\right]\left[x^k u^l\right] = \int \left(x^i u^k \phi\right)\left(x^i u^k \phi\right) dx$$

This sort of integral is rearranged by the linear combination of those terms

$$M\left[x^m u^n\right] = \int \phi\left(x^m u^n \phi\right) dx.$$

The the moment matrix (indexed by $1, x, u$) is given as:

$$\begin{pmatrix} 1 & M[x] & 0 \\ M[x] & M[xx] & -h/2 \\ 0 & -h/2 & M[-uu] \end{pmatrix}.$$

(In the above, $M[-uu] = -M[uu]$ due to the linearity of the constant.) In order to compute that matrix, we have used use the relations:

$$M[u][1] = \int \left(h\frac{d}{dx}\phi\right)\phi dx = 0$$

$$M[u][u] = \int \left(h\frac{d}{dx}\phi\right)\left(h\frac{d}{dx}\phi\right) dx = \int \phi\left(-h^2\frac{d^2}{dx^2}\phi\right) dx = M[-uu]$$

$$\begin{aligned} M[u][x] &= \int \left(h\frac{d}{dx}\phi\right)(x\phi)\,dx = \int \phi\left(-h\frac{d}{dx}\cdot x\right)\phi\,dx = -M[ux] \\ &= \int \phi\left(-h - x\frac{d}{dx}\right)\phi dx = -M[xu] - h. \end{aligned}$$

In order to see the necessity of $h/2$, let us consider the quadratic form:

$$\int \left[(au+bx)\phi\right]\left[(au+bx)\phi\right] dx (\geq 0)$$

This quadratic form is represented by

$$\begin{aligned} & -a^2 M[uu] + b^2 M[xx] + ab\left(-M[ux] + M[xu]\right) \\ = & -a^2 M[uu] + b^2 M[xx] - abh \\ = & (a,b)\begin{pmatrix} M[-uu] & -h/2 \\ -h/2 & M[zz] \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} (\geq 0) \end{aligned}$$

The semi-positive definiteness of the quadratic form is replaced by that of the matrix.

Semi-positive definiteness of the moment matrix demands these relations:

$$M[xx] \geq 0$$

$$M[-uu] \geq 0$$

$$M[xx]M[-uu] - \frac{h^2}{4} \geq 0$$

$$\det(M) \geq 0$$

$$M[xx] - M[x]M[x] \geq 0$$

(The diagonal entries of the matrix are positive; the values of determinant of 2 by 2 minors, taken along the diagonal, are positive; and the determinant of the matrix is positive.)

With this condition, the optimum of $E = M[-uu] + M[xx]$ is obtained at $M[xx] = M[-uu] = \frac{1}{2}h$ and $M[x] = 0$. The solution might be obtained by several methods. The authors of this article (Kikuchi and Kikuchi) had tried several algorithms to solve them in the sequence of works: the solution by means of QE in [63]; by means of particle swarm optimiza on in [64]; by means of directly determining the measure μ itself in [65].

Maybe the significance of this algorithm is that one can "quantize" the polynomial equations by providing the variables $\{x_i\}$ with the differential operators $\left\{h\frac{d}{dx}\right\}$; the search of the roots of the polynomial $W(x)$ is replaced by the ground-state computation of the quantum Hamiltonian $H = -h^2\frac{d^2}{dx^2} + W(x)$; in the limit $h \to 0$, the "probability distribution" of the quantum system shall coincide with the affine algebraic set $V(W)$. It is not so audacious to say that we discover the seminal idea of "wave geometry" [66], which is the counterpart in mathematics to the "wave mechanics" in physics. In the middle of twentieth century, in fact, Mimura et al. proposed the idea of "wave geometry": their fundamental idea is to assume the line elements ds^2 in differential geometry as the operator in quantum mechanics, to which, therefore, the differential operator $\{h\frac{d}{ds}$ is coupled. In contrast to that theory, our idea of "wave geometry" is based upon algebraic geometry, and we expect that our idea

would be applicable to quantitative – numeric or symbolic – computation by means of powerful techniques developed for quantitative simulation of quantum dynamics and also by means of the modern theory of algebra.

Available Packages of Symbolic Computation

There are several packages of symbolic computation by which we can compute Gröbner bases or primary ideal decomposition.

- CoCoA : Computer algebra system [67].
- GAP: Software for computational discrete algebra. The chief aim of the package is to execute the computation in the group theory, but it could process polynomials [68]. As for the application of GAP software in material physics, see the work of Kikuchi [69], and the article by Kikuchi and Kikuchi .
- Macaulay 2: Computer algebra system [70, 71].
- Mathematica: Technical computing system for almost all fields of science and industry [60].
- Maple: Symbolic computation software for general purpose. The primary ideal decomposition is implemented at the package "Regular Chains Package" [61].
- Maxima: Symbolic computation software for general purpose [72].
- Reduce: Computer algebra system [62].
- SINGULAR: Computer algebra system [73]. It contains various libraries to solve the problems in algebraic geometry. It also contains the extension package "Plural" for non-commutative algebra. One can learn how to compute by Singular from introductory textbooks [40,74].
- As for quantifier elimination, also there are available packages.
- QEPCAD: A free software, which does quantifier elimination by means of Partial Cylindrical Algebraic Decomposition [59].
- Reduce
- Mathematica
- Maple
- There is a platform system which bundles several free software packages in mathematical science.
- SageMath: Open-Source Mathematical Software System. From this platform, one can utilize a lot of software packages both of numerical and symbolic computations (in which Gap, Maxima, and Singular are included) [75].
- There are a lot of research centers of symbolic computations. A great deal of computer algebra systems are the products of the studies over long years in several universities. One can find software implementations of the latest researches of INRIA in France:
- INRIA: l'institut national de recherche dédié aux sciences du numérique. The research programs, at the interplay of algebra, geometry and computer science, are ongoing now [76-79].

Summary

Dear readers, our voyage has now ended up the planned course. How do you think about the connection between quantum mechanics and algebraic geometry? We have found it even in the familiar region of quantum chemistry. Algebraic geometry is not a language of another sphere; it is a tool to solve actual problems with quantitative precision. Is it interesting for you? Or have you judged coldly that it is a plaything?

In this article, at first, we have demonstrated a model case of symbolic-numeric computation of molecular orbital theory with the taste of algebraic geometry. Then we have expounded the related mathematical concepts in commutative algebra and algebraic geometry with simple examples. In addition, we have introduced several mathematical and computational methods, which would be connected to this post-contemporary theory of quantum chemistry. The two main principles of the theory are *to represent the involved equations by polynomials* and *to process the polynomials by computer algebra*. Then one can analyze the polynomial equations and unravel the dependence between the variables. In the traditional molecular orbital theory, the principal mathematical tool is the linear algebra. Indeed, it is a subset of the commutative algebra. For instance, the diagonalization of the matrix and the orthonormality of eigenstates would be comprehensible in a wider context: the primary ideal decomposition. And the latter has a close relation to the other fundamental ideas in algebraic geometry: the resolution of singularity and the normalization of the variety. Besides, the polynomial approximation (inevitable in our theory) should ideally be embedded into the "completion" of commutative rings; we do this approximation with the finite number of symbols for the sake of facile computations in the limited resources. Without doubt, there are a lot of other concepts in commutative algebra and algebraic geometry which would be embodied in the application of computational quantum mechanics. You should Ask, and it will be given to you...

Or,

petite, et dabitur vobis; quaerite, et invenietis; pulsate, et aperietur vobis.

It will be a felicity for us, for the authors of this article, if you enjoy every bite of the "quantum chemistry with the view toward algebraic geometry" and if this article stirs your curiosity; we heartily greet your participation in the research of this new theme.

Acknowledgment

The authors are grateful to all readers who have spent the precious time to accompany with the authors through the seemingly "arid" topics toward the end of the article.

References

1. Attila Szabo, Neil S Ostlund (2012) Modern quantum chemistry: introduction to advanced electronic structure theory.

2. Akihito Kikuchi (2013) An approach to rst principles electronic structure computation by symbolic-numeric computation. QScience Connect.
3. David Eisenbud (2013) Commutative Algebra: with a view toward algebraic geometry. Springer Science & Business Media.
4. Miles Reid, Reid Miles (1995) Undergraduate commutative algebra. Cambridge University Press.
5. Daniel Perrin (2007) Algebraic geometry: an introduction. Springer Science & Business Media.
6. David A Cox, John Little, Donal O'shea (2006) Using algebraic geometry. Springer Science & Business Media.
7. David Cox, John Little, Donal OShea (2013) Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra. Springer Science & Business Media.
8. Thomas Becker, Volker Weispfenning (1993) Gröbner bases. In Gröbner Bases. Springer.
9. Viviana Ene, J rgen Herzog (2011) Gröbner Bases in Commutative Algebra. American Mathematical Soc.
10. Wolfram Decker, Theo de Jong, Gert-Martin Greuel, Gerhard Pster (1999) The normalization: a new algorithm, implementation and comparisons. Computational Methods for Representations of Groups and Algebras 173: 177-185.
11. Wolfram Decker, Christoph Lossen (2006) Computing in algebraic geometry. Algorithms and computation in mathematics.
12. Jacek Bochnak, Michel Coste, Marie-Francoise Roy (2013) Real algebraic geometry. Springer Science & Business Media.
13. Jean Bernard Lasserre (2015) An introduction to polynomial and semi-algebraic optimization,volume 52. Cambridge University Press.
14. Teresa Crespo, Zbigniew Hajto, Juan Jose Morales Ruiz (2007) Introduction to di erential Galois theory.
15. Primitivo Acosta-Humanez and David Blazquez-Sanz (2006) Non-integrability of some hamiltonians with rational potentials.
16. Primitivo Belen Acosta-Humanez, Henock Venegas-Gomez (2019) Liouvillian solutions of schrn" odinger equation with polynomial potentials using grn" obner basis.
17. Daniel Lazard (1983) Gröbner bases, gaussian elimination and resolution of systems of algebraic equations. In European Conference on Computer Algebra, Springer.
18. Patrizia Gianni, Barry Trager, Gail Zacharias (1988) Gröbner bases and primary decomposition of polynomial ideals. Journal of Symbolic Computation 6: 149-167.
19. Antonio Montes and Michael Wibmer (2010) Gröbner bases for polynomial systems with parameters. Journal of Symbolic Computation 45: 1391-1425.
20. Bruno Buchberger (1965) An algorithm for finding a basis for the residue class ring of a zerodimensional polynomial ideal.
21. Bruno Buchberger (1965) Ein algorithmus zum aunden der basiselemente des restklassenringesnach einem nulldimensionalen polynomideal.
22. Rudiger Gebauer, H Michael Moller (1988) On an installation of buchberger's algorithm. Journal of Symbolic Computation 6: 275-286.
23. Ene V, Jurgen Herzog (2012) Gröbner bases in Commutative ALgebra. American Mathematical Society.
24. Grete Hermann (1998) The question of nitely many steps in polynomial ideal theory. ACM SIGSAM Bulletin 32: 8-30.
25. Thomas W Dube (1990) The structure of polynomial ideals and Gröbner bases. SIAM Journal on Computing 19: 750-773.
26. Manuela Wiesinger-Widi (2011) Gröbner bases and generalized sylvester matrices. ACM Comm.Computer Algebra 45: 137-138.
27. Ernst W Mayr, Albert R Meyer (1982) The complexity of the word problems for commutative semigroups and polynomial ideals. Advances in mathematics 46: 305-329.
28. Dung T Huynh (1986) A superexponential lower bound for Gröbner bases and church-rosser commutative thue systems. Information and Control 68: 196-206.
29. Marc Giusti (1984) Some selectivity problems in polynomial ideal theory. International Symposium on Symbolic and Algebraic Manipulation, Springer.
30. H Michael Moller and Ferdinando Mora (1984) Upper and lower bounds for the degree of Gröbner bases. International Symposium on Symbolic and Algebraic Manipulation, Springer.
31. Francis Sowerby Macaulay (1902) Some formulae in elimination. Proceedings of the London Mathematical Society 1: 3-27.
32. Marc Giusti (1985) A note on the complexity of constructing standard bases. In European Conference on Computer Algebra, Springer.
33. Magali Bardet, Jean-Charles Faugere, Bruno Salvy (2015) On the complexity of the f5 Gröbner basis algorithm. Journal of Symbolic Computation 70: 49-70.
34. Jean-Charles Faugere (1999) A new ecient algorithm for computing Gröbner bases (f4). Journal of pure and applied algebra 139: 61-88.
35. Jean Charles Faugere (2002) A new ecient algorithm for computing Gröbner bases without reduction to zero (f 5). Proceedings of the 2002 international symposium on Symbolic and algebraic computation.
36. Jean-Charles Faugere, Patrizia Gianni, Daniel Lazard, Teo Mora (1993) Efficient computation of zero-dimensional Gröbner bases by change of ordering. Journal of Symbolic Computation 16: 329-344.
37. Alessandro Giovini, Teo Mora, Gianfranco Niesi, Lorenzo Robbiano, Carlo Traverso (1991) one sugar cube, please" or selection strategies in the buchberger algorithm. Proceedings of the ISSAC'91.
38. Michael Brickenstein (2010) Slimgb: Gröbner bases with slim polynomials. Revista Matematica Complutense 23: 453-466.
39. Carlo Traverso (1988) Gröbner trace algorithms. International Symposium on Symbolic and Algebraic Computation, Springer.
40. Wolfram Decker, Gerhard Pster (2013) A first course in computational algebraic geometry. Cambridge University Press.
41. Irena Swanson. Primary ideal decomposition.
42. David Eisenbud, Craig Huneke, Wolmer Vasconcelos (1992) Direct methods for primary decomposition. Inventiones mathematicae 110: 207-235.
43. Patrizia Gianni, Barry Trager, Gail Zacharias (1988) Gröbner basis and primary decomposition of polynomial ideals. Journal of Symbolic Computation 6:149-167.
44. Shimoyama T, Yokoyama K (1996) Localization and primary decomposition of polynomial ideals. Journal of Symbolic Computation 22: 247-277.
45. Michael Moller H (1993) On decomposing systems of polynomial equations with finitely many solutions. Applicable Algebra in Engineering, Communication and Computing 4: 217-230.
46. Changbo Chen, James, John PM, Marc Moreno Maza, Bican Xia, Rong Xiao (2013) Triangular decomposition of semi-algebraic systems. Journal of Symbolic Computation 49: 3-26.
47. Daniel Lazard (1992) Solving zero-dimensional algebraic systems. Journal of symbolic computation 13: 117-131.
48. Jean B Lasserre (2001) Global optimization with polynomials and the problem of moments. SIAM Journal on optimization 11: 796-817.
49. Grigoriy Blekherman, Pablo AP, Rekha RT (2012) Semidenite optimization and convex algebraic geometry. SIAM.
50. Didier Henrion, Jean-Bernard L, Johan Lofberg (2009) Gloptipoly 3: moments, optimization and semidenite programming. Optimization Methods & Software 24: 761-779.

51. Monique Laurent (2009) Sums of squares, moment matrices and optimization over polynomials. Emerging applications of algebraic geometry, Springer.

52. Alfred Tarski (1931) Sur les ensembles denissables de nombres reels. Fundamenta mathematicae 17: 210-239.

53. Alfred Tarski (1998) A decision method for elementary algebra and geometry. Quantier elimination and cylindrical algebraic decomposition, Springer.

54. Dennis S Arnon, George E Collins, Scott McCallum (1984) Cylindrical algebraic decomposition i: The basic algorithm. SIAM Journal on Computing 13: 865-877.

55. Dennis S Arnon, George EC, Scott McCallum (1984) Algebraic decomposition ii: an adjacency algorithm for the plane. SIAM Journal on Computing 13: 878-889.

56. Scott McCallum (1993) Solving polynomial strict inequalities using cylindrical algebraic decomposition. The Computer Journal 36: 432-438.

57. Changbo Chen, Marc Moreno Maza (2016) Quantier elimination by cylindrical algebraic decomposition based on regular chains. Journal of Symbolic Computation 75:74-93.

58. Chaouki TA, Peter Dorato, Richard Liska, Stanly Steinberg, Wei Yang (1995) Applications of quantier elimination theory to control theory.

59. Hoon Hong, Christopher WB. Qepcad version b.

60. Wolfram Inc. Symbolic computation software mathematica.

61. http://www.maplesoft.com.

62. Anthony C Hearn, REDUCE Developers. Reduce computer algebra system.

63. Ichio Kikuchi, Akihito Kikuchi (2018) Polynomial optimization and quantier elimination in quantum mechanics. OSF Preprints.

64. Ichio Kikuchi, Akihito Kikuchi (2018) A formulation of quantum particle swarm optimization. OSF Preprints.

65. Ichio Kikuchi, Akihito Kikuchi (2018) Quantum mechanical aspect in bayesian optimization. OSF Preprints.

66. Yositaka Mimura, Hyoitiro Takeno (1962) Wave geometry. Sci Rept Res Inst Theoret Phys, Hiroshima Univ.

67. Abbott J, Bigatti AM, Robbiano L (2006) CoCoA: a system for doing Computations in Commutative Algebra.

68. The Gap Group (2019) Gap - groups, algorithms, programming - a system for computational discrete algebra.

69. Ichio Kikuchi, Akihito Kikuchi (2017) Lie algebra in quantum physics by means of computer algebra. arXiv preprint.

70. http://www2.macaulay2.com/Macaulay2/

71. David Eisenbud, Daniel R Grayson, Mike Stillman, Bernd Sturmfels (2001) Computations in algebraic geometry with Macaulay 2. Springer Science & Business Media.

72. Project Maxima. Maxima, a computer algebra system.

73. Decker W, Greuel GM, Pster G, Schoenemann H. Computer algebra system singular.

74. Gert-Martin Greuel, Gerhard Pster (2012) A Singular introduction to commutative algebra. Springer Science & Business Media.

75. The Sage Foundation. Sagemath - free open-source mathematics software system.

76. INRIA. L'institut national de recherche d'edie aux sciences du numerique.

77. Akihito Kikuchi (2018) Computer Algebra and Materials Physics: A Practical Guidebook to Group Theoretical Computations in Materials Science. Springer.

78. Jean B Lasserre (2006) Convergent sdp-relaxations in polynomial optimization with sparsity. SIAM Journal on Optimization 17: 822-843.

79. Teo Mora (1994) An introduction to commutative and noncommutative Gröbner bases. Theoretical Computer Science 134: 131-173.

Citation: Kikuchi A, Kikuchi I (2019) Computational Algebraic Geometry and Quantum Mechanics: An Initiative toward Post Contemporary Quantum Chemistry. J Multidis Res Rev Vol: 1, Issu: 2 (47-79).