Integrand reduction via Groebner basis

Yang Zhang

(Dated: November 25, 2019)

In this section, we introduce the systematic integrand reduction method for higher loop orders via Groebner basis.

It was a long-lasting problem in the history that for the higher-loop amplitude, it is not clear how to reduce the integrand sufficiently, such that the coefficients of the reduced integrand can be completely determined by the generalized unitarity. This problem was solved by using a modern mathematical tool in computational algebraic geometry (CAG), Groebner basis [1].

CAG aims at multivariate polynomial and rational function problems in the real world. It began with *Buchberger's algorithm* in 1970s, which obtained the Gröbner basis for a *polynomial ideal*. Buchberger's algorithm for polynomials is similar to Gaussian Elimination for linear algebra: the latter finds a linear basis of a subspace while the former finds a "good" generating set for an ideal. Then CAG developed quickly and now people use it outside mathematics, like in robotics, cryptography and game theory. I believe that CAG is crucial for the deep understanding of multi-loop scattering amplitudes.

I. ISSUES AT HIGHER LOOP ORDERS

Since OPP method is very convenient for one-loop cases, the natural question is: is it possible to generalize OPP method for higher loop orders?

Of course, higher loop diagrams contain more loop momenta and usually more propagators. Is it a straightforward generalization? The answer is "no". For example, consider the $4D$ 4-point massless double box diagram (see Fig. 1), associated with the integral,

$$I_{\rm dbox}[N] = \int \frac{d^4l_1}{i\pi^2}\frac{d^4l_2}{i\pi^2}\frac{N}{D_1D_2D_3D_4D_5D_6D_7}. \tag{1}$$

The denominators of propagators are,

$$\begin{aligned} D_1 = l_1^2, \quad D_2 = (l_1-k_1)^2, \quad D_3 = (l_1-k_1-k_2)^2, \quad D_4 = (l_2+k_1+k_2)^2, \\ D_5 = (l_2-k_4)^2, \quad D_6 = l_2^2, \quad D_7 = (l_1+l_2)^2\,. \end{aligned} \tag{2}$$

The goal of reduction is to express,

$$N_{\rm dbox} = \Delta_{\rm dbox} + h_1D_1 + \ldots + h_7D_7 \tag{3}$$

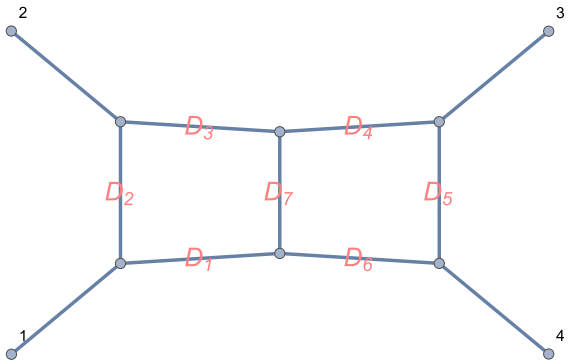

FIG. 1: two-loop double box diagram

such that Δ_{dbox} is the "simplest". (In the sense that all its coefficients in Δ_{dbox} can be uniquely fixed from unitarity, as in the box case.)

We use van Neerven-Vermaseren basis as before, $\{e_1, e_2, e_3, e_4\} = \{k_1, k_2, k_4, \omega\}$. Define

$$x_i = l_1 \cdot e_i, \quad y_i = l_2 \cdot e_i, \quad i = 1, \dots 4. \tag{4}$$

Then we try to determine Δ_{dbox} in these variables like one-loop OPP method.

$$\begin{aligned} x_1 &= \frac{1}{2}(D_1 - D_2)\,, \\ x_2 &= \frac{1}{2}(D_2 - D_3) + \frac{s}{2}\,, \\ y_2 &= \frac{1}{2}(D_4 - D_6) - y_1 - \frac{s}{2}\,, \\ y_3 &= \frac{1}{2}(D_6 - D_5)\,, \end{aligned} \tag{5}$$

Hence we can remove RSPs: x_1, x_2, y_2 and y_3 in Δ_{dbox}. (We trade y_2 for y_1, by symmetry consideration: under the left-right flip symmetry of double box, $x_3 \leftrightarrow y_1$.) There are 4 ISPs, x_3, y_1, x_4 and y_4.

Then following the one-loop OPP approach, the quadratic terms in $(l_i \cdot \omega)$ can be removed from the integrand basis, since,

$$\begin{aligned} x_4^2 &= x_3^2 - t x_3 + \frac{t^2}{4} + \mathcal{O}(D_i)\,, \\ y_4^2 &= y_1^2 - t y_1 + \frac{t^2}{4} + \mathcal{O}(D_i)\,, \\ x_4 y_4 &= \frac{s+2t}{s} x_3 y_1 + \frac{t}{2} x_3 + \frac{t}{2} y_1 - \frac{t^2}{4} + \mathcal{O}(D_i)\,. \end{aligned} \tag{6}$$

Then the trial version of integrand basis has the form,

$$\Delta_{\text{dbox}} = \sum_m \sum_n \sum_\alpha \sum_\beta c_{m,n,\alpha,\beta} x_3^m y_1^n x_4^\alpha y_4^\beta\,, \tag{7}$$

	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4
(1)	0	$\frac{s}{2}$	z_1	$z_1-\frac{t}{2}$	0	$-\frac{s}{2}$	0	$\frac{t}{2}$
(2)	0	$\frac{s}{2}$	z_2	$-z_2+\frac{t}{2}$	0	$-\frac{s}{2}$	0	$-\frac{t}{2}$
(3)	0	$\frac{s}{2}$	0	$\frac{t}{2}$	z_3	$-z_3-\frac{s}{2}$	0	$z_3-\frac{t}{2}$
(4)	0	$\frac{s}{2}$	0	-$\frac{t}{2}$	z_4	$-z_4-\frac{s}{2}$	0	$-z_4+\frac{t}{2}$
(5)	0	$\frac{s}{2}$	$\frac{z_5-s}{2}$	$\frac{z_5-s-t}{2}$	$\frac{s(s+t-z_5)}{2z_5}$	$-\frac{s(s+t)}{2z_5}$	0	$\frac{(s+t)(s-z_5)}{2z_5}$
(6)	0	$\frac{s}{2}$	$\frac{z_6-s}{2}$	$\frac{-z_6+s+t}{2}$	$\frac{s(s+t-z_6)}{2z_6}$	$-\frac{s(s+t)}{2z_6}$	0	$-\frac{(s+t)(s-z_6)}{2z_6}$

TABLE I: solutions of the $4D$ double box heptacut.

where $(\alpha,\beta)\in\{(0,0),(1,0),(0,1)\}$. The renormalization condition is,

$$m+\alpha\leq 4,\quad n+\beta\leq 4,\quad m+n+\alpha+\beta\leq 6\,. \tag{8}$$

By counting, there are 56 terms in the basis. Is this basis correct?

Have a look at the unitarity solution. The heptacut $D_1=\ldots D_7=0$ has a complicated solution structure [2]. (See table. I). There are 6 branches of solutions, each of which is parameterized by a free parameter z_i. Solutions (5) and (6) contain poles in z_i, hence we need Laurent series for tree products,

$$S^{(i)}=\sum_{k=-4}^{4} d_k^{(i)} z_i^k,\quad i=5,6\,. \tag{9}$$

The bounds are from renormalization conditions, so there are 9 nonzero coefficients for each case. Solutions (1), (2), (3), (4) are relatively simpler,

$$S^{(i)}=\sum_{k=0}^{4} d_k^{(i)} z_i^k,\quad i=1,2,3,4\,. \tag{10}$$

So there are 5 nonzero coefficients for each case. These solutions are not completely indenpendent, for example, solution (1) at $z_1=s$ and solution (6) at $z_6=t/2$ correspond to the same loop momenta. Therefore,

$$S^{(1)}(z_1\to s)=S^{(6)}(z_6\to t/2)\,. \tag{11}$$

There are 6 such intersections, namely between solutions (1) and (6), (1) and (4), (2) and (3), (2) and (5), (3) and (6), (4) and (5). Hence, there are $9\times 2+5\times 4-6=32$ independent $d_k^{(i)}$'s.

Now the big problem emerges,

$$56>32\,. \tag{12}$$

There are more terms in the integrand basis than those determined from unitarity cut. That means this integrand basis is redundant. However, it seems that we already used all algebraic constraints in (5) and (6). Which constraint is missing?

II. ELEMENTARY COMPUTATIONAL ALGEBRAIC GEOMETRY METHODS

A. Basic facts of algebraic geometry in affine space I

In order to apply the new method, we need to list some basic concepts and facts on algebraic geometry [3].

We start from a polynomial ring $R = \mathbb{F}[z_1, \dots z_n]$ which is the collection of all polynomials in n variables $z_1, \dots z_n$ with coefficients in the *field* $\mathbb{F}$. For example, $\mathbb{F}$ can be $\mathbb{Q}$, the rational numbers, $\mathbb{C}$, the complex numbers, $\mathbb{Z}/p\mathbb{Z}$, the *finite field* of integers modulo a prime number p, or $\mathbb{C}(c_1, c_2, \dots c_k)$, the complex rational functions of parameters $c_1, \dots, c_k$.

Recall that the right hand side of (3) contains the sum $h_1 D_1 + \ldots + h_7 D_7$ where D_i's are known polynomials and h_i's are arbitrary polynomials. What are general properties of such a sum? That leads to the concept of *ideal*.

Definition 1. *An ideal I in the polynomial ring $R = \mathbb{F}[z_1, \dots z_n]$ is a subset of R such that,*

- *$0 \in I$. For any two $f_1, f_2 \in I$, $f_1 + f_2 \in I$. For any $f \in I$, $-f \in I$.*
- *For $\forall f \in I$ and $\forall h \in R$, $hf \in I$.*

The ideal in the polynomial ring $R = \mathbb{F}[z_1, \dots z_n]$ generated by a subset S of R is the collection of all such polynomials,

$$\sum_i h_i f_i, \quad h_i \in R, \quad f_i \in S. \tag{13}$$

This ideal is denoted as $\langle S \rangle$. In particular, $\langle 1 \rangle = R$, which is an ideal which contains all polynomials. Note that even if S is an infinite set, the sum in (13) is always restricted to a sum of a finite number of terms. S is called the generating set of this ideal.

Example 2. *Let $I = \langle x^2 + y^2 + z^2 - 1, z \rangle$ in $\mathbb{Q}[x, y, z]$. By definition,*

$$I = \{h_1(x^2 + y^2 + z^2 - 1) + h_2 \cdot z, \ \forall h_1, h_2 \in R\}, \tag{14}$$

Pick up $h_1 = 1$, $h_2 = -z$, and we see $x^2 + y^2 - 1 \in I$. Furthermore,

$$x^2 + y^2 + z^2 - 1 = (x^2 + y^2 - 1) + z \cdot z\,. \tag{15}$$

Hence $I = \langle x^2 + y^2 - 1, z\rangle$. *We see that, in general, the generating set of an ideal is not unique.*

Our integrand reduction problem can be rephrased as: given N and the ideal $I = \langle D_1, \ldots, D_7\rangle$, how many terms in N are in I? To answer this, we need to study properties of ideals.

Theorem 3 (Noether)**.** *The generating set of an ideal* I *of* $R = \mathbb{F}[z_1, \ldots z_n]$ *can always be chosen to be finite.*

Proof. See Zariski, Samuel [4]. □

This theorem implies that we only need to consider ideals generated by finite sets in the polynomial ring R.

Definition 4. *Let* I *be an ideal of* R*, we define an equivalence relation,*

$$f \sim g, \quad \text{if and only if } f - g \in I\,. \tag{16}$$

We define an equivalence class, $[f]$ *as the set of all* $g \in R$ *such that* $g \sim f$*. The quotient ring* R/I *is set of equivalence classes,*

$$R/I = \{[f] | f \in R\}\,. \tag{17}$$

with multiplication $[f_1][f_2] \equiv [f_1 f_2]$*. (Check this multiplication is well-defined.)*

To study the structure of an ideal, it is very useful to consider the algebra-geometry relation.

Definition 5. *Let* $\mathbb{K}$ *be a field,* $\mathbb{F} \subset \mathbb{K}$*. The* n*-dimensional* $\mathbb{K}$*-affine space* $\mathbf{A}^n_{\mathbb{K}}$ *is the set of all* n*-tuple of* $\mathbb{K}$*. Given a subset* S *of the polynomial ring* $\mathbb{F}[z_1, \ldots, z_n]$*, its algebraic set over* $\mathbb{K}$ *is,*

$$\mathcal{Z}_{\mathbb{K}}(S) = \{p \in \mathbf{A}^n_{\mathbb{K}} | f(p) = 0, \text{ for every } f \in S\}. \tag{18}$$

If $\mathbb{K} = \mathbb{F}$*, we drop the subscript* $\mathbb{K}$ *in* $\mathbf{A}^n_{\mathbb{K}}$ *and* $\mathcal{Z}_{\mathbb{K}}(S)$*.*

So the algebraic set $\mathcal{Z}(S)$ consists of all *common solutions* of polynomials in S. Note that to solve polynomials in S is equivalent to solve all polynomials simultaneously in the ideal generated by S,

$$\mathcal{Z}(S) = \mathcal{Z}(\langle S\rangle), \tag{19}$$

since if $p \in \mathcal{Z}(S)$, then $f(p) = 0$, $\forall f \in S$. Hence,

$$h_1(p)f_1(p) + \ldots + h_k(p)f_k(p) = 0, \quad \forall h_i \in R,\ \forall f_i \in S. \tag{20}$$

So we always consider the algebraic set of an ideal.

For example, $\mathcal{Z}(\langle 1\rangle) = \emptyset$ (empty set) since $1 \neq 0$. For the ideal $I = \langle x^2 + y^2 + z^2 - 1, z\rangle$ in example 2, $\mathcal{Z}(I)$ is the unit circle on the plane $z = 0$.

We want to learn the structure of an ideal from its algebraic set. First, for the empty algebraic set,

Theorem 6 (Hilbert's weak Nullstellensatz)**.** *Let I be an ideal of $\mathbb{F}[z_1, \dots z_n]$ and $\mathbb{K}$ be an algebraically closed field [14] , $\mathbb{F} \subset \mathbb{K}$. If $\mathcal{Z}_{\mathbb{K}}(I) = \emptyset$, then $I = \langle 1\rangle$.*

Proof. See Zariski and Samuel, [5, Chapter 7]. □

Remark. *The field extension $\mathbb{K}$ must be algebraically closed. Otherwise, say, $\mathbb{K} = \mathbb{F} = \mathbb{Q}$, the ideal $\langle x^2 - 2\rangle$ has empty algebraic set in $\mathbb{Q}$. (The solutions are not rational). However, $\langle x^2 - 2\rangle \neq \langle 1\rangle$. On the other hand, $\mathbb{F}$ need not be algebraically closed. $I = \langle 1\rangle$ means,*

$$1 = h_1 f_1 + \ldots + h_k f_k, \quad f_i \in I,\ h_i \in \mathbb{F}[z_1, \dots z_n]\,. \tag{21}$$

where h_i's coefficients are in $\mathbb{F}$, instead of an algebraic extension of $\mathbb{F}$.

Example 7. *We prove that, generally, the $4D$ pentagon diagrams are reduced to diagrams with fewer than 5 propagators, D-dimensional hexagon diagram are reduced to diagrams with fewer than 6 propagators, in the integrand level.*

For the $4D$ pentagon case, there are 5 denominators from propagators, namely $D_1, \dots D_5$. There are 4 Van Neerven-Vermaseren variables for the loop momenta, namely x_1, x_2, x_3 and x_4. So D_i's are polynomials in $x_1, \dots, x_4$ with coefficients in $\mathbb{F} = \mathbb{Q}(s_{12}, s_{23}, s_{34}, s_{45}, s_{15})$. Define $I = \langle D_1, \dots D_5, \rangle$. Generally 5 equations in 4 variables,

$$D_1 = D_2 = D_3 = D_4 = D_5 = 0\,, \tag{22}$$

have no solution (even with algebraic extensions). Hence by Hilbert's weak Nullstellensatz, $I = \langle 1\rangle$. Explicitly, there exist 5 polynomials f_i's in $\mathbb{F}[x_1, x_2, x_3, x_4]$ such that

$$f_1 D_1 + f_2 D_2 + f_3 D_3 + f_4 D_4 + f_5 D_5 = 1\,. \tag{23}$$

Therefore,

$$\begin{aligned}\int d^4l \frac{1}{D_1 D_2 D_3 D_4 D_5} = &\int d^4l \frac{f_1}{D_2 D_3 D_4 D_5} + \int d^4l \frac{f_2}{D_1 D_3 D_4 D_5} + \int d^4l \frac{f_3}{D_1 D_2 D_4 D_5} \\ &\int d^4l \frac{f_4}{D_1 D_2 D_3 D_5} + \int d^4l \frac{f_5}{D_1 D_2 D_3 D_4}\,,\end{aligned} \tag{24}$$

where each term in the r.h.s is a box integral (or simpler). Note that f_i's are in $\mathbb{F}[x_1, x_2, x_3, x_4]$, so the coefficients of these polynomials are rational functions of Mandelstam variables $s_{12}, s_{23}, s_{34}, s_{45}, s_{15}$. Weak Nullstellensatz theorem does not provide an algorithm for finding such f_i's. The algorithm will be given by the Gröbner basis method in next subsection, or by the resultant method [6].

Notice that in the DimReg case, we have one more variable $\mu_{11} = -(l^\perp)^2$. The same argument using Weak Nullstellensatz leads to the result.

For a general algebraic set, we have the important theorem:

Theorem 8 (Hilbert's Nullstellensatz)**.** *Let $\mathbb{F}$ be an algebraically closed field and $R = \mathbb{F}[z_1, \dots z_n]$. Let I be an ideal of R. If $f \in R$ and,*

$$f(p) = 0, \quad \forall p \in \mathcal{Z}(I), \tag{25}$$

then there exists a positive integer k such that $f^k \in I$.

Proof. See Zariski and Samuel, [5, Chapter 7]. □

Hilbert's Nullstellensatz characterizes all polynomials vanishing on $\mathcal{Z}(I)$, they are "not far away" from elements in I. For example, $I = \langle (x-1)^2 \rangle$ and $\mathcal{Z}(I) = \{1\}$. The polynomial $f(x) = (x-1)$ does not belong to I but $f^2 \in I$.

Definition 9. *Let I be an ideal in R, define the radical ideal of I as,*

$$\sqrt{I} = \{f \in R | \exists k \in \mathbb{Z}^+, f^k \in I\}. \tag{26}$$

For any subset V of $\mathbf{A}^n$, define the ideal of V as

$$\mathcal{I}(V) = \{f \in R | f(p) = 0, \ \forall p \in V\}. \tag{27}$$

Then Hilbert's Nullstellensatz reads, over an algebraically closed field,

$$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}. \tag{28}$$

An ideal I is called radical, if $\sqrt{I} = I$.

If two ideals I_1 and I_2 have the same algebraic set $\mathcal{Z}(I_1) = \mathcal{Z}(I_2)$, then they have the same radical ideals $\sqrt{I_1} = \sqrt{I_2}$. On the other hand, if two sets in $\mathbb{A}^n$ have the same ideal, what could we say about them? To answer this question, we need to define topology of $\mathbb{A}^n$:

Definition 10 (Zariski topology)**.** *Define Zariski topology of* $\mathbf{A}^n_{\mathbb{F}}$ *by setting all algebraic set to be topologically closed. (Here* $\mathbb{F}$ *need not be algebraic closed.)*

Remark. *The intersection of any number of Zariski closed sets is closed since,*

$$\bigcap_i \mathcal{Z}(I_i) = \mathcal{Z}(\bigcup_i I_i). \tag{29}$$

The union of two closed sets is closed since,

$$\mathcal{Z}(I_1) \bigcup \mathcal{Z}(I_2) = \mathcal{Z}(I_1 I_2) = \mathcal{Z}(I_1 \cap I_2). \tag{30}$$

$\mathbf{A}^n_{\mathbb{F}}$ *and* $\emptyset$ *are both closed because* $\mathbf{A}^n_{\mathbb{F}} = \mathcal{Z}(\{0\})$, $\emptyset = \mathcal{Z}(\langle 1 \rangle)$. *That means Zariski topology is well-defined. We leave the proof of* (29) *and* (30) *as an exercise.*

Note that Zariski topology is different from the usual topology defined by Euclidean distance, for $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. *For example, over* $\mathbb{C}$, *the "open" unit disc defined by* $D = \{z||z| < 1\}$ *is not Zariski open in* $\mathbf{A}^1_{\mathbb{C}}$. *The reason is that* $\mathbb{C} - D = \{z||z| \geq 1\}$ *is not Zariski closed, i.e.* $\mathbb{C} - D$ *cannot be the solution set of one or several complex polynomials in* z.

Zariski topology is the foundation of affine algebraic geometry. With this topology, the dictionary between algebra and geometry can be established.

Proposition 11. *(Here* $\mathbb{F}$ *need not be algebraic closed.)*

1. *If* $I_1 \subset I_2$ *are ideals of* $\mathbb{F}[z_1, \ldots z_n]$, $\mathcal{Z}(I_1) \supset \mathcal{Z}(I_2)$
2. *If* $V_1 \subset V_2$ *are subsets of* $\mathbf{A}^n_{\mathbb{F}}$, $\mathcal{I}(V_1) \supset \mathcal{I}(V_2)$
3. *For any subset* V *in* $\mathbf{A}^n_{\mathbb{F}}$, $\mathcal{Z}(\mathcal{I}(V)) = \overline{V}$, *the Zariksi closure of* V.

Proof. The first two statements follow directly from the definitions. For the third one, $V \subset \mathcal{Z}(\mathcal{I}(V))$. Since the latter is Zariski closed, $\overline{V} \subset \mathcal{Z}(\mathcal{I}(V))$. On the other hand, for any Zariski closed set X containing V, $X = \mathcal{Z}(I)$. $I \subset \mathcal{I}(V)$. From statement 1, $X = \mathcal{Z}(I) \supset \mathcal{Z}(\mathcal{I}(V))$. As a closed set, $\mathcal{Z}(\mathcal{I}(V))$ is contained in any closed set which contains V, hence $\mathcal{Z}(\mathcal{I}(V)) = \overline{V}$. □

In the case $\mathbb{F}$ is algebraic closed, the above proposition and Hilbert's Nullstellensatz established the one-to-one correspondence between radical ideals in $\mathbb{F}[z_1, \ldots z_n]$ and closed sets in $\mathbf{A}^n_{\mathbb{F}}$. We will study geometric properties like reducibility, dimension, singularity later in these lecture notes. Before this, we turn to the computational aspect of affine algebraic geometry, to see how to explicitly compute objects like $I_1 \cap I_2$ and $\mathcal{Z}(I)$.

Consider $I = \{x^2 - y^2, x^3 + y^3 - z^2\}$ in $\mathbb{C}[x, y, z]$. From naive counting, $\mathcal{Z}(I)$ is a curve since there are 2 equations in 3 variables. However, the plot of $\mathcal{Z}(I)$ (Figure 2) looks like a line and a cusp curve. So $\mathcal{Z}(I)$ is *reducible*, in the sense that it can be decomposed into smaller algebraic sets. So we need the concept of *primary decomposition*.

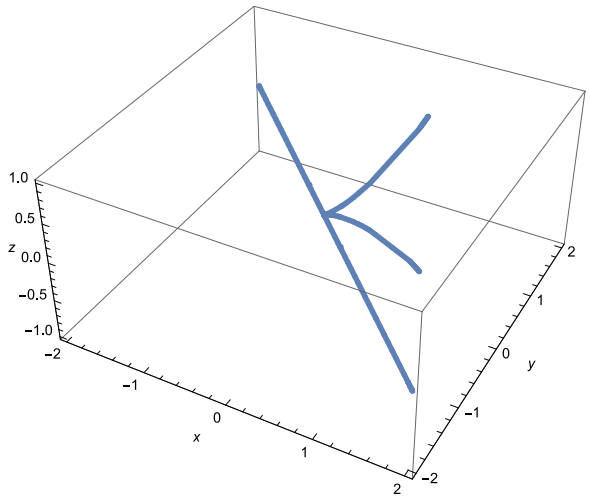

FIG. 2: A reducible algebraic set (in blue), defined by $\mathcal{Z}(\{x^2 - y^2, x^3 + y^3 - z^2\})$.

Definition 12. *An ideal I in a ring R is called prime, if $\forall ab \in I$ $(a,\, b \in R)$ then $a \in I$ or $b \in I$. An ideal I in R is called primary is if $ab \in I$ $(a,\, b \in R)$ then $a \in I$ or $b^n \in I$, for some positive integer n.*

A prime ideal must be a primary ideal. On the other hand,

Proposition 13. *If I is a primary ideal, then the radical of I, $\sqrt{I}$ is a prime ideal.*

Proof. See Zariski and Samuel [4, Chapter 3]. □

Note that $I = \{x^2 - y^2, x^3 + y^3 - z^2\}$ is not a prime ideal or primary ideal. Define $a = x - y$, $b = x + y$, clearly $ab \in I$, but $a \notin I$ and $b^n \notin I$ for any positive integer n. (The point $P = (2, 2, 4) \in \mathcal{Z}(I)$. If $(x + y)^n \in I$ then $(x + y)^n|_P = 0$. It is a contradiction.)

For another example, $J = \langle (x - 1)^2 \rangle$ in $\mathbb{C}[x]$ is primary but not prime. $\mathcal{Z}(J)$ contains only one point $\{1\}$ with the multiplicity 2. $(x - 1)(x - 1) \in J$ but $(x - 1) \notin J$. For there examples, we see primary condition implies that the corresponding algebraic set cannot be decomposed to smaller algebraic sets, while prime condition further requires that the multiplicity is 1.

Theorem 14 (Lasker-Noether)**.** *For an ideal I in $\mathbb{F}[z_1, \ldots z_n]$, I has the primary decomposition,*

$$I = I_1 \cap \ldots \cap I_m \,, \tag{31}$$

such that,

- *Each I_i is a primary ideal in $\mathbb{F}[z_1, \dots z_n]$,*
- *$I_i \not\supset \cap_{j\neq i} I_j$,*
- *$\sqrt{I_i} \neq \sqrt{I_j}$, if $i \neq j$.*

Although primary decomposition may not be unique, the radicals $\sqrt{I_i}$'s are uniquely determined by I up to orders.

Proof. See Zariski, Samuel [4, Chapter 4]. □

Note that unlike Gröbner basis, primary decomposition is very sensitive to the number field. For an ideal $I \subset \mathbb{F}[z_1, \dots z_n]$, $\mathbb{F} \subset \mathbb{K}$, the primary decomposition results of I in $\mathbb{F}[z_1, \dots z_n]$ and $\mathbb{K}[z_1, \dots, z_n]$ can be different. Primary decomposition can be computed by MACAULAY2 or SINGULAR. However, the computation is heavy in general.

Primary decomposition was also used for studying string theory vacua [**?**].

Example 15. *Consider $I = \{x^2 - y^2, x^3 + y^3 - z^2\}$. Use* MACAULAY2 *or* SINGULAR*, we find that, $I = I_1 \cap I_2$, where,*

$$I_1 = \langle z^2, x + y\rangle, \quad I_2 = \langle 2y^3 - z^2, x - y\rangle \tag{32}$$

Then $\sqrt{I_1} = \langle z, x + y\rangle$ is a prime ideal, where I_2 itself is prime.

When $I \subset \mathbb{F}[z_1, \dots z_n]$ has a primary decomposition $I = I_1 \cap \dots \cap I_m$, $m > 1$, then $\mathcal{Z}_{\mathbb{F}}(I) = \mathcal{Z}_{\mathbb{F}}(I_1) \cup \dots \cup \mathcal{Z}_{\mathbb{F}}(I_m)$. Then algebraic set decomposed to the union of sub algebraic sets. We switch the study of reducibility to the geometric side.

Definition 16. *Let V be a nonempty closed set in $\mathbf{A}_{\mathbb{F}}$ in Zariski topology, V is irreducible, if V cannot be a union of two closed proper subsets of V.*

Proposition 17. *Let $\mathbb{K}$ be an algebraic closed field. There is a one-to-one correspondence:*

$$\begin{array}{ccc} \textit{prime ideals in } \mathbb{K}[z_1, \dots z_n] & & \textit{irreducible algebraic sets in } \mathbf{A}_{\mathbb{K}} \\ I & \longrightarrow & \mathcal{Z}_{\mathbb{K}}(I) \\ \mathcal{I}(V) & \longleftarrow & V \end{array} \tag{33}$$

Proof. (Sketch) This follows from Hilbert Nullstellensatz (28). □

We call an irreducible Zariski closed set "affine variety". Similar to primary decomposition of ideals, algebraic set has the following decomposition,

Theorem 18. *Let V be an algebraic set. V uniquely decomposes as the union of affine varieties, $V = V_1 \cup \ldots \cup V_m$, such that $V_i \not\supset V_j$ if $i \neq j$.*

Proof. Let $I = \mathcal{I}(V)$. The primary decomposition determines that $I = I_1 \cap \ldots \cap I_m$. Since I is a radical ideal, all I_i's are prime. Then $V = \mathcal{Z}(I) = \cap_{i=1}^m \mathcal{Z}(I_i)$. Each $\mathcal{Z}(I_i)$ is an affine variety. If $\mathcal{Z}(I_i) \supset \mathcal{Z}(I_j)$, then $I_i \subset I_j$ which is a violation of radical uniqueness of Lasker-Noether theorem.

If there are two decompositions, $V = V_1 \cup \ldots \cup V_m = W_1 \cup \ldots \cup W_l$. $V_1 = V_1 \cap (W_1 \cup \ldots \cup W_l) = (V_1 \cap W_1) \cup \ldots (V_1 \cap W_l)$. Since V_1 is irreducible, V_1 equals some $V_1 \cap W_j$, , say $j = 1$. Then $V_1 \subset W_1$. By the same analysis $W_1 \subset V_i$ for some i. Hence $V_1 \subset V_i$ and so $i = 1$. We proved $W_1 = V_1$. Repeat this process, we see that the two decompositions are the same. □

Example 19. *As an application, we use primary decomposition to find cut solutions of 4D double box in Table I. It is quite messy to derive all unitarity solutions by brute force computation. In this situation, primary decomposition is very helpful.*

Use van Neerven-Vermaseren variables, the ideal $I = \langle D_1, \ldots D_7 \rangle$ decomposes as $I = I_1 \cap I_2 \cap I_3 \cap I_4 \cap I_5 \cap I_6$.

$$
\begin{aligned}
I_1 &= \{2y_4 - t, s + 2y_2, -t + 2x_3 - 2x_4, y_3, \frac{s}{2} + y_1 + y_2, x_2 - \frac{s}{2}, x_1\}, \\
I_2 &= \{t + 2y_4, s + 2y_2, -t + 2x_3 + 2x_4, y_3, \frac{s}{2} + y_1 + y_2, x_2 - \frac{s}{2}, x_1\}, \\
I_3 &= \{s + t + 2y_2 + 2y_4, 2x_4 - t, x_3, y_3, \frac{s}{2} + y_1 + y_2, x_2 - \frac{s}{2}, x_1\}, \\
I_4 &= \{s + t + 2y_2 - 2y_4, t + 2x_4, x_3, y_3, \frac{s}{2} + y_1 + y_2, x_2 - \frac{s}{2}, x_1\}, \\
I_5 &= \{s + t + 2y_2 + 2y_4, x_4(2s + 2t) + y_4(2s + 2t) + st + t^2 + 4x_4y_4, \\
&\quad -t + 2x_3 - 2x_4, y_3, \frac{s}{2} + y_1 + y_2, x_2 - \frac{s}{2}, x_1\}, \\
I_6 &= \{s + t + 2y_2 - 2y_4, x_4(-2s - 2t) + y_4(-2s - 2t) + st + t^2 + 4x_4y_4, \\
&\quad -t + 2x_3 + 2x_4, y_3, \frac{s}{2} + y_1 + y_2, x_2 - \frac{s}{2}, x_1\}. \qquad (34)
\end{aligned}
$$

Each I_i is prime and corresponds to a solution in Table I. SINGULAR *computes this primary decomposition in about* 3.6 *seconds on a laptop. In practice, the computation can be sped up if we first eliminate all RSPs.*

Hence the unitarity solution set $\mathcal{Z}(I)$ consists of six irreducible solution sets $\mathcal{Z}(I_i)$, $i = 1 \ldots 6$. Each one can be parametrized by a free parameter.

For a variety V, we want to define its dimension. Intuitively, we may test if V contains a point, a curve, a surface...? So the dimension of V is defined as the length of variety sequence in V,

Definition 20. *The dimension of a variety V,* $\dim V$*, is the largest number n in all sequences $\emptyset \neq W_0 \subset W_1 \ldots \subset W_n \subset V$, where W_i's are distinct varieties.*

On the algebraic side, let $V = \mathcal{Z}(I)$, where I is an ideal in $R = \mathbb{F}[z_1, \ldots z_n]$. Consider the quotient ring R/I. Roughly speaking, the remaining "degree of freedom" of R/I should be the same as $\dim V$. Krull dimension counts "the degree of freedom",

Definition 21 (Krull dimension)**.** *The Krull dimension of a ring S, is the largest number n in all sequences $p_0 \subset p_1 \ldots \subset p_n$, where p_i's are distinct prime ideals in S.*

If for a prime ideal I, R/I is has Krull dimension zero then I is a *maximal ideal*. A maximal ideal I in R is an ideal which such that for any proper ideal $J \supset I$, $J = I$. I is a maximal idea, if and only if R/I is a field. (R itself is not a maximal idea of R). When $\mathbb{F}$ is algebraically closed, then any maximal ideal I in $R = \mathbb{F}[z_1, \ldots z_n]$ has the form [7],

$$I = \langle z_1 - c_1, \ldots z_n - c_n \rangle, \quad c_i \in \mathbb{F}. \tag{35}$$

Note that the point $(c_1, \ldots, c_n)$ is zero-dimensional, and $R/I = \mathbb{F}$ has Krull dimension 0. More generally,

Proposition 22. *If $\mathbb{F}$ is algebraically closed and I a prime proper ideal of $R = \mathbb{F}[z_1, \ldots z_n]$. Then the Krull dimension of R/I equals* $\dim \mathcal{Z}(I)$*.*

Proof. See Hartshorne [3, Chapter 1]. Note that Krull dimension of R/I is different from the linear dimension $\dim_{\mathbb{F}} R/I$. □

In summary, we has the algebra-geometry dictionary (Table II), where the last two rows hold if $\mathbb{F}$ is algebraic closed.

B. Gröbner basis

1. One-variable case

We see that ideal is the central concept for the algebraic side of classical algebraic geometry. An ideal can be generated by different generating sets, some may be redundant or complicated.

Algebra		Geometry
Ideal I in $\mathbb{F}[z_1, \dots z_n]$		algebraic set $\mathcal{Z}(I)$
$I_1 \cap I_2$		$\mathcal{Z}(I_1 \cap I_2) = \mathcal{Z}(I_1) \cup \mathcal{Z}(I_2)$
$I_1 + I_2$		$\mathcal{Z}(I_1 + I_2) = \mathcal{Z}(I_1) \cap \mathcal{Z}(I_2)$
$I_1 \subset I_2$	$\Rightarrow$	$\mathcal{Z}(I_1) \supset \mathcal{Z}(I_2)$
prime ideal I	$\Rightarrow$	$\mathcal{Z}(I)$ (irreducible) variety
maximal ideal I	$\Rightarrow$	$\mathcal{Z}(I)$ is a point
Krull dimension of $\dim \mathbb{F}[z_1, \dots z_n]/I$	$=$	$\dim \mathcal{Z}(I)$

TABLE II: algebraic geometry dictionary

In linear algebra, given a linear subspace $V = \text{span}\{v_1 \dots v_k\}$ we may use Gaussian elimination to find the linearly-independent basis of V or Gram-Schmidt process to find an orthonormal basis. For ideals, a "good basis" can also dramatically simplify algebraic geometry problems.

Example 23. *As a toy model, consider some univariate cases.*

- *For example, $I = \langle x^3 - x - 1 \rangle$ in $R = \mathbb{Q}[x]$. Clearly, I consists of all polynomials in x proportional to $x^3 - x - 1$, and every nonzero element in I has the degree higher or equal than 3. So we say $B(I) = \{x^3 - x - 1\}$ is a "good basis" for I. $B(I)$ is useful: for any polynomial $F(x)$ in $\mathbb{Q}[x]$, polynomial division determines,*

$$F(x) = q(x)(x^3 - x - 1) + r(x), \quad q(x), r(x) \in \mathbb{Q}[x], \ \deg r(x) < 3 \tag{36}$$

  Hence $F(x)$ is in I if and only if the remainder r is zero. It also implies that $R/I = \text{span}_{\mathbb{Q}}\{[1], [x], [x^2]\}$.

- *Consider $J = \langle x^3 - x^2 + 3x - 3, x^2 - 3x + 2 \rangle$. Is the naive choice $B(J) = \{f_1, f_2\} = \{x^3 - x^2 + 3x - 3, x^2 - 3x + 2\}$ a good basis? For instance, $f = f_1 - x f_2 = 2x^2 + x - 3$ is in I but it is proportional to neither f_1 nor f_2. Polynomial division over this basis is not useful, since f's degree is lower than f_1, the only division reads,*

$$f = 2f_2 + (7x - 7)\,. \tag{37}$$

  The remainder does not tell us the membership of f in I. Hence $B(J)$ does not characterize I or R/I, and it is not "good". Note that $\mathbb{Q}[x]$ is a principal ideal domain (PID), any ideal can be generated by one polynomial. Therefore, use Euclidean algorithm (Algorithm 1) to find the greatest common factor of f_1 and f_2,

$$(x - 1) = \frac{1}{7} f_1(x) - \frac{x + 2}{7} f_2(x), \quad (x - 1) | f_1(x), \ (x - 1) | f_2(x) \tag{38}$$

Hence $J = \langle x - 1 \rangle$. *We can check that* $\tilde{B}(J) = \{x - 1\}$ *is a "good" basis in the sense that Euclidean division over* $\tilde{B}(J)$ *solves membership questions of* J *and determined* $R/J = \text{span}_{\mathbb{Q}}\{[1]\}$.

Algorithm 1 Euclidean division for greatest common divisor

1: **Require:** f_1, f_2, $\deg f_1 \geq \deg f_2$
2: **while** $f_2 \not| f_1$ **do**
3: polynomial division $f_1 = qf_2 + r$
4: $f_1 := f_2$
5: $f_2 := r$
6: **end while**
7: **return** f_2 (gcd)

Recall that in (3), given inverse propagators $D_1, \ldots, D_7$, we need to solve the membership problem of $I = \langle D_1 \ldots D_7 \rangle$ and compute R/I. However, in general, a set like $\{D_1 \ldots D_7\}$ is not a "good basis", in the sense that the polynomial division over this basis does not solve the membership problem or give a correct integrand basis (as we see previously). Since it is a multivariate problem, the polynomial ring R is not a PID and we cannot use Euclidean algorithm to find a "good basis".

Look at Example 23 again. For the univariate case, there is a natural monomial order $\prec$ from the degree,

$$1 \prec x \prec x^2 \prec x^3 \prec x^4 \prec \ldots , \tag{39}$$

and all monomials are sorted. For any polynomial F, define the *leading term*, $\text{LT}(F)$ to be the highest monomial in F by this order (with the coefficient). For multivariate cases, the degree criterion is not fine enough to sort all monomials, so we need more general monomial orders.

Definition 24. *Let* M *be the set of all monomials with coefficients* 1*, in the ring* $R = \mathbb{F}[z_1, \ldots z_n]$. *A monomial order* $\prec$ *of* R *is an ordering on* M *such that,*

1. $\prec$ *is a total ordering, which means any two different monomials are sorted by* $\prec$.
2. $\prec$ *respects monomial products, i.e., if* $u \prec v$ *then for any* $w \in M$, $uw \prec vw$.
3. $1 \prec u$, *if* $u \in M$ *and* u *is not constant.*

There are several important monomial orders. For the ring $\mathbb{F}[z_1, \ldots z_n]$, we use the convention $1 \prec z_n \prec z_{n-1} \prec \ldots \prec z_1$ for all monomial orders. Given two monomials, $g_1 = z_1^{\alpha_1} \ldots z_n^{\alpha_n}$ and $g_2 = z_1^{\beta_1} \ldots z_n^{\beta_n}$, consider the following orders:

- Lexicographic order (*lex*). First compare α_1 and β_1. If $\alpha_1 < \beta_1$, then $g_1 \prec g_2$. If $\alpha_1 = \alpha_2$, we compare α_2 and β_2. Repeat this process until for certain α_i and β_i the tie is broken.

- Degree lexicographic order (*grlex*). First compare the total degrees. If $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$, then $g_1 \prec g_2$. If total degrees are equal, we compare (α_1, β_1), (α_2, β_2) ... until the tie is broken, like *lex*.

- Degree reversed lexicographic order (*grevlex*). First compare the total degrees. If $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$, then $g_1 \prec g_2$. If total degrees are equal, we compare α_n and β_n. If $\alpha_n < \beta_n$, then $g_1 \succ g_2$ (reversed!). If $\alpha_n = \beta_n$, then we further compare $(\alpha_{n-1}, \beta_{n-1})$, $(\alpha_{n-2}, \beta_{n-2})$ ... until the tie is broken, and use the reversed result.

- Block order. This is the combination of *lex* and other orders. We separate the variables into k blocks, say,

$$\{z_1, z_2, \dots z_n\} = \{z_1, \dots z_{s_1}\} \cup \{z_{s_1+1}, \dots z_{s_2}\} \dots \cup \{z_{s_{k-1}+1}, \dots z_n\}\,. \tag{40}$$

  Furthermore, define the monomial order for variables in each block. To compare g_1 and g_2, first we compare the first block by the given monomial order. If it is a tie, we compare the second block... until the tie is broken.

Example 25. *Consider $\mathbb{Q}[x, y, z]$, $z \prec y \prec x$. We sort all monomials up to degree 2 in lex, grlex, grevlex and the block order $[x] \succ [y, z]$ with grevlex in each block. This can be done be the following* MATHEMATICA *code:*

$\boldsymbol{F = 1 + x + x^2 + y + xy + y^2 + z + xz + yz + z^2;}$

$\boldsymbol{MonomialList[F, \{x, y, z\}, Lexicographic]}$

$\boldsymbol{MonomialList[F, \{x, y, z\}, DegreeLexicographic]}$

$\boldsymbol{MonomialList[F, \{x, y, z\}, DegreeReverseLexicographic]}$

$\boldsymbol{MonomialList[F, \{x, y, z\}, \{\{1, 0, 0\}, \{0, 1, 1\}, \{0, 0, -1\}\}]}$

and the output is,

$\{x^2, xy, xz, x, y^2, yz, y, z^2, z, 1\}$ $\{x^2, xy, xz, y^2, yz, z^2, x, y, z, 1\}$ $\{x^2, xy, y^2, xz, yz, z^2, x, y, z, 1\}$

$\{x^2, xy, xz, x, y^2, yz, z^2, y, z, 1\}$

Note that for lex, $x \succ y^2$, $y \succ z^2$ since we first compare the power of x and the y. The total degree is not respected in this order. On the other hand, grlex and grevlex both consider the total degree first. The difference between grlex and grevlex is that, $xz \succ_{grlex} y^2$ while $xz \prec_{grevlex} y^2$. So grevlex tends to set monomials with more variables, lower, in the list of monomials with a fixed

degree. This property is useful for computational algebraic geometry. Finally, for this block order, $x \succ y^2$ *since* x*'s degrees are compared first. But* $y \prec z^2$*, since* $[y, z]$ *block is in grevlex.*

With a monomial order, we define the leading term as the highest monomial (with coefficient) of a polynomial in this order. Back to the second part of Example 23,

$$\mathrm{LT}(f_1) = x^3 \quad \mathrm{LT}(f_2) = x^2, \quad \mathrm{LT}(x-1) = x \tag{41}$$

The key observation is that although $x-1 \in J$, its leading term is not divisible by the leading term of either f_1 or f_2. This makes polynomial division unusable and $\{f_1, f_2\}$ is not a " good basis". This leads to the concept of Gröbner basis.

2. Gröbner basis

Definition 26. *For an ideal* I *in* $\mathbb{F}[z_1, \dots z_n]$ *with a monomial order, a Gröbner basis* $G(I) = \{g_1, \dots g_m\}$ *is a generating set for* I *such that for each* $f \in I$*, there always exists* $g_i \in G(I)$ *such that,*

$$\mathrm{LT}(g_i) | \, \mathrm{LT}(f) \, . \tag{42}$$

We can check that for the ideal J in Example 23, $\{f_1, f_2\}$ is not a Gröbner basis with respect to the natural order, while $\{x-1\}$ is.

3. Multivariate polynomial division

To harness the power of Gröbner basis we need the multivariate division algorithm, which is a generalization of univariate Euclidean algorithm (Algorithm 2). The basic procedure is that: given a polynomial F and a list of k polynomials f_i's, if $\mathrm{LT}(F)$ is divisible by some $\mathrm{LT}(f_i)$, then remove $\mathrm{LT}(F)$ by subtracting a multiplier of f_i. Otherwise move $\mathrm{LT}(F)$ to the remainder r. The output will be

$$F = q_1 f_1 + \dots q_k f_k + r \, , \tag{43}$$

where r consists of monomials cannot be divided by any $LT(f_i)$. Let $B = \{f_1, \dots f_k\}$, we denote $\overline{F}^B$ as the remainder r.

Recall that the one-loop OPP integrand reduction and the naive trial of two-loop integrand reduction are very similar to this algorithm.

Algorithm 2 Multivariate division algorithm

Require: F, $f_1 \dots f_k$, $\succ$
$q_1 := \dots := q_k = 0$, $r := 0$
while $F \neq 0$ **do**
    $reductionstatus := 0$
    for $i = 1$ to k **do**
        if $\mathrm{LT}(f_i) | \mathrm{LT}(F)$ **then**
            $q_i := q_i + \frac{\mathrm{LT}(F)}{\mathrm{LT}(f_i)}$
            $F := F - \frac{\mathrm{LT}(F)}{\mathrm{LT}(f_i)} f_i$
            $reductionstatus := 1$

        end if
    end for
    if $reductionstatus = 0$ **then**
        $r := r + \mathrm{LT}(F)$
        $F := F - \mathrm{LT}(F)$
    end if
end while
return $q_1 \dots q_k$, r

Note that for a general list of polynomials, the algorithm has two drawbacks: (1) the remainder r depends on the order of the list, $\{f_1, \dots f_n\}$ (2) if $F \in \langle f_1 \dots f_n \rangle$, the algorithm may not give a zero remainder r. These made the previous two-loop integrand reduction unsuccessful. Gröbner basis eliminates these problems.

Proposition 27. *Let $G = \{g_1, \dots g_m\}$ be a Gröbner basis in $\mathbb{F}[z_1, \dots z_n]$ with the monomial order $\succ$. Let r be the remainder of the division of F by G, from Algorithm 2.*

1. *r does not depend on the order of $g_1, \dots g_m$.*

2. *If $F \in I = \langle g_1, \dots g_m \rangle$, then $r = 0$.*

Proof. If the division with different orders of $g_1, \dots g_n$ provides two remainder r_1 and r_2. If $r_1 \neq r_2$, then $r_1 - r_2$ contains monomials which are not divisible by any $\mathrm{LT}(g_i)$. But $r_1 - r_2 \in I$, this is a contradiction to the definition of Gröbner basis.

If $F \in I$, then $r \in I$. Again by the definition of Gröbner basis, if $r \neq 0$, $\mathrm{LT}(r)$ is divisible by some $\mathrm{LT}(g_i)$. This is a contradiction to multivariate division algorithm. □

Then the question is: given an ideal $I = \langle f_1 \dots f_k \rangle$ in $\mathbb{F}[z_1, \dots z_n]$ and a monomial order $\succ$, does the Gröbner basis exist and how do we find it? This is answered by Buchberger's Algorithm, which was presented in 1970s and marked the beginning of computational algebraic geometry.

4. Buchberger algorithm

Recall that for one-variable case, Euclidean algorithm (Algorithm 1) computes the gcd of two polynomials hence the Gröbner basis is given. The key step is to cancel leading terms of two polynomials. That inspires the concept of S-polynomial in multivariate cases.

Definition 28. *Given a monomial order $\succ$ in $R = \mathbb{F}[z_1, \dots z_n]$, the S-polynomial of two polynomials f_i and f_j in R is,*

$$S(f_i, f_j) = \frac{\mathrm{LT}(f_j)}{\gcd\big(\mathrm{LT}(f_i), \mathrm{LT}(f_j)\big)} f_i - \frac{\mathrm{LT}(f_i)}{\gcd\big(\mathrm{LT}(f_i), \mathrm{LT}(f_j)\big)} f_j. \tag{44}$$

Note that the leading terms of the two terms on the r.h.s cancel.

Theorem 29 (Buchberger)**.** *Given a monomial order $\succ$ in $R = \mathbb{F}[z_1, \dots z_n]$, Gröbner basis with respect to $\succ$ exists and can be found by Buchberger's Algorithm (Algorithm 3).*

Proof. See Cox, Little, O'Shea [7]. □

Algorithm 3 Buchberger algorithm

Require: $B = \{f_1 \dots f_n\}$ and a monomial order $\succ$
queue := all subsets of B with exactly two elements
while *queue*! $= \emptyset$ **do**
    $\{f, g\}$:= head of *queue*
    $r := \overline{S(f,g)}^{B}$
    if $r \neq 0$ **then**
        $B := B \cup r$
        queue << $\{\{B_1, r\}, \dots \{\text{last of } B, r\}\}$
    end if
    delete head of *queue*
end while
return B (Gröbner basis)

The uniqueness of Gröbner basis is given via *reduced Gröbner basis*.

Definition 30. *For $R = \mathbb{F}[z_1, \dots z_n]$ with a monomial order $\succ$, a reduced Gröbner basis is a Gröbner basis $G = \{g_1, \dots g_k\}$ with respect to $\succ$, such that*

1. *Every $\mathrm{LT}(g_i)$ has the coefficient 1, $i = 1, \dots, k$.*
2. *Every monomial in g_i is not divisible by $\mathrm{LT}(g_j)$, if $j \neq i$.*

Proposition 31. *For $R = \mathbb{F}[z_1, \dots z_n]$ with a monomial order $\succ$, I is an ideal. The reduced Gröbner basis of I with respect to $\succ$, $G = \{g_1, \dots g_m\}$, is unique up to the order of the list $\{g_1, \dots g_m\}$. It is independent of the choice of the generating set of I.*

Proof. See Cox, Little, O'Shea [7, Chapter 2]. Note that given a Gröbner basis $B = \{h_1 \dots h_m\}$, the reduced Gröbner basis G can be obtained as follows,

1. For any $h_i \in B$, if $\mathrm{LT}(h_j) | \mathrm{LT}(h_i)$, $j \neq i$, then remove h_i. Repeat this process, and finally we get the *minimal basis* $G' \subset B$.
2. For every $f \in G'$, divide f towards $G' - \{f\}$. Then replace f by the remainder of the division. Finally, normalize the resulting set such that every polynomial has leading coefficient 1, and we get the reduced Gröbner basis G.

□

Note that Buchberger's Algorithm reduces only one polynomial pair every time, more recent algorithms attempt to (1) reduce many polynomial pairs at once (2) identify the "useless" polynomial pairs *a priori*. Currently, the most efficient algorithms are Faugere's F4 and F5 algorithms [8, 9].

Usually we compute Gröbner basis by programs, for example,

- MATHEMATICA The embedded **GroebnerBasis** computes Gröbner basis by Buchberger algorithm. The relation between Gröbner basis and the original generating set is not given. Usually, Gröbner basis computation in MATHEMATICA is not very fast.
- MAPLE Maple computes Gröbner basis by either Buchberger's Algorithm or highly efficient F4 algorithm.
- SINGULAR is a powerful computer algebraic system [10] developed in University of Kaiserslautern. SINGULAR uses either Buchberger's Algorithm or F4 algorithm to computer Gröbner basis.

- MACAULAY2 is a sophisticated algebraic geometry program [11], which orients to research mathematical problems in algebraic geometry. It contains Buchberger's Algorithm and experimental codes of F4 algorithm.

- Fgb package [12]. This is a highly efficient package of F4 and F5 algorithms by Jean-Charles Faugére. It has both MAPLE and C++ interfaces. Usually, it is faster than the F4 implement in MAPLE. Currently, coefficients of polynomials are restricted to $\mathbb{Q}$ or $\mathbb{Z}/p$, in this package.

Example 32. *Consider* $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$. *Compute the Gröbner basis of* $I = \langle f_1, f_2 \rangle$ *with grevlex and* $x \succ y$.

We use Buchberger's Algorithm.

1. *In the beginning, the list is* $B := \{h_1, h_2\}$ *and the pair set* $P := \{(h_1, h_2)\}$, *where* $h_1 = f_1$, $h_2 = f_2$,

$$S(h_1, h_2) = -x^2, \quad h_3 := \overline{S(h_1, h_2)}^B = -x^2\,, \tag{45}$$

with the relation $h_3 = yh_1 - xh_2$.

2. *Now* $B := \{h_1, h_2, h_3\}$ *and* $P := \{(h_1, h_3), (h_2, h_3)\}$. *Consider the pair* (h_1, h_3),

$$S(h_1, h_3) = 2xy, \quad h_4 := \overline{S(h_1, h_3)}^B = 2xy\,, \tag{46}$$

with the relation $h_4 = -h_1 - xh_3$.

3. $B := \{h_1, h_2, h_3, h_4\}$ *and* $P := \{(h_2, h_3), (h_1, h_4), (h_2, h_4), (h_3, h_4)\}$. *For the pair* (h_2, h_3),

$$S(h_2, h_3) = -x + 2y^2, \quad h_5 := \overline{S(h_2, h_3)}^B = -x + 2y^2\,, \tag{47}$$

The new relation is $h_5 = -h_2 - yh_3$.

4. $B := \{h_1, h_2, h_3, h_4, h_5\}$ *and*

$$P := \{(h_1, h_4), (h_2, h_4), (h_3, h_4), (h_1, h_5), (h_2, h_5), (h_3, h_5), (h_4, h_5)\}. \tag{48}$$

For the pair (h_1, h_4),

$$S(h_1, h_4) = -4xy^2, \quad \overline{S(h_1, h_4)}^B = 0 \tag{49}$$

Hence this pair does not add information to Gröbner basis. Similarly, all the rests pairs are useless.

Hence the Groebner basis is

$$B = \{h_1, \dots h_5\} = \{x^3 - 2xy, x^2y + x - 2y^2, -x^2, 2xy, 2y^2 - x\}. \tag{50}$$

Consider all the relations in intermediate steps, we determine the conversion between the old basis $\{f_1, f_2\}$ *and* B*,*

$$\begin{aligned} h_1 = f_1, \quad h_2 = f_2, \quad h_3 = f_1 y - f_2 x \\ h_4 = -f_1(1 + xy) + f_2 x^2, \quad h_5 = -f_1 y^2 + (xy - 1) f_2 \end{aligned} \tag{51}$$

Then we determine the reduced Gröbner basis. Note that $\mathrm{LT}(h_3) | \mathrm{LT}(h_1)$*,* $\mathrm{LT}(h_4) | \mathrm{LT}(h_2)$*, so* h_1 *and* h_2 *are removed. The minimal Gröbner basis is* $G' = \{h_3, h_4, h_5\}$*. Furthermore,*

$$\overline{h_3}^{\{h_4, h_5\}} = h_3, \quad \overline{h_4}^{\{h_3, h_5\}} = h_4, \quad \overline{h_5}^{\{h_3, h_4\}} = h_5 \tag{52}$$

so $\{h_3, h_4, h_5\}$ *cannot be reduced further. The reduced Gröbner basis is*

$$G = \{g_1, g_2, g_3\} = \{-h_3, \frac{1}{2}h_4, \frac{1}{2}h_5\} = \{x^2, xy, y^2 - \frac{1}{2}x\}. \tag{53}$$

The conversion relation is,

$$g_1 = -yf_1 + xf_2, \quad g_2 = -\frac{(1 + xy)}{2} f_1 + \frac{1}{2}x^2 f_2, \quad g_3 = -\frac{1}{2}y^2 f_1 + \frac{1}{2}(xy - 1) f_2. \tag{54}$$

MATHEMATICA *finds* G *directly via* ***GroebnerBasis[{x^3 − 2xy, x^2y − 2y^2 + x}, {x, y}, MonomialOrder → DegreeReverseLexicographic]****. However, it does not provide the conversion* (54)*. This can be found by* MAPLE *or* MACAULAY2*.*

As a first application of Gröbner basis , we can see some fractions can be easily simplified (like integrand reduction),

$$\begin{aligned} \frac{x^2}{(x^3 - 2xy)(x^2y - 2y^2 + x)} &= \frac{-yf_1 + xf_2}{f_1 f_2} = -\frac{y}{f_2} + \frac{x}{f_1} \\ \frac{xy}{(x^3 - 2xy)(x^2y - 2y^2 + x)} &= \frac{-(1 + xy)f_1/2 + x^2 f_2/2}{f_1 f_2} = -\frac{1 + xy}{2f_2} + \frac{x^2}{2f_1} \\ \frac{y^2}{(x^3 - 2xy)(x^2y - 2y^2 + x)} &= \frac{h_5 + x/2}{f_1 f_2} = \frac{x}{2f_1 f_2} - \frac{y^2}{2f_2} + \frac{xy - 1}{2f_1} \end{aligned} \tag{55}$$

In first two lines, we reduce a fraction with two denominators to fractions with only one denominator. In the last line, a fraction with two denominators is reduced to a fraction with two denominators but lower numerator degree ($y^2 \to x$)*. Higher-degree numerators can be reduced in the same way. Hence we conclude that all fractions* $N(x, y)/(f_1 f_2)$ *can be reduced to,*

$$\frac{1}{f_1 f_2}, \quad \frac{x}{f_1 f_2}, \quad \frac{y}{f_1 f_2} \tag{56}$$

and fractions with fewer denominators. Note that even with this simple example, one-variable partial fraction method does not help the reduction.

We have some comments on Gröbner basis:

1. For $\mathbb{F}[z_1, \dots z_n]$, the computation of polynomial division and Buchberger's Algorithm only used addition, multiplication and division in $\mathbb{F}$. No algebraic extension is needed. Let $\mathbb{F} \subset \mathbb{K}$ be a field extension. If $B = \{f_1, \dots, f_k\} \subset \mathbb{F}[z_1, \dots z_n]$, then the Gröbner basis computation of B in $\mathbb{K}[x_1, \dots, x_n]$ produces a Gröbner basis which is still in $\mathbb{F}[z_1, \dots z_n]$, irrelevant of the algebraic extension.

2. The form of a Gröbner basis and computation time dramatically depend on the monomial order. Usually, *grevlex* is the fastest choice while *lex* is the slowest. However, in some cases, Gröbner basis with *lex* is preferred. In these cases, we may instead consider some "midway" monomial order the like block order, or convert a known *grevlex* basis to *lex* basis [13].

3. If all input polynomials are linear, then the reduced Gröbner basis is the *echelon form* in linear algebra.

C. Application of Gröbner basis

Gröbner basis is such a powerful tool that once it is computed, most computational problems on ideals are solved.

1. Ideal membership and fraction reduction

A Gröbner basis immediately solves the ideal membership problem. Given an $F \in R = \mathbb{F}[z_1, \dots z_n]$, and $I = \langle f_1, \dots f_k \rangle$. Let G be a Gröbner basis of I with a monomial order $\succ$. $F \in I$ if and only if $\overline{F}^G = 0$, i.e., the division of F towards G generates zero remainder (Proposition 27).

G also determined the structure of the quotient ring R/I (Definition 4). $f \sim g$ if and only if $f - g \in I$. The division of $f_1 - f_2$ towards G detects equivalent relations. In particular,

Proposition 33. *Let M be the set of all monic monomials in R which are not divisible by any leading term in G. Then the set,*

$$V = \{[p] | p \in M\} \tag{57}$$

is an $\mathbb{F}$-linear basis of R/I.

Proof. For any $F \in R$, $\overline{F}^G$ consists of monomials which are not divisible by any leading term in G. Hence $[F]$ is a linear combination of finite elements in V.

Suppose that $\sum_j c_j[p_j] = 0$ and each p_j's are monic monomials which are not divisible by leading terms of G . Then $\sum_j c_j p_j \in I$, but by the Algorithm 2. $\overline{\sum_j c_j p_j}^G = \sum_j c_j p_j$. So $\sum_j c_j p_j = 0$ in R and c_j's are all zero. □

As an application, consider fraction reduction for $N/(f_1 \dots f_k)$, where N is polynomial in R,

$$\frac{N}{f_1 \dots f_k} = \frac{r}{f_1 \dots f_k} + \sum_{j=1}^{k} \frac{s_i}{f_1 \dots \hat{f}_j \dots f_k}. \tag{58}$$

The goal is to make r simplest, i.e., r should not contain any term which belongs to $I = \langle f_1, \dots f_k \rangle$. We compute the Gröbner basis of I, $G = \{g_1, \dots g_l\}$ and record the conversion relations $g_i = \sum_{j=1}^{k} f_j a_{ji}$ from the computation.

Polynomial division of N towards G gives,

$$N = r + \sum_{i=1}^{l} q_i g_i \tag{59}$$

where r is the remainder. The result,

$$\frac{N}{f_1 \dots f_k} = \frac{r}{f_1 \dots f_k} + \sum_{j=1}^{k} \frac{\left(\sum_{i=1}^{l} a_{ji} q_i\right)}{f_1 \dots \hat{f}_j \dots f_k}, \tag{60}$$

gives the complete reduction since by the properties of G, no term in r belongs to I. (60) solves integrand reduction problem for multi-loop diagrams. In practice, there are shortcuts to compute numerators like $\left(\sum_{i=1}^{l} a_{ji} q_i\right)$.

2. Solve polynomial equations with Gröbner basis

In general, it is very difficult to solve multivariate polynomial equations since variables are entangled. Gröbner basis characterizes the solution set and can also remove variable entanglements.

Theorem 34. *Let $f_1 \dots f_k$ be polynomials in $R = \mathbb{F}[x_1, \dots x_n]$ and $I = \langle f_1 \dots f_k \rangle$. Let $\bar{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$. The solution set in $\bar{\mathbb{F}}$, $\mathcal{Z}_{\bar{\mathbb{F}}}(I)$ is finite, if and only if R/I is a finite dimensional $\mathbb{F}$-linear space. In this case, the number of solutions in $\bar{\mathbb{F}}$, counted with multiplicity, equals* $\dim_{\mathbb{F}}(R/I)$.

Proof. See Cox, Little, O'Shea [6]. □

Note that again, we distinguish $\mathbb{F}$ and its algebraic closure $\bar{\mathbb{F}}$, since we do not need computations in $\bar{\mathbb{F}}$ to count total number of solutions in $\bar{\mathbb{F}}$. $\dim_{\mathbb{F}}(R/I)$ can be obtained by counting all monomials not divisible by $\mathrm{LT}(G(I))$, leading terms of the Gröbner basis. Explicitly, $\dim_{\mathbb{F}}(R/I)$ is computed by **vdim** of SINGULAR.

Example 35. *Consider* $f_1 = -x^2 + x + y^2 + 2, f_2 = x^3 - xy^2 - 1$. *Determine the number of solutions* $f_1 = f_2 = 0$ *in* $\mathbb{C}^2$.

Compute the Gröbner basis for $\{f_1, f_2\}$ *in grevlexwith* $x \succ y$, *we get,*

$$G = \{y^2 + 3x + 1, x^2 + 2x - 1\}. \tag{61}$$

Then $\mathrm{LT}(G)$=$\{y^2, x^2\}$. *Then* M *in Proposition 33 is clearly* $\{1, x, y, xy\}$. *The linear basis for* $\mathbb{Q}[x, y]/\langle f_1, f_2\rangle$ *is* $\{[1], [x], [y], [xy]\}$. *Therefore there are* 4 *solutions in* $\mathbb{C}^2$. *Note that Bézout's theorem would give the number* $2 \times 3 = 6$. *However, we are considering the solutions in affine space, so there are* $6 - 4 = 2$ *solutions at infinity. Another observation is that the second polynomial in* G *contains only* x, *so the variable entanglement disappears and we can first solve for* x *and then us* x*-solutions to solve* y. *This idea will be developed in the next topic, elimination theory.*

3. Solving polynomial equations

One very common question is to solve,

$$f_1(x_1 \dots x_n) = \dots = f_k(x_1 \dots x_n) = 0\,. \tag{62}$$

when the solution number is *finite*. This problem can be solved by Groebner basis. In fact, many modern computer programs already used Groebner basis approach.

An related question is that: let S be the solution set of 62. Instead of computing all the solutions, we are interested in a polynomial F, summed over all solutions,

$$\sum_{p_i \in S} F(p_i) \tag{63}$$

As we will see, this sum can be directly obtained from Groebner basis. Furthermore, the sum must be a rational function of the coefficients in the input polynomials f's! The Groebner basis method provides a way to compute the sum, in an analytic way.

Let $I = \langle f_1, \dots f_k\rangle$, and R/I be the quotient ring. From the discussion in the previous subsection, we know the R/I is a finite-dimensional linear space, if the solution if a finite set. That implies that we can transfer a multivariate polynomial problem to a linear algebra problem.

Suppose the we get the Groebner basis $G(I)$ of I in some ordering. Explicitly,

$$R/I = \text{span}_{\mathbb{F}}\big(m_1, \ldots, m_N\big) \tag{64}$$

where m's are the monomials which are not divided by the leading terms of $G(I)$.

Definition 36. *For any given polynomial F, we define the companion matrix M_F as*

$$[Fm_j] = \sum_{i=1}^{N} M_{F,ij}[m_i], \quad \forall 1 \leq j \leq N \tag{65}$$

The $N \times N$ matrix M_F is thus defined by the elements $M_{F,ij}$. Here N is the number of solutions.

It is clear that by the polynomial division, M's elements are just numbers in the coefficient ring. It is easy to see that

$$M_F + M_G = M_{F+G}, \quad M_F M_G = M_{FG} \tag{66}$$

Hence the companion matrix is a representation of the polynomials in the quotient ring R/I.

Proposition 37. *1. The eigenvalues of M_F are the values $F(p)$'s, for all $p \in S$.*

2. If $F(p)$, $p \in S$ are all distinct, then any left eigenvectors of M_F, up to an overall factor, has the form

$$\Big(m_1(p), \ldots m_N(p)\Big) \tag{67}$$

for some $p \in S$.

The proof is in [6].

From this proposition, we see that

$$\sum_{p \in S} F(p) = \text{tr}\, M_F \tag{68}$$

Since to get M_F, we just used Groebner basis and polynomial division, we see that no algebraic extension is needed. Therefore the formula gives the analytic sum instead of the numeric sum. This is a very useful computational tool used for the CHY formalism and the Bethe Ansatz equation.

Note that to use the second statement of proposition, we can design a generic F like

$$F = c_1 x_1 + \ldots c_N x_N \tag{69}$$

with random-integer valued c_i. With a large probability, all values of F on the solution set are distinct. It is a powerful tool to solve polynomial equation numerically and has been adopted in many computer softwares.

We already see that Gröbner basis can remove variable entanglement, here we study this property via elimination theory,

Theorem 38. *Let $R = \mathbb{F}[y_1, \dots y_m, z_1, \dots z_n]$ be a polynomial ring and I be an ideal in R. Then $J = I \cap \mathbb{F}[z_1, \dots z_n]$, the elimination ideal, is an ideal of $\mathbb{F}[z_1, \dots z_n]$. J is generated by $G(I) \cap \mathbb{F}[z_1, \dots z_n]$, where $G(I)$ is the Gröbner basis of I in lex order with $y_1 \succ y_2 \dots \succ y_m \succ z_1 \succ z_2 \dots \succ z_n$.*

Proof. See Cox, Little and O'Shea [7]. □

Note that elimination ideal J tells the relations between $z_1 \dots z_n$, without the interference with y_i's. In this sense, y_i's are "eliminated". It is very useful for studying polynomial equation system. In practice, Gröbner basis in *lex* may involve heavy computations. So frequently, we use block order instead, $[y_1, \dots y_m] \succ [z_1, \dots z_n]$ while in each block *grevlex* can be applied.

Here we give a simple example in IMO,

Example 39 (International Mathematical Olympiad, 1961/1)**.**
Problem *Solve the system of equations:*

$$\begin{aligned} x + y + z &= a \\ x^2 + y^2 + z^2 &= b^2 \\ xy &= z^2 \end{aligned} \tag{70}$$

where a and b are constants. Give the conditions that a and b must satisfy so that x, y, z (the solutions of the system) are distinct positive numbers.
Solution *The tricky part is the condition for positive distinct x, y, z. Now with Gröbner basis this problem can be solved automatically.*

First, eliminate x, y by Gröbner basis in lex with $x \succ y \succ z$. For example, in MATHEMATICA

$$\begin{aligned} &\mathbf{GroebnerBasis[\{-a + x + y + z, -b^2 + x^2 + y^2 + z^2, xy - z^2\}, \{x, y, z\},} \\ &\mathbf{MonomialOrder \to Lexicographic, CoefficientDomain \to RationalFunctions]} \end{aligned}$$

and the resulting Gröbner basis is,

$$G = \left\{a^2 - 2az - b^2, -a^4 + y\left(2a^3 + 2ab^2\right) + 2a^2b^2 - 4a^2y^2 - b^4, a^2 - 2ax - 2ay + b^2\right\}. \tag{71}$$

The first element is in $\mathbb{Q}(a,b)[z]$*, hence it generates the elimination ideal. Solve this equation, we get,*

$$z = \frac{a^2 - b^2}{2a}\,. \tag{72}$$

Then eliminate y, z *by Gröbner basis in lex with* $z \succ y \succ x$*. We get the equation,*

$$a^4 + x(-2a^3 - 2ab^2) - 2a^2b^2 + 4a^2x^2 + b^4 = 0\,. \tag{73}$$

To make sure x *is real we need the discriminant,*

$$-4a^2(a^2 - 3b^2)(3a^2 - b^2) \geq 0\,. \tag{74}$$

Similarly, to eliminate x, z*, we use lex with* $z \succ x \succ y$ *and get*

$$a^4 + y(-2a^3 - 2ab^2) - 2a^2b^2 + 4a^2y^2 + b^4 = 0\,, \tag{75}$$

and the same real condition as (74)*. Note that* x *and* y *are both positive, if and only if* x, y *are real,* $x + y > 0$ *and* $xy > 0$*. Hence positivity for* x, y, z *means,*

$$z = \frac{a^2 - b^2}{2a} > 0$$

$$x + y = a - z = a - \frac{a^2 - b^2}{2a} > 0 \tag{76}$$

$$-4a^2(a^2 - 3b^2)(3a^2 - b^2) \geq 0. \tag{77}$$

which implies that,

$$a > 0, \quad b^2 < a^2 \leq 3b^2. \tag{78}$$

To ensure that x*,* y *and* z *are distinct, we consider the ideal in* $\mathbb{Q}[a,b,x,y,z]$*.*

$$J = \{-a + x + y + z, -b^2 + x^2 + y^2 + z^2, xy - z^2, (x-y)(y-z)(z-x)\}. \tag{79}$$

Note that to study the a*,* b *dependence, we consider* a *and* b *as variables. Eliminate* x, y, z*, we have,*

$$g(a,b) = (a-b)(a+b)(a^2 - 3b^2)^2(3a^2 - b^2) \in J. \tag{80}$$

If all the four generators in J *are zero for some value of* (a,b,x,y,z)*, then* $g(a,b) = 0$*. Hence, if* $g(a,b) \neq 0$*,* x*,* y *and* z *are distinct in the solution. So it is clear that inside the region defined by* (78)*, the subset set*

$$a > 0, \quad b^2 < a^2 < 3b^2. \tag{81}$$

satisfies the requirement of the problem. On the other hand, if $a^2 = 3b^2$*, explicitly we can check that* x*,* y *and* z *are not distinct in all solutions. Hence* x, y, z *in a solution are positive and distinct, if and only if* $a > 0$ *and* $b^2 < a^2 < 3b^2$*. With* (72) *and* (73)*, it is trivial to obtain the solutions.*

5. Intersection of ideals

In general, given two ideals I_1 and I_2 in $R = \mathbb{F}[z_1, \dots z_n]$, it is very easy to get the generating sets for $I_1 + I_2$ and $I_1 I_2$. However, it is difficult to compute $I_1 \cap I_2$. Hence again we refer to Gröbner basis especially to elimination theory.

Proposition 40. *Let I_1 and I_2 be two ideals in $R = \mathbb{F}[z_1, \dots z_n]$. Define J as the ideal generated by $\{tf | f \in I_1\} \cup \{(1-t)g | g \in I_2\}$ in $\mathbb{F}[t, z_1, \dots z_n]$. Then $I_1 \cap I_2 = J \cap R$, and the latter can be computed by elimination theory.*

Proof. If $f \in I_1$ and $f \in I_2$, then $f = tf + (1-t)f \in J$. So $I_1 \cap I_2 \in J \cap R$. On the other hand, if $F \in J \cap R$, then

$$F(t, z_1, \dots, z_n) = a(t, z_1, \dots, z_n) t f(z_1, \dots, z_n) + b(t, z_1, \dots, z_n)(1-t) g(z_1, \dots, z_n)\,, \tag{82}$$

where $f \in I_1$, $g \in I_2$. Since $F \in R$, F is t independent. Plug in $t = 1$ and $t = 0$, we get,

$$F = a(1, z_1, \dots, z_n) f(z_1, \dots, z_n), \quad F = b(0, z_1, \dots, z_n) g(z_1, \dots, z_n)\,. \tag{83}$$

Hence $F \in I_1 \cap I_2$, $J \cap R \subset I_1 \cap I_2$. □

In practice, terms like tf and $(1-t)g$ increase degrees by 1, hence this elimination method may not be efficient.

---

[1] Y. Zhang, JHEP **1209**, 042 (2012), 1205.5707.

[2] D. A. Kosower and K. J. Larsen, Phys. Rev. **D85**, 045017 (2012), 1108.1180.

[3] R. Hartshorne, *Algebraic geometry* (Springer-Verlag, New York, 1977), ISBN 0-387-90244-9, graduate Texts in Mathematics, No. 52.

[4] O. Zariski and P. Samuel, *Commutative algebra. Vol. 1* (Springer-Verlag, New York-Heidelberg-Berlin, 1975), with the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28.

[5] O. Zariski and P. Samuel, *Commutative algebra. Vol. II* (Springer-Verlag, New York-Heidelberg, 1975), reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.

[6] D. A. Cox, J. B. Little, and D. O'Shea, *Using algebraic geometry*, Graduate texts in mathematics (Springer, New York, 1998), ISBN 0-387-98487-9, URL `http://opac.inria.fr/record=b1094391`.

[7] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Undergraduate Texts in Mathematics (Springer, Cham, 2015), 4th ed., ISBN 978-3-319-16720-6; 978-3-319-16721-3, an introduction

to computational algebraic geometry and commutative algebra, URL http://dx.doi.org/10.1007/978-3-319-16721-3.

[8] J.-C. Faugère, Journal of Pure and Applied Algebra **139**, 61 (1999), ISSN 0022-4049, URL http://www.sciencedirect.com/science/article/pii/S0022404999000055.

[9] J. C. Faugère, in *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation* (ACM, New York, NY, USA, 2002), ISSAC '02, pp. 75–83, ISBN 1-58113-484-3, URL http://doi.acm.org/10.1145/780506.780516.

[10] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann, SINGULAR *4-0-2 — A computer algebra system for polynomial computations*, http://www.singular.uni-kl.de (2015).

[11] D. R. Grayson and M. E. Stillman, *Macaulay2, a software system for research in algebraic geometry*, Available at http://www.math.uiuc.edu/Macaulay2/.

[12] J.-C. Faugère, in *Mathematical Software - ICMS 2010*, edited by K. Fukuda, J. Hoeven, M. Joswig, and N. Takayama (Springer Berlin / Heidelberg, Berlin, Heidelberg, 2010), vol. 6327 of *Lecture Notes in Computer Science*, pp. 84–87.

[13] J. Faugère, P. Gianni, D. Lazard, and T. Mora, Journal of Symbolic Computation **16**, 329 (1993), ISSN 0747-7171, URL http://www.sciencedirect.com/science/article/pii/S0747717183710515.

[14] A field $\mathbb{K}$ is algebraically closed, if any non-constant polynomial in $\mathbb{K}[x]$ has a solution in $\mathbb{K}$. $\mathbb{Q}$ is not algebraically closed, the set of all algebraic numbers $\bar{Q}$ and $\mathbb{C}$ are algebraically closed.