Methods of computational algebraic geometry in higher dimensional systems theory

Hyungju Park
Korea Institute for Advanced Study
email: alanpark@kias.re.kr

1 Introduction

Computational methods in commutative algebra and algebraic geometry has relatively short history. While mathematicians like Macaulay demonstrated constructive spirit at the turn of the 20th century, their work has been largely forgotten during most of the 20th century and only recently their influence is being rediscovered in several contexts.

Most significant contribution in this line of work is Buchberger's introduction of Gröbner basis in 60s [1, 2]. It took many years for this concept to be accepted by main-stream mathematicians. With the ever-growing power of computers, it is now viewed as a universal engine behind algebraic or symbolic computation.

Besides mathematical interests, algebraic computation also found many interesting applications to other areas which include systems theory and signal processing. Many problems in digital signal processing can be solved using the existing methods of algebraic and symbolic computation. This is made possible essentially because many signal processing problems can be modeled in the form of polynomial equations, which can then be solved by the methods of computational algebra, notably Gröbner basis.

2 Monomial Ideals

Let $X$ be a subvariety or a subscheme of $\mathbb{A}_k^n$, and $\mathcal{F}$ be a vector bundle or a coherent sheaf on $X$. Our goal is to manipulate such objects by computers.

Algebraically, we consider $S = k[x_1, \ldots, x_n]$, an ideal $I \subset S$, and a finitely generated $S$-module $M$. The main idea is to deform $I$ to a monomial ideal in a "nice" way. This is mainly because many or most interesting
problems for monomial ideals have simple combinatorial solutions. Without going into full justifications, we will list some examples to support this claim.

**Example 2.1 Dickson’s Lemma:** Any monomial ideal in \( k[x_1, \ldots, x_n] \) is generated by finitely many monomials, and there is an algorithm for finding such monomial generators.

**Example 2.2 Ideal Membership:** For monomials \( m_1, \ldots, m_l \) in \( S = k[x_1, \ldots, x_n] \), consider the monomial ideal \( I = \langle m_1, \ldots, m_l \rangle \) and a polynomial \( f \in S \). Does \( f \) belong to the ideal \( I \)?

To answer the question, write \( f \) as a sum of disjoint monomials: \( f = q_1 + \cdots + q_t \). Then it is easy to see that \( f \in I \) if and only if every monomial \( q_i \) is a multiple of some \( m_j \).

**Example 2.3 Computation of Hilbert functions:** For the monomial ideal \( I = \langle xy^2, y^3 \rangle \), compute its Hilbert function, i.e.

\[
H_I(s) := \dim(k[x, y]_{\leq s}/I_{\leq s}).
\]

By taking the exponent vectors of the monomials in \( k[x, y] \), the monomials belonging to the monomial ideal \( I \) can be visualized as the integral points in the shadowed region in Figure 1.

![Figure 1: Combinatorial Description of the Monomial Ideal I](image)

In this space of exponent vectors of monomials, \( H_I(s) \) is the number of lattice points in the first quadrant not belonging to \( I \) below the line connecting \((s, 0)\) and \((0, s)\). This is a simple counting problem. One easily observes

\[
H_I(0) = 1, \ H_I(1) = 3, \ H_I(2) = 6, \ H_I(3) = 8, \ldots
\]
and $H_I(s) = 2s + 2$, $s \geq 2$. Another obvious consequence is $\dim(I) = 1$ since $\dim(I)$ is equal to the degree of the Hilbert polynomial of $I$.

**Example 2.4** Syzygy computation: A syzygy of $f_1, \ldots, f_m \in S$ is a polynomial vector $(h_1, \ldots, h_m) \in S^m$ such that

$$h_1f_1 + \cdots + h_m f_m = 0.$$ 

The module of syzygies $F_1 := \text{Syz}(f_1, \ldots, f_m)$ is the module generated by all syzygies of $f_1, \ldots, f_m$. It should be noted that an effective algorithm for computing a set of generators for the syzygy module $F_1$ has far-reaching consequences for many problems. For instance, such an algorithm enables one to obtain a free resolution for a given ideal or a module.

Interestingly, the module of syzygies of “monomials” is easy to compute. For two terms $ax^\alpha, bx^\beta$, their syzygy is clearly $(bx^\alpha, -ax^\beta)$ where the monomials $x^\gamma$ and $x^\delta$ are uniquely determined by the requirement

$$x^\gamma x^\alpha = x^\delta x^\beta = \text{lcm}(x^\alpha, x^\beta).$$

The module of syzygies of $m$ such monomials is generated by pairwise syzygies.

### 3 Gröbner basis

We will use the shorthand notation for a monomial, $x^\alpha := x_1^{\alpha_1} \cdots x_m^{\alpha_m}$.

**Definition 3.1** A monomial order (or a term order on $k[x_1, \ldots, x_n]$) is a total ordering on the set of monomials in $k[x_1, \ldots, x_n]$ such that

1. $x^\alpha \geq 1$ for all monomials $x^\alpha$.
2. $x^\alpha \geq x^\beta$ implies $x^\gamma x^\alpha \geq x^\gamma x^\beta$ for all monomials $x^\gamma$.

To a given ideal $I \subset k[x_1, \ldots, x_n]$, one can associate a monomial ideal $\text{in}(I)$ which encodes a lot of information about $I$ itself.

**Definition 3.2** Fix a term order on $S = k[x_1, \ldots, x_n]$. For an ideal $I \subset S$, its initial ideal is defined by

$$\text{in}(I) := \langle \{lt(f) \mid f \in I\} \rangle,$$

where $lt(f)$ is the leading term of the polynomial $f$. 

95
Since in(I) is a monomial ideal, many interesting computations on in(I) can be carried out in straightforward combinatorial ways. Now we need to understand how the results of these computations can be "lifted" to analogous statements about the original ideal I.

Let λ be an integral weight function and 0 \neq t \in \mathbb{k}. Consider the following automorphism induced by the torus action:

\[ \Lambda : S = k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n] \]
\[ x_i \mapsto t^{-\lambda(x_i)} x_i. \]

For \( I_t := \text{the image of } I \text{ under } \Lambda \), all \( S/I_t \) are clearly isomorphic as long as \( t \neq 0 \). As \( t \to 0 \), the initial terms of polynomials in \( I_t \) come to dominate the polynomials and the limit (i.e. the fiber over \( t = 0 \)) becomes \( S/\text{in}_\lambda(I) \). This is a flat deformation, i.e. the family \( S/I_t \) is a flat family. Therefore, the properties for I preserved under a flat deformation can be investigated with the simpler object in(I). Such results can be directly translated to statements about the original ideal I. Examples of such properties include the dimension and the Hilbert function of I. Note that, for any term order, one can find a suitable integral weight function \( \lambda \) such that the initial ideal of I w.r.t. the term order is equal to \( \text{in}_\lambda(I) \).

The power of deforming to a monomial ideal comes from the fact that even the properties on I not preserved under a flat deformation can be retrieved from the analogous properties on in(I). This is done by carefully tracking the deformation process. Such tracking can be done by using a remarkably nice set of generators for I, namely a Gröbner basis.

Before making a formal definition, note that, for an ideal \( I = \langle f_1, \ldots, f_m \rangle \subset S \), its initial ideal w.r.t. a fixed term order is not necessarily equal to the monomial ideal \( \langle \text{lt}(f_1), \ldots, \text{lt}(f_m) \rangle \). In general, \( \text{in}(I) \) contains \( \langle \text{lt}(f_1), \ldots, \text{lt}(f_m) \rangle \) and could be strictly bigger. For a simple example, consider the ideal \( I := \langle x^2 - xy, y^2 \rangle \subset k[x, y, z] \) w.r.t. the lexicographic order \( x > y > z \).

A Gröbner basis \( G = \{ g_1, \ldots, g_m \} \) for I is a nice set of generators for I from which \( \text{in}(I) \) can be directly computed simply by taking the ideal generated by the leading terms of \( g_i \)'s. Such generators allow us to reduce the seemingly difficult computations on I to much simpler computations on a monomial ideal.
4 Basic Concepts from Signal Processing

4.1 1-D Discrete-time Signals

Definition 4.1 1. A one-dimensional (1-D) discrete-time signal is a sequence of real numbers, i.e., \( (a_n)_{n \in \mathbb{Z}} = (\ldots, a_{-2}, a_{-1}, a_0, a_1, a_2, \ldots) \), where \( a_n \in \mathbb{R} \) and there exists \( N \in \mathbb{Z} \) such that \( a_n = 0 \) for all \( n < N \).

2. The set of 1-D discrete-time signals is denoted by \( S \).

Discrete-time signals arise naturally, for example, by sampling continuous-time signals: for a continuous-time signal \( f(t) \), define \( a_n \) to be \( f(nT) \) where \( T \) is a preset sampling period.

Remark 4.2 The above definition is a formal one. In practice, a 1-D discrete-time signal often means a square-summable sequence. The set of such square-summable sequences is denoted by \( l_2(\mathbb{Z}) \).

Remark 4.3 In this paper, a 1-D signal \( (a_n)_{n \in \mathbb{Z}} \) will be abbreviated as \( (a_n) \).

The set \( S \) of 1-D discrete-time signals naturally forms an \( \mathbb{R} \)-vector space with the well-defined operations of the superposition and the scalar multiplication of sequences.

Definition 4.4 Convolution of discrete-time signals: For given two signals \( (a_n) \) and \( (c_n) \), their convolution \( (b_n) := (a_n) \ast (c_n) \) is defined by \( b_n := \sum_{i+j=n} a_i c_j \).

Definition 4.5 For a fixed \( (c_n) \in S \), the operator \( L(c_n) \) on the set \( S \) of discrete-time signals is defined by \( L(c_n)((a_n)) := (a_n) \ast (c_n) \)

Trivially, the map \( L(c_n) : S \rightarrow S \) is a linear map of \( \mathbb{R} \)-vector spaces. And the set \( S \) of discrete-time signals equipped with the two operations of superposition and convolution forms a commutative ring with identity \( (\delta_{n,0}) \), where \( \delta_{0,0} = 1 \) and \( \delta_{n,0} = 0, \forall n \neq 0 \).

4.2 Linear Time-invariant Systems

Definition 4.6 Then an \( \mathbb{R} \)-linear map \( L : S \rightarrow S \) is said to be time-invariant if, for any fixed integer \( i \),

\[
L((a_n)) = (b_n) \quad \text{implies} \quad L((a_{n+i})) = (b_{n+i}).
\]
Such an operator can be described by the following Single-Input Single-Output (SISO) system.

\[
\begin{array}{c}
\ldots,a_{-1},a_0,a_1,\ldots \quad \overset{L}{\longrightarrow} \quad \ldots,b_{-1},b_0,b_1,\ldots
\end{array}
\]

**Lemma 4.7** Let \( S \) be the \( \mathbb{R} \)-vector space of discrete-time signals. Then a map \( L : S \to S \) is \( \mathbb{R} \)-linear and time-invariant if and only if \( L \) is \( S \)-linear.

**Proof:** An easy exercise \( \square \)

**Corollary 4.8** Let \( S \) be the \( \mathbb{R} \)-vector space of discrete-time signals. If a map \( L : S \to S \) is linear and time-invariant, then it can be represented by a convolution, i.e., there exists a unique discrete-time signal \( (c_n) \in S \) such that \( L = L(c_n) \).

In such a case, \( (c_n) \) is called the **modulating signal** for \( L \) or the **impulse response** for \( L \).

If \( L = L(c_n) \) with \( c_n = 0, \forall n < 0 \), then \( L \) is called a **causal** system. In this case, \( b_n \) is determined completely by \( a_i \)’s with \( i \leq n \). Loosely speaking, the present value in the output signal does not depend on the future values in the input signal.

If \( L = L(c_n) \) and \( (c_n) \) is a discrete-time signal of finite duration i.e., a finite sequence, then \( L \) is called an **FIR** (Finite Impulse Response) system.

**Definition 4.9** Let \( S \) be the ring of discrete-time signals, and \( p, q \in \mathbb{N} \). Then an \( S \)-module homomorphism \( A : S^p \to S^q \) is called a linear time-invariant Multi-Input Multi-Output (MIMO) system.

**Remark 4.10** To understand this definition, consider a map \( A : S^p \to S^q \), which can be viewed as a map between \( \mathbb{R} \)-vector spaces. If \( A \) is \( \mathbb{R} \)-linear and time-invariant, then it is actually an \( S \)-module homomorphism.

A MIMO system \( A : S^p \to S^q \) can be described by the following picture:

\[
\begin{array}{c}
\begin{array}{c}
(a_n^1) \quad \cdots \quad (a_n^p) \\
\vdots \\
(b_n^1) \\
\vdots \\
(b_n^q)
\end{array}
\end{array}
\]

In this case, such a \( p \)-input \( q \)-output linear time-invariant system is an operator from the module \( S^p \) to the module \( S^q \) defined by convolutions with various fixed signals.
4.3 Perfect Reconstruction of Signals

Let $A$ and $S$ be a $p$-input $q$-output MIMO system and a $q$-input $p$-output MIMO system, respectively. Suppose that, when an incoming signal goes into $A$ and the subsequent output is fed into $S$, the resulting output of $S$ is identical to the original input signal of $A$. If this is true for any input, then the combined effect of the overall system made of $A$ and $S$ is complete preservation of inputs.

For a given $p$-input $q$-output MIMO system $A$, if there exists a $q$-input $p$-output MIMO system $S$ such that the overall system (made of $A$ and $S$) preserves inputs completely, then $A$ is said to have the perfect reconstruction (PR) property. In this case, $A$ and $S$ are said to make a PR system, and $A$ ($S$, resp.) is called the analysis (synthesis, resp.) part of the overall system.

5 Algebraic Formulation

5.1 Z-transform

In the previous section, it was established that the set $S$ of 1-D discrete-time signals equipped with the operations of superposition and convolution forms a commutative ring. This ring $S$ is isomorphic to the ring $\mathbb{C}[[z^{-1}]]_{z^{-1}}$, a localization of the formal power series ring $\mathbb{C}[[z^{-1}]]$, via the following correspondence:

$$(a_n) \mapsto \sum_{n=-\infty}^{\infty} a_n z^{-n}.$$  

This mapping is usually called the $Z$-transform in signal processing literature.

A Single-Input Single-Output system can be viewed as an operator on $\mathbb{C}[[z^{-1}]]_{z^{-1}}$.

$$\sum a_n z^n \rightarrow f \rightarrow \sum b_n z^n$$
If $f$ is a linear time-invariant system, then it is a multiplication by a power series in $\mathbb{C}[[z^{-1}]]z^{-1}$, and causal system is a multiplication by a power series in $\mathbb{C}[[z^{-1}]]$.

If $f$ is an FIR system, then it is a multiplication by a Laurent polynomial in $\mathbb{C}[z^{-1}]z^{-1} = \mathbb{C}[z, z^{-1}]$, and therefore, a causal FIR system is a multiplication by a polynomial in $\mathbb{C}[z^{-1}]$.

This is readily generalized to a (linear time-invariant) Multi-Input Multi-Output system, that is, a linear time-invariant $p$-input $q$-output FIR system $A : (\mathbb{C}[z\pm1])^p \rightarrow (\mathbb{C}[z\pm1])^q$ is a multiplication by a matrix, i.e.

$$A \in M_{pq}(\mathbb{C}[z\pm1]).$$

This matrix $A$ is sometimes called the transfer matrix of the underlying MIMO system.

Remark 5.1 Various signal processing problems can be understood in terms of MIMO systems which are characterized by their transfer matrices [7]. For example, by using the method of polyphase decomposition, the design of PR oversampled filter bank can be reduced to the design of a PR MIMO system [6].

5.2 Perfect Reconstruction in Z-transform Domain

Consider a given $p$-input $q$-output MIMO system whose Z-transform representation is a $q \times p$ matrix $A$. Then clearly, this MIMO system has the perfect reconstruction property if and only if $A$ has a left inverse $S$ such that

$$SA = I_p,$$

where $I_p$ is the $p \times p$ identity matrix. In this case, the overall system made of $A$ and $S$ makes a PR system, and $A$ ($S$, resp.) is the analysis (synthesis, resp.) part of the overall system.

Remark 5.2 In signal processing literature, the MIMO system represented by a $q \times p$ Laurent polynomial matrix $A$, $q \geq p$, is often said to have the perfect reconstruction property if there is a $p \times q$ Laurent polynomial matrix $S$ and an integer $d$ such that

$$SA = z^d I_p.$$

In this context, the integer $|d|$ is called a delay if $d$ is negative, and is called an advance if $d$ is positive.

Note that these two definitions of perfect reconstruction are actually identical: That is, if $SA = z^d I_p$, then $z^{-d} S$ is the left inverse of $A$. 

100
6 Extensions to Higher Dimensions

Definition 6.1 An m-D discrete-time signal is a multiply-indexed sequence of real numbers, i.e. \((a_{i_1\ldots i_m})_{(i_1\ldots i_m)\in\mathbb{Z}^m}\), or an infinite m-Dimensional array of numbers, where each \(a_{i_1\ldots i_m} \in \mathbb{R}\) and there exists \(N \in \mathbb{Z}\) such that \(a_{i_1\ldots i_m} = 0\) if \(i_i < N\) for some \(i_i\).

One can define superposition and convolution of m-D discrete-time signals as in the 1-D case. Linear time-invariant m-D systems are defined in the same way. It is easy to check that the set of m-D discrete-time signals forms a commutative ring with these two operations. This set is naturally isomorphic to the ring \(\mathbb{C}[z_{i_1}^{-1}, \ldots, z_{i_m}^{-1}]\), a localization of the multivariate formal power series ring \(\mathbb{C}[z_{i_1}^{-1}, \ldots, z_{i_m}^{-1}]\), via the Z-transform.

All the concepts introduced for 1-D signals in the preceding sections can be readily extended to the m-D signals. For example, in the Z-transform domain, an m-D FIR MIMO system is described by a matrix whose entries are Laurent polynomials in m variables, i.e. elements of \(\mathbb{C}[z_{i_1}^{\pm 1}, \ldots, z_{i_m}^{\pm 1}]\). The method of polyphase representation can be extended to multidimensional filter banks. In this case, the delay chain is replaced by cosets of a fixed sampling lattice (see [4]).

7 Unimodularity and Perfect Reconstruction

Definition 7.1 Let \(R\) be a commutative ring.

1. Let \(v = (v_1, \ldots, v_n)^t \in R^n\) for some \(n \in \mathbb{N}\). Then \(v\) is called a unimodular column vector if its components generate \(R\), i.e. if there exist \(g_1, \ldots, g_n \in R\) such that \(v_1g_1 + \cdots + v_ng_n = 1\).

2. A matrix \(A \in M_{pq}(R)\) is called a unimodular matrix if its maximal minors generate the unit ideal in \(R\).

Theorem 7.2 A \(q \times p\) Laurent polynomial matrix, \(q \geq p\), has a left inverse if and only if it is unimodular.

A proof of this assertion in the case of polynomial matrices can be found in [5]. An immediate corollary of this theorem is
Corollary 7.3 A \( p \)-input \( q \)-output FIR MIMO system can be the analysis portion of a PR FIR MIMO system if and only if its Z-transform representation is a unimodular Laurent polynomial matrix.

Therefore, the study of perfect reconstruction FIR linear time-invariant MIMO systems can be viewed as the study of unimodular matrices over Laurent polynomial rings.

Example 7.4 Consider an FIR MIMO system whose Z-transform representation is given by

\[
U = \begin{pmatrix}
\frac{3}{z} - 2 - 2z + 2z^2 & \frac{6}{z} + 25 - 23z - 16z^2 + 20z^3 \\
\frac{3}{z} - 2z & \frac{6}{z} + 29 - 4z - 20z^2 \\
2z & 2 + 4z + 20z^2
\end{pmatrix}.
\]

Determine if this system allows perfect reconstruction of arbitrary input signals.

Solution: The three maximal minors of \( U \) are \(-1, -4 + 6/z - 2z + 2z^2, 6/z - 2z\). These three Laurent polynomials do not have a common zero in \( \mathbb{C}^* \), and by a Laurent polynomial analogue of Nullstellensatz, generate the unit ideal. Hence the given system allows perfect reconstruction of arbitrary input signals.

8 Construction of Synthesis Matrix

Consider a unimodular \( q \times p \) matrix \( A, q \geq p \), with Laurent polynomial entries. By Theorem 7.2, \( A \) represents a perfect reconstruction MIMO system, and there exists a \( p \times q \) matrix \( S \) such that \( SA = I_p \).

In 1-D case, such a matrix \( S \) (not unique unless \( p = q \)) can be easily computed by using a Laurent polynomial analogue of Euclidean Division Algorithm.

Example 8.1 Consider the FIR MIMO system in Example 7.4, which allows perfect reconstruction of arbitrary input signals. Let us explicitly construct a synthesis system which will reconstruct the original inputs.

Using the Laurent polynomial analogue of Euclidean Division Algorithm, we can successively apply elementary row operations to reduce \( U \) to its row echelon form:

\[
EU = \begin{pmatrix}
1 & 0 \\
0 & 1 \\
0 & 0
\end{pmatrix},
\]

102
where the $3 \times 3$ matrix $E$ is found as

$$
\begin{pmatrix}
\frac{5}{36}(-18-125z-188z^2+252z^3-215z^4+178z^5+6z^6) \\
\frac{5}{6}(3+19z-32z^2+23z^3-9z^4-8z^5+6z^6) \\
z(-4z+23z^2-5z^3+z^4+8z^5-2z^6)
\end{pmatrix}
\begin{pmatrix}
\frac{5}{3}(-2-27z+30z^2+z^3) \\
z(4-3z-z^2+z^3) \\
2z(-3+2z+2z^2-z^3)
\end{pmatrix}
\begin{pmatrix}
\frac{1}{2}(-12-89z+51z^2-60z^3-2z^4) \\
9/2-4z+3z^2/2+z^3-z^4 \\
-6+6z-z^2-2z^3+2z^4
\end{pmatrix}
$$

The $3 \times 3$ matrix $E$ represents the series of elementary row operations applied to $U$, and the first two rows of $U$ make a left inverse of $U$.

In $m$-D case, however, this method for the univariate case is no longer applicable as the Euclidean Division Algorithm is not available any more, and computing $S$ should resort to Gröbner basis. For example, consider the 2-D linear time-invariant system whose $Z$-transform representation is given by

$$
A = \begin{pmatrix}
\frac{1}{z_2} + \frac{z_1}{z_2} + \frac{z_1}{z_2} \\
\frac{z_1}{z_2} + \frac{1}{z_2} + \frac{z_1}{z_2}
\end{pmatrix} \in (\mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}])^2.
$$

**References**


