Groebner bases under composition and multivariate matrix factorization

Mingsheng Wang

Institute of Software, Chinese Academy of Sciences
Contents of the talk

In this talk, I will introduce some of my work related to Groebner bases.

I. Behavior of a Groebner basis under composition — New Results;

II. Multivariate polynomial matrix factorization — New progress.
PART(I)
Groebner bases under composition
Groebner bases under composition

Hoon Hong initiated the study of Groebner bases under composition
Groebner bases under composition

Early papers:


Basic research Problem

Let us consider the polynomial ring in n variables: $K[x] = k[x_1, \ldots, x_n]$, and a given term ordering $>$. The basic problem can be described as follows:

For an endomorphism $U$ of $k[x]$, and a finite subset $G$ of $k[x]$, how can we compute a Groebner basis of $U(G)$ under the term ordering $>$ by means of a Groebner basis of $G$ and $U$?
Hong’s Theorem

For any Grobner basis $G$ of $k[X]$, $U(G)$ is a Groebner basis if and only if

(a) for any terms $p$ and $q$, $p < q$ implies $lt(U(p)) < lt(U(q))$;

(b) $lt(U)$ is a permuted powering, that is, every component of $U$ has a power of one variable as the leading term, where $U = (u_1, \ldots, u_n)$: $x_j \rightarrow u_j$. and $lt(U) = (lt(u_1), \ldots, lt(u_n))$. 
Result of Gutirrez etc.

Gutirrez etc. have proved a result on reduced case. Their result is:
For any reduced Groebner basis G, U(G) is a reduced Groebner basis if and only if

(a) for any terms p, q, p<q implies lt(U(p))<lt(U(q)).

(b) every component of U is a polynomial in one variable, and different polynomial involves in different variable.
A generalization

First, we establish a more general framework:

Let $U$ be a homomorphism from $k[x] = K[x_1, \ldots, x_n]$ to $k[y] = k[y_1, \ldots, y_m]$ s.t. $n < m$ or $n = m$.

Given two term orderings $>_1$ on $k[x]$ and $>_2$ on $K[y]$. In this case $u_j$ is in $k[y]$. 
A generalization

Under this new framework, Hong’s theorem can be **generalized** as follows:

For any Groebner basis $G$ with respect to $<_1$, $U(G)$ is a Groebner basis with respect to $<_2$ if and only if

1. for any terms $p$, $q$, $p < _1 q$ implies that $\text{lt}(U(p)) < _2 \text{lt}(U(q))$;
2. $\text{lt}(u_i)$ and $\text{lt}(u_j)$ are pairwise coprime for different $i$ and $j$. 
A generalization

But in reduced case, it seems to lack a sufficient and necessary condition in this generalization case.

Details can be found in:

*Remarks on Groebner basis for ideals under composition, ISSAC, 2001.*
Check the term ordering conditions

From the above theorems, we need to solve the term ordering compatible problem in order to apply these theorems:

Find an efficient algorithm to check if for any terms p and q, \( p <_1 q \) implies \( \text{lt}(U(p)) <_2 \text{lt}(U(q)) \)? (Hong)
Let $T$ be the matrix corresponding to exponent vectors of leading terms of $u_j$, where $U = (u_1, \ldots, u_n)$.

Let term ordering $>_1$ be represented by a $n \times n$ matrix $A$, and $>_2$ be represented by matrix $B$. Thus our method is using rational elementary transformation to $A$ and $TB$ simultaneously to obtain some standard form in some sense, then check if these standard form are the “same” which is up to a positive number multiple.
So called elementary rational transformation for the real matrices we mean:

I. Multiplying a row of a matrix by a non-zero rational number;

II. Interchanging any two rows;

III. Adding a rational multiple of one row to another row

See JSC(2003), vol.35.
Homogeneous case

An interesting problem is:

Under what conditions that for any homogeneous groebner bases $G$, $U(G)$ is homogeneous groebner bases?

Journal of Algebra, computational algebra section, In press.
Homogeneous case

We have provided a complete answer:

For any homogeneous Groebner bases $G$, $U(G)$ is a homogeneous Groebner bases if and only if

(I) for any terms $p,q$ with $\deg(p)=\deg(q)$, $p<q$ implies $\lt(u(p))<\lt(u(q))$;

(ii) $\lt(U)$ is a permuted powering, and every $u_i$ has the same degree.
Further results

The problems can be further extended more general case. Let $L$ be an arbitrary grading on $k[x]$, we may ask:

Under what conditions that for any $L$-homogeneous groebner bases $G$, $U(G)$ is Groebner bases?
For any L-homogeneous Gb G, U(G) is GB if and only if
(I) for any terms p > q, L(p) = L(q) implies \( \text{lt}(U(p)) > \text{lt}(U(q)) \);
(II) \( \text{lt}(U) \) is a permuted powering;
Remarks

This new result unifies all the previous results. Because if $L(x_i)=0$ for every $I$, we get Hong’s theorem; if $L(x_i)=1$ for every $I$, we get the usual homogeneous result.

The proof is slightly hard; submitted to Journal of Algebra, CA section.
Summary

- From above descriptions, we see that only universal cases are considered.
- For the basic problem: Given a Groebner basis $G$, and a homomorphism $U$, How can we compute the Groebner basis of $U(G)$ by means of $G$ and $U$?
- We have not solved the basic problem! It seems to have some difficulties.
Summary

- There are a lot of related work in Resultant, subresultant, Sagbi bases, non-commutative Groebner bases etc.
- See related papers.
PART(II)

Multivariate polynomial matrix factorization
Basic Problem

Given a nD polynomial matrix $F$ with full row rank of size $(l, m)$.

Let $d$ be the gcd of all the $l$-minors, $f|d$, whether or not there exists square matrix $G$ and matrix $F_1$, such that

$$F = GxF_1$$

with $\det(G) = f$?
The History

- When $n=1$, this is solved completely using Gauss elimination, and play an essential role in linear systems and control theory, convolutional codes.

- When $n=2$, this is solved using pseudodivision by N. K. Bose and others, used in 2-D systems and signal processing.

- When $n \geq 3$, this is thought as very hard! Because previous methods can not be generalized to this case.
Motivation for research

Why we concern about this problem?

(i). Generalize linear system theory to multidimensional systems theory since 1976.
(ii). Many problems in multidimensional systems and signal processing can be formulated in multivariate matrix problems.
(iii). May be useful in multidimensional convolutional codes.
(iv). Possibly other applications.
Reduced minors

In order to introduce Lin-Bose Problem, we give a basic definition as follows:

Let $F$ be a full row rank matrix of size $(l, m)$, let $a_1, \ldots, a_k$ be all the $l$-minors of $F$, $d$ be the g.c.d of $a_1, \ldots, a_k$, and let $b_1, \ldots, b_k$ such that $a_j = dx b_j$. $b_1, \ldots, b_k$ is said to be the reduced minors of $F$. 
Some research papers

There are many papers concerning this problems, we just mention:


Research papers

Z. Lin, Further results on nD polynomial matrix factorization, Multidimensional system and system processing, Vol 12, 2001, pp199-208.

Research papers

Zero prime factorization

A full row rank matrix is zero prime if all its maximal order minors generate the unit ideal.

Lin-Bose propose the following problem:
Given $F$, full row rank of size $l \times m$, if all the reduced minors generate the unit ideal, then whether or not $F$ can be factorized as $F=GxF_1$, with $\det(G)=d$, $d$ the gcd, and $F_1$ being zero prime?
Zero prime factorization

J.F. Pommaret gave a proof using algebraic analysis method in 2001 Euro control conference, his method only holds for the complex number field.

We give a full proof for any field. Linear algebra and applications, 2004
Minor prime factorization

Let $F$ be as above, $d$ the gcd of all the $I$-minors of $F$. Whether or not there exists $G$ such that $F = Gx^1F_1$ and $\det(G) = d$?

If such factorization exists, we call it **minor prime factorization** of $F$.

Several people gave counter-examples to showed that the above problem may have no solution in 1976-1979;

However, **no one** propose a sufficient and necessary condition!
Minor prime factorization

We first found a **sufficient and necessary** condition.

Let $K$ be submodule generated by all the rows of $F$. There exists a minor prime factorization if and only if the colon submodule $K:d$ is a free module of rank 1.
Remarks to the proof

The proof of the above result relies on a characterization of so-called **minor left prime** (MLP) matrix.

A full row rank matrix $F$ of size $l \times m$ is said to be a MLP matrix if all the $l$-minors have only trivial common divisors.

The result just holds for any field. See *Mathematics of control, signals and systems, 2005* for details.
Remarks to proof

We first prove, a matrix $F$ is a MLP if and only if $K:d=K$, where $K$=submodule generated by all the rows of $F$, $d$ the g.c.d of all the $lxl$ minors of $F$.

Then using a lifting to the linear mapping, we get the factor.

Note that when $F$ is not full rank, this result will not hold, and above result does not hold either.
An algorithm

Based on above theorem, we propose an algorithm as follows:

**Step 1** Let $F$ as above, $d$ the g.c.d of all $l$ times $l$ minors of $F$. Compute the syzygy module of row vectors of $F$ and $-dxI_m$. If this syzygy module is free of rank $l$, then form a generating matrix $[G|H]$ such that $G$ is a $lxl$ matrix, thus $dG^{-1}$ is the desired matrix factor;

**Step 2** If this syzygy module is not free, then there do not exist such a matrix factor.
We can easily check if a submodule is free using Fitting ideals.
Factor prime matrix

F is said to be factor prime, if for any square matrix G, \( F = G \times F_1 \), implies that \( \det(G) \) is a non-zero constant.

A basic problem is to check if F is factor prime matrix.
Factor prime matrix

Checking if a matrix is factor prime is a long-standing open problem since the concept was proposed in 1979.


We have also obtained some partial answers!
Remarks for checking of FLP

No any other methods available to attack deciding problem of factor prime matrix;
This is the first result concerning factor prime matrix.
Full solutions can not obtained at this time, to be submit.
Remarks to the algorithm

Major problem is: how to extract a system of generators with \( I \) elements from a system of generators of syzygy module?

Book “Computational Commutative algebra I” by Martin Kreuzer and Lorenzo Robbiano provides a partial answer in Corollary 3.1.12 which was implemented in CoCoA.
Compare with other related work

- Previous papers only deal with very special cases.
- Above results are true for any field, that is, without restriction to characteristic zero and algebraically closed.
- Only Groebner bases theory is available to attack matrix factorization problems currently.
Some problems

I’d like to list some problems which deserve to be considered:

- Problem 1: if there are other efficient methods to deal with this problem?
- Problem 2: How to find a minimal generating system from a given generating system?
- Problem 3: If there are other criteria to assure that the existence of a generating system of \(l\) elements? (\(l=\text{rank}\))
Some problems

- Problem 4: If elementary transformations for multivariate polynomial matrices can be used to find matrix factor?
- Problem 5: Find other characterizations for the existence of the matrix factor!
- Problem 6: Find the methods for dealing with non-full rank cases.
Conclusion

- Matrix factorization problems connect with many problems in system theory, for example, rational matrix fraction description.

- Generalization of convolutional codes in one variable to multidimension also needs to develop multivariate matrix theory.

- It needs to develop new algorithmic methods!
Thank you for your attention!