Записки научных
семинаров ПОМИ
Том 373, 2009 г.

N. Vassiliev, D. Pavlov

STRONG NON–NOETHERITY OF POLYNOMIAL REDUCTION

It is well known result by A.Reeves and B.Sturmfels, that the reduction modulo a marked set of polynomials is Noetherian if and only if the marking is induced from an admissible term order. For finite sets of polynomials with non-admissible order, there is a constructive proof of existence of infinite reduction sequence, although the finite one is might still be possible. On the base of our specialized software for combinatorics of monomial orders, we have found some examples, for which there is not any finite reduction sequence. This is what we call "strong" non-noetherity.

1. Introduction

One of the most important properties of the Gröbner bases of polynomial ideals is that any polynomial have unique *normal form* with respect to the given Gröbner base. Moreover, the normal form of any polynomial can be calculated in finite number of *reduction* steps. For one reduction step, any of base polynomials can be selected, from those whose *initial terms* divide the initial term of the polynomial being reduced. When the resulting polynomial can not be reduced with any of the base polynomials, it is the normal form. With Gröbner base, process of reduction is always finite ([2], Chapter 2).

Proper definition of Gröbner basis involves the concept of admissible *monomial ordering* (or simply "monomial ordering" in [2]), which is total monomial ordering $>$ on $\mathbb{Z}_+^n$ satisfying the following conditions:
1. $\forall \alpha, \beta, \gamma \in \mathbb{Z}_+^n, \gamma \neq 0 \quad \alpha > \beta \Rightarrow \alpha + \gamma > \beta + \gamma$
2. $\mathbb{Z}_+^n$ contains no infinite descending chains

The second condition, as shown in [2], can be replaced with that $\alpha \geq 0$ for all $\alpha \in \mathbb{Z}_+^n$.

Aside from the admissible orderings, we are also considering the larger class of *weak-admissible orderings*, which are total monomial orderings on

Ключевые слова : polynomial reduction, monomial ordering, noetherity, Gröbner base.

$\mathbb{Z}_+^n$ satisfying the following condition:

$$\forall \alpha, \gamma \in \mathbb{Z}_+^n, \gamma \neq 0 \quad \alpha + \gamma > \alpha.$$

In terms of monomial arithmetic, this means that the weak-admissible orderings are compatible with the divisibility. The admissible orderings are also compatible with the monomial multiplication. Each admissible ordering is weak-admissible.

We denote $K[x_1, \dots, x_n]$ the set of all polynomials in variables $x_1, \dots, x_n$ with coefficients in the field K. Given some set of polynomials $\mathcal{F} \subset K[x_1, \dots, x_n]$ and some ordering $<$, we associate to each polynomial $f \in \mathcal{F}$ the *initial term* $in(f) \in \mathbb{Z}_+^n$. $in(f)$ is the $<$-leading term of f. If $<$ is admissible ordering, we say, as in [1], that $\mathcal{F}$ is marked *coherently.*

We denote $\rightarrow_{\mathcal{F}}$ the *reduction relation modulo* $\mathcal{F}$. As stated in [reduction], $\rightarrow_{\mathcal{F}}$ is Noetherian (i.e. the reduction sequence always terminates) iff $\mathcal{F}$ is marked coherently. For finite sets of polynomials, there is a constructive proof of existence of infinite reduction sequence.

2. Zero-dimensional ideals

Let $\mathfrak{A}$ denote the polynomial ideal in $K[x_1, \dots, x_n]$. Let A denote the quotient algebra of $\mathfrak{A}$:

$$A = K[x_1, \dots, x_n]/\mathfrak{A}$$

We call ideal $\mathfrak{A}$ *zero-dimensional* is its quotient algebra A has finite dimension. The FGLM algorithm [3] builds the Gröbner basis of zero-dimensional ideal $\mathfrak{A}$ for any given (admissible) monomial ordering $<$, given the Gröbner basis for any other admissible ordering. The algorithm builds the monomial basis (*MBasis*) of the quotient algebra A, starting with the empty basis and adding monomials one-by-one, keeping three conditions:

1. Before t is added to *MBasis*, all the strict divisors of t must already be there.
2. $\forall m \in$ *MBasis*$, t \notin$ *MBasis* $: m < t$
3. The normal forms of *MBasis* monomials (w.r.t. the original Gröbner basis) should be linearly independent.

The second condition says that no linear combination of *MBasis* monomials belongs to $\mathfrak{A}$. After the algorithm ends, *MBasis* forms the monomial basis of A. For each t_i of the monomials that that respect conditions 1 and 2 but break condition 3, we have

$$f_i = t_i + \sum_{m \in \ MBasis} \lambda_m m$$

Clearly, $t_i = in(f_i)$ according to the new ordering. As shown in [3], $\mathcal{F} = \{f_i\}$ form the Gröbner basis of $\mathfrak{A}$.

3. Reduction for weak-admissible orderings

Let us consider what happens if we run FGLM algorithm on zero-dimensional ideal and weak-admissible ordering $<$. Condition 2 is reduced exactly to condition 1, so we can say that condition 1 and 3 will hold and condition 2 will disappear. Also, we are still getting $t_i = in(f_i)$ and $f_i \in \mathfrak{A}$.

MBasis does not necessary form the basis of the whole A, although it forms the basis of some subspace of A. Hence, $\mathcal{F} = \{f_i\}$ would not necessary be the basis of $\mathfrak{A}$, although the ideal generated by $\mathcal{F}$ $\langle\mathcal{F}\rangle \subset \mathfrak{A}$.

But another important property of $\mathcal{F}$ will hold, despite the change of admissible ordering into weak-admissible one: any $g \in \mathfrak{A}, g \neq 0$ is divisible by some $f_i \in \mathcal{F}$. Supposing that it is not true, g is formed by the monomials of *MBasis*, so $g \in A$, so (assuming $g \neq 0$), g can not belong to $\mathfrak{A}$. It is contradiction.

If we take some $g \in \mathfrak{A}, g \notin \langle\mathcal{F}\rangle$, it will never reduce to zero, because it does not belong to $\langle\mathcal{F}\rangle$, and it will never reduce to some polynomial from $\langle$ *MBasis*$\rangle$, because it does belong to $\mathfrak{A}$. That would be the example of polynomial reduction sequence, that goes infinite in any way.

4. An example

Let us examine the ideal given by its Gröbner base for the lexicographical ordering:

$$x^2 + y^5, xy + y^8, y^9 + y^6.$$

One of the "pseudo-bases" obtained by our computation is

$$\mathcal{F} = \{f_1 = x^3 + x^2y, f_2 = xy^2 + x^2y, f_3 = y^5 + x^2\}.$$

Clearly, $\mathcal{F}$ is not marked coherently (if it was, we would have considered $x > y$ from f_1, but $y > x$ from f_2). The Gröbner basis of $\langle\mathcal{F}\rangle$ for the lexicographical ordering is

$$x^2 + y^5, xy^2 - y^6, y^9 + y^6,$$

which is different from the initial Gröbner basis. It can be easily seen that $g = xy + y^8$ does not belong to $\langle\mathcal{F}\rangle$, so the reduction of g modulo $\mathcal{F}$ will go infinite, regardless of which exactly $f_i \in \mathcal{F}$ will be selected on each step of the reduction. So, the relation $\to_{\mathcal{F}}$ is "strongly" non-Noetherian.

Usually, *MBasis* generate the whole A, so our "pseudo-bases" are regular bases (not necessary Gröbner bases). The examples of such "strongly non-Noetherian" bases are rare, but can be easily found by our specialized software for combinatorics of monomial orders. Also, zero-dimensional ideals have not specific relation to strongly non-Noetherian bases, and such bases could be found in ideals of any dimension. However, our program is currently limited to zero-dimensional ideals.

Литература

1. A. Reeves, B. Sturmfels, *A note on polynomial reduction.* — J. Symb. Comput. **16** (1993), 273–277.
2. D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Third Edition (2007), Springer.
3. J. C. Faugère, P. Gianni, D. Lazard, T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering.* — J. Symb. Comput. **16**, No. 4 (1993), 329–344.

St.Petersburg Department
of Steklov Institute of Mathematics,
27 Fontanki emb.,
191011 St.Petersburg, Russia
E-mail: vasiliev@pdmi.ras.ru

Поступило 30 ноября 2009 г.

St.Petersburg State Polytechical University,
Polytechnicheskaya 29,
195251 St.Petersburg, Russia
E-mail: dmitry.pavlov@gmail.com