объединенный
институт
ядерных
исследований
дубна

E5-94-49

V.P.Gerdt, N.V.Khutornoy, A.Yu.Zharkov*

IMPLEMENTATION OF ZERO-DIMENSIONAL GRÖBNER BASES TRANSFORMATION FROM ONE ORDER INTO ANOTHER

Submitted to the Conference "New Computer Technologies in Control Systems" (Pereslavl-Zalessky, Russia, July 11-15, 1994)

* Saratov University, Astrakhanskaya 83, Saratov, Russia

1994

Гердт В.П., Хуторной Н.В., Жарков А.Ю. E5-94-49
Реализация алгоритма преобразования базисов Гребнера
из одного упорядочения в другое

В данной работе описан новый модуль программного пакета ASYS, написанного на языке аналитических вычислений REDUCE и предназначенного для исследования систем нелинейных алгебраических уравнений. Этот модуль выполняет преобразование базиса Гребнера нульмерного идеала в другой базис Гребнера, определяемый другим упорядочением мономов. Такое преобразование особенно полезно на практике для решения систем полиномиальных уравнений. Для ряда примеров приведены времена счета в сравнении со стандартным пакетом GROEBNER, встроенным в систему REDUCE.

Работа выполнена в Лаборатории вычислительной техники и автоматизации ОИЯИ.

Препринт Объединенного института ядерных исследований. Дубна, 1994

Gerdt V.P., Khutornoy N.V., Zharkov A.Yu. E5-94-49
Implementation of Zero-Dimensional Gröbner Bases
Transformation from One Order into Another

In this paper a new module in the REDUCE package ASYS has been designed for analysis of nonlinear algebraic equations is described. This module performs the transformation of a Gröbner basis of zero-dimensional polynomial ideal into any other Gröbner basis specified by change of monomial ordering. Such a transformation is especially useful in practice for solving polynomial equation systems. The timings for a number of examples are given in comparison with the transformation module of the REDUCE standard package GROEBNER.

The investigation has been performed at the Laboratory of Computing Techniques and Automation, JINR.

Preprint of the Joint Institute for Nuclear Research. Dubna, 1994

1 Introduction

In [1] a new version of the special-purpose computer algebra package ASYS for analysis of multivariate polynomial systems by the Gröbner basis technique [2] was described. The package has two built-in term orders: lexicographical and degree-reverse-lexicographical. The former order is the most important for the root computation. However, the complexity of the lexicographical Gröbner basis construction is much higher than of one in degree-reverse-lexicographical order. So, in zero-dimensional case (finitely many solutions) the complexity are d^{n^2} and d^n respectively, where d is a degree and n is a number of variables in the system.

Recently the most optimal strategy of the lexicographical Gröbner basis computation for zero-dimensional ideals was proposed in [3]. The basic idea is to compute the degree-reverse-lexicographical basis and than to convert it into the lexicographical one by the algorithmic method incorporating linear algebra technique. The complexity of the converting procedure is d^n. Hence, one can compute lexicographical bases with the same asymptotic complexity as total degree ones.

The method of paper [3] has been implemented in computer algebra system REDUCE [4] as a part of the GROEBNER package [5] included in the system. In this paper we present a version of the algorithm [3] implemented in the form of a module of ASYS [1]. This very recent implementation allowed us to construct lexicographical bases which could not be computed neither with ASYS nor with GROEBNER using the straightforward computational procedure. Some of such large examples are presented below.

2 Algorithm

In this section we present the detailed version of the algorithm of paper [3] which has been implemented in ASYS.

Let $K[x_1, \ldots, x_n]$ be a ring of polynomials in n variables over the field K, and I be a zero-dimensional ideal in $K[x_1, \ldots, x_n]$. Let $<_1, <_2$ be two different admissible term orderings and G be a Gröbner basis of I w.r.t. $<_1$. The problem is to find a reduced Gröbner basis H of ideal I w.r.t. $<_2$.

The mathematical foundation and general description of the algorithm for solving this problem was proposed in [3]. Here we present the stepwise form of that algorithm.

1. Let $H := \emptyset,\ S := \emptyset,\ L := \{1\},\ k := 0.$

2. If $L = \emptyset$ then return H.

3. Let u be the minimal (w.r.t. $<_2$) monomial in L. Remove u from L.

4. If u is a multiplé of some element in S, then go to Step 2.

5. Compute the polynomial $p := NF(u,G)$, where $NF(u,G)$ is the normal form of u modulo G w.r.t. $<_1$.

6. Check whether the linear relation holds

$$p + \sum_{i=1}^{k-1} \lambda_i p_i = 0,\ \lambda_i \in K \qquad (1)$$

where p_i are the normal forms of monomials m_i have been earlier considered at Step 5.

7. If relation (1) holds, then add the polynomial $u + \sum_{i=1}^{k-1} \lambda_i m_i$ to H, then add u to S and go to Step 2.

8. If relation (1) does not hold then put $k := k+1$, $m_k := u$, $p_k := p$, add all the products $u \cdot x_i$ $(i = 1, \ldots, n)$ to L and go to Step 2.

The correctness of the algorithm was proved in [3]. There it was also shown that the running cost of the algorithm is $O(nD^3)$ field operations, where n is a number of variables and D is a number of roots of ideal I counting their multiplicities.

The key point of the algorithm is verification of (1). Considering λ_i in (1) as unknowns and collecting the like terms we obtain the overdetermined system of linear algebraic equations in λ_i. Hence, the problem is reduced to investigating the compatibility and solving the system. This direct approach based on solving the linear system has been implemented in the standard package GROEBNER [5] has, however, the practical complexity at least $O(D^4)$ instead of the theoretical one $O(nD^3)$. Indeed, it is easy to see that solving a linear system in k unknowns of Step 5 needs $O(k^3)$ operations with k running from 1 to at least D.

In this paper we propose much more efficient implementation of the FGLM algorithm. The idea is to introduce an auxiliary "triangular" polynomial basis F. In addition to polynomial p we compute the polynomial $p' = NF'(p,F)$, where $NF'(p,F)$ is the reduced form of p modulo F w.r.t. $<_1$, such that the reductions of p are performed only multiplying elements of F by elements of K but not by power products as in usual computation of the normal form.

In this way one obtains the representation

$$p' = p - \sum_i \alpha_i f_i, \qquad (2)$$

where $\alpha_i \in K$ and $lt(p') <_1 lt(f_i)$ for all i[1].

[1] Here and below we denote $lt(p)$ and $lc(p)$ the leading monomial and the leading coefficient of p w.r.t. $<_1$, respectively.

If $p' \neq 0$ we go to Step 7, assign p' to the variable f_k where index k corresponds to the loop variable in the above algorithm.

This process guarantees that at each step of the algorithm the set $F = \{f_1, f_2, \ldots, f_k\}$ has the "triangular" structure:

$$lt(f_i) \neq lt(f_j),\ i \neq j$$

It follows that condition (2) and the equality $NF'(p,F) = 0$ are equivalent. Storing the coefficients α_i in representation (2) at each computation of NF' allows one to determine λ_i in (1) by recurrent relations rather than by solving linear algebraic systems.

Taking all that into account the algorithm for a Gröbner basis conversion can be presented in the following structured form

Algorithm: $H = FGLM(G)$.

Input: $<_1, <_2$ – admissible term orderings,
G– Gröbner basis for zero-dimensional ideal $I \subset K[x_1, \ldots, x_n]$ w.r.t $<_1$.

Output: H– reduced Gröbner basis of ideal I w.r.t. $<_2$.

```
$H := \emptyset$; $F := \emptyset$; $S := \emptyset$; $L := \{1\}$; $k := 0$;
while $L \neq \emptyset$ do
    $u :=$ a minimal element of $L$ w.r.t. $<_2$
    $L := L \setminus \{u\}$;
    if $u$ is not a multiple of any element of $S$ then
        $p := NF(u,G)$;
        $p' := NF'(p,F) \equiv p - \sum_{i=1}^{k-1} \alpha_i f_i$
        if $p' \neq 0$ then
            $k := k+1$; $f_k := p'/lc(p')$; $F := F \cup \{f_k\}$;
            $m_k := u$; $p_k := p$; $\beta_{kk} := 1/lc(p')$;
            for $i := 1 : k-1$ do $\beta_{ki} := -\beta_{kk} \sum_{j=i}^{k-1} \alpha_i \beta_{ji}$;
            for $i := 1 : n$ do $L := L \cup \{u \cdot x_i\}$;
        else
            $H := H \cup \{u - \sum_{i=1}^{k-1} (\sum_{j=i}^{k-1} \alpha_j \beta_{ji}) \cdot m_i\}$;
            $S := S \cup \{u\}$;
```

3 Examples

In this section a number zero-dimensional polynomial systems which are well-known as benchmarks for Gröbner bases software [1],[3],[6] are considered as illustrations.

Example 1

Ordering - $a > b > c$.

$$\begin{aligned}&a^2bc + ab^2c + abc^2 + abc + ab + ac + bc = 0,\\&a^2b^2c + ab^2c^2 + a^2bc + abc + bc + a + c = 0,\\&a^2b^2c^2 + a^2b^2c + ab^2c + abc + ac + c + 1 = 0.\end{aligned}$$

Example 2

Ordering - $x > y > z$.

$$\begin{aligned}&x^3 + y^2 + z - 3 = 0,\\&y^3 + z^2 + x - 3 = 0,\\&z^3 + x^2 + y - 3 = 0.\end{aligned}$$

Example 3

Ordering - $x > y > z > t$.

$$\begin{aligned}&y^2z + 2xyt - 2x - z = 0,\\&-x^3z + 4xy^2z + 4x^2yt + 2y^3t + 4x^2 - 10y^2 + 4xz - 10yt + 2 = 0,\\&2yzt + xt^2 - x - 2z = 0,\\&-xz^3 + 4yz^2t + 4xzt^2 + 2yt^3 + 4xz + 4z^2 - 10yt - 10t^2 + 2 = 0.\end{aligned}$$

Example 4

Ordering - $x_1 > x_2 > x_3 > x_4 > x_5$.

$$\begin{aligned}&x_1 + x_2 + x_3 + x_4 + x_5 = 0,\\&x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 = 0,\\&x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2 = 0,\\&x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_1 + x_4x_5x_1x_2 + x_5x_1x_2x_3 = 0,\\&x_1x_2x_3x_4x_5 - 1 = 0.\end{aligned}$$

Example 5

Ordering - $x_5 > x_4 > x_3 > x_6 > x_2 > x_1$.

$$\begin{aligned}&x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 0,\\&x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_1 = 0,\\&x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_6 + x_5x_6x_4 + x_6x_1x_2 = 0,\\&x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_6 + x_4x_5x_6x_1 + x_5x_6x_1x_2 + x_6x_1x_2x_3 = 0,\\&x_1x_2x_3x_4x_5 + x_2x_3x_4x_5x_6 + x_3x_4x_5x_6x_1 + x_4x_5x_6x_1x_2 +\\&x_5x_6x_1x_2x_3 + x_6x_1x_2x_3x_4 = 0,\\&x_1x_2x_3x_4x_5x_6 - 1 = 0.\end{aligned}$$

Example 6

Ordering - $u_5 > u_3 > u_4 > u_2 > u_1 > u_0$.

$$\begin{aligned}&u_0^2 - u_0 + 2u_1^2 + 2u_2^2 + 2u_3^2 + 2u_4^2 + 2u_5^2 = 0,\\&2u_0u_1 + 2u_1u_2 + 2u_2u_3 + 2u_3u_4 + 2u_4u_5 - u_1 = 0,\\&2u_0u_2 + u_1^2 + 2u_1u_3 + 2u_2u_4 + 2u_3u_5 - u_2 = 0,\\&2u_0u_3 + 2u_1u_2 + 2u_1u_4 + 2u_2u_5 - u_3 = 0,\\&2u_0u_4 + 2u_1u_3 + 2u_1u_5 + u_2^2 - u_4 = 0,\\&u_0 + 2u_1 + 2u_2 + 2u_3 + 2u_4 + 2u_5 - 1 = 0.\end{aligned}$$

Example 7

Ordering - $x_3 > x_1 > x_2 > x_4 > x_5$.

$$\begin{aligned}&x_1 + x_2 + x_3 + x_4 + x_5 = 0,\\&x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 = 0,\\&x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2 = 0,\\&x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_1 + x_4x_5x_1x_2 + x_5x_1x_2x_3 = 0,\\&x_1x_2x_3x_4x_5 - 1 = 0.\end{aligned}$$

In Table 1 we give the timings for the above examples on SPARC station *IPX* with the 32 Mb memory.

Table 1

	ASYS	GROEBNER
Example 1	4.0"	28.6"
Example 2	8.9"	69.5"
Example 3	7.7"	57.4"
Example 4	10.6"	66.9"
Example 5	58"	6112"
Example 6	1693"	11295"
Example 7	4176"	26796"

Acknowledgements. This research was supported in part by the Russian Foundation for Fundamental Research (Project 93-02-14428).

References

[1] V.P.Gerdt, N.V.Khutornoy, A.Yu.Zharkov ASYS2: A New Version of Computer Algebra Package ASYS for Analysis and Simplification of Polynomial Systems. Preprint JINR E11-93-468, Dubna, 1993.

[2] Buchberger B. Gröbner bases: an Algorithmic Method in Polynomial Ideal Theory. In: (Bose N.K., ed.) Recent Trends in Multidimensional System Theory, Reindel, 1985, 184-232.

[3] J.C.Faugere, P.Gianni, D.Lazard, T.Mora Efficient computation of zero-dimensional Gröbner bases by change of ordering. Technical Report LITP 89-52, 1989.

[4] Hearn A.C. REDUCE User's Manual. Version 3.5 Konrad-Zuse-Zentrum, Berlin, 1993.

[5] Melenk H., Möller H.M., Neun W. GROEBNER: A Package for Calculating Groebner Bases, Nov.1995. Available through the REDUCE library e.g. at `redlib@rand.org`

[6] Boege W., Gebauer R., Kredel H. Some Examples for Solving Systems of Algebraic Equations by Calculating Gröbner Bases, J. Symb. Comp., 1986, v.2, 83-98.

Received by Publishing Department
on February 21, 1994.