сообщения
объединенного
института
ядерных
исследований
дубна

E5-94-318

A.Yu.Zharkov, Yu.A.Blinkov

INVOLUTIVE BASES OF ZERO-DIMENSIONAL IDEALS

1994

1 Introduction

In this paper we propose a new algorithm for solving systems of polynomial equations in the zero-dimensional case (finite number of solutions). Our work has its origins in the constructive theory of partial differential equations, going back to the pioneering works of Riquier [1] and Janet [2] and developed in [3] in a modern way. This theory may be applied as well to polynomial systems taking into account the formal correspondence between polynomials and linear homogeneous PDE with constant coefficients and one unknown function. That is, unknown function in the differential case corresponds to unity in the algebraic case, differentiation - to multiplication by variable and other operations are left unchanged. E.g., differential expression $u_{xxy} - 2u_z + 3u$ corresponds to polynomial $x^2y - 2z + 3$.

Our method is based on the construction of involutive basis of polynomial ideal which is a special form of non-reduced Gröbner basis (see [4]). In this paper we give an improved version of algorithm for constructing involutive bases and prove its correctness in the zero-dimensional case. Unlike Buchberger's algorithm [5], our algorithm uses prolongations (i.e. multiplications by variables) instead of S-polynomials and it is arranged so that the degrees of intermediate polynomials do not increase more than it is necessary to obtain an answer. Another point is that we have no need to do all possible reductions in the system, but only the so-called "Janet reductions". The algorithm is implemented in the form of REDUCE package INVSYS. The results of comparison between INVSYS and the standard REDUCE package GROEBNER show that the computation of involutive bases using our algorithm may be performed faster (at least, for the total-degree orderings) than the computation of reduced Gröbner bases by means of Buchberger's algorithm. Furthermore, it turns out that the roots of zero-dimensional ideals come easily from involutive bases computed in the total-degree orderings. We show that to obtain the roots one needs only linear algebra algorithms.

2 Involutive Systems

In this section we present the basic concepts and results of the involution approach to investigating polynomial systems [4]. Throughout, we shall use the notations:

$K-$ arbitrary zero characteristic field;
$a, b-$ elements of K;
$K[x_1, \ldots, x_n]-$ polynomial ring over K;
$f, g, h, p-$ polynomials from $K[x_1, \ldots, x_n]$;
$F, G, H, P-$ finite subsets in $K[x_1, \ldots, x_n]$;
$u, v, w, s-$ terms in polynomials (without coefficients from K);
$deg(u)-$ total degree of u;
$cf(f, u)-$ coefficient of u in f;
$Ideal(F)-$ ideal generated by F.

Let variables x_i be ordered as $x_1 < \ldots < x_n$ and fix some admissible term ordering

$<_T$. Denote
$lt(f)$– leading term in f w.r.t. $<_T$;
$lc(f) = cf(f, lt(f))$;
$lt(F) = \{lt(f) \mid f \in F\}$;
$deg(F) = max\{deg(lt(f)) \mid f \in F\}$.

Definition 1 [3]. Variable x_i is *multiplicative* for the term u if its index i is not greater than the index of the lowest variable in u. Otherwise x_i is *non-multiplicative* for u

For a given polynomial g denote by $Nonmult(g)$ a set of non-multiplicative variables for $lt(g)$.

Definition 2. *Class of a term* is the index of its lowest variable. *Class of a polynomial* is the class of its leading term.

Denote $u \cdot v$ by $u \times v$ if all variables in v are multiplicative for u or if $deg(v) = 0$. Write also $g \cdot u = g \times u$ if $lt(g) \cdot u = lt(g) \times u$.

Definition 3. Term u is called a *Janet divisor* for the term w if there exists a term v such that $w = u \times v$ (symbolically $u \mid_J w$).

The following properties of Janet divisors are obvious.
1. If $u \mid_J v$ and $v \mid_J w$ then $u \mid_J w$ *(transitivity)*.
2. If $u \mid_J w$ and $v \mid_J w$ then $u \mid_J v$ or $v \mid_J u$.
3. If $\neg(u \mid_J v)$ then $\forall_{w,s} \neg(u \times w \mid_J v \times s)$.

Definition 4. Polynomial f *reduces to* h *modulo* G *in the sense of Janet* if there exist $g \in G$ and u such that $lt(g) \cdot u \equiv lt(g) \times u$, $a \equiv cf(f, lt(g) \times u) \neq 0$ and $h = f - a \cdot g \times u$. Polynomial f is given in *Janet normal form* modulo G if for each term in f there are no Janet divisors in $lt(G)$. Polynomial h is a *Janet reduced form* of f modulo G (symbolically $h = NF_J(f, G)$) if there exists a chain of Janet reductions from f to h and h is given in Janet normal form modulo G.

In contrast to Janet normal form we denote by $NF(f, G)$ a usual normal form of f modulo G. An algorithm for computing NF_J may be obtained from one for computing NF [5] replacing usual division of terms by Janet division.

Example 1. $G = \{xy\}$, $f = x^2y + xy^2$, $x > y$. $NF_J(f, G) = x^2y \neq NF(f, G) = 0$.

Definition 5. G is *autoreduced* (in the sense of Janet) if $\forall_{g,g' \in G, g \neq g'} \neg(lt(g) \mid_J lt(g'))$. G is *completely autoreduced* if $\forall_{g \in G} NF_J(g, G \setminus \{g\}) = g$

Proposition 1. If G is autoreduced then for any u there exists no more than one Janet divisor in $lt(G)$.

Proof. This is immediate from definition 5 and property 2 of Janet divisors. □

Denote by $Autoreduce(F)$ a function that for given F computes G which is autoreduced and $Ideal(F) = Ideal(G)$. An algorithm for computing $Autoreduce$ may be obtained from the well-known algorithm *ReduceAll* [5] replacing usual NF by NF_J.

Denote by $M(G)$ a set of finite sums

$$M(G) = \{\sum_{ij} a_{ij} g_i \times u_{ij} \mid g_i \in G\}.$$

The following properties are obvious.

1. $\forall_{f,h \in M(G)} (f \pm h) \in M(G)$.
2. $h = NF_J(f, G) \rightarrow (f - h) \in M(G)$.

Theorem 1 [4]. If G is autoreduced and $f \in M(G)$ then $NF_J(f, G) = 0$ for any sequence of Janet reductions. □

Theorem 2 [4]. *(Uniqueness of Janet normal form).* If G is autoreduced and h_1, h_2 are Janet normal forms of f modulo G then $h_1 = h_2$. □.

Theorem 3 [4]. *(Linearity of Janet normal form).* If G is autoreduced then

$$\forall_{f,h,a,b} NF_J(a \cdot f + b \cdot h, G) = a \cdot NF_J(f, G) + b \cdot NF_J(h, G). \ □$$

Definition 6. *Prolongation* of polynomial g by variable x is a product $g \cdot x$. If $x \in Nonmult(g)$ then the prolongation is called *non-multiplicative*, otherwise *multiplicative*.

Definition 7 [3, 4]. G is *involutive system* if it is autoreduced and

$$\forall_{g \in G} \forall_{x \in Nonmult(g)} NF_J(g \cdot x, G) = 0 \qquad (1)$$

Note that involution conditions (1) are non-trivial because any non-multiplicative prolongation $g \cdot x$ does not reduce to zero in the sense of Janet by means of g.

Theorem 4 [4]. If G is involutive, then $\forall_{f \in Ideal(G)} NF_J(f, G) = 0$. □

Corollary 1 [4]. Any involutive system is a Gröbner basis (generally redundant). □

Definition 8. G is *normalized* if $lc(g) = 1$ for all $g \in G$.

Definition 9. G is *involutive basis* of $Ideal(G)$ if it is involutive and normalized.

Theorem 5. *(Uniqueness of involutive basis).* If G, H are involutive bases and $Ideal(G) = Ideal(H) = I$ then $lt(G) = lt(H)$. Furthermore, if G, H are completely autoreduced then $G = H$.

Proof. We assume that $lt(G) \neq lt(H)$ and force a contradiction. Let there exists $g \in G$ such that $lt(g) \neq lt(h)$ for all $h \in H$. Since $g \in I$ and because of theorem 4, $NF_J(g, H) = 0$. Hence there exists $h' \in H$ such that $lt(h') \mid_J lt(g)$ and, by our assumption, $lt(h') \neq lt(g)$. On the other hand, $h' \in I$, hence $NF_J(h', G) = 0$ and there exists $g' \in G$ such that $lt(g') \mid_J lt(h')$. By the transitivity of Janet divisors, $lt(g') \mid_J lt(g)$. Furthermore $lt(g') \neq lt(g)$, since $lt(g') \mid_J lt(h')$ and $lt(h') \neq lt(g)$. This contradicts the fact that G is autoreduced. Hence $lt(G) = lt(H)$.

Let G, H be completely autoreduced. We must prove that $G = H$. Assume that there exist $g \in G$, $h \in H$ such that $lt(g) = lt(h)$ but $g \neq h$. Consider $f = g - h$. Since $lc(g) = lc(h) = 1$ and G, H are completely autoreduced, $lt(f)$ has no Janet divisor in $lt(G)$. On the other hand, $f \in I$, hence $NF_J(f, G) = 0$ and $lt(f)$ must have Janet divisor in $lt(G)$. The obtained contradiction proves that $G = H$. □

One may observe that involutive basis (in the sense of (1)) exists not for any polynomial ideal. E.g., for ideal generated by a single polynomial f involutive basis exists if and only if $lt(f)$ is a power of the leading variable. In the next section we prove that any zero-dimensional ideal possesses an involutive basis and propose an algorithm for computing it.

3 Algorithm Description

Throughout this section by $<_T$ is meant any admissible *total degree* term ordering. Below, the notion of complete polynomial system is introduced and algorithm *Complete* for constructing such system is given together with the proof of its correctness. We use *Complete* as a subalgorithm in algorithm *Invbase* intended for computing involutive bases. Then we prove the correctness of algorithm *Invbase* for zero-dimensional ideals.

Definition 10. G is *complete* if it is autoreduced, normalized and

$$\forall_{g \in G} \forall_{x \in Nonmult(g)} \; deg(lt(g) \cdot x) \leq deg(G) \rightarrow NF_J(g \cdot x, G) = 0 \qquad (2)$$

Theorem 6. Let G be complete. Then

$$\forall_{g \in G} \forall_u \; deg(lt(g) \cdot u) \leq deg(G) \rightarrow NF_J(g \cdot u, G) = 0 \qquad (3)$$

Proof. Let g be a polynomial from G, u be an arbitrary term such that conditions $deg(lt(g) \cdot u) \leq deg(G)$ are satisfied. If $u \neq 1$ we may represent $g \cdot u$ as $v \cdot (g \times w)$ where $v \cdot w = u$, all variables in v are non-multiplicative and all variables in w are multiplicative for g. Fix some variable x in v and write $g \cdot u = v_1 x (g \times w)$ where $v_1 = v/x$. Because of (2),

$$x \cdot g = g_1 \times s_1 + \sum_{k,l} a_{kl} g_k \times s_{kl}$$

where $g_i \in G$, $a_{kl} \in K$ and g_1 is such that $lt(g_1) \times s_1 = x \cdot lt(g)$. By proposition 1, g_1 is defined uniquely. From the algorithm of Janet normal form it follows that $max\,\{lt(g_k) \times s_{kl}\} <_T lt(g_1) \times s_1$ where by max is meant the maximal term w.r.t. $<_T$. Substituting $g \cdot x$ into the equality $g \cdot u = v_1 x (g \times w)$ we have

$$g \cdot u = v_1 \cdot (g_1 \times w_1) + \sum_{k,l} a_{kl} g_k \cdot u_{kl}$$

where $w_1 = s_1 \cdot w$ and, by admissibility of the ordering $<_T$, $max\,\{lt(g_k) \cdot u_{kl}\} <_T lt(g) \cdot u$. It is obvious that $deg(lt(g_1) \cdot v_1) \leq deg(G)$. Consequently, if $v_1 \neq 1$, we may repeat the

same process for $g_1 \cdot v_1$. Then, taking into account that $deg(v_1) < deg(v)$ and acting recursively, we obtain after a finite number of steps

$$g \cdot u = g_1' \times w_1' + \sum_{k,l} a_{kl}' g_k' \cdot u_{kl}'$$

where $g_i' \in G$, $a_{kl}' \in K$, $lt(g_1') \times w_1' = lt(g) \cdot u$ and $max\,\{lt(g_k') \cdot u_{kl}'\} <_T lt(g) \cdot u$. Repeating the same process for each item in the right hand side of the last equation and taking into account the fact that the ordering $<_T$ is noetherian, we obtain after finite number of steps

$$g \cdot u = \sum_{i,j} \tilde{a}_{ij} \tilde{g}_i \times \tilde{w}_{ij}$$

where $\tilde{g}_i \in G$, $\tilde{a}_{ij} \in K$. Hence, $g \cdot u \in M(G)$ and, by theorem 1, $NF_J(g \cdot u, G) = 0$. □

The following algorithm for given F computes an equivalent complete system G

Algorithm 1 ($G = Complete(F)$).
Input: F
Output: G - complete system such that $Ideal(G) = Ideal(F)$
$G := Autoreduce(F)$;
while exist $g \in G$, $x \in Nonmult(g)$
  such that $deg(lt(g) \cdot x)) \leq deg(G)$ **and** $h \equiv NF_J(g \cdot x, G) \neq 0$ **do**
    $G := Autoreduce(G \cup \{h\})$;

To prove the correctness of algorithm 1 we need the following technical lemma.

Lemma 1. Let S be an arbitrary finite set. Any infinite sequence $\{S_i\}$ of subsets $S_i \subseteq S$, satisfying the condition $\forall_{i,k>i} (S_i \setminus S_{i+1}) \cap S_k = \emptyset$, has equal neighbour elements, i.e. there exists m such that $S_m = S_{m+1}$.

Proof. Obvious. □

Proof of the correctness of algorithm 1. Assume that algorithm 1 does not terminate. Let G_i be G computed at the i-th step of algorithm 1. By transitivity of Janet division, if some $g \in G_i$ reduces, then $lt(g)$ does not occur in $lt(G_k)$ for all $k > i$. Furthermore, $deg(G_i) \leq deg(F)$ for all $i = 1, 2, 3, \ldots$. Taking into account that the total-degree ordering is sequential (each term has only finitely many predecessors), we conclude that $lt(G_i)$ satisfies the conditions of lemma 1. Hence, there exists the number m such that $lt(G_m) = lt(G_{m+1})$. Let us show that G_m is complete. If it is not so, then there exist $g \in G_m$, $x \in Nonmult(g)$ such that $deg(lt(g \cdot x)) \leq deg(G_m)$ and $h \equiv NF_J(g \cdot x, G_m) \neq 0$. Since $lt(h)$ has no Janet divisors in $lt(G_m)$, it generates an element in $lt(G_{m+1})$ which differs from each element of $lt(G_m)$. But this contradicts the fact that $lt(G_m) = lt(G_{m+1})$. Hence G_m is complete and algorithm 1 terminates after computing G_m. □

Now we present algorithm *Invbase* which uses *Complete* as a subalgorithm and computes an involutive basis of *Ideal(F)* for given system F.

Algorithm 2 ($G = Invbase(F)$).
Input: F
Output: G - involutive basis of $Ideal(F)$
$G := Complete(F)$;
while exist $g \in G$, $x \in Nonmult(g)$
 such that $deg(lt(g) \cdot x)) > deg(G)$ **and** $h \equiv NF_J(g \cdot x, G) \neq 0$ **do**
  $G := Complete(G \cup \{h\})$;

We shall prove that algorithm 2 is correct in the zero-dimensional case. We use the following lemma.

Lemma 2. Let G_i be a system G computed at the i-th step of algorithm 2. If there exists the number q such that $deg(G_i) < q$ for all $i = 1, 2, 3, \ldots$, then algorithm 2 terminates.

Proof. Completely analogous to the proof of the correctness of algorithm 1. □

Theorem 7. Let F have finite number of solutions, i.e. dimension of $Ideal(F)$ is zero. Then involutive basis of $Ideal(F)$ exists and may be computed by a finite number of steps of algorithm 2.

Proof. Assume that algorithm 2 does not terminate and force a contradiction. Let G_i be a system G computed at the i-th step of algorithm 2. From the algorithm of Janet normal form it follows that for all i each f from the initial system F may be expressed as $f = \sum_j g_j \cdot p_j$ where $g_j \in G_i$, $p_j \in K[x_1, \ldots, x_n]$ and $deg(lt(g_j) \cdot lt(p_j)) \leq deg(lt(f))$. From theorems 3,6 and lemma 2 it follows that for each $p \in Ideal(F)$ there exists i such that $NF_J(p, G_i) = 0$. According to [5], if dimension of $Ideal(F)$ is zero, then for each $k = 1, \ldots, n$ there exists $p_k \in Ideal(F)$ such that $lt(p_k) = x_k^{d_k}$, $d_k \geq 1$. Let p_k be such elements of $Ideal(F)$ with minimal d_k. For each $k = 1, 2, \ldots, n$ denote by U_k a finite set of terms of the form $x_n^{l_n} \ldots x_k^{l_k}$ satisfying the conditions $l_j < d_j$. By lemma 2, there exists the number m such that $NF_J(p_k \cdot u, G_m) = 0$ for each k and for each $u \in U_{k+1}$. It is easy to observe that any term of the class k which is not contained in U_k has Janet divisor in $lt(G_m)$. Hence, for all $i > m$, $deg(G_i)$ has an upper bound $d_n + \ldots + d_1 - n + 1$ and, by lemma 2, algorithm 2 terminates. It means that the last **while**-condition fails, hence, as the last G is complete, it is nothing else but an involutive basis. □

Corollary 2. Let G be an involutive basis of zero-dimensional ideal. Then for each $k = 1, \ldots, n$ there exists $g \in G$ such that $lt(g) = x_k^{d_k}$. Furthermore, each term u such that $deg(u) \geq deg(G)$ has a Janet divisor in $lt(G)$. □

Example 2. Let $x > y > z$ and $F = \{x^3+y^2+z-3,\ y^3+z^2+x-3,\ z^3+x^2+y-3\}$. Dimesion of $Ideal(F)$ is zero. Applying algorithm 2, we obtain the following involutive basis G of $Ideal(F)$ in the degree reverse lexicographical ordering

$$
\begin{aligned}
G = \{ \quad & x^2y^2z^3 - 3x^2y^2 - xy^2z - x^2z^2 + xyz^2 + \\
& x^2y + 3xy^2 + 3x^2 - 3xy + y^2 + z - 3, \\
& x^2yz^3 + x^2y^2 - 3x^2y - xyz + xz^2 + x^2 + 3xy - 3x, \\
& xy^2z^3 - 3xy^2 - y^2z - xz^2 + yz^2 - x^2 + xy + 3y^2 + 3x - 3y, \\
& x^2y^3 + x^2z^2 - 3x^2 - y^2 - z + 3, \\
& x^2z^3 + x^2y - xy^2 - 3x^2 - xz + 3x, \\
& xyz^3 + xy^2 - 3xy - yz + z^2 + x + 3y - 3, \\
& y^2z^3 + x^2y^2 - 3y^2 - z^2 - x + 3, \\
& xy^3 + xz^2 + x^2 - 3x, \\
& xz^3 + xy - y^2 - 3x - z + 3, \\
& yz^3 + x^2y + y^2 - 3y, \\
& x^3 + y^2 + z - 3, \\
& y^3 + z^2 + x - 3, \\
& z^3 + x^2 + y - 3 \quad \}.
\end{aligned}
$$

Remark 1. As for positive-dimensional ideals, there exist "sufficiently regular" systems for which algorithm 2 terminates with desirable result and "irregular" ones for which it does not terminate. It turns out (see [3]) that the irregular systems becomes regular after the *most* linear changes of variables. However, the preliminary change of variables may be considered as a practical computational method only for systems of low degrees. Another possibility to generalize our approach to the positive-dimensional case is to use more sophisticated concept of multiplicative and non-multiplicative variables, as in [2]. This work is now in progress.

4 Separation of Variables

In this section we propose a method of separating variables in zero-dimensional total-degree involutive bases. We prove that only simple linear algebra is sufficient for this purpose (compare with [6]). Our method is based on the following theorem.

Theorem 8. Let G be completely autoreduced involutive basis of zero-dimensional ideal in the total-degree ordering. Let G_1 be a subset of G containing all its elements of the class 1. Then G_1 is not empty and is none other than a system of $N+1$ linear equations over $K(x_1)$ w.r.t. the terms of the form $x_n^{k_n} \ldots x_2^{k_2}$ considered as unknowns, where N is the total number of such terms in the elements of G_1. These equations are linearly independent over $K(x_1)$.

Proof. Let g_i $(i = 1, \ldots, N)$ be all elements of G_1 with leading terms $lt(g_i) = u_i \times x_1^{l_i}$, $u_i \neq 1$, class of each u_i is greater than 1. By corollary 2, G_1 contains one more element of class 1, namely g_{N+1}, such that $lt(g_{N+1}) = x_1^{l_{N+1}}$. Let us show that the set $\{u_i\}$ contains all the terms of classes > 1 which have no Janet divisors in $lt(G \setminus G_1)$. Indeed, if u is such a term and $u \neq u_i$ for all $i = 1, \ldots, N$, then the terms $u \cdot x_1^m$, where $deg(u) + m \geq deg(G)$, have no Janet divisors in $lt(G)$ that contradicts corollary 2.

Since G is completely autoreduced, all the terms contained in the elements of G_1 have the form $u_i \times x_1^k$ or x_1^l. Hence, G_1 is a system of $N+1$ linear algebraic equations w.r.t. N unknowns u_i. From proposition 1 it follows that these equations are linearly independent over $K(x_1)$. □

For a given total-degree zero-dimensional involutive basis G, considering G_1 as a linear system mentioned above and writing the compatibility condition for this system, we immediately obtain an equation in a single variable x_1. In most cases, reducing G_1 (as a linear system w.r.t. u_i) to the triangular form is sufficient to obtain the equivalent triangular form of G. The exceptions may occur when some equations of G_1 are identically equal to zero by force of the compatibility condition. In this case it is necessary to consider the elements of G of the classes ≤ 2 over $K(x_1, x_2)$ and to repeat the process recursively. As a result, we should obtain an equivalent triangular form of G, i.e. lexicographical Gröbner basis.

Example 3. Involutive basis G in example 2 contains 9 polynomials of class 1 which form a linear algebraic system over $Q(z)$ w.r.t. x^2y^2, x^2y, xy^2, x^2, xy, y^2, x, y. The compatibilty condition gives

$$z^{27} - 27z^{24} + 317z^{21} - 18z^{19} - 2067z^{18} - 50z^{17} + 279z^{16} + 8156z^{15} +$$
$$645z^{14} - 1674z^{13} - 20359z^{12} - 3044z^{11} + 4645z^{10} + 33644z^9 + 6288z^8 - 6388z^7 -$$
$$36936z^6 - 5925z^5 + 4957z^4 + 23187z^3 + 4063z^2 - 4342z - 5352 = 0.$$

Solving the linear system w.r.t. the terms x, y and eliminating other terms, we obtain two equations of the form $x + p_1(z) = 0$, $y + p_2(z) = 0$, $deg(lt(p_1)) = deg(lt(p_2)) = 26$, which give a reduced lexicographical Gröbner basis together with equation in z.

5 Examples

An improved version of algorithm 2 is implemented in the form of REDUCE package INVSYS. We present the results of comparison of INVSYS with standard REDUCE package GROEBNER [7, 8] for several examples of zero-dimensional ideals taken from the paper [6]. Note that examples (II) and (III) distinguish from each other in only one term and this leads to drastic distinction in computing time.

Example (I)

$$x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2 + x_1x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 = 0,$$
$$x_1^2x_2^2x_3 + x_1x_2^2x_3^2 + x_1^2x_2x_3 + x_1x_2x_3 + x_2x_3 + x_1 + x_3 = 0,$$
$$x_1^2x_2^2x_3^2 + x_1^2x_2^2x_3 + x_1x_2^2x_3 + x_1x_2x_3 + x_1x_3 + x_3 + 1 = 0.$$

Example (II)

$$x_1 + x_2 + x_3 + x_4 + x_5 = 0,$$

$$x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 = 0,$$
$$x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2 = 0,$$
$$x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_1 + x_4x_5x_1x_2 + x_5x_1x_2x_3 = 0,$$
$$x_1x_2x_3x_4x_5 - 1 = 0.$$

Example (III)

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

Example (IV)

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 0,$$
$$x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_1 = 0,$$
$$x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_6 + x_5x_6x_1 + x_6x_1x_2 = 0,$$
$$x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_6 + x_4x_5x_6x_1 + x_5x_6x_1x_2 + x_6x_1x_2x_3 = 0,$$
$$x_1x_2x_3x_4x_5 + x_2x_3x_4x_5x_6 + x_3x_4x_5x_6x_1 +$$
$$x_4x_5x_6x_1x_2 + x_5x_6x_1x_2x_3 + x_6x_1x_2x_3x_4 = 0,$$
$$x_1x_2x_3x_4x_5x_6 - 1 = 0.$$

All computations using INVSYS and GROEBNER have been performed for the degree reverse lexicographical term ordering on an 25 MHz MS-DOS based AT/386 computer with 8 Mb RAM. The results of comparison for different variable orderings are given in the table below. We use the notations:

- T_1 - the time for computing involutive basis using INVSYS
- T_2 - the time for computing reduced Gröbner basis using GROEBNER
- N_1 - the number of elements in involutive basis
- N_2 - the number of elements in reduced Gröbner basis

EXAMPLE, variable ordering	T_1(sec.)	T_2(sec.)	N_1	N_2
(I) $x_1 > x_2 > x_3$	16	33	15	15
(II) $x_1 > x_2 > x_3 > x_4 > x_5$	11	8	23	20
(II) $x_1 > x_2 > x_5 > x_3 > x_4$	9	7	23	20
(III) $x_1 > x_2 > x_3 > x_4 > x_5$	149	341	31	25
(III) $x_1 > x_2 > x_5 > x_3 > x_4$	1948	3050	32	24
(III) $x_4 > x_1 > x_5 > x_2 > x_3$	87	1190	32	23
(IV) $x_1 > x_2 > x_6 > x_3 > x_4 > x_5$	7657	>140000	46	-
(IV) $x_5 > x_4 > x_3 > x_6 > x_2 > x_1$	3795	77400	46	45

The results of comparison enable to hope that the method of involutive bases is a sufficiently powerful tool for solving zero-dimensional polynomial systems.

Aknowledgements. We are grateful to V.P.Gerdt and T.Mora for useful discussions.

References

[1] Riquier C.H. Les système d'équations aux deriveés partielles. Gauthier-Villars, Paris, 1910.

[2] Janet M. Lecons sur les systémes d'équations aux deriveés partielles. Gauthier-Villars, Paris, 1929.

[3] Pommaret J.F. Systems of partial differential equations and Lie pseudogroups. Gordon and Breach Science Publishers, 1978.

[4] Zharkov A.Yu., Blinkov Yu.A. Involution Approach to Solving Systems of Algebraic Equations. Proceedings of the IMACS'93, 1993, 11-16.

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

[6] Faugère J.C., Gianni P., Lazard D., Mora T. Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering, Technical Report LITP 89-52, 1989.

[7] Hearn A.C. REDUCE User's Manual. Version 3.4. The Rand Corporation, Santa Monica, 1991.

[8] Melenk H., Möller H.M., Neun W. Symbolic Solution of Large Stationary Chemical Kinetics Problems, Impact of Computing in Science and Engineering, 1989, v.1, 138-167.

Received by Publishing Department
on August 1, 1994