SOLVING ZERO-DIMENSIONAL INVOLUTIVE SYSTEMS

A.Yu.Zharkov
Saratov University, Astrakhanskaya 83, Saratov 410071, Russia
e-mail: postmaster@scnit.saratov.su

Abstract

A new method for solving zero-dimensional polynomial systems is proposed. Given a set of generators of a zero-dimensional ideal, the method computes an involutive basis of this ideal in the total-degree term ordering and then converts it to a triangular basis in the lexicographical ordering. We show that only simple linear algebra is needed for this purpose. We prove also that in most cases of zero-dimensional ideals the result of a conversion algorithm is a minimal lexicographical standard basis.

1 Introduction

In our recent paper [1], the notion of involutive bases of polynomial ideals was introduced and an algorithm for computing involutive bases was presented. The improved form of this algorithm together with the proof of its correctness in the zero-dimensional case is given in [2]. In the positive-dimensional case, a linear change of variables is generally required for constructing involutive bases defined in our sense. It turns out that when the involutive basis exists (without change of variables) it can be computed considerably faster by our algorithm than the minimal standard basis by Buchberger's algorithm [3]. On the other hand, an involutive basis computed in the total-degree term ordering often looks more complicated than the corresponding minimal standard basis. The reason is that the involutive basis of a zero-dimensional ideal is nothing but a standard basis enlarged to an "overdetermined" linear algebraic system in monomials irreducible modulo this ideal. From this fact, some interesting properties of involutive bases may be deduced and a simple method for solving zero-dimensional systems may be constructed.

In the second section of this paper we recall the notions of the Janet normal form and involutive bases of polynomial ideals. We present also a new version of algorithm *Invbase* for computing involutive bases with further improvements in comparison with that presented in [2]. In the third section we systematically investigate the structure of zero-dimensional involutive bases. In the forth section we describe the method of converting the total-degree involutive basis to the pure lexicographical reduced standard basis in case the shape lemma holds [7].

2 Involutive Bases

Throughout, we use the following notations.

$K-$ arbitrary field of characteristic zero;
$K[x_1,\dots,x_n]-$ polynomial ring over K;
$f,g,h-$ polynomials from $K[x_1,\dots,x_n]$;
$F,G,H-$ finite subsets in $K[x_1,\dots,x_n]$;
$card(F)-$ number of elements (cardinality) of F;
$u,v,w-$ terms in polynomials (without coefficients from K);
$deg(u,x_i)-$ degree of u in variable x_i;
$deg(u)-$ total degree of u;
$cf(f,u)-$ coefficient of u in f;
$(F)-$ ideal generated by F.

Let variables x_i be ordered as $x_1 < \ldots < x_n$ and let $<_T$ be some admissible term ordering. 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. 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. The *class of a term* u (symbolically $class(u)$) is the index of the lowest variable contained in u with a non-zero power. The class of a unit term (containing all variables in zero powers) is defined to be $n+1$, where n is the number of variables. The *class of a polynomial* g (symbolically $class(g)$) is the class of $lt(g)$.

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

Definition 4. The 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 $h = f - a \cdot g \times u$. The polynomial f is given in *Janet normal form* modulo G if for each term in f there are no Janet divisors in $lt(G)$.The 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 [3] replacing usual division of terms by Janet division.

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 $\forall_{g \in G} NF_J(g, G \setminus \{g\}) = g$

Denote by $Autoreduce(F)$ a function that for a given F computes G which is autoreduced and $(F) = (G)$. An algorithm for computing $Autoreduce$ may be obtained from the well-known algorithm *ReduceAll* [3] replacing usual NF by NF_J.

Definition 6 [1]. G is an *involutive basis* if it is autoreduced and

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

Some general properties of the involutive bases established in [1, 2] are summarized below.

Properties of involutive bases [1, 2].

- If G is involutive then $\forall_{f \in (G)} NF_J(f, G) = 0$.
- If G is involutive then $\forall_h NF_J(h, G) = NF(h, G)$.
- Any involutive basis is a standard basis, generally not minimal.
- Let G be an involutive basis and G_{min} be a minimal standard basis of (G). Then, for each term u there exist $g \in G$ such that $lt(g) \mid_J u$ if and only if there exist $g' \in G_{min}$ such that $lt(g') \mid u$.
- If G, H are involutive bases and $(G) = (H)$ then $lt(G) = lt(H)$. Moreover, if G, H are completely autoreduced then $G = H$ up to multiplication of polynomials by non-zero elements of K.
- If G is involutive then for each $g \in G$ and for each term u such that $u \mid_J lt(g)$ and $class(u) > class(g)$ there exist exactly one $g' \in G$ such that $class(u) = class(g')$ and $u \mid_J lt(g')$.
- Let G be involutive. The dimension of (G) is k if and only if $T(x_i) \cap lt(G) = \emptyset$ for $1 \leq i \leq k$ and $T(x_j) \cap lt(G) \neq \emptyset$ for $k+1 \leq j \leq n$ where for any subset $S \subseteq \{x_1, ..., x_n\}$ we let $T(S)$ be the set of all terms of variables in S.
- For any zero-dimensional ideal there exist an involutive basis.
- For any positive-dimensional ideal an invertible linear change of variables may be found such that involutive basis of a given ideal does exist in terms of the new variables.

Below, an improved version of algorithm *Invbase* for constructing involutive basis G of the ideal generated by a given set F is presented (see [4]).

Algorithm 1 ($G = Invbase(F)$).
Input: $F = \{f \mid f \in K[x_1, ..., x_n]\}$
Output: G - involutive basis of (F)
$G := Autoreduce(F)$;
$L := lt(G)$;
while $L \neq \emptyset$ **do**
  $g :=$ element of G with minimal $lt(g) \in L$;
  $L := L \setminus \{lt(g)\}$;
  $L_1 := lt(G)$;
  for each x **in** $Nonmult(g)$ **do**
    $G := Autoreduce(G \cup \{g \cdot x\})$;
  $L_2 := lt(G)$;
  $L := (L \cap L_2) \cup (L_2 \setminus L_1)$;

Algorithm 1 may be obtained from the algorithm *Invbase* of the paper [2] by avoiding the so-called repeated prolongations. That is, in each step of the **while**-loop we add a product $g \cdot x$ to the current basis only if such product with the same $lt(g)$ and x has not been already considered in the previous steps. Using a noetherian argument, it can be proved that the repeated prolongations in fact reduce to zero, a detailed proof is to be given elsewhere. Our computational experience shows that avoiding such zero-reduced prolongations construction gives a considerable speed-up.

3 Structure of Zero-Dimensional Involutive Bases

Throughout this section by G is meant an involutive basis of a *zero-dimensional* ideal in some admissible term-ordering $<_T$. Now we are beginning to study some properties of zero-dimensional involutive bases.

Theorem 1. For any term v such that $deg(v) \geq deg(G)$ there exist $g \in G$ such that $lt(g) \mid_J v$.

Proof. Since G is an involutive basis, and consequently a standard basis, of a zero-dimensional ideal, then for each $1 \leq i \leq n$ there exist $g_i^* \in G$ such that $lt(g_i^*) = x_i^{d_i}$ and $d_i > 0$ [3]. Assume for contradiction that there exist a term u such that $deg(u) \geq deg(G)$ and u has no Janet divisors in $lt(G)$. Consider two alternative cases. First assume that there exist i such that $deg(u, x_i) \geq d_i$. In this case u may be represented as $u = v \cdot lt(g_i^*)$. Since polynomial $v \cdot g_i^* \in (G)$, its leading term u has a Janet divisor in $lt(G)$, which contradicts our assumption. Another possibility is $deg(u, x_i) < d_i$ for each $i = 1, ..., n$. Let $u' = u \mid_{x_1=1}$. Since $u' \cdot g_1^* \in (G)$, the term $u' \times x_1^{d_1}$ has a Janet divisor, say v, in $lt(G)$. The latter should have the form $v = u' \times x_1^p$ where $deg(u, x_1) < p \leq d_1$ because otherwise v would be a Janet divisor for u. Hence $deg(u) < deg(v) \leq deg(G)$ which contradicts the fact that $deg(u) > deg(G)$. □

Let U be a set of all irreducible terms (in the sense of Janet) modulo G. By the properties of involutive bases (see above), U is nothing but the set of all irreducible terms (in the usual sense) modulo a standard basis. Since (G) is zero-dimensional, U is finite and $D \equiv card(U)$ is the number of roots of (G) counting their multiplicities [3]. Let us denote

$$U_i = \{u \in U \mid class(u) > i\}, \quad D_i = card(U_i), \quad i = 1, ..., n.$$

Remind that $class(1) = n + 1$, therefore $U_n = \{1\}$. It is natural to set $U_0 = U$ and $D_0 = D$. Evidently $U_{i+1} \subseteq U_i$, hence $D_{i+1} \leq D_i$. Denote also

$$G_i = \{g \in G \mid class(g) = i\}.$$

Now we are ready to state the following interesting property of zero-dimensional involutive bases.

Theorem 2. Let G be an involutive basis of zero-dimensional ideal and let G_i, U_i be defined as above. Then for all $i = 1, 2, ..., n$ and for all $g \in G_i \quad lt(g) \mid_{x_i=1} \in U_i$. Conversely, for all $i = 1, 2, ..., n$ and for each $u \in U_i$ there exist exactly one $g \in G_i$ such that $u = lt(g) \mid_{x_i=1}$.

Proof. Let $g \in G_i$, that is, $lt(g) = u \times x_i^k, \quad class(u) > i$. Since G is autoreduced, u has no Janet divisors in $lt(G)$. Therefore, $u \equiv lt(g) \mid_{x_i=1} \in U_i$.
Conversely, let $u \in U_i$. Consider $v = u \times x_i^N$ such that $deg(v) \geq deg(G)$. From theorem 1 it follows that there exist $g \in G$ such that $lt(g) \mid_J v$, that is, $lt(g) = u \times x_i^k$. Since u is irreducible modulo G, $\quad k > 0$, hence $g \in G_i$. Since any monomial has no more than one Janet divisor in $lt(G)$ (see [1], proposition 1), g is determined uniquely. $\square$

Theorem 3. The number of elements in G is

$$card(G) = \sum_{i=1}^{n} D_i = \sum_{i=1}^{n} i \cdot N_{i+1}$$

where D_i is defined as above and N_j is a number of all terms of the class j irreducible modulo G.

Proof. Since $G = \cup_{i=1}^{n} G_i$ and $G_i \cap G_j = \emptyset$ for $i \neq j$, then $card(G) = \sum_{i=1}^{n} card(G_i)$. By theorem 2, $card(G_i) = D_i$. Hence $card(G) = \sum_{i=1}^{n} D_i$. Taking in account the recurrence relations $D_{i-1} = D_i + N_i, \quad i = n, n-1, ..., 1$ we obtain that $card(G) = \sum_{i=1}^{n} i \cdot N_{i+1}$. $\square$

Corollary 1. Let G_{inv} be an involutive basis of a zero-dimensional ideal, G_{min} be a corresponding minimal standard basis. Then the following chain of inequalities obviously holds:

$$card(G_{min}) \leq card(G_{inv}) \leq 1 + (n-1)D_1 \leq nD_1 \leq nD.$$

Theorem 4. Let G be an involutive basis of zero-dimensional ideal. Then

$$D_{i-1} = \sum_{g \in G_i} deg(g, x_i).$$

Proof. By theorem 2,

$$lt(G_i) = \{u_k \cdot x_i^{d_k} \mid u_k \in U_i,\ d_k > 0,\ k = 1, ..., D_i\}, \quad i = 1, 2, ..., n.$$

where $u_l \neq u_m$ for $l \neq m$. It is easy to observe that U_{i-1} is a union of D_i disjoint sets $\{u_k \cdot x_i^j \mid 0 \leq j < d_k\}$ where $k = 1, ..., D_i$. From this it immediately follows $D_{i-1} = \sum_{k=1}^{D_i} d_k$, which proves the theorem. $\square$

Corollary 2. Let G be an involutive basis of zero-dimensional ideal. The number of roots of (G) counting their multiplicities is

$$D = \sum_{g \in G} deg(g, x_1).$$

4 Conversion to lexicographical standard basis

In this section we propose a method for converting an involutive basis of zero dimensional ideal in any admissible (normally, total degree) term ordering to the pure lexicographical minimal standard basis. We describe the theoretical foundations of the method as well as a version of the corresponding algorithm. Our method is based on the following property of zero-dimensional involutive bases resulting from the theory developed in the previous section.

Theorem 5. Let G be a completely autoreduced involutive basis of a zero-dimensional ideal and let G_i, U_i, D_i be as defined above theorem 2. Then G_i is nothing but a system of D_i linear algebraic equations in $D_i - 1$ unknowns $u \in U_i \setminus \{1\}$ over $K[x_1, ..., x_i]$. These equations are linearly independent over $K[x_1, ..., x_i]$.

Proof. Since G is *completely* autoreduced, any term w in the reductum of any polynomial $g \in G_i$ should have the form $w = u \times v$ where $u \in U_i$. Indeed, if u were not an element of U_i, the term w could not be irreducible in the sense of Janet. On the other hand, by theorem 2, for each $g \in G_i$ its leading term has the form $lt(g) = u \times x_i^k,\ k > 0,\ u \in U_i$ (including $u = 1$), which gives a one-to-one correspondence between the sets U_i and $lt(G_i)$. Thus, G_i is evidently a linear algeraic system of D_i equations in $D_i - 1$ unknowns $u \in U_i \setminus \{1\}$ over $K[x_1, ..., x_i]$.

Assume for a contradiction that these equations are not linearly independent over $K[x_1, ..., x_i]$, that is $c_1 \cdot g_1 + c_2 \cdot g_2 + ... + c_k \cdot g_k = 0$ where $c_j \in K[x_1, ..., x_i]$, $\quad g_j \in G_i$ and, say, $c_1 \neq 0$. Since $class(g_j) = i$, we may write

$$lt(g_1) \times lt(c_1) = max\{lt(g_2) \times lt(c_2), ..., lt(g_k) \times lt(c_k)\}$$

where by max is meant the maximal term in the sense of $<_T$ ordering. Let $lt(g_2) \times lt(c_2)$ be such a term. Then the term $lt(g_1) \times lt(c_1)$ has 2 different Janet divisors in G_i: the term $lt(g_1)$ and the term $lt(g_2)$. This contradicts the fact that G_i is autoreduced in the sense of Janet (see [1], proposition 1). $\square$

An immediate consequence of theorem 5 is an algorithm for isolating the lowest variable x_1. Indeed, assuming $i = 1$ in theorem 5 and denoting D_1 by N, we see that G_1 is nothing else but the set of components of the vector $A(x_1) \cdot \mathbf{u}$ where $A(x_1)$ is a square $N \times N$ matrix whose elements are univariate polynomials in x_1 and $\mathbf{u}$ is a vector with D_1 components $u_i \in U_1$ arranged so that $u_i > u_j$ for $i < j$ w.r.t. the pure lexicographic ordering (note that $u_N = 1$). By theorem 5, the elements of G_1 are linearly independent over $K(x_1)$, hence $det\, A(x_1) \neq 0$. Polynomial matrix $A(x_1)$ may be transformed to the equivalent *upper triangular form*

$$B(x_1) = \| \; b_{ij}(x_1) \; \|, \quad b_{ij}(x_1) = 0 \; (i > j), \quad i, j = 1, ...N$$

by means of the *left elementary operations* (see [5], Chapter VI, Theorem 1):

1. Multiplication of the row by a non-zero number
2. Addition to some row another row multiplied by any polynomial in x_1
3. Permutation of two rows

Applying the algorithm described in [5] one can find the following representation of the matrix $A(x_1)$

$$A(x_1) = Q(x_1) \cdot B(x_1), \quad det\, Q(x_1) = c \neq 0, \quad c \in K$$

where $Q(x_1)$ is a square $N \times N$ matrix whose elements are polynomials in x_1. From this relation and inequality $det\, A(x_1) \neq 0$ it follows $detB(x_1) \neq 0$ that implies $b_{ii}(x_1) \neq 0$ for $i = 1, ...N$. Let $\tilde{G}_1$ be a set of components of the vector $B(x_1) \cdot \mathbf{u}$. Since the left elementary operations correspond to the equivalent transformations of the polynomial set G_1, we have $(\tilde{G}_1) = (G_1)$ (we shall refer to $\tilde{G}_1$ as a *triangular set* equivalent to G_1). Taking into account that $u_N = 1$, we have $b_{NN}(x_1) \in (G_1)$. Below it will be proved that $b_{NN}(x_1)$ is just the lowest element of the lexicographical standard basis of (G).

The algorithm for constructing the triangular set $\tilde{G}_1$ [5] may be formally described in the following way. Let $<_T$ be any admissible (normally, total-degree) term ordering, $<_L$ be the pure lexicographical term ordering with the same order of variables and let G be completely autoreduced zero-dimensional involutive basis in $<_T$ ordering.

Algorithm 2.

Input: $G_1 = \{g \in G \mid class(g) = 1\}$

Output: $\tilde{G}_1$ - a triangular basis w.r.t. $<_L$ such that $(\tilde{G}_1) = (G_1)$

1. Fix $<_L$ term ordering and rearrange G_1 w.r.t. $<_L$
2. $\tilde{G}_1 := Reduce(G_1, 1)$

The function $Reduce(F, i)$ in algorithm 2 computes an autoreduced form of F in terms of the so-called i-division. We say that the term u is an i-divisor of the term v iff $u \mid v$ and $u \mid_{x_1 = ... = x_i = 1} = v \mid_{x_1 = ... = x_i = 1}$. The algorithm for computing $Reduce(..., i)$ may be obtained from the well-known algorithm $ReduceAll$ [3] by replacing usual division by i-division in the normal form algorithm.

As it is shown above, the minimal w.r.t. $<_L$ element of $\tilde{G}_1$ is an equation in the single variable x_1. To prove that it is just the minimal element of the corresponding minimal lexicographical standard basis we need the following theorem.

Theorem 6. Let G be a completely autoreduced zero-dimensional involutive basis w.r.t. $<_T$ ordering and $G_{1...i} = \{g \in G \mid class(g) \leq i\}$. Let H be the minimal standard basis of (G) w.r.t $<_L$ ordering and $H_i = H \cap K[x_1...x_i]$. Then for each $i = 1, ..., n$ and for each $h \in H_i$ the equality $NF_J(h, G_{1...i}) = 0$ holds where NF_J is computed w.r.t. $<_T$ ordering.

Proof. For fixed $i = 1, ..., n$ we let $P(U_i)$ be the set of all finite sums of the form

$$P(U_i) = \{\sum_{j,k} \alpha_{jk} \cdot u_j \times v_{jk} \mid \alpha_{jk} \in K,\ u_j \in U_i\}.$$

Evidently, any $f \in P(U_i)$ is in Janet normal form modulo $G \setminus G_{1...i}$. Since G is completely autoreduced, and since for any term $u \in U_i$ all its Janet divisors also lie in U_i, from theorem 5 it follows that $G_{1...i} \subset P(U_i)$. Note that H_i is also a subset of $P(U_i)$ (with all $u_j = 1$). Consider any $h \in H_i$. From $h \in (G)$ it follows that $NF_J(h, G) = 0$. We have to prove that in fact a stronger condition holds, namely $NF_J(h, G_{1...i}) = 0$. First we claim that any $f \in P(U_i)$ may be reduced by means of polynomials from $G_{1...i}$ and not from $G \setminus G_{1...i}$. Indeed, otherwise the terms in f could not have the form $u \times v\, (u \in U_i)$ since u would not be irreducible modulo G. So, as $h \in P(U_i) \cap (G)$, then $NF_J(h, G_{1...i}) = 0$. □

Corollary 3. $(H_i) \subseteq (G_{1...i})$ for each $i = 1, ..., n$. □

Corollary 4. The minimal element of H coincides with the minimal element of $\tilde{G}_1$ computed by algorithm 2.

Proof. Let $\tilde{g}_1 \in K[x_1]$ be the minimal element of $\tilde{G}_1$ and $h_1 \in K[x_1]$ be the minimal element of H. As above, we let G_1 be subset of involutive basis G containing all the elements of class 1. ¿From algorithm 2 it follows that each $g_i \in G_1$ is a linear combination of $\tilde{g}_j \in \tilde{G}_1\, (i, j = 1, ..., D_1)$ with coefficients in $K[x_1]$. Because of theorem 6, $NF_J(h_1, G_1) = 0$ (w.r.t.$<_T$), hence

$$h_1 = \sum_{i=1}^{D_1} c_i(x_1) \cdot g_i = \sum_{j=1}^{D_1} \tilde{c}_j(x_1) \cdot \tilde{g}_j, \quad c_i(x_1), \tilde{c}_j(x_1) \in K[x_1].$$

Taking into account the triangular structure of $\tilde{G}_1$ mentioned above algorithm 2, we conclude that $\tilde{c}_j(x_1) = 0$ for $j = 2, ..., n$, and so $h_1 = \tilde{c}_1(x_1) \cdot \tilde{g}_1$. On the other hand, since H is a standard basis of (G) in $<_L$ ordering and $\tilde{g}_1 \in K[x_1] \cap (G)$, the equality $NF(\tilde{g}_1, \{h_1\}) = 0$ (w.r.t.$<_L$) holds, i.e. $\tilde{g}_1 = c(x_1) \cdot h_1$ where $c(x_1) \in K[x_1]$. Hence $\tilde{g}_1 = h_1$ (up to multiplication by non-zero element of K). □

In most cases, applying algorithm 2 gives not only the minimal equation but the whole lexicographical standard basis. So, the following theorem holds.

Theorem 7. Let G, H be as in theorem 6, $<_T$ be the total degree and $<_L$ be the pure lexicographical term ordering. Suppose $card(H) = n$ and $\{x_2, ..., x_n\} \subset lt(H)$. Assume moreover that $(G) \cap E = \emptyset$ where $E \subset K[x_1, ..., x_n]$ is the set of all linear forms in $x_1, ..., x_n$. Then, after removing redundant elements, $\tilde{G}_1$ computed by algorithm 2 coincides with H.

Proof. For each $i = 2, ..., n$ let h_i be the element of H such that $lt(h_i) = x_i$ and $\tilde{g}_i$ be the element of $\tilde{G}_1$ such that $lt(\tilde{g}_i) \mid_{x_1=1} = x_i$ where the leading terms are defined w.r.t.$<_L$. Since $<_T$ is the total degree ordering, the assumption $(G) \cap E = \emptyset$ implies $\{x_2, ..., x_n\} \subset U_1$. Consequently, $H \subset P(U_1)$ and so $NF_J(h_i, G_1) = 0$ for each $i = 2, ..., n$. Repeating the same reasonings as in the proof of corollary 4, we obtain

$$h_i = \sum_{j=1}^{D_1} c_j \cdot \tilde{g}_j, \quad \tilde{g}_j \in \tilde{G}_1, \quad c_j \in K[x_1], \quad i = 2, ..., n.$$

Taking into account the triangular form of $\tilde{G}_1$ and considering successively each $i = 2, ..., n$, one can easily observe that the only possibility is $h_i = \tilde{g}_i$ for each i. Together with corollary 4 this proves the theorem. □

Note that the form of H supposed in theorem 7 is known to happen for zero-dimensional radicals in generic position [6] and, more generally, for the sets of curvilinear points in generic position [7]. It means that algorithm 2 computes the whole lexicographical standard basis for the *most* zero-dimensional ideals and may be considered as an alternative to the well-known FGLM-technique [**?**].

Some "natural" generalization of algorithm 2 for the arbitrary zero-dimensional ideals is given below.

Algorithm 3 ($H = Invlex(G)$).
Input: G - zero-dimensional involutive basis w.r.t.$<_T$
Output: H - triangular basis of (G) w.r.t.$<_L$
$H := \emptyset$;
for $i := 1 : n$ **do**
  $H := Reduce(H \cup G_i,\ i)$;
  if $lt(H) \cap T(x_k) \neq \emptyset$ for all $k \in \{1, .., n\}$ **then go to** *exit*;
exit: $H := Remred(H)$;

The function $Reduce(..., i)$ is computed w.r.t. $<_L$ ordering by using i-division. The function *Remred* removes in a given set all redundant elements, i.e. those elements whose leading terms are the multiples (in the usual sense) of the leading terms of other elements.

Algorithm 3 had been tested on many examples, mainly for non-radical ideals. Almost always the output set H is just the minimal lexicographical standard basis. However, there are some examples (i.e. the so-called cyclic root problems with 5 and 6 variables) for which the result of algorithm 3 is not a standard basis though is very closed to it. Thus if the output set H has no the form as in theorem 7 one should apply Buchberger's algorithm w.r.t. $<_L$-ordering with H as input. Since H is closed to a standard basis or coincides with it this computation is rather fast.

The algorithm *Invlex* has been implemented in the computer algebra system REDUCE. By using this implementation the author has computed the lexicographical standard basis for the famous polynomial system by K.Rimey [9] unsolvable during the last 10 years by any computer algebra tools and considered as hopeless. The computation took about 10 hours on the computer ALPHA/DEC with 50 Mb memory.

Aknowledgements. The author is grateful to J.Apel, Yu.Blinkov, V.Gerdt and T.Mora for useful discussions.

References

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

[2] Zharkov A.Yu., Blinkov Yu.A. Involutive Bases of Zero-Dimensional Ideals. To appear in Journal Symbolic Computation.

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

[4] Zharkov A.Yu., Blinkov Yu.A. Involutive Systems of Algebraic Equations. To appear in Russian journal "Programmirovanie" (in Russian).

[5] Gantmacher R.F. *Theory of Matrices.* Moscow, "Nauka", 1988 (in Russian).

[6] Gianni P., Mora T. Algebraic Solution of Systems of Polynomial Equations using Gröbner Bases. Lecture Notes in Computer Science, Springer 1989, v.356, 247-257.

[7] Mora T. The shape of the Shape Lemma. To appear.

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

[9] Rimey K. A System of Polynomial Equations and a Solution by an Unusual Method. ACM-SIGSAM Bull. 1984, v.18, 30-32.