~~1998A~~ ~~1998A~~

1998-00-00-C

London Mathematical Society Lecture Note Series. 251

1998-00-00-A

Gröbner Bases and Applications

Edited by

B. Buchberger & F. Winkler
Johannes Kepler University of Linz

CAMBRIDGE
UNIVERSITY PRESS

An Algorithmic Criterion for the Solvability of a System of Algebraic Equations[1]

Bruno Buchberger

1 Problem Statement

We start from the polynomial ring $K[x_1, \ldots, x_n]$ over a commutative field K (abbreviated $K[x_i]$) and an arbitrary polynomial ideal $\mathcal{A} = (f_1, \ldots, f_s)$ ($f_j \in K[x_i]$ for $j = 1, \ldots, s$). (Notions not explicitly defined here will be used in precisely the sense defined in Gröbner (1949) and van der Waerden (1937).)

The residue class ring $\mathcal{O} = K[x_i]/\mathcal{A}$ is well known to be an (in general, infinite dimensional) algebra over K. If $\mathcal{A}$ is zero dimensional, then $\mathcal{O}$ has finite dimension over K, and conversely. The residue classes of the power products (abbreviated PP) $x_1^{i_1} \cdots x_n^{i_n}$ form a basis of the algebra, which is linearly dependent in the case $\mathcal{A} \neq (0)$. (Since in what follows we will speak often of the basis of an ideal and of the basis of the corresponding residue class algebra, we adopt the following convention to avoid ambiguity: we say simply *basis* if we mean the basis of the residue class algebra and *ideal basis* otherwise.)

The goal of the present study is to develop an algorithm which, given an ideal basis $(f_1, \ldots, f_s)$, extracts a linearly independent basis for $\mathcal{O}$ from the set of all residue classes of PPs, and, for two arbitrary elements of this basis, allows a representation of its product to be computed as a linear combination of basis elements (i.e. produces the complete multiplication table in the finite dimensional case). For zero dimensional ideals, Gröbner (1964a) suggested such an algorithm, for which it was still undecided, when it could be terminated in concrete cases. The justification that the algorithm suggested here can be applied to arbitrary polynomial ideals emerged during the investigation of this last question. By applying the algorithm, an assertion is possible about the existence of a zero for the ideal as well as the dimension of the ideal.

[1] Original article appeared as 'Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungsystems', *Aeq. Math.* **4** (1970), 374-383. Received 27 March 1969, and in revised form 11 November 1969. Translation by Michael Abramson and Robert Lumbert.

2 Description of the Algorithm

2.1 Definitions

For the purposes of our study, we order the PPs by increasing degree and within the same degree lexicographically in the sense that $x_1^{i_1} \cdots x_n^{i_n}$ precedes $x_1^{i'_1} \cdots x_n^{i'_n}$ if $i_1 > i'_1$ or $i_t = i'_t$ (for $t = 1, \ldots, k$ and $1 \leq k < n$) and $i_{k+1} > i'_{k+1}$. Beginning with $x_1^0 \cdots x_n^0$, we associate the integers $1, 2, 3, \ldots$ to these ordered PPs as the *indices of the corresponding PPs*. The PP having the highest index among those occuring in a polynomial, will be called the *LPP of this polynomial.*

Let the basis polynomials of the above polynomial ideal $\mathcal{A} = (f_1, \ldots, f_s)$ be

$$f_j = x_1^{I_{j,1}} \cdots x_n^{I_{j,n}} + \sum a^{(j)}_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \qquad (j = 1, \ldots, s) \qquad (2.1)$$

Let $pp_j = x_1^{I_{j,1}} \cdots x_n^{I_{j,n}}$ be the LPP of f_j and let the other terms of f_j be collected under the summation sign in (1). Without loss of generality, we have assumed the coefficient of pp_j to be 1. Because of (1) we have

$$x_1^{I_{j,1}+v_1} \cdots x_n^{I_{j,n}+v_n} \leftrightarrow - \sum a^{(j)}_{i_1 \ldots i_n} x_1^{i_1+v_1} \cdots x_n^{i_n+v_n} \qquad (2.2)$$

($j = 1, \ldots, s$ and $v_t = 0, 1, 2, \ldots$ for $t = 1, \ldots, n$. We use "$\leftrightarrow$" as the symbol for *congruent modulo* $\mathcal{A}$).

A PP $x_1^{i_1} \cdots x_n^{i_n}$ is called a *multiple* of the PP $x_1^{k_1} \cdots x_n^{k_n}$ if $i_t \geq k_t$ for $t = 1, \ldots, n$. PPs which are multiples of at least one of the pp_j $(j = 1, \ldots, s)$, i.e. occur at least once on the left-hand side of (2), will be called *MPPs relative to the ideal basis* $(f_1, \ldots, f_s)$. Otherwise a PP will be called *NPP relative to the ideal basis* $(f_1, \ldots, f_s)$. When no ambiguity is possible, we will omit the phrase "relative to the ideal basis $(f_1, \ldots, f_s)$". Polynomials, in which only NPPs occur and terms containing the same PPs are collected, are called *NPP-polynomials* (relative to the ideal basis $(f_1, \ldots, f_s)$).

A given polynomial (for which we do not wish to assume that terms containing the same PPs are collected) can now be transformed into a congruent NPP-polynomial, which is in general not necessarily unique, by successively replacing all MPPs by the corresponding right-hand sides of (2) and by collecting all like terms in arbitrary stages of this reduction procedure (which we call *M-reduction*). Thus the residue classes of the NPPs already form a basis for $\mathcal{O}$, although still linearly dependent in general.

2.2 A Lemma

The following now holds:

Lemma. *If an ideal basis $(f_1, \ldots, f_s)$ has the property that all possible M-reductions of a polynomial lead to the same result, then the residue classes of the NPPs relative to the ideal basis form a linear independent basis for $\mathcal{O}$.*

Proof. A linear dependency between residue classes of NPPs would correspond to an NPP-polynomial q in $\mathcal{A}$ which would possess a representation

$$q \equiv \sum_{j=1}^{s} h_j \cdot f_j \qquad \text{with} \quad h_j \in K[x_j] \quad \text{for } j = 1, \dots, s. \tag{2.3}$$

Multiplying out the $h_j \cdot f_j$ ($j = 1, \dots, s$) without collecting terms containing the same PPs produces a polynomial on the right-hand side of (3) that can be M-reduced in two different ways with two different results, contradicting the assumption of the lemma: It can be M-reduced to $q \not\equiv 0$ precisely by collecting like terms. And it can be trivially M-reduced to 0 by subtracting the polynomials $h_j \cdot f_j$ and afterwards collecting like terms. (Notice that both procedures satisfy the definition of M-reduction!) □

2.3 Description of One Step of the Algorithm

In one step of the algorithm, the following procedure is carried out: Form the *least common multiple* (abbreviated LCM) of the LPPs pp_j and pp_k of two distinct basis polynomials f_j and f_k, namely the PP

$$pp_{j,k} = x_1^{L_{j,k,1}} \cdots x_n^{L_{j,k,n}}, \qquad \text{where} \quad L_{j,k,t} = \max(I_{j,t}, I_{k,t}) \quad (t = 1, \dots, n).$$

For $pp_{j,k}$, both of the following congruences arise from (2):

$$pp_{j,k} \leftrightarrow -\sum a^{(j)}_{i_1 \dots i_n} x_1^{i_1 + d_{j,1}} \cdots x_n^{i_n + d_{j,n}} \tag{2.4}$$

and

$$pp_{j,k} \leftrightarrow -\sum a^{(k)}_{i_1 \dots i_n} x_1^{i_1 + d_{k,1}} \cdots x_n^{i_n + d_{k,n}} \tag{2.5}$$

where

$$d_{j,t} = L_{j,k,t} - I_{j,t} \quad \text{and} \quad d_{k,t} = L_{j,k,t} - I_{k,t} \qquad (t = 1, \dots, n).$$

We call the polynomial that results from forming the difference of the right-hand sides of (4) and (5) the *S-polynomial corresponding to $pp_{j,k}$*. Two situations can arise through M-reduction of this polynomial relative to the ideal basis in question:

1. The S-polynomial corresponding to $pp_{j,k}$ is M-reduced to zero. In this case, we go immediately to the next step, as indicated in 2.4.

2. The S-polynomial corresponding to $pp_{j,k}$ is M-reduced to a polynomial (6) which does not vanish:

$$a x_1^{I_1} \cdots x_n^{I_n} + \sum a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n} \qquad (a \in K, \quad a \neq 0), \tag{2.6}$$

where again we have singled out the LPP $x_1^{I_1} \cdots x_n^{I_n}$ of this polynomial. In this case, we add the resulting polynomial in the form

$$x_1^{I_1} \cdots x_n^{I_n} + \frac{1}{a} \sum a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \tag{2.7}$$

to the ideal basis. By doing this, we also increase the set of relations appearing in (2) and thereby the number of possible M-reductions that can possibly be carried out in the future for any polynomial. In accordance with 2.4, we go to the next step.

2.4 Combination of Steps

The operations given in 2.3 will be carried out in succession for all $pp_{j,k}$, where $j = 1, \ldots, s-1$ and $k = j+1, \ldots, s$. Notice that during the execution of the algorithm, the number of generating polynomials changes in general. For practical computation, it is advisable to process the $pp_{j,k}$ with smallest index first, since this can reduce the computation time considerably.

For a specific combination of indices j and k, one of the following special cases can arise:

S1. $pp_{j,k} = pp_j$ (or $pp_{j,k} = pp_k$). In this case, the basis polynomial f_j (f_k resp.) can be deleted from the basis, after which the operations defined in 2.3 are carried out for $pp_{j,k}$.

S2. $pp_{j,k} = pp_j \cdot pp_k$. In this case, we need not carry out the operations defined in 2.3.

The algorithm is terminated when all $pp_{j,k}$ have been processed according to the instructions of 2.3. We will now prove the following two claims:

B1. *Let $(g_1, \ldots, g_u)$ be the current ideal basis when the algorithm terminates. Then $(g_1, \ldots, g_u)$ has the property required by the hypothesis of the lemma.*

B2. *The algorithm terminates for every ideal in finitely many steps.*

3 The Proofs

3.1 Proof of B1

Let

$$g_j = x_1^{S_{j,1}} \cdots x_n^{S_{j,n}} + \sum c^{(j)}_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \quad (j = 1, \ldots, u)$$

be the new basis polynomials.

For this special ideal basis, we have: If we were to process every $pp_{j,k}$ ($pp_{j,k}$ would now be the LCM of $x_1^{S_{j,1}} \cdots x_n^{S_{j,n}}$ and $x_1^{S_{k,1}} \cdots x_n^{S_{k,n}}$) once more according to the instructions of the algorithm ($j = 1, \ldots, u-1$ and $k = j+1, \ldots, u$), then we could now M-reduce every resulting S-polynomial to zero in at least one way, since we have just added the necessary polynomials of the form (7) to the ideal basis during the previous run of the algorithm.

In the case $pp_{j,k} = pp_j \cdot pp_k$ (pp_j is now the abbreviation for $x_1^{S_{j,1}} \cdots x_n^{S_{j,n}}$), the corresponding S-polynomial has the form

$$-\sum c^{(j)}_{i_1 \ldots i_n} x_1^{i_1+S_{k,1}} \cdots x_n^{i_n+S_{k,n}} + \sum c^{(k)}_{k_1 \ldots k_n} x_1^{k_1+S_{j,1}} \cdots x_n^{k_n+S_{j,n}}.$$

The special M-reduction, in which we replace every

$$x_1^{i_1+S_{k,1}} \cdots x_n^{i_n+S_{k,n}}$$

by

$$-\sum c^{(k)}_{k_1 \ldots k_n} x_1^{k_1+i_1} \cdots x_n^{k_n+i_n}$$

and every

$$x_1^{k_1+S_{j,1}} \cdots x_n^{k_n+S_{j,n}}$$

by

$$-\sum c^{(j)}_{i_1 \ldots i_n} x_1^{i_1+k_1} \cdots x_n^{i_n+k_n}$$

makes this polynomial zero immediately. Thus in this case, an M-reduction to zero of the corresponding S-polynomial always exists, even when the operations defined in 2.3 were not carried out for $pp_{j,k}$.

We now show that every M-reduction relative to the ideal basis $(g_1, \ldots, g_u)$ of a given polynomial leads to the same result. We prove this by induction and begin with $x_1^0 \cdots x_n^0$. $x_1^0 \cdots x_n^0$ has a uniquely determined M-reduced form relative to every ideal basis, because it is either an NPP and therefore already (uniquely) M-reduced, or an MPP and therefore M-reducible to zero.

The induction hypothesis is: For every polynomial whose LPP does not have a greater index than a fixed PP pp_0, the M-reduction relative to $(g_1, \ldots, g_u)$ produces a uniquely determined NPP-polynomial.

What must be shown is: For a polynomial

$$f = c_1 \cdot x_1^{V_1} \cdots x_n^{V_n} + \ldots + c_p \cdot x_1^{V_1} \cdots x_n^{V_n} + \sum a_{v_1 \ldots v_n} x_1^{v_1} \cdots x_n^{v_n},$$

whose LPP $x_1^{V_1} \cdots x_n^{V_n}$ has an index that is greater by one than pp_0, the M-reduction produces a uniquely determined NPP-polynomial. (Note that we must prove the claim for polynomials in which like terms are not yet collected because we used them in this form in 2.2.)

We distinguish between three cases:

Case A. $x_1^{V_1} \cdots x_n^{V_n}$ is NPP. Then M-reduction of f means: M-reduction of

$$\sum a_{v_1 \ldots v_n} x_1^{v_1} \cdots x_n^{v_n}$$

which produces a unique result by the induction hypothesis, and collection of the terms $c_q \cdot x_1^{V_1} \cdots x_n^{V_n}$ $(q = 1, \ldots, p)$ which leads similarly to a unique result.

Case B. $x_1^{V_1} \cdots x_n^{V_n}$ is a multiple of precisely one $x_1^{S_{j,1}} \cdots x_n^{S_{j,1}}$ $(1 \leq j \leq u)$. At some stage of the M-reduction of f, every term $c_q \cdot x_1^{V_1} \cdots x_n^{V_n}$ $(q = 1, \ldots, p)$ must first be replaced by $c_q \cdot \sum(j)$, where

$$\sum(j) = \sum c^{(j)}_{i_1 \ldots i_n} x_1^{i_1+d_{j,1}} \cdots x_n^{i_n+d_{j,n}} \qquad (d_{j,t} = V_t - S_{j,t} \text{ for } t = 1, \ldots, n),$$

and then, together with the other terms of the polynomial, be further M-reduced, leading again to a unique result because of the induction hypothesis.

Case C. $x_1^{V_1} \cdots x_n^{V_n}$ is a multiple of several $x_1^{S_{j,1}} \cdots x_n^{S_{j,n}}$, e.g. $j = j_1, \ldots, j_z$ $(1 \leq z \leq u)$. During the M-reduction of f, every $c_q \cdot x_1^{V_1} \cdots x_n^{V_n}$ $(q = 1, \ldots, p)$ will be replaced by a polynomial $c_q \cdot \sum(j_{r_q})$ where $j_{r_q} \in \{j_1, \ldots, j_z\}$. Thus a fixed combination of indices $(j_{r_1}, \ldots, j_{r_p})$ characterizes a family of M-reductions of f, which all use the same "initial substitutions" for the terms $c_q \cdot x_1^{V_1} \cdots x_n^{V_n}$ and all produce the same result, as we can easily check by slightly modifying the argument in case B. In particular, every M-reduction characterized by the p-tuple $(j_1, j_1, \ldots, j_1)$ leads to the same NPP-polynomial. We are done if we can show that among the M-reductions characterized by a specific combination $(j_{r_1}, \ldots, j_{r_p})$ and those characterized by $(j_1, \ldots, j_1)$, one of each can be specified which leads to the same result. In any case, a suitable M-reduction from the class characterized by $(j_1, \ldots, j_1)$ will first replace $c_q \cdot x_1^{V_1} \cdots x_n^{V_n}$ in f $(q = 1, \ldots, p)$ by

$$c_q \cdot \sum c^{(j_1)}_{i_1 \ldots i_n} x_1^{V_1'+i_1+d_{j_1,1}} \cdots x_n^{V_n'+i_n+d_{j_1,n}}, \qquad (3.1)$$

where

$$V_t' = V_t - L_{j_1,j_{r_q},t} \qquad d_{j_1,t} = L_{j_1,j_{r_q},t} - S_{j_1,t}$$
$$L_{j_1,j_{r_q},t} = \max(S_{j_1,t}, S_{j_{r_q},t})$$
$$\text{(exponents of the LCM } pp_{j_1,j_{r_q}}), \quad t = 1, \ldots, n.$$

An appropriate M-reduction from the class characterized by $(j_{r_1}, \ldots, j_{r_p})$ will first replace $c_q \cdot x_1^{V_1} \cdots x_n^{V_n}$ $(q = 1, \ldots, p)$ by

$$c_q \cdot \sum c^{(j_{r_q})}_{i_1 \ldots i_n} x_1^{V_1'+i_1+d_{j_{r_q},1}} \cdots x_n^{V_n'+i_n+d_{j_{r_q},n}} \qquad (3.2)$$

where

$$d_{j_{r_q},t} = L_{j_1,j_{r_q},t} - S_{j_{r_q},t} \qquad (t = 1, \ldots, n).$$

The polynomials (8) and (9) are precisely the polynomials whose difference yielded the S-polynomial corresponding to $pp_{j_1,j_{r_q}}$, except both are multiplied by $x_1^{V_1'} \cdots x_n^{V_n'}$. From an M-reduction that reduces this S-polynomial to zero (and that always exists relative to $(g_1, \ldots, g_u)$ because of the argument at the beginning of this section), we can immediately obtain an M-reduction to zero of the polynomial consisting of the difference of (8) and (9) by multiplying all PPs resulting from the M-reduction of the S-polynomial by $x_1^{V_1'} \cdots x_n^{V_n'}$. However if the difference of two polynomials to M-reduces to zero, then it is easily seen that each of the two polynomials can be M-reduced to the same polynomial in at least one way. Hence, among the M-reductions of f characterized by $(j_1, \ldots, j_1)$ and those characterized by $(j_{r_1}, \ldots, j_{r_p})$, there is at least one of each which leads to the same NPP-polynomial. With this, B1 is proved. □

The justification of the treatment of the special case S1 still remains open. However, we can easily convince ourselves that by removing a generating polynomial which has the property specified in S1, the family of possible M-reductions will not be reduced, as long as we add the NPP-polynomial corresponding to the S-polynomial to the ideal basis, as the algorithm specifies. The claim that all of the S-polynomials corresponding to $pp_{j,k}$ can be M-reduced to zero relative to the ideal basis $(g_1, \ldots, g_u)$, which forms the basis for the proof of uniqueness of M-reduction, remains correct after removing a basis polynomial in step S1.

3.2 Proof of B2

During the processing of an LCM $pp_{j,k}$ according to the algorithm, the ideal basis will eventually be enlarged by the addition of a polynomial whose LPP is an NPP relative to the previous ideal basis. B2 is proved if we can prove the following theorem:

Theorem. *A sequence of PPs* $x_1^{I_{j,1}} \cdots x_n^{I_{j,n}}$ $(j = 1, 2, 3, \ldots)$*, which has the property that* $x_1^{I_{k,1}} \cdots x_n^{I_{k,n}}$ $(k = 2, 3, \ldots)$ *is not a multiple of any* $x_1^{I_{m,1}} \cdots x_n^{I_{m,n}}$ $(m < k)$*, has only finitely many elements. (A sequence of PPs with this property will be called an M-sequence).*

Proof. The theorem is easily seen for $n = 1$. We assume its correctness for all $n < N$ and consider an M-sequence which begins with $x_1^{I_1} \cdots x_N^{I_N}$. Let $x_1^{v_1} \cdots x_N^{v_N}$ be another element of the M-sequence, then $v_i < I_i$ for at least one i $(1 \leq i \leq N)$. For an arbitrary combination of indices $(i_1, \ldots, i_k)$ $(1 \leq k \leq N$, $1 \leq i_1 < \ldots < i_k \leq n)$, there are only finitely many k-tuples $(v_{i_1}, \ldots, v_{i_k})$ of positive integers (including zero) which satisfy $v_{i_j} < I_{i_j}$ for $j = 1, \ldots, k$. Therefore, the PPs of an M-sequence belong to finitely many types, each of which is characterized by a fixed combination of exponents $(v_{i_1}, \ldots, v_{i_k})$ of k fixed variables $x_{i_1}, \ldots, x_{i_k}$.

In an M-sequence with infinitely many elements, an infinite subsequence must exist whose elements all belong to the same type. By removing the variables $x_{i_1}, \ldots, x_{i_k}$ for which the PPs of this subsequence have fixed exponents

$(v_{i_1}, \ldots, v_{i_k})$, an infinite M-sequence in $n - k$ variables arises from these PPs, contradicting our induction hypothesis. □

Remark. This proof shows that the algorithm is finite in principal, independent of special properties of the ideal (e.g. the dimension), but says nothing about its practicality. In this setting, the following fact seems to be interesting: When applied to a system of linear equations, the algorithm becomes the Gaussian elimination procedure, as one can easily verify. It is therefore a generalization of the Gaussian algorithm in a certain sense.

4 Results about the Existence of a Zero and the Dimension

It is well known that a polynomial ideal $\mathcal{A}$ has no zeros if and only if $\mathcal{A} = (1)$, i.e. the corresponding residue class ring $\mathcal{O}$ consists of only one residue class. This is the case if and only if during the course of the algorithm, the polynomial $x_1^0, \ldots, x_n^0$ must be adjoined to the ideal basis. (If, after termination of the algorithm, $x_1^0, \ldots, x_n^0$ is not present in the ideal basis, then there is more than one NPP and therefore more than one residue class in $\mathcal{O}$!) Hence, we have:

Criterion 4.1. *A polynomial ideal has no zeros if and only if, during the course of the algorithm, the polynomial $x_1^0, \ldots, x_n^0$ must be adjoined to the ideal basis.*

Moreover, we arrive at the following criterion about the dimension of the ideal:

Criterion 4.2. *A polynomial ideal has dimension greater than zero if and only if the ideal basis $(g_1, \ldots, g_u)$ produced by the algorithm has the following property: There is an i $(1 \leq i \leq n)$, such that no PP of the form x_i^h $(h \geq 0)$ occurs among the LPPs of the basis polynomials.*

Proof. Applying the definition of the dimension of a polynomial ideal ([1, p. 98]), we easily see that a polynomial ideal has dimension zero if and only if the residue class algebra is finite dimensional. But the number of basis elements of the residue class algebra (= the number of NPPs relative to $(g_1, \ldots, g_u)$) is infinite if and only if the condition expressed in Criterion 4.2 holds. □

5 Calculating the Multiplication Table of the Residue Class Algebra

Let $\overline{x_1^{i_1} \cdots x_n^{i_n}}$ and $\overline{x_1^{k_1} \cdots x_n^{k_n}}$ be quantities which were constructed as basis elements for $\mathcal{O}$ by the algorithm. (By the bar, we denote the the corresponding residue class.) Then we obtain a representation of their product $\overline{x_1^{i_1+k_1} \cdots x_n^{i_n+k_n}}$ as a linear combination of the residue classes of the NPPs through the M-reduction of $x_1^{i_1+k_1} \cdots x_n^{i_n+k_n}$ relative to the ideal basis produced by the algorithm.

6 Remark on the Construction of Zeros

We suggest here a method for finding the zeros of the polynomial ideal using the knowledge about the structure of the residue class algebra. First we consider the zero dimensional case: Let $u_1, \ldots, u_m$ be the PPs whose residue classes form a basis for $\mathcal{O}$. Using the multiplication table, we can successively find representations for all $\overline{x_1^k}$ $(k = 0, 1, \ldots)$ as linear combinations of the $\overline{u_j}$ $(j = 1, \ldots, m)$, and for each $\overline{x_1^k}$, we can test whether it already depends linearly on $1, \overline{x_1}, \ldots, \overline{x_1^{k-1}}$. Let $k = m_1$ $(m_1 \leq m + 1)$ be the first time this is the case, then $p_1(\overline{x_1}) = 0$ holds, where $p_1(x_1)$ is a polynomial of degree m_1 in $K[x_1]$.

Next, we form the representations of the residue classes of the PPs which arise by multiplying $1, x_1, \ldots, x_1^{m_1-1}$ by $x_2, x_2^2, \ldots,$ until for a fixed residue class $\overline{x_1^{i_1} x_2^{i_2}}$, a linear dependency with previous PP-residue classes is found which can be written in the form

$$p_2(\overline{x_1}, \overline{x_2}) = 0 \qquad \text{with} \qquad p_2(x_1, x_2) \in K[x_1, x_2].$$

We continue similarly and obtain a sequence of polynomials $p_k(x_1, \ldots, x_k) \in \mathcal{A}$ $(k = 1, \ldots, n)$, *which we can solve successively.* Certainly, every zero of the ideal occurs among the set of zeros of the p_k, but the converse is not the case in general. Precautions must still be taken (by taking additional polynomials from $\mathcal{A}$) in order to eliminate extraneous zeros. A detailed study addressing questions in this context is however beyond the scope of the present work.

The d dimensional case $(d > 0)$ can be reduced to the zero dimensional case by substituting numerical values for d independent variables relative to $\mathcal{A}$. Thereby we can obtain at least finitely many solutions. For every solution point, under certain assumptions, we can construct the family of solutions in the neighborhood of these points, e.g. with the help of Lie series (Gröbner (1964b), p. 72ff). However many questions remain to be studied in detail.

7 An Example and a Remark on Programming

In order to illustrate the steps of the algorithm, we give a simple example:

$$\mathcal{A} = (x_3^2 - \tfrac{1}{2}x_1^2 - \tfrac{1}{2}x_2^2, \quad x_1x_3 - 2x_3 + x_1x_2, \quad x_1^2 - x_2).$$

We consider first the $pp_{1,2}$, namely $x_1x_3^2$. The corresponding S-polynomial is

$$S_{1,2} = \tfrac{1}{2}x_1^3 + \tfrac{1}{2}x_1x_2^2 - 2x_3^2 + x_1x_2x_3.$$

M-reduction of $S_{1,2}$ produces

$$x_1x_2^2 - x_1x_2 + 2x_2 + 2x_2^2 - 4x_2x_3.$$

We adjoin this polynomial to the ideal basis. We must treat the other $pp_{j,k}$, where $j = 1, \ldots, s-1$ and $k = 2, \ldots, s$, in an analogous manner. s is 3 at the start, but becomes 4 by addition of the new basis polynomial and changes again several times during the course of the algorithm. For example, $pp_{1,3}$ is a PP for which the arguments of the special case S2 apply, so the M-reduction of $S_{1,3}$ can be skipped.

Finally we obtain the new ideal basis

$$\begin{aligned}\mathcal{A} \;=\; & (x_3^2 - \tfrac{1}{2}x_2^2 - \tfrac{1}{2}x_2, \quad x_1x_3 - 2x_3 + x_1x_2, \quad x_1^2 - x_2, \\ & x_1x_2^2 + 7x_1x_2 + 2x_2 + 6x_2^2 - 16x_3, \\ & x_2x_3 + x_2^2 + 2x_1x_2 - 4x_3, \quad x_2^3 - 12x_2 - 29x_2^2 + 64x_3 - 24x_1x_2).\end{aligned}$$

The LPPs of the six basis polynomials are x_3^2, x_1x_3, x_1^2, $x_1x_2^2$, x_2x_3, x_2^3. Therefore, Criterion 4.2 shows that $\mathcal{A}$ is zero dimensional. The residue classes of the PPs 1, x_1, x_2, x_3, x_1x_2, x_2^2 form a basis of the residue class algebra. The representation of the product of the fourth and sixth basis elements, for example, is formed from the the M-reduction of $x_2^2x_3$. It produces

$$x_2^2x_3 \leftrightarrow -18x_1x_2 + 48x_3 - 8x_2 - 21x_2^2.$$

The remaining elements of the multiplication table can be found similarly.

Of course, the computation time increases very quickly with increased number of variables and increased degree of the polynomials. The programming of the algorithm is very easy because of its simple structure. It is advantageous to use list processing concepts. Programs exist in Freiburg Code and machine code of the ZUSE Z 23.

For other results on questions studied in the present paper, Hermann (1926) should be consulted.

I would like to use this opportunity to express sincere thanks to my distinguished teacher, Professor W. Gröbner.

References

Gröbner, W. (1949). *Moderne algebraische Geometrie.* Springer-Verlag, Vienna, Innsbruck.

Gröbner, W. (1964a). *Teoria degli ideali e geometria algebrica.* Seminari dell'Istituto Nazionale di Alta Matematica 1962-1963. Edizione Cremonese, Rome.

Gröbner, W. (1964b). Oral communication in the Math. Seminar of the University of Innsbruck.

Hermann, G. (1926). 'Die Frage der endlich vielen Schritte in der Theorie der Polynomideale'. *Math. Ann.* **95**, 736-788.

van der Waerden, B. L. (1939). *Moderne Algebra*, Volume 2, 2nd Edition. Springer-Verlag, Berlin.

Universität Innsbruck