記号処理 41－2
（1987. 6. 26）

頭項消去に基づくいくつかの代数的算法

佐々木 建昭
（理化学研究所）

$F_1, \cdots, F_r$を係数が多項式環$K[u_1, \cdots, u_m]$に属し，変数が$X_1, \cdots, X_n$である多項式とする。多くの代数的問題は，与えられた$F_1, \cdots, F_r$から変数$X_1, \cdots, X_n$を消去して，$K[u_1, \cdots, u_m]$の要素である多項式を計算することに帰着できる。本稿では，この消去を係数環$K[u_1, \cdots, u_m]$上のイデアル（$F_1, \cdots, F_r$）のグレブナー基底（標準基底）の計算として定式化し，多項式環上のグレブナー基底の算法を与える。次いで，この算法を用いて，1)連立代数方程式の解法，2) U終結式の計算，3)代数関係式の計算，4)多項式の簡単化，のそれぞれに対して新しい算法を与える。さらに，これらの算法を効率化するためのアイデアを与え，それが非常に有効であることを実際にインプリメントして示す。

Some Algebraic Algorithms Based on Head Term Elimination over Polynomial Rings

Tateaki Sasaki

The Institute of Physical and Chemical Research
Wako-shi, Saitama 351-01, Japan

Let F_1, ..., F_r be polynomials in X_1, ..., X_n with coefficients in $K[u_1,...,u_m]$. Many algebraic problems can be reduced to calculating polynomials in $K[u_1,...,u_m]$ by eliminating X_1, ..., X_n from F_1, ..., F_r. We formulate this elimination in terms of the Gröbner basis of polynomial ideal $(F_1,...,F_r)$ over $K[u_1,...,u_m]$. The elimination theory developed is applied to several typical problems. Furthermore, some ideas which make the elimination procedure efficient are presented, with timing data by actual implementation.

§1. Introduction

Many algebraic calculations are reduced to the elimination of variables. The conventional elimination method is the leading term elimination. For polynomials F and G in main variable X, the leading term elimination is defined by the formula

$$\frac{\mathrm{lcm}}{\ell t(F)}\cdot F - \frac{\mathrm{lcm}}{\ell t(G)}\cdot G, \qquad \mathrm{lcm} = \mathrm{Lcm}(\ell t(F), \ell t(G)), \qquad (1)$$

where ℓt and Lcm denote the "leading term" and "least common multiple", respectively. (The resultant calculation is nothing but a successive application of the leading term elimination.)

Another kind of elimination is the head term elimination which plays an essential role in the construction of Gröbner basis of the polynomial ideal [Buch65]. (For precise definition of "head term", see §2.) For polynomials F and G with coefficients in a field, the head term elimination is defined by the formula

$$\frac{\mathrm{lcm}}{\mathrm{ht}(F)}\cdot F - \frac{\mathrm{lcm}}{\mathrm{ht}(G)}\cdot G, \qquad \mathrm{lcm} = \mathrm{Lcm}(\mathrm{ht}(F), \mathrm{ht}(G)), \qquad (2)$$

where ht denotes the head term. (This is nothing but the S-polynomial of F and G.) Note the similarity between the formulas (1) and (2).

Although the leading term elimination is employed in many algorithms, the superiority of head term elimination is being recognized in many calculations. This is because that the head term elimination is more general than the leading term elimination in that the latter can be attained by successive application of the former. Furthermore, we can determine the term ordering variously for head term elimination, while the term ordering for leading term elimination is unique when we have determined the main variable.

In many algorithms, the following elimination is required: given polynomials F_1, ..., F_r in $R[X_1,\dots,X_n]$, where $R = K[u_1,\dots,u_m]$, calculate polynomial(s) in u_1, ..., u_m by eliminating X_1, ..., X_n from F_1, ..., F_r. Following Buchberger [Buch65,84], we formulate this elimination as a construction of Gröbner basis of the polynomial ideal over ring $R = K[u_1,\dots,u_m]$.

§2. Gröbner basis of polynomial ideal over polynomial ring

After Buchberger's pioneering work on Gröbner basis [Buch65], which is for polynomials with coefficients in a field, various extensions have been made. As for extending the coefficient domain, Lauer [Lauer76] and Buchberger [see Buch84] developed Gröbner basis theories over the integer ring, and Kandri-Rody and Kapur extended them to Euclidean rings [Ka&Ka84]. In this section, we extend the coefficient domain to polynomial rings, which is straightforward.

We denote the set of nonnegative integers by $\mathbb{Z}_0$ and the Cartesian product $\mathbb{Z}_0\times\cdots\times\mathbb{Z}_0$ by $\mathbb{Z}_0^r$. Let K be a field and R a ring $K[u_1,\dots,u_m]$. We abbreviate the rings $K[u_1,\dots,u_m]$ and $R[X_1,\dots,X_n]$ to $K[u]$ and $R[X]$, respectively. Similarly, we abbreviate monomials $cu_1^{a_1}\cdots u_m^{a_m}$ and $CX_1^{A_1}\cdots X_n^{A_n}$, where $c \in K$ and $C \in R$, to cu^a and CX^A, respectively. The ideal generated by F_1, ..., F_r is denoted by $(F_1,\dots,F_r)$. Furthermore, we denote the pair of a and b by <a,b>.

Definition 1 [order > for elements of $\mathbb{Z}_0^r$]. Let $a = (a_1,\dots,a_r)$ and b =

$(b_1,\dots,b_r)$ be elements of $\mathbb{Z}_0^r$. We define $a > b$ iff there exists an integer k such that $a_k > b_k$ and $a_i = b_i$, $i=1,\dots,k-1$ when $k > 1$. //

Definition 2 [total degree]. Let $t = cu_1^{a_1}\cdots u_m^{a_m}$ and $T = CX_1^{A_1}\cdots X_n^{A_n}$, with $c \in K$ and $C \in R$, be monomials in K[u] and R[X], respectively. Total degrees of t and T, which are abbreviated to tdeg(t) and Tdeg(T), respectively, are $a_1 + \cdots + a_m$ and $A_1 + \cdots + A_n$. //

Definition 3 [order $\mathrel{|\!>}$ for monomials in K[u] and R[X]]. Let $t_a = c_a u_1^{a_1}\cdots u_m^{a_m}$ and $t_b = c_b u_1^{b_1}\cdots u_m^{b_m}$, with $c_a, c_b \in K$, be monomials in K[u]. The lexicographic order $\mathrel{|\!>}$ between t_a and t_b is defined as $t_a \mathrel{|\!>} t_b$ iff $(a_1,\dots,a_m) > (b_1,\dots,b_m)$. The total-degree order $\mathrel{|\!>}$ is defined as $t_a \mathrel{|\!>} t_b$ iff $(\mathrm{tdeg}(t_a), a_1,\dots,a_m) > (\mathrm{tdeg}(t_b), b_1,\dots,b_m)$. Let $T_A = C_A X_1^{A_1}\cdots X_n^{A_n}$ and $T_B = C_B X_1^{B_1}\cdots X_n^{B_n}$, with $C_A, C_B \in R$, be monomials in R[X]. We define the lexicographic order $\mathrel{|\!>}$ between T_A and T_B by n-tupples $(A_1,\dots,A_n)$ and $(B_1,\dots,B_n)$ and the total-degree order $\mathrel{|\!>}$ by (n+1)-tupples $(\mathrm{Tdeg}(T_A), A_1,\dots,A_n)$ and $(\mathrm{Tdeg}(T_B), B_1,\dots,B_n)$, respectively, just the same as for the monomials in K[u]. //

Definition 4 [head term]. Let f be a polynomial in K[u] and t the highest order monomial in f. We call t the head term of f and abbreviate to ht(f). Similarly, the head term is defined for polynomial F in R[X], with abbreviation Ht(F). //

Definition 5 [head power product, head coefficient]. Let $f \in K[u]$ and $\mathrm{ht}(f) = cu^a$, with $c \in K$. We call u^a and c the head power product of f and the head coefficient of f, respectively, and abbreviate to hp(f) and hc(f). Similarly, for polynomial F in R[X] with $\mathrm{Ht}(F) = CX^A$, $C \in R$, we call X^A and C the head power product of F and head coefficient of F, respectively, with abbreviations Hp(F) and Hc(F). //

Definition 6 [order $\mathrel{|\!\gg}$ for monomials in K[u,X]]. Let $T_a = c_a u^a X^A$ and $T_b = c_b u^b X^B$, with $c_a, c_b \in K$, be monomials in K[u,X]. We define $T_a \mathrel{|\!\gg} T_b$ iff either $X^A \mathrel{|\!>} X^B$ or $A = B$ and $u^a \mathrel{|\!>} u^b$. //

Remark. We can define $\mathrel{|\!\gg}$ similarly as $\mathrel{|\!>}$. For example, if $\mathrel{|\!>}$ is the total-degree order in both K[u] and R[X], then we can define the order $\mathrel{|\!\gg}$ for monomial $cu_1^{a_1}\cdots u_m^{a_m} X_1^{A_1}\cdots X_n^{A_n}$, with $c \in K$, by the order of (m+n+2)-tupple $(\Sigma A_j, A_1,\dots,A_n, \Sigma a_i, a_1,\dots,a_m)$.

Definition 7 [abbreviations Hhp and Hhc]. We abbreviate hp(Hc(F))·Hp(F) and hc(Hc(F)) to Hhp(F) and Hhc(F), respectively. //

Definition 8 [S-polynomial in R[X] = K[u][X]]. Let $F,G \in R[X]$. The S-polynomial of F and G, to be abbreviated to Spol(F,G), is defined as

$$\mathrm{Spol}(F,G) = \frac{\mathrm{LCM}}{\mathrm{Hhp}(F)}\cdot F - \frac{\mathrm{LCM}}{\mathrm{Hhp}(G)}\cdot\frac{\mathrm{Hhc}(F)}{\mathrm{Hhc}(G)}\cdot G, \qquad (3)$$

where $\mathrm{LCM} = \mathrm{Lcm}(\mathrm{Hhp}(F),\mathrm{Hhp}(G))$. //

Definition 9 [M-reduction in R[X]]. Let $F,G \in R[X]$. If a monomial T of F is such that $T = X^A \mathrm{Hp}(G)\cdot\{ \cdots + cu^a\cdot\mathrm{ht}(\mathrm{Hc}(G)) + \cdots \}$, then $F' = F - cu^a X^A\cdot G$ is a procedure of replacing T by lower order terms. This procedure is the M-reduction of F by G and expressed as $F \xrightarrow[G]{} F'$. //

Remark. When Hhp(G) | Hhp(F), the Spol(F,G) in Def. 8 is nothing but the M-reduction of (head term of) F by G.

Definition 10 [normal form in R[X]]. Let $\Gamma = \{G_1,\dots,G_s\}$ be a subset of R[X]. When F is M-reduced by $G_1, \dots, G_s$ as far as possible to $\tilde{F}$, we call $\tilde{F}$ the normal form of F w.r.t. Γ and express as $F \xrightarrow[\Gamma]{} \tilde{F}$. //

Definition 11 [Gröbner basis in R[X]]. Let $\{F_1,\dots,F_r\}$ and Γ =

$\{G_1,\dots,G_s\}$ be subsets of $R[X]$. The set Γ is a Gröbner basis of ideal $(F_1,\dots,F_r)$ if the following two conditions are satisfied:

(1) $(F_1,\dots,F_r) = (G_1,\dots,G_s)$,

(2) for any pair $<G_i,G_j>$ in Γ, $\mathrm{Spol}(G_i,G_j) \underset{\Gamma}{\twoheadrightarrow} 0$. //

Given a set $\{F_1,\dots,F_r\}$ in $R[X]$, we can construct a Gröbner basis $\{G_1,\dots,G_s\}$ of ideal $(F_1,\dots,F_r)$ by Buchberger's celeborated procedure, see [Buch65].

Theorem. Buchberger's procedure in $R[X]$ terminates and the basis $\{G_1,\dots,G_s\}$ constructed is a Gröbner basis of $(F_1,\dots,F_r)$.

Proof. Let us consider that $F_1, \dots, F_r$ and $G_1, \dots, G_s$ are elements in $K[u,X]$ with the monomial order $|\!\gg$ defined in Def. 6 (see Remark to Def. 6, also). Then, definitions of S-polynomial in Def. 8 and M-reduction in Def. 9 are the same as conventional ones in $K[u,X]$. Hence, the proof for the conventional Gröbner basis over the field can be applied to prove the theorem. //

Corollary. Let $\Gamma = \{G_1,\dots,G_s\}$ be a Gröbner basis of $(F_1,\dots,F_r)$, then

(1) for any F in $(F_1,\dots,F_r)$, $F \underset{\Gamma}{\twoheadrightarrow} 0$,

(2) for any F in $R[X]$, normal form of F w.r.t. Γ is unique,

(3) $\Gamma \cap K[u]$ is a Gröbner basis of ideal $(F_1,\dots,F_r) \cap K[u]$. //

§3. Applications of head term elimination

As we have seen in the Theorem in §2, successive application of the head term elimination terminates and we can use Buchberger's procedure as a general elimination procedure. Since the elimination is a very elementary operation, the head term elimination will be applied to various algebraic calculations.

We note that, in Buchberger's procedure above, we may choose the term order $\rhd$ and the pair $<G_i,G_j>$ arbitrarily. The efficiency of elimination depends on the choice strongly, and we select the following choices.

Choice 1. We set $\rhd$ to the total-degree order as far as possible. This is because the total-degree order is much more desirable than the lexicographic order for efficient elimination.

Choice 2. The G_i and G_j are chosen to be as low order elements as possible. The importance of this choice will become clear below.

With these choices in mind, we describe four typical applications of the head term elimination in $K[u][X]$, below.

3.1. Solving a system of algebraic equations

Consider solving a system of algebraic equations

$$\{F_1 = 0, \cdots, F_r = 0\}, \tag{5}$$

where $F_i \in K[X]$, $i=1,\dots,r$, and we assume that the dimension of solution space is 0. Most algebraic methods for solving (5) are such that an equation in a single variable, X_1 for example, is derived by eliminating $X_2, \dots, X_n$. One practical method performs this elimination by calculating a Gröbner basis of $(F_1,\dots,F_r)$ with the ordering $X_n \rhd \cdots \rhd X_1$ (i.e., the lexicographic order).

Some authors proposed to solve the system (5) by calculating a Gröbner basis with total-degree order, see [Buch84] and [Mori86]. The method is simple, but our method below is even simpler (and will be efficient). We calculate polynomials $Q_1(X_1)$ and $Q_i(X_i,X_1)$, $i=2,\dots,n$, directly, where Q_1 and Q_i satisfy $Q_1(X_1) = 0$ and $Q_i(X_i,X_1) = 0$, respectively, for the values X_1 and X_i of the roots of (5).

Algorithm A (reducing a system of algebraic equations).

Input : Polynomials $F_1, \dots, F_r$ in $K[X]$;

Output: Polynomials $Q_1(X_1)$ and $Q_i(X_i,X_1)$, $i=2,\dots,n$, such that $Q_1,Q_i \in (F_1,\dots,F_r)$, with as small $\deg_{X_i}(Q_i)$ as possible;

Step 1: Treat $F_1, \dots, F_r$ as elements in $R[X_2,\dots,X_n]$, $R = K[X_1]$, and calculate a Gröbner basis Γ_1 of $(F_1,\dots,F_r)$ with the total-degree order;

Step 2: For each i, $2 \leq i \leq n$, treat $F_1, \dots, F_r$ as elements in $R[X_2,\dots X_{i-1},X_{i+1}\dots X_n]$, $R = K[X_1,X_i]$, and calculate a Gröbner basis Γ_i of $(F_1,\dots,F_r)$ with the total-degree order for $X_2, \dots X_{i-1}, X_{i+1}, \dots X_n$ and the lexicographic order for X_i and X_1;

Return: Return Q_1 and Q_i, $i=2,\dots,n$, where $Q_1 \in \Gamma_1 \cap K[X_1]$, $Q_i \in \Gamma_i \cap K[X_1,X_i]$ and $\deg_{X_i}(Q_i)$ is the smallest. //

3.2. Calculating U-resultant

The classical method of calculating the U-resultant is inefficient. In 1977, Lazard presented a practical method [Laza77], and Lazard's method has been made efficient by Kobayashi et al. by using the Gröbner basis [K&F&F86]. (This paper also presents a practical method for factoring the U-resultant into linear factors.) However, the calculation is still complicated and time consuming.

Our method using the head term elimination is quite simple, yet it is efficient for small-sized problems. (For large-sized problems, the method of Kobayashi et al. will be better.) Our method calculates the U-resultant by eliminating $X_1, \dots, X_n$ from the system of algebraic equations $\{F_0=0, F_1=0, \cdots, F_r=0\}$.

Algorithm B (U-resultant).

Input : $F_1, \dots, F_r$ in $K[X]$ and indeterminates $u_0, u_1, \dots, u_n$;

Output: U-resultant of $\{F_1=0, \cdots, F_r=0\}$;

Method: Treat $F_0, F_1, \dots, F_r$ as elements in $R[X]$, $R = K[u]$, and calculate a Gröbner basis Γ of ideal $(F_0,F_1,\dots,F_r)$ with the total-degree order for both $X_1, \dots, X_n$ and $u_0, \dots, u_n$;

Return: Return the lowest order element G such that $G \in \Gamma \cap K[u]$. //

3.3. Calculating algebraic relations

Let $P_1, \dots, P_r$ be polynomials in $K[X]$, and let $\rho(u_1,\dots,u_r)$ be a polynomial in $K[u_1,\dots,u_r]$. If ρ satisfies $\rho(P_1,\dots,P_r) = 0$, then ρ is called an algebraic relation of $P_1, \dots, P_r$.

Calculation of algebraic relations of given $P_1, \dots, P_r$ are simple in principle: we have only to eliminate variables $X_1, \dots, X_n$ from the set of polynomials $\{P_1-u_1, \cdots, P_r-u_r\}$. The use of Buchberger's procedure to calculate algebraic relations is described in [Ar&Se84]. This method calculates a Gröbner basis in $K[u_1,\dots,u_r, X_1,\dots,X_n]$. In order to eliminate $X_1, \dots, X_n$ first, one usually employs the lexicographic order for $X_n, \dots, X_1, u_r, \dots, u_1$. If we calculate a Gröbner basis in $R[X]$, where $R = K[u_1,\dots,u_r]$, then we can employ the total-degree order. Note that, with a Gröbner basis calculation, we can calculate a complete set of generators of the algebraic relations (cf. Corollary to Theorem in §2).

Algorithm C (algebraic relations).

Input : Polynomials $P_1, \dots, P_r$ in $K[X]$;

Output: Gröbner basis of the ideal generated by algebraic relations;

Method: Treat $P_1-u_1, \cdots, P_r-u_r$ as elements in $R[X]$, $R = K[u]$, and calculate a Gröbner basis Γ of the ideal $(P_1-u_1, \cdots, P_r-u_r)$ with the total-degree order for both $X_1, \ldots, X_n$ and $u_1, \ldots, u_r$;

Return: Return $\Gamma \cap K[u]$. //

3.4. Representing a polynomial by other polynomials

Given polynomials P and $P_1, \ldots, P_r$ in $K[X]$, we want to determine whether there exists a polynomial $Q(u_1,\ldots,u_r)$ in $K[u_1,\ldots,u_r]$ such that $P = Q(P_1,\ldots,P_r)$, and we want to determine Q when exists. An algorithm performing this calculation will be quite useful for simplifying large polynomials. It is easy to see that this calculation is a special case of calculating algebraic relations described in 3.3. Therefore, we have the following algorithm.

Algorithm D (polynomial composition).

Input : Polynomials P, $P_1, \ldots, P_r$ in $K[X]$;

Output: Polynomial $Q(u_1,\ldots,u_r)$, if exists, s.t. $P = Q(P_1,\ldots,P_r)$;

Method: Treat P, $P_1, \ldots, P_r$ as elements in $R[X]$, $R = K[u]$, and calculate a Gröbner basis Γ of $(P_1-u_1, \cdots, P_r-u_r)$ with the total-degree order for both $X_1, \ldots, X_n$ and $u_1, \ldots, u_r$. Then, P $\xrightarrow[\Gamma]{}$ Q;

Return: If $Q \in K[u]$ then return Q else return NIL. //

§4. Devices for efficient elimination

Although we have formulated the variable elimination as the construction of a Gröbner basis, we need not always calculate the full set of Gröbner basis but may stop the computation when the required elimination is accomplished. For example, in the calculation of U-resultant we may stop the computation when all the variables $X_1, \ldots, X_n$ are eliminated. (Then, the U-resultant calculated may contain an extra monomial factor.) This device will save the computation time drastically, as we will see from the actual timing data. Note that, with Choice 2 given in §3, the required elimination will be performed by avoiding wasteful computation as far as possible.

The second device is the removal of monomial factors from the S-polynomials constructed, which is quite easy to execute. For example, monomial factors in algebraic relations are meaningless and we can remove them. Note that, even if such a monomial factor is meaningful, we can often remove it so long as the removed factor is processed suitably. For example, suppose $P_i = \tilde{P}_i X_k^a$ in Algorithm A, then we can split the system of algebraic equations into two systems as $\{P_1=0, \ldots, P_{i-1}=0, \tilde{P}_i=0, P_{i+1}=0, \ldots, P_r=0\}$ and $\{P_1=0, \ldots, P_{i-1}=0, X_k^a=0, P_{i+1}=0, \ldots, P_r=0\}$. Hence, only if the latter system is also solved, we can remove the monomial factor X_k^a from P_i.

In the current implementation of our Gröbner basis package, the user can choose one of the following three modes for controlling the truncation of computation.

(T0) No truncation (default mode);

(T1) Truncate the computation when all the variables $X_1, \ldots, X_n$ are eliminated;

(T2) Truncate the computation when variables $X_1, \ldots, X_n$ and parameters

$u_1, \ldots, u_{m-1}$ are eliminated (the final polynomial is in $K[u_m]$). Furthermore, the user can choose one of the following three modes for controlling the removal of the monomial factors.

(R0) No removal (default mode);

(R1) Monomial factors in $K[u]$ are removed;

(R2) Monomial factors in $K[u,X]$ are removed.

Including the above-mentioned devices, the algorithms given in the previous section can be improved as follows.

Algorithm A' (reducing algebraic equations).

Perform the second step of Algorithm A with modes (T1) and (R2), and calculate $Q_1(X_1)$ by eliminating, for example, X_2 from elements in the set Γ_2. (The removed factors should be saved for the later computation.) //

Algorithm B' (U-resultant).

Perform Algorithm B with modes (T1) and (R1). //

Algorithm C' (algebraic relations).

Perform Algorithm C with modes (T1) and (R1). //

Let us show the effectiveness of the above-mentioned devices by several examples. The test has been done by using a Gröbner basis package on the algebra system GAL. The test problems are as follows.

Problem 1 (reducing a system of algebraic equations).

$$F_1 = 2(X_4^2 + X_3^2 + X_2^2 + X_1^2) - X_1 = 0,$$

$$F_2 = 2(X_4X_3 + X_3X_2 + X_2X_1) - X_2 = 0,$$

$$F_3 = 2(X_4X_2 + X_3X_1) + X_2^2 - X_3 = 0,$$

$$F_4 = 2(X_4 + X_3 + X_2) + X_1 - 1 = 0.$$

Problem 2 (calculating a U-resultant).

$$F_1 = X_1^2 + X_2^2 - 2 = 0, \quad F_2 = X_1X_2 - 1 = 0.$$

Adding $F_0 = u_0 + u_1X_1 + u_2X_2 = 0$ to the above system, we can calculate the following polynomial as the U-resultant:

$$\begin{aligned} U(u_0,u_1,u_2) &= u_0^4 - 2u_0^2u_1^2 - 4u_0^2u_1u_2 - 2u_0^2u_2^2 \\ &\quad + u_1^4 + 4u_1^3u_2 + 6u_1^2u_2^2 + 4u_1u_2^3 + u_2^4. \end{aligned}$$

Problem 3 (calculating an algebraic relation).

$$P_1 = (X_1^6 + X_2^6) + 522(X_1^5X_2 - X_1X_2^5) - 10005(X_1^4X_2^2 + X_1^2X_2^4),$$

$$P_2 = -(X_1^4 + X_2^4) + 228(X_1^3X_2 - X_1X_2^3) - 494X_1^2X_2^2,$$

$$P_3 = X_1X_2(X_1^2 + 11X_1X_2 - X_2^2)^5.$$

The algebraic relation of these polynomials is $P_1^2 + P_2^3 - 1728P_3 = 0$.

Problem 4 (polynomial composition).

$$P_1 = X_1^2X_2 + 2X_1^2 - 3X_1X_2 + 5X_2,$$

$$P_2 = 2X_1^3 - 4X_1^2X_2 - 3X_1X_2^2 + X_2^3,$$

$$P = -2X_1^9X_2^3 + 4X_1^8X_2^4 + 3X_1^7X_2^5 + \cdots + 4X_1^2 - 6X_1X_2 + 10X_2.$$

Given these polynomials (P is composed of 49 terms), we derive a polynomial $Q(u_1,u_2)$ such that $P = Q(P_1,P_2)$. The form of Q in this example is

$$Q(u_1,u_2) = -u_1^3u_2 + u_1u_2^2 + 2u_1 - 3u_2.$$

Algorithm	Prob. 1	Prob. 2	Prob. 3	Prob. 4
A – D	17,080	1,136	251	115
A' – C'	690	65	122	****

Table I. Timing data (in milliseconds)

Table I shows the timing data, where the computation has been done by

GAL on a FACOM-M380 computer. We see that the truncation mode is often quite effective. This effectiveness is due partly to Choice 1 given in §3 and partly to skipping the termination check in Buchberger's procedure. For Problem 2, for example, the elimination has been performed after constructing 11 S-polynomials while we must construct 16 S-polynomials for the Gröbner basis calculation. The removal mode is effective only for Problem 2 in our test. In mode (R1), we obtain the U-resultant just when X_1 and X_2 are eliminated, through successive removal of monomials u_2, u_1, and u_1. On the other hand, in mode (R0), we obtain $u_1^2 u_2 \cdot U(u_0,u_1,u_2)$ just when X_1 and X_2 have been eliminated, and we have to construct 19 more S-polynomials to get $U(u_0,u_1,u_2)$. We have also solved Problem 2 by applying Algorithm 2 with modes (T0) and (R1) (i.e., no truncation but removal of monomial factors), and the computation time was 707 milliseconds. This shows that the removal mode is also effective considerably.

Although the above test is restricted within a small number of examples which are of small-sized, we have seen that our devices are quite effective in many cases. The devices will become more effective for larger-sized problems.

Acknowledgement. The author thanks Prof. Kobayashi and Mr. Furukawa for stimulating discussions and comments.

References

[Ar&Se84] D. Arnon and T. Sederberg, "Implicit equations for parametric surfaces by Gröbner basis", Proc. of 1984 MACSYMA User's Conf. (ed. V.E. Golden), General Electric, pp. 431-435.

[Buch65] B. Buchberger, "An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal (German)", Ph.D. Thesis, Math. Inst., Univ. of Innsbruck (Austria), 1965.

[Buch84] B. Buchberger, "Gröbner bases : An algorithmic method in polynomial ideal theory", in Recent Trends in Multidimensional Systems Theory (ed. R. Bose), Reidel, 1984.

[Ka&Ka84] A. Kandri-Rody and D. Kapur, "Algorithms for computing Gröbner bases of polynomial ideals over various Euclidean rings", Proc. of EUROSAM '84 (ed. J. Fitch), 1984 (Lecture Notes Comp. Sci. 174, Springer-Verlag), pp. 195-206.

[K&F&F86] H. Kobayashi, T. Fujise, and A. Furukawa, "Solving systems of algebraic equations by general elimination method", preprint of Dept. Math., Nihon Univ., Tokyo, 1986 (to be published).

[Lauer76] M. Lauer, "Canonical representatives for the residue classes of a polynomial ideal (German)", Diploma Thesis, Dept. Math., Univ. Kaiserslautern, 1976.

[Laza77] D. Lazard, "Algèbre linéaire sur $K[x_1,x_2,\dots,x_n]$ et éllimination", Bull. Soc. Math. France, No. 105 (1977), pp. 165-190.

[Mori86] S. Moritsugu, "On solving a system of algebraic equations by using Gröbner basis", preprint of Dept. Inf. Sci., Univ. of Tokyo, 1987.