An Attempt to Enhance Buchberger's Algorithm by Using Remainder Sequences and GCDs (II)

Tateaki Sasaki
Professor emeritus, University of Tsukuba
Tsukuba-shi, Ten-noudai, Ibaraki 305-8571, Japan
E-mail address: sasaki@math.tsukuba.ac.jp

Masaru Sanuki
Dept. Clinical Medicine, University of Tsukuba
Tsukuba-shi Ten-noudai, Ibaraki 305-8571, Japan
E-mail address: sanuki@md.tsukuba.ac.jp

Daiju Inaba
The Mathematics Certification Institute of Japan
Ueno 5-1-1, Tokyo 110-0005, Japan
E-mail address: d.inaba@su-gaku.net

Fujio Kako
Inst. Computer Science, Nara Women's University
Nara-shi Kita-uoya, Nara 630-8506, Japan
E-mail address: kako@ics.nara-wu.ac.jp

Abstract

Let $\mathcal{F} = \{F_1, \dots, F_{m+1}\} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{u}]$ be a given system, where $m+1 \geq 3$, $(\boldsymbol{x}) = (x_1, \dots, x_m)$ and $(\boldsymbol{u}) = (u_1, \dots, u_n)$, with $\forall x_i \succ \forall u_j$. Let $\mathrm{GB}(\mathcal{F}) = \{\widehat{G}_1, \widehat{G}_2, \cdots\}$, with $\widehat{G}_1 \prec \widehat{G}_2 \prec \cdots$, be the reduced Gröbner basis of $\mathcal{F}$ w.r.t. the lexicographic order. In a previous paper [10], one of the authors proposed a method of enhancing Buchberger's algorithm for computing $\mathrm{GB}(\mathcal{F})$. His idea is to compute a set $\mathcal{G}' := \{\widetilde{G}_1, \widetilde{G}_2, \dots\} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{u}]$, such that each $\widetilde{G}_i$ is either 0 or a small multiple of $\widehat{G}_i$, and apply Buchberger's algorithm to $\mathcal{F} \cup \mathcal{G}'$. He proposed a scheme of computing $\widetilde{G}_1, \widetilde{G}_2, \dots$ by the PRSs (polynomial remainder sequences) and the GCDs in "$\widetilde{G}_1 \Rightarrow \widetilde{G}_2 \Rightarrow \cdots$" order, without computing Spolynomials. The scheme is supported by two new useful theorems and one proposition to remove the *extraneous factor*. In fact, for a simple but never toy example, his scheme has computed $\widetilde{G}_1$ successfully ($\widetilde{G}_1$ became $\widehat{G}_1$ by the proposition mentioned above). However, an unexpected difficulty occurred in computing $\widetilde{G}_2$; it contained a pretty large extraneous factor which was not removed by the proposition. In this paper, we find a surprising phenomenon with which we can remove the above mentioned extraneous factor in $\widetilde{G}_2$ and obtain $\widehat{G}_2$. As for $\widehat{G}_3$ and $\widehat{G}_4$, we obtain very good "body doubles" of them, by eliminating variables in leading coefficients of intermediate remainders of the PRSs computed for $\widetilde{G}_1$. For systems of many sub-variables, $n \geq 3$, our method introduces an extra factor in $\mathbb{Q}[u_3, \dots, u_n]$, into the "LCtoW" polynomial; see the text for the LCtoW polynomial. Furthermore, we present several techniques to enhance the computation.

1 Introduction

In this paper, by $\mathbb{K}$, $\boldsymbol{x}$ and $\boldsymbol{u}$ we denote a number field, variables $x_1,\dots,x_m$ $(m \ge 2)$ and sub-variables $u_1,\dots,u_n$, where x_i and u_j are ordered as $\forall x_i \succ \forall u_j$. By $\langle \mathcal{F} \rangle$, with $\mathcal{F} \subset \mathbb{K}[\boldsymbol{x},\boldsymbol{u}]$, we denote an ideal generated by the polynomials of $\mathcal{F}$. By $\mathrm{PRS}_x(G,H)$, with $G,H \in \mathbb{K}[x,\boldsymbol{u}]$, we denote a *polynomial remainder sequence* (*PRS* in short) w.r.t. x, started from G and H. In this paper, we mostly discuss on the PRS and only a little on the Gröbner basis. So, we explain basic concepts on Gröbner basis here. We use, without explanation, the *leading monomial* (abbreviated to "lmn", and used as $\mathrm{lmn}(P)$), the *Spolynomial*, $\mathrm{Spol}(P_1,P_2)$ for $P_1,P_2 \in \mathbb{K}[\boldsymbol{x},\boldsymbol{u}]$, and the *Mreduction* ("M" means monomial). By $G \xrightarrow{H}\!\!\!\rightarrow \widetilde{G}$, we denote successive Mreductions of G by H so that each monomial of $\widetilde{G}$ is Mirreducible w.r.t. H. By $\mathrm{GB}(\mathcal{F})$, we denote the *reduced Gröbner basis w.r.t. the lexicographic (LEX) order, of* $\mathcal{F}$; here, "reduced" means that any elements G_i and $G_{j\neq i}$ of $\mathrm{GB}(\mathcal{F})$ are mutually Mirreducible.

Let $G,H \in \mathbb{K}[x,\boldsymbol{u}]$ be relatively prime. The last element of $\mathrm{PRS}_x(G,H)$ is in $\mathbb{K}[\boldsymbol{u}]$, and called the *resultant* $R = \mathrm{res}_x(G,H)$. R is a (often a large) multiple of the lowest-order element $\widehat{G}$ of the elimination ideal $\langle\{G,H\}\rangle \cap \mathbb{K}[\boldsymbol{u}]$. Polynomial $R/\widehat{G}$ is called the *extraneous factor* in the algebraic elimination; see a nice introductory paper by Kapur [7]. $\widehat{G}$ is also the lowest-order element of $\mathrm{GB}(\{G,H\})$, and we can compute it by Buchberger's algorithm [4, 5]. Buchberger's algorithm is known to be quite heavy, in particular, for the LEX order and when $m+n \gg 1$. So, the authors of [11] tried to compute $\widehat{G}$ by the PRS method. They got the following nice theorem in [11]; $\mathrm{cont}_x(A)$ below is the *content* of A w.r.t. x.
<u>Theorem A</u>: *Let P_k be the last element of* $\mathrm{PRS}_x(G,H)$*, and A_k and B_k be the cofactors of P_k, satisfying $P_k = A_k G + B_k H$. Then, $P_k/\gcd(\mathrm{cont}_x(A_k),\mathrm{cont}_x(B_k))$ is a constant multiple of $\widehat{G}$.* □

The above authors tried to extend Theorem A to $(m+1)$-polynomial system $\mathcal{F} := \{F_1,\dots,F_{m+1}\} \subset \mathbb{K}[\boldsymbol{x},\boldsymbol{u}]$. They failed but obtained a very useful theorem, Theorem B below, by restricting $\mathcal{F}$ to be "healthy" in [12]. $\mathcal{F}$ is called *healthy* if i) all the m variables $\boldsymbol{x}$ can be eliminated, ii) none of n sub-variables $\boldsymbol{u}$ can be eliminated, and iii) $\mathrm{GB}(\mathcal{F}) \cap \mathbb{K}[\boldsymbol{u}] \neq \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{l>1}$ where $\mathcal{B}_1,\dots,\mathcal{B}_l$ are non-empty reduced Gröbner bases in $\mathbb{K}[\boldsymbol{u}]$, s.t. $\mathrm{Spol}(P_i,P_j) \xrightarrow{P_i,P_j}\!\!\!\rightarrow 0$ for any pair $(P_i,P_{j\neq i})$, $P_i \in \mathcal{B}_i$ and $P_j \in \mathcal{B}_j$.
<u>Theorem B</u>: *If $\mathcal{F}$ is healthy then* $\mathrm{GB}(\mathcal{F}) \cap \mathbb{K}[\boldsymbol{u}] = \{\widehat{G}\}$. □ This theorem is not useful if we compute only one multiple of $\widehat{G}$. Sasaki proposed a simple and outstanding idea which he called "rectangular PRSs" (*rectPRSs* in short); see **2**. With rectPRSs we can compute several different multiples of $\widehat{G}$. Applying this idea to a system shown in **3**, he found that the GCD of the multiples was a small multiple of $\widehat{G}$.

Thus, so long as $\widehat{G}$ is concerned, we are now able to compute $\widehat{G}$ or its small multiple $\widetilde{G}$ by the PRSs and the GCDs quite fast. This pushed Sasaki to propose a method of enhancing Buchberger's algorithm by using PRSs and GCDs in [10]. His idea is to compute small multiples of important elements of $\mathrm{GB}(\mathcal{F})$, by utilizing the intermediate elements of PRSs computed for $\widehat{G}$, and apply Buchberger's algorithm for the system $\mathcal{F} \cup \mathcal{G}'$, where $\mathcal{G}'$ is a set of polynomials thus computed by the PRSs and the GCD operation.
<u>Remark 1</u>: *We note that many elements of $\mathcal{G}'$ are not multiples of corresponding ones of* $\mathrm{GB}(\mathcal{F})$*. What happens actually is as follows. Let $\widetilde{G}_i \in \mathcal{G}'$ be a "body double" of $\widehat{G}_i \in \mathrm{GB}(\mathcal{F})$. Then, $\mathrm{lmn}(\widetilde{G}_i)$ is a small multiple of $\mathrm{lmn}(\widehat{G}_i)$. We express this situation as that $\widetilde{G}_i$* is a small lmn-multiple of $\widehat{G}_i$. //

Let $\mathrm{GB}(\mathcal{F}) = \{\widehat{G}_1, \widehat{G}_2, \widehat{G}_3, \cdots\}$, where $\widehat{G} = \widehat{G}_1 \prec \widehat{G}_2 \prec \widehat{G}_3 \prec \cdots$. Let $\mathcal{R} := \{R_1,\dots,R_l\}$ be a family of remainders of rectPRSs, of the same main variable and the same degree. For computing polynomials in $\mathcal{G}'$, Sasaki eliminated variables of the leading coefficients of $\mathcal{R}$. Let $\overline{c}$ be the GCD of the variable-eliminated leading coefficients. Then, Sasaki constructed a polynomial $\mathrm{LCtoW}(\overline{c}) \in \langle \mathcal{F} \rangle$, having $\overline{c}$ as its leading coefficient; he called it "LeadingCoefficient-to-Whole" polynomial; see **4.1** for details. For $\widetilde{G}_2$ of the example shown in **3**, however, the LCtoW polynomial contained a large extraneous factor which could not be removed by Proposition 1. That is, Sasaki faced a big problem in [10].

In **2**, we explain critical concepts in our scheme of elimination: the leading-term elimination and PRSs, rectangular PRSs, $\boldsymbol{u}$-cofactors and relating proposition for removing the extraneous factors. In **3**, we explain our current problem in details. In **4**, we show an unexpected phenomenon which opens a door to solve the difficulty mentioned above, and explain how we have solved the difficulty. In **5**, we show how $\widetilde{G}_3$ and $\widetilde{G}_4$ are computed by Sasaki's scheme. Finally, in **6**, we give various theoretical and computational considerations. In particular, we modify the previous definition of LCtoW polynomial.

2 Preliminary and a brief survey

Recursive representation and leading-term elimination It is well-known that the Gröbner basis theory is based on the *monomial representation* of polynomials. So, in this paper, we explain only the *recursive representation* of polynomials. In computing the PRS, polynomial $G \in \mathbb{K}[\boldsymbol{x}]$, with $x_1 \succ \cdots \succ x_m$, and its coefficients are represented recursively w.r.t. its variables, as follows.

$$G \;=\; g_d\, x_1^d + g_{d-1}\, x_1^{d-1} + \cdots + g_0, \quad \text{where } \forall i,\; g_i \in \mathbb{K}[x_2, \ldots, x_m]. \tag{1}$$

By $\deg(G)$, $\mathrm{ltm}(G)$, $\mathrm{lcf}(G)$ we denote the *degree* d, the *leading term* $g_d\, x_1^d$, and the *leading coefficient* g_d, of G, respectively. Given G and $H = h_e x_1^e + h_{e-1} x_1^{e-1} + \cdots \in \mathbb{K}[\boldsymbol{x}]$, with $d \ge e$, the *leading-term elimination* of G and H is defined by (the "lcm" below is the operation of the least common multiple):

$$\mathrm{ltmElim}(G, H) \;\stackrel{\text{def}}{=}\; \frac{\mathrm{LCM}}{\mathrm{lcf}(G)}\, G - \frac{\mathrm{LCM}}{\mathrm{lcf}(H)}\, x_1^{d-e} H, \quad \text{where } \mathrm{LCM} = \mathrm{lcm}(\mathrm{lcf}(G), \mathrm{lcf}(H)). \tag{2}$$

Let $(E_1 = G,\, E_2 = H,\, E_3, \ldots, E_i, \ldots, E_k)$ be a *leading-term elimination sequence* (*LES* in short) w.r.t. x_1, computed by formula $E_i := \mathrm{ltmElim}(E_{i-2}, E_{i-1}) = \eta_{i-2} E_{i-2} - \eta_{i-1} x^{d_{i-1}} E_{i-1}$, where $i \ge 3$, $d_{i-1} = \deg(E_{i-2}) - \deg(E_{i-1})$, and η_{i-2} and η_{i-1} are multipliers specified in (2). Then, the cofactors A_i and B_i of E_i for $i \ge 3$, with $(A_1, A_2) = (1, 0)$ and $(B_1, B_2) = (0, 1)$, are computed by the formulas

$$A_i := \eta_{i-2} A_{i-2} - \eta_{i-1}\, x^{d_{i-1}} A_{i-1}, \qquad B_i := \eta_{i-2} B_{i-2} - \eta_{i-1}\, x^{d_{i-1}} B_{i-1}. \tag{3}$$

Note that $\mathrm{ltmElim}(G, H)$ is quite similar in shape to $\mathrm{Spol}(G, H)$. In fact, by eliminating $\mathrm{ltm}(G)$ by $\mathrm{ltm}(H)$ with Buchberger's algorithm, we obtain $\mathrm{ltmElim}(G, H)$. This shows that both eliminations are connected with each other in the most basic level. We obtain the PRS by taking out strictly degree-decreasing sub-sequence of the LES.

"Rectangular PRSs" to utilize Theorem B By $\mathrm{lastPRS}_{x_i}(F_{j_1}, F_{j_2})$ and $\mathrm{nmlastPRS}_{x_i}(F_{j_1}, F_{j_2})$ we denote the last element of $\mathrm{PRS}_{x_i}(F_{j_1}, F_{j_2})$ and its normalized version by Theorem A, respectively.

The conventional way of eliminating $\boldsymbol{x}$ is to triangularize $\mathcal{F}$ w.r.t. $\boldsymbol{x}$. On the other hand, we eliminate $\boldsymbol{x}$ as follows: $\{F_1, F_2, \ldots, F_{m+1}\} \Rightarrow \{G_1, G_2, \ldots, G_{m+1}\} \Rightarrow \cdots \Rightarrow \{H_1, H_2, \ldots, H_{m+1}\}$, where $G_j := \mathrm{nmlastPRS}_{x_1}(F_j, F_{j+1})$ with $F_{m+1} = F_1$, $\cdots$, $H_j := \mathrm{nmlastPRS}_{x_m}(G'_j, G'_{j+1})$ with $G'_{m+1} = G'_1$. Thus, we obtain $m \times (m+1)$ PRSs, which we call *rectangular PRSs* (*rectPRSs* in short). By Theorem B, each H_j is a multiple of $\widehat{G}$, so $\overline{H} \stackrel{\text{def}}{=} \gcd(H_1, \ldots, H_{m+1})$ will be a small multiple of $\widehat{G}$.

$\boldsymbol{u}$-cofactors and removal of remaining extraneous factors Theorem B is quite powerful, however, $\overline{H}$ defined above usually contains extraneous factors. In [12], the authors presented a method of predicting extraneous factors in $H_1, \ldots, H_{m+1}$ (hence in $\overline{H}$). Each H_i can be expressed as $H_i = A_{i,1} F_1 + \cdots + A_{i,m+1} F_{m+1}$. Since $A_{i,j}$ is often a big polynomial, the authors introduced ***u**-cofactors* as follows.

$$(a_{i,1}, \ldots, a_{i,m+1}) \;\stackrel{\text{def}}{=}\; (A_{i,1}, \ldots, A_{i,m+1})|_{\boldsymbol{x}=\boldsymbol{s}}, \tag{4}$$

where $\boldsymbol{s} = (s_1, \ldots, s_m) \in \mathbb{Z}^m$; we usually choose $\boldsymbol{s} = (0, \ldots, 0)$ if no polynomial of $\mathcal{F}$ disappears by this choice. On $\boldsymbol{u}$-cofactors , they proved the following proposition; see [12] for the proof.
Proposition 1: Let $(f_1, \ldots, f_{m+1}) := (F_1, \ldots, F_{m+1})|_{\boldsymbol{x}=\boldsymbol{s}}$. *If* $\overline{f} := \gcd(f_1, \ldots, f_{m+1})$ *is a non-numeric polynomial then* $\overline{f}$ *is a factor of* $\widehat{G}$. *Let* $\overline{a}_i := \gcd(a_{i,1}, \ldots, a_{i,m+1})$. *If* $\overline{a}_i$ *is a non-numeric polynomial then* $\overline{a}_i$ *is an extraneous factor of* $\overline{H}$ (hence not a factor of $\widehat{G}$) .

3 Explanation of current big problem by an example

Example $\mathcal{F}_{\mathrm{Ex1}}$ being used so far So far, we used the following example mainly:

$$\mathcal{F}_{\mathrm{Ex1}} = \begin{cases} F_1 \;=\; x^4\cdot(y{+}u) + x^2\cdot(y{-}2w) + (2u{+}w), \\ F_2 \;=\; x^4\cdot(\,y\,u\,) \;+ x^2\cdot(y{+}2w) + (3u{-}w), \\ F_3 \;=\; x^4\cdot(y{-}u) + x^2\cdot(2y{+}u) + (u{-}2w). \end{cases} \tag{5}$$

The Gröbner basis $\mathrm{GB}(\mathcal{F}_{\mathrm{Ex1}})$ contains 10 polynomials; we show only the last four.

$$\begin{array}{rcl} G_7 &=& 176158\cdots y^2w + y\times(286608\cdots w^7 - 2549237\,w^6 - 424132\,w^5 + \cdots - 659890\cdots w^3 + 239969\cdots w^2) \\ && +\, 985216\cdots u^6w^4 - \cdots + 686666\cdots u^5w^5 + \cdots - 642027\cdots u^4w^6 + \cdots - 358260\cdots u^3w^7 + \cdots + \cdots + \cdots, \\ G_8 &=& y\times(142799\cdots u - 168202\cdots w^7 + \cdots - 192531\cdots w^2 + 291426\cdots w) \\ && -\, 578194\cdots u^6w^4 + \cdots - 402984\cdots u^5w^5 + \cdots + 963657\cdots u^4w^6 + \cdots + 210252\cdots u^3w^7 + \cdots + \cdots + \cdots, \\ G_9 &=& y\times(48000\,w^8 - 419640\,w^7 - \cdots - 1041048\,w^2) \;+\; 6500\,u^6w^5 - 430980\,u^6w^4 - \cdots - 5430496\,w^3, \\ G_{10} &=& 33\,u^7 + 23\,u^6w - 126\,u^6 - 55\,u^5w^2 - 343\,u^5w + 316\,u^5 - 12\,u^4w^3 - 130\,u^4w^2 + 544\,u^4w - 202\,u^4 + 32\,u^3w^4 \\ && +\, 218\,u^3w^3 + 548\,u^3w^2 - 128\,u^3w + 144\,u^2w^4 + 428\,u^2w^3 - 420\,u^2w^2 + 144\,uw^4 - 256\,uw^3 - 32\,w^4. \end{array}$$

The numerical coefficients of $G_1 \sim G_8$ are of about 30 digits, and G_9 and G_{10} consist of 61 and 20 monomials, respectively. Note that G_{10} is simplest in both the number of terms and the coefficient size.

Unexpected difficulty happened in the computation of $\widetilde{G}_9$ The $\widetilde{G}_9$ is computed from three remainders of degree 1 in y, with leading coefficients $C_1, C_2, C_3 \in \mathbb{Z}[u,w]$. Since C_1, C_2, C_3 are of degrees $14, 12, 12$, respectively, w.r.t. u, each (R_j, C_j) was Mreduced as $(R_j, C_j) \xrightarrow{G_{10}}\!\!\!\!\rightarrow (R'_j, C'_j)$, which gives

$$\begin{array}{rcl} R'_1 &=& y\times(-349136896959\,u^6w^8 + \cdots + 249988316347584\,w^4) \\ &+& \quad(-915846376989\,u^6w^8 + \cdots - 417398434490880\,w^4), \end{array} \tag{6}$$

for example. Coefficients of both y^1- and y^0-terms consist of 68 monomials. Even by this Mreduction, the computation of PRSs and cofactors is quite expensive (computational difficulty). For example, a_1 and b_1 satisfying $c_1 := \mathrm{nmlastPRS}_u(C'_1, C'_2) = a_1C'_1 + b_1C'_2$ consist of 432 and 420 monomials, respectively, and $W'_1 := \mathrm{LCtoW}(c_1) = a_1R'_1 + b_1R'_2 \in \mathbb{Z}[y,u,w]$ consists of 1016 monomials.

The computational difficulty mentioned above will be reduced very much by devising efficient PRS algorithms. However, in [10], the author faced a theoretical difficulty, too; he found that, for each $j \in \{1,2,3\}$, G_9 was obtained as $W'_j \xrightarrow{G_{10}}\!\!\!\!\rightarrow W''_j \;\Rightarrow\; G_9 = W''_j/\mathrm{cont}_y(W''_j)$, but he could not give any theoretical justification of this. Without solving this problem, he could not advance anymore.

4 On LCtoW polynomial of second-lowest element of $\mathrm{GB}(\mathcal{F})$

We consider the computation of LCtoW polynomial for $\widetilde{G}_9$ in Example $\mathcal{F}_{\mathrm{Ex1}}$, with variable notations used in the example. Without changing the essence of computation, we set $\mathbb{K} = \mathbb{Z}_p$ with $p = 1073738843$, so as to simplify the outputs. Hence, given are $\{R_1, R_2, R_3\} \subset \mathbb{Z}_p[y,u,w]$, and $\{C_1, C_2, C_3\} \subset \mathbb{Z}_p[u,w]$, where, for each $j \in \{1,2,3\}$, $\deg_y(R_j) = 1$ and $C_j = \mathrm{lcf}_y(R_j)$. Furthermore, C_1, C_2, C_3 are mutually prime. We treat the case where both $\mathcal{R}$ and $\mathcal{C}$ have been Mreduced by G_{10}, so treat R'_j and C'_j. (If a polynomial P is Mreduced by G_{10} twice then we express the Mreduced polynomial as P'').

In our computation, a procedure `Mreduce` plays an important role. Given polynomials G and H, with $\deg(G) \ge \deg(H)$, expressed recursively w.r.t. their variables, `Mreduce`(G,H) performs successive Mreductions of G by H, $G \xrightarrow{H}\!\!\!\!\rightarrow R$, as if G and H are given in the monomial representation, and returns R by saving a polynomial Q satisfying $G = QH + R$. We express Q and R as `quopol`(G,H) and `rempol`(G,H), respectively.

4.1 Computation of LCtoW polynomial for $\widetilde{G}_9$ in Example $\mathcal{F}_{\mathrm{Ex1}}$

Let $c'_j := \mathrm{lastPRS}_u(C'_j, C'_{j+1})$, where $C'_4 = C'_1$. Then, we obtained

$$\left\{\begin{array}{rcl} c'_1 &=& 182913124\,w^{79} - 310233643\,w^{78} + \cdots + 301414704\,w^{11}, \\ c'_2 &=& 504782002\,w^{79} + 105447348\,w^{78} + \cdots + 465634055\,w^{11}, \\ c'_3 &=& -242692664\,w^{67} - 17207621\,w^{66} + \cdots + 211285272\,w^{11}, \end{array}\right. \tag{7}$$

and cofactors a'_j and b'_j satisfying $c'_j = a'_jC'_j + b'_jC'_{j+1}$. By these, we obtained $\overline{c}' := \gcd(c'_1, c'_2, c'_3)$ as follows (we set $\overline{c}'$ monic, because GCD modulo p can be determined only up to a numerical multiplier).

$$\begin{array}{rcl} \overline{c}' &=& w^{17} - 56371298\,w^{16} + 138243860\,w^{15} - 521121094\,w^{14} \\ && -\,96457750\,w^{13} - 382429906\,w^{12} - 247496825\,w^{11}. \end{array} \tag{8}$$

Secondly, we computed $W'_j := \mathrm{LCtoW}(c'_j) = a'_j R'_j + b'_j R'_{j+1}$. Thirdly, we computed $\overline{W}' := \mathrm{LCtoW}(\overline{c}')$, as follows. As for $\mathcal{F}_{\mathrm{Ex1}}$, we noticed that $\overline{c}' = \gcd(c'_i, c'_j) \in \mathbb{Z}_p[w]$ for $\forall i \neq \forall j$. This allows us to compute $\overline{c}'$ as $\overline{c}' := \mathrm{lastPRS}_w(c'_1, c'_2)$. Let the cofactors of $\overline{c}'$ thus computed be $\alpha'_1, \beta'_1 \in \mathbb{Z}_p[w]$, which satisfy $\overline{c}' = \alpha'_1 c'_1 + \beta'_1 c'_2$. Hence, we obtain $\overline{W}' = \alpha'_1 W'_1 + \beta'_1 W'_2$. We note that not only W'_j but also $\overline{W}'$ is in $\langle \mathcal{F}_{\mathrm{Ex1}} \rangle$, because $a'_j, b'_j \in \mathbb{Z}_p[u, w]$ and $\alpha'_1, \beta'_1 \in \mathbb{Z}_p[w]$.

Remark 2: *The above c'_1 and c'_2 are in $\mathbb{Z}_p[w]$, so are cofactors α'_1 and β'_1, too. Hence, we can compute both $\overline{c}'$ and (α'_1, β'_1) by the PRS method easily. In general case, although we have $\overline{c}' \in \mathbb{K}[w_1, \ldots, w_{n\geq 2}]$, we have $\alpha'_1, \beta'_1 \in \mathbb{K}(w_2, .., w_n)[w_1]$. In* **6.1**, *we will discuss this point in details. //*

The a'_j and b'_j are dense polynomials of degree 5 w.r.t. u and pretty large, making W'_j a big polynomial; for example, W'_1 consists of 1016 monomials. $\overline{W}'$ is a polynomial of the form $\overline{c}' y + \overline{W}'_0$, where $\overline{W}'_0 \in \mathbb{Z}_p[u, w]$, of degree 11 w.r.t. u. Hence, we Mreduce it by G_{10}, $\overline{W}'' := \mathtt{Mreduce}(\overline{W}', G_{10})$, obtaining

$$\begin{array}{rcl} \overline{W}'' & = & y \times (\quad w^{17} - 56371298\, w^{16} + \cdots - 247496825\, w^{11}) \\ & + & u^6 \times (503315083\, w^{14} + 511368115\, w^{13} + \cdots + 365540993\, w^9) \\ & + & u^5 \times (123032576\, w^{15} + 461931391\, w^{14} - \cdots + 29125264\, w^9) \\ \vdots & & \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ & + & u^0 \times (357912951\, w^{18} + 304225978\, w^{17} - \cdots - 342880717\, w^{12}). \end{array} \tag{9}$$

If we compute the above $\overline{W}''$ over $\mathbb{Z}$ then we have $\overline{W}'' = w^9 \times G_9$ (w^9 is the extraneous factor).

Summarizing the above derivation, we can express $\overline{W}''$ as follows.

$$\overline{W}'' = \mathtt{redpol}(\alpha'_1 \overline{W}'_1 + \beta'_1 \overline{W}'_2, G_{10}) = \mathtt{redpol}\big(\alpha'_1(a'_1 R'_1 + b'_1 R'_2) + \beta'_1(a'_2 R'_2 + b'_2 R'_3), G_{10}\big). \tag{10}$$

4.2 Surprising phenomenon observed on $\overline{W}''$ in (10)

How did the extraneous factor w^9 appear in $\overline{W}''$? We thought that two Mreductions by G_{10} created the factor. In order to check this expectation, we have computed $\mathtt{redpol}(u^i, G_{10})$ for $i = 7, \ldots, 11$, and recognized that the effect of the Mreduction was not large. In fact, we will see below that the Mreduction does not create the w^9 factor. Cofactors a'_j and b'_j have no common factor. In fact, the tuple (c'_j, a'_j, b'_j) has been normalized so that we have $\gcd(\mathrm{cont}_u(a'_j), \mathrm{cont}_u(b'_j)) = 1$. (Without this normalization, cofactors have a common factor w^{21} which has been removed by Theorem A.)

How can we remove the extraneous factor w^9 of $\overline{W}''$? The $\boldsymbol{u}$-cofactors method seems to be most hopeful; we can define $\boldsymbol{u}$-cofactors for $\overline{W}'$ and $\overline{W}''$ (the latter is obtained by Mreducing the former by G_{10}). We have computed $\boldsymbol{u}$-cofactors of $\overline{W}'$ and $\overline{W}''$; the former consists of 4746 monomials and the latter 2900 monomials. We found that the contents of these $\boldsymbol{u}$-cofactors w.r.t. u are 1, which means that Proposition 1 cannot remove any extraneous factor. We thought that our computation could be formulated by a determinant theory like the sub-resultant theory of two multivariate polynomials [6, 2, 3]. Developing such a theory seems to be quite difficult; see [9] for your reference. Thus, removing the w^9 factor was a big problem for us many months.

We have tested various possibilities. One day, observing $a'_j R'_j$ and $b'_j R'_{j+1}$ ($j \in \{1, 2\}$) separately, we found the following surprising fact; below, by $[P]'$ we denote the Mreduction of polynomial P by G_{10}.

$$\left\{ \begin{array}{ll} \mathtt{redpol}(a'_j R'_j, w) \not\equiv 0 \pmod{p}, & \mathtt{redpol}(b'_j R'_{j+1}, w) \not\equiv 0 \pmod{p}, \\ \mathtt{redpol}([a'_j R'_j]', w) \not\equiv 0 \pmod{p}, & \mathtt{redpol}([b'_j R'_{j+1}]', w) \not\equiv 0 \pmod{p}, \end{array} \right. \tag{11}$$

These relations tell that the Mreduction by G_{10} does not create the factor w^9. On the other hand, the $\overline{W}''$ in (9) and relations in (11) tell that, for $0 \leq \forall i \leq 9$, the w^i-terms of $a'_j R'_j$ and $b'_j R'_{j+1}$ (resp. $[a'_j R'_j]'$ and $[b'_j R'_{j+1}]'$) cancel one another in each coefficient w.r.t. u. That is, we have

$$\left\{ \begin{array}{rcl} \mathtt{redpol}(a'_j R'_j, w^9) & \equiv & -\mathtt{redpol}(b'_j R'_{j+1}, w^9) \pmod{p}, \\ \mathtt{redpol}([a'_j R'_j]', w^9) & \equiv & -\mathtt{redpol}([b'_j R'_{j+1}]', w^9) \pmod{p}. \end{array} \right. \tag{12}$$

Similar relations hold for $a'_j C'_j$ and $b'_j C'_{j+1}$; we omit them because of the page limit.

4.3 Removal of the extraneous factor w^9 of $\overline{W}''$ in (10)

Relations in (12) suggest us strongly that the term cancellations in the additions $\overline{W}'_j := a'_j R'_j + b'_j R'_{j+1}$ and $\overline{W}''_j := [a'_j R'_j]' + [b'_j R'_{j+1}]'$ occurred systematically. Systematic term-cancellations occur frequently in the PRS computation. However, the cancellations seem to be not reflected on $\boldsymbol{u}$-cofactors; in fact, what we have done on cofactors is only to make them relatively primitive by Theorem A. If this observation is correct, we must modify the $\boldsymbol{u}$-cofactors so as to reflect the systematic cancellations.

Lemma 1
The w^j-terms, $\forall j \le 9$, in the $\boldsymbol{u}$-cofactors of $\overline{W}'_j$ and $\overline{W}''_j$ can be cut off.

Proof It is enough to show that $\overline{W}'_j$ and $\overline{W}''_j$ are not changed by this cutoff. $\boldsymbol{u}$-cofactors of $\overline{W}'_j$, for example, are expressed by a function $U_{\mathrm{cof}}(\%P[1], \%P[2], \%P[3]) := a'_{j,1}\,\%P[1] + a'_{j,2}\,\%P[2] + a'_{j,3}\,\%P[3]$, satisfying $U_{\mathrm{cof}}(F_1, F_2, F_3) = \overline{W}'_j$, where $(a'_{j,1}, a'_{j,2}, a'_{j,3})$ is the tuple of $\boldsymbol{u}$-cofactors and each $\%P[i]$ is a system variable representing F_i. Since each $F_i(\mathbf{0}, u, w)$ has a w^0-term, all the w^j-terms, $j \le 9$, of $a'_{j,1}$, $a'_{j,2}$, $a'_{j,3}$ cancel each other if we substitute $F_i(\mathbf{0}, u, w)$ for $\%P[i]$, $1 \le \forall i \le 3$. This means that the w^j-terms, $j \le 9$, play no role in the $\boldsymbol{u}$-cofactors, so can be cut off. □

Now, we return back to the system $\mathcal{F}$ and put $(\boldsymbol{u}') := (u_2, .., n_n)$, for simplicity. Let the given remainder set be $\{R_1, \dots, R_l\} \subset \mathbb{K}[x_m, u_1, \boldsymbol{u}']$, with $l \ge 3$ and $\deg_{x_m}(R_1) = \cdots = \deg_{x_m}(R_l) = 1$. For $\forall j \in \{1, \dots, l\}$, let $C_j := \mathrm{lcf}_{x_m}(R_j) \in \mathbb{K}[u_1, \boldsymbol{u}']$ and compute $c_j := \mathrm{lastPRS}_{u_1}(C_j, C_{j+1}) \in \mathbb{K}[\boldsymbol{u}']$, with $C_{l+1} = C_1$, and $W_j := \mathrm{LCtoW}(c_j)$. Then, compute $\overline{c} := \gcd(c_1, \dots, c_l)$ and $\overline{W} := \mathrm{LCtoW}(\overline{c}) = \alpha_1 W_1 + \cdots + \alpha_l W_l$, where $\alpha_1, \dots, \alpha_l \in \mathbb{K}[\boldsymbol{u}']$ are determined to satisfy $\check{c}\,\overline{c} = \alpha_1 c_1 + \cdots + \alpha_l c_l$; for $\check{c}$, see **6.1**. If necessary, we Mreduce $\overline{W}$ by $\widehat{G}$: $\texttt{Mreduce}(\overline{W}, \widehat{G}) = \overline{W}'$. Then, similarly as in (10), we can express $\overline{W}'$ as $\overline{W}' = [\alpha_1 W_1 + \cdots + \alpha_l W_l]'$.

Proposition 2
Put $(\boldsymbol{u}') = (u_2, .., u_n)$. Let $\overline{f} := \gcd(f_1, \dots, f_{m+1})$, where $f_i := \mathrm{cont}_{u_1}(F_i(\mathbf{0}, u_1, \boldsymbol{u}'))$ for $i = 1, \dots, m+1$. If $\overline{f}$ and $\overline{W}'$ are such that, for each $i \in \{2, \dots, n\}$ and for at least one $j \in \{1, \dots, l\}$, we have

$$\begin{cases} \overline{f} \text{ is divisible by } u_i^{\overline{e}_i}, & \text{but not by } u_i^{\overline{e}_i+1}, \\ \texttt{redpol}(\overline{W}', u_i^{d_i}) \ne 0 & \text{for } \quad d_i = d_{i,\max}, \\ \texttt{redpol}(\overline{W}', u_i^{d_i}) = 0 & \text{for any } \quad d_i < d_{i,\max}, \\ \texttt{redpol}(\alpha_j R_j, u_i^{e_j}) \ne 0 & \text{for some } \quad e_j < d_{i,\max}. \end{cases} \tag{13}$$

Then, $\prod_{i=2}^{n} u_i^{d_{i,\max} - \overline{e}_i}$ is an extraneous factor of $\overline{W}'$.

Proof The top condition in (13) is the same as the first claim of Proposition 1 in **2**. Middle two conditions are for the above Lemma 1. The bottom condition is to confirm the cancellation of low u_i-power terms. Then, Lemma 1 allows us to cut off low-power part of $\boldsymbol{u}$-cofactors, so the second claim of Proposition 1 leads us to this proposition. □

Remark 3: *Contrary to Proposition 1 which requires expressions of $\boldsymbol{u}$-cofactors, Proposition 2 does not require $\boldsymbol{u}$-cofactors. Proposition 2 is available only if we know the cancellation of low u_i-power terms from $\overline{W}'$ and $\alpha_1 R_1, \dots, \alpha_l R_l$. //*

5 Utilizing intermediate elements of rctPRSs fully

First of all, we give a simple and widely usable theorem for the intermediate elements of the PRS.

Theorem 3
Assume that $\mathcal{F}$ is healthy. For each $i = 1, 2, \dots, m$, let the i-th PRS of the rectPRSs of $\mathcal{F}$ start from R_1 and R_2 in $\mathbb{K}[x_i, .., \boldsymbol{u}]$ and end at R_k in $\mathbb{K}[x_{i+1}, .., \boldsymbol{u}]$, where $x_{m+1} = nil$. Let R_j $(3 \le \forall j < k)$ be the j-th remainder of this PRS, and A_j, B_j be cofactors of R_j. If $A_j, B_j \in \mathbb{K}[x_i, .., \boldsymbol{u}]$ then $R_j \in \langle \mathcal{F} \rangle$. Furthermore, if $c := \gcd(\mathrm{cont}_{x_i}(A_j), \mathrm{cont}_{x_i}(B_j))$ is a non-numeric polynomial then $R_j / c \in \langle \mathcal{F} \rangle$.

Proof Since $R_j = A_jR_1 + B_jR_2$ and $R_1, R_2 \in \mathbb{K}[x_i, .., \boldsymbol{u}] \subset \mathbb{K}[\boldsymbol{x}, \boldsymbol{u}]$, the former part is obvious. The latter part of the theorem is a direct consequence of $R_j = A_jR_1 + B_jR_2$. □

Now, we consider the computation of lmn-multiples of elements G_8 and G_7 of GB($\mathcal{F}_{\rm Ex1}$), with variable notations used in $\mathcal{F}_{\rm Ex1}$, by setting $\mathbb{K} = \mathbb{Z}_p$ ($p = 1073738843$), as in **4**. We will see that our method based on the PRSs and GCDs are quite effective for these elements, too, and that our method will eliminate variables in the leading coefficients recursively. Furthermore, we will show in **5.2** very simple techniques for reducing the order of LCtoW polynomials quickly, without using Mreductions.

5.1 Computation of lmn-multiples of G_8 and G_7

We first consider G_8 of GB($\mathcal{F}_{\rm Ex1}$). For computing the G_9 in **4**, we used the remainders $R'_1, R'_2, R'_3 \in \mathbb{Z}_p[y, u, w]$, with $\deg_y(R'_j) = 1$, and their leading coefficients $C'_1, C'_2, C'_3 \in \mathbb{Z}_p[u, w]$, where $\deg_u(C'_j) = 6$. Then, in **4**, we have eliminated u by computing $c'_j := \mathrm{lastPRS}_u(C'_j, C'_{j+1})$, $(j = 1, 2, 3)$.

In order to compute an lmn-multiple of G_8, we utilize the same remainders R'_1, R'_2, R'_3 and the same leading coefficients $C'_1, C'_2, C'_3 \in \mathbb{Z}_p[u, w]$ as above. Furthermore, we compute $\mathrm{PRS}_u(C'_j, C'_{j+1})$ for each $j \in \{1, 2, 3\}$. However, in the case of G_8, we utilize the second-last element of the PRS, let it be $\widetilde{C}'_j$, such that $\widetilde{C}'_j = \widetilde{c}'_j u + \widetilde{c}'_{j,0}$, where $\widetilde{c}'_j, \widetilde{c}'_{j,0} \in \mathbb{Z}_p[w]$. For reference, we show $\widetilde{C}'_1, \widetilde{C}'_2, \widetilde{C}'_3$.

$$\left\{\begin{array}{rcl} \widetilde{C}'_1 &=& u\times(-400332453\,w^{83} - 486798555\,w^{82} + \cdots + 610926431\,w^{21}) \\ && (-847591772\,w^{83} - \;\; 61235712\,w^{82} - \cdots - 480188577\,w^{22}), \\ \widetilde{C}'_2 &=& u\times(-132983355\,w^{83} + 431258669\,w^{82} - \cdots - 1005915583\,w^{21}) \\ && (-319905788\,w^{83} - 433089862\,w^{82} - \cdots + \;670117391\,w^{22}), \\ \widetilde{C}'_3 &=& u\times(-619696314\,w^{73} - 749238305\,w^{72} + \cdots + 351193054\,w^{21}) \\ && (-504553108\,w^{73} - 211546057\,w^{72} - \cdots - 900386305\,w^{22}). \end{array}\right. \tag{14}$$

Let $\widetilde{a}'_j, \widetilde{b}'_j \in \mathbb{Z}_p[u, w]$ be the cofactors of $\widetilde{C}'_j$, satisfying $\widetilde{C}'_j = \widetilde{a}'_j C'_j + \widetilde{b}'_j C'_{j+1}$. At this point, we noticed that $\gcd(\widetilde{c}'_1, \widetilde{c}'_2) = \gcd(\widetilde{c}'_2, \widetilde{c}'_3) = \gcd(\widetilde{c}'_3, \widetilde{c}'_1) = w^{24}$ and that $\mathrm{cont}_u(\widetilde{a}'_j) = \mathrm{cont}_u(\widetilde{b}'_j) = w^{12}$ for each j. So, Theorem 3 allows us to replace $(\widetilde{C}'_j, \widetilde{a}'_j, \widetilde{b}'_j)$ by $(\widetilde{C}'_j/w^{12},\ \widetilde{a}'_j/w^{12},\ \widetilde{b}'_j/w^{12})$. The LCtoW polynomial for $\widetilde{C}'_j$ is given by $\widetilde{W}'_j := \widetilde{a}'_j R'_j + \widetilde{b}'_j R'_{j+1}$. For reference, we show $\widetilde{W}'_1$:

$$\begin{array}{rcl} \widetilde{W}'_1 &=& y\times[\; u\times(-\,400332453\,w^{71} - 486798555\,w^{70} + \cdots - 462812412\,w^{9}) \\ && \qquad + 226147071\,w^{71} + \;\; 61235712\,w^{70} + \cdots - 480188577\,w^{10}\;] \\ &+& u^{10}\times(-\,257318739\,w^{68} + 143266264\,w^{67} + \cdots - 292767155) \\ &+& u^{9}\times(-\,259677448\,w^{69} + 498387731\,w^{68} + \cdots - 201039176) \\ \vdots && \quad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \end{array} \tag{15}$$

This $\widetilde{W}'_j$ is a big polynomial, of degree 10 w.r.t. u, so we Mreduce it by G_{10}: $\widetilde{W}''_j := \mathtt{rempol}(\widetilde{W}'_j, G_{10})$. By this Mreduction, $\widetilde{W}'_1$ which consists of 908 monomials, for example, becomes $\widetilde{W}''_1$ consisting of 564 monomial. However, its coefficients w.r.t. u are still of high degrees.

The next step, which was the final step so far, is to compute an LCtoW polynomial $\overline{W}'' := \mathrm{LCtoW}(\overline{c})$, where $\overline{c} := \gcd(\widetilde{c}'_1, \widetilde{c}'_2, \widetilde{c}'_3) = w^{12}$. Since $\overline{c} = \gcd(\widetilde{c}'_1, \widetilde{c}'_2)$, we compute $\gamma := \mathrm{lastPRS}_w(\widetilde{c}'_1, \widetilde{c}'_3)$, for example. Let $\alpha, \beta \in \mathbb{Z}_p[w]$ be cofactors of γ, then we obtain $\overline{W}'' := \alpha\,\widetilde{W}''_1 + \beta\,\widetilde{W}''_3$.

$$\begin{array}{rcl} \overline{W}'' &=& y\times[\; u\times(-\,404859241\,w^{9}) \\ && \qquad -\,204727648\,w^{132} + 206842818\,w^{131} + \cdots + 103862554\,w^{10}\;] \\ &+& u^{10}\times(\;\;119889236\,w^{129} + \;\;55962549\,w^{128} + \cdots - 111119948) \\ &+& u^{9}\times(-\,377202328\,w^{130} + 508306222\,w^{129} + \cdots + 143418763) \\ \vdots && \quad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \end{array} \tag{16}$$

$\overline{W}''$ consists of 908 monomials; we surprise that the coefficients w.r.t. u are of very high degrees.

So, we simplify $\overline{W}''$ by G_9 and $G_{10}(=\widehat{G})$. We see that G_9 simplifies only the terms proportional to y and G_{10} does the terms proportional to u^7. By $\overline{W}'''$ we denote the result of these two Mreductions.

$$\begin{array}{rcl} \overline{W}''' & = & y\times[\,u\times(\ \ 356795158\,w^7 + \ 73463847\,w^6 + \cdots + 767455355\,w^2\,) \\ & & \qquad\qquad - 253977356\,w^7 - 607493081\,w^6 - \cdots + 745350398\,w^2\,)\,] \\ & + & u^6\times(\ \ 364685846\,w^4 + 395558891\,w^3 + \cdots - 226413303\,) \\ & + & u^5\times(-334168995\,w^5 + 111185898\,w^4 + \cdots + 962099779\,) \\ \vdots & & \vdots \qquad\qquad \vdots \qquad\qquad \vdots \end{array} \tag{17}$$

We surprise that the Mreductions by G_9 and G_{10} make $\overline{W}'''$ so simple; $\overline{W}'''$ consists of only 59 monomials. However, compared with G_8, we must decrease the order of $\overline{W}'''$ further, which will be done in **5.2**.
Remark 4: *Although the expression $\overline{W}'''$ is simple, an intermediate expression $\overline{W}''$ is very big. This is the intermediate expression growth which occurs often in the algebraic computation. In* **6.2**, *we present a tiny idea to suppress this intermediate expression growth. //*

5.2 Decreasing the leading monomials by leading-term elimination

We have seen that the Mreductions are very effective for reducing LCtoW polynomials. In this subsection, we show that the leading-term elimination is very effective for reducing the leading coefficients. Furthermore, we will compute an lmn-multiple polynomial $\widetilde{G}_7$ for G_7.

Our technique is to apply the leading-term elimination to $\overline{W}'''$ and $u\times G_9$. Let the yu-terms of $\overline{W}'''$ and $u\times G_9$ be $\overline{c}'''\times yu$ and $\widetilde{g}_9\times yu$, respectively, hence $\overline{c}''', \widetilde{g}_9 \in \mathbb{Z}_p[w]$, where $\deg_w(\overline{c}''') = 7$ and $\deg_w(\widetilde{g}_9) = 8$. Let $\widetilde{\gamma} := \mathrm{lastPRS}_w(\overline{c}''', \widetilde{g}_9)$ and $\widetilde{\alpha}, \widetilde{\beta}$ be cofactors of $\widetilde{\gamma}$, satisfying $\widetilde{\gamma} = \widetilde{\alpha}\,\overline{c}''' + \widetilde{\beta}\,\widetilde{g}_9$. We obtain $\widetilde{\gamma} = -39740130\,w^2$ and $\widetilde{W}''' := \widetilde{\alpha}\,\overline{W}''' + \widetilde{\beta}\,u\times G_9$ consisting of 108 monomials. Finally, Mreducing $\widetilde{W}'''$ by G_9 and G_{10}, we obtain $\widetilde{G}_8 := \texttt{redpol}(\widetilde{W}''', G_9, G_{10})$, as follows.

$$\begin{array}{rcl} \widetilde{G}_8 & = & y\times[\,u\times(-39740130\,w^2\,) \\ & & \qquad - 598398494\,w^7 + 512248306\,w^6 + \cdots - \ 5175136\,w^2\,] \\ & + & u^6\times(-272808160\,w^4 + 232623453\,w^3 + \cdots + 759618044\,) \\ & + & u^5\times(-255214102\,w^5 - 803994460\,w^4 + \cdots - 362431630\,) \\ \vdots & & \vdots \qquad\qquad \vdots \qquad\qquad \vdots \end{array} \tag{18}$$

$\widetilde{G}_8$ is our lmn-multiple of G_8. Note that $\mathrm{lmn}(\widetilde{G}_8) = \mathrm{const}\times w\,\mathrm{lmn}(G_8)$.

We will compute an lmn-multiple of G_7 from remainders $R_1, R_2, R_3 \in \mathbb{Z}[y,u,w]$, $\deg_y(R_j) = 2$, and their leading coefficients $C_1, C_2, C_3 \in \mathbb{Z}[u,w]$. (See [10] for rough expression of R_j.)

Let $c_j := \mathrm{lastPRS}_u(C_j, C_{j+1})$ $(j = 1,2,3)$ and $\overline{c} := \gcd(c_1, c_2, c_3)$.

$$\left\{\begin{array}{rcl} c_1 & = & -69120000000\,w^{15} + 770976000000\,w^{14} + \cdots - 170537400000\,w^5, \\ c_2 & = & -57600000000\,w^{17} + 712320000000\,w^{16} + \cdots - \ 46510200000\,w^5, \\ c_3 & = & -1440000000\,w^{14} + \ 15072000000\,w^{13} + \cdots + \ \ 5167800000\,w^5, \\ \overline{c} & = & \gcd(c_1, c_2, c_3) \ = \ c_3. \end{array}\right. \tag{19}$$

Using cofactors $a_3, b_3 \in \mathbb{Z}[u,w]$ of c_3, we computed $W_7 := \mathrm{LCtoW}(c_3) = a_3R_3 + b_3R_1 \in \mathbb{Z}[y,u,w]$, and found that $\texttt{redpol}(a_3R_3 + b_3R_1, w^5) \neq 0$ and $\texttt{redpol}(a_3R_3 + b_3R_1, w^5) \neq 0$. Hence, the method of extraneous-factor removal described in **4.2** failed in this case. This is reasonable because Theorem B is not used in the above W_7.

Fortunately, we can compute an lmn-multiple of G_7, similarly as we have computed the lmn-multiple polynomial $\widetilde{G}_8$ of G_8 above. Let $c_9 := \mathrm{lcf}_y(G_9)$ and $\widetilde{c}_7 := \mathrm{lcf}_y(W_7)/100$. For reference, we show $\widetilde{c}_7$:

$$\widetilde{c}_7 \ = \ - \ 14400000\,w^{14} + 150720000\,w^{13} - 2040884700\,w^{12} - 195976380\,w^{11} + \cdots + 51678000\,w^5. \tag{20}$$

We compute the GCD of $\widetilde{c}_7$ and c_9 by the PRS method, obtaining $\gamma := \gcd(\widetilde{c}_7, c_9) = 260166204\,w^2$ and its cofactors $\alpha, \beta \in \mathbb{Z}[w]$ satisfying $\alpha\,\widetilde{c}_7 + \beta\,c_9 = \gamma$. Since $W_7 = \widetilde{c}_7\,y^2 + y^1\text{-terms} + y^0\text{-terms}$ and

$G_9 = c_9\, y + y^0$-terms, we can decrease the order of W_7 by G_9 as $\widetilde{G}_7 := \alpha\, W_7 + \beta\, y \times G_9$, where $\widetilde{G}_7$ is as follows.

$$
\begin{array}{rcl}
\widetilde{G}_7 & = & y^2 \times (\ \ 260166204\, w^2\ ) \\
& + & y^1 \times [\ u^6 \times (\ \ 890901532\, w^{16} + \cdots + 736495066\, w - 263471195\ ) \\
& & \quad + u^5 \times (-360952533\, w^{17} + \cdots - 539864510\, w - 470888958\ ) \\
& \vdots & \qquad \vdots \qquad\qquad\qquad \vdots \qquad\qquad] \\
& + & y^0 \times [\ u^6 \times (\ \ 890901532\, w^{16} + \cdots + 736495066\, w - 263471195\ ) \\
& & \quad + u^5 \times (-360952533\, w^{17} + \cdots - 539864510\, w - 470888958\ ) \\
& \vdots & \qquad \vdots \qquad\qquad\qquad \vdots \qquad\qquad].
\end{array}
\tag{21}
$$

$\widetilde{G}_7$ is our lmn-multiple of G_7. Note that $\mathrm{lcf}(\widetilde{G}_7) = \mathrm{const} \times y^2 w^2$, while $\mathrm{lcf}(G_7) = \mathrm{const} \times y^2 w$.

6 Various theoretical and computational considerations

6.1 On LCtoW polynomials of many sub-variables

In this sub-section, we use the variables notations $\boldsymbol{x}$ and $\boldsymbol{u}$ for $\mathcal{F}$, with $n \geq 3$, and put $(\boldsymbol{u}') := (u_2, .., u_n)$, $(\boldsymbol{u}'') := (u_3, .., u_n)$. For $1 \leq \forall j \leq l$, we express the remainder by $R_j \in \mathbb{K}[x_m, \boldsymbol{u}]$, $C_j = \mathrm{lcf}_{x_m}(R_j) \in \mathbb{K}[\boldsymbol{u}]$, $c_j = \mathrm{nmlastPRS}_{u_1}(C_j, C_{j+1}) \in \mathbb{K}[\boldsymbol{u}']$, $\overline{c} = \gcd(c_1, \ldots, c_l) \in \mathbb{K}[\boldsymbol{u}']$, and $\mathrm{LCtoW}(\overline{c})$, as in **4**.

1) We discard Proposition 1 in page 31 of the paper [10], because it is useless.

2) If $n \geq 4$, we can eliminate u_2 of the set $\{c_1, \ldots, c_l\}$ as $\gamma_j = \mathrm{nmlastPRS}_{u_2}(c_j, c_{j+1})$ $(1 \leq j \leq l)$. This will give LCtoW polynomials with leading monomials $x_m u_2^{e_2}, x_m u_3^{e_3}, \cdots$.

3) As we mentioned in **4.1**, if $n \geq 3$, we must be careful in computing $\mathrm{LCtoW}(\overline{c})$. If we set the leading coefficient of $\mathrm{LCtoW}(\overline{c})$ to $\overline{c}$ then many coefficients of the LCtoW polynomial become rational functions in $\boldsymbol{u}''$. In this sub-section, we clarify this point in details, and show how to compute LCtoW polynomials with polynomial coefficients. It must be noted first that we compute $\gcd(c_1, \ldots, c_l)$ $(l \geq 3)$ by repeating two-argument GCDs as follows: $\overline{c}_{1,j} := \gcd(c_1, c_j)$ $(j \in \{2, .., l\}) \Rightarrow \overline{c}_{1,2,j} := \gcd(\overline{c}_{1,2}, \overline{c}_{1,j})$ $(j \in \{3, .., l\})$, and so on.

We assume that $c_1, c_2 \in \mathbb{K}[\boldsymbol{u}']$ are made primitive w.r.t. u_2, i.e., $\mathrm{cont}_{u_2}(c_1) = \mathrm{cont}_{u_2}(c_2) = 1$, and $\overline{c} := \gcd(c_1, c_2)$ is such that $\deg_{u_2}(\overline{c}) < \min(\deg_{u_2}(c_1), \deg_{u_2}(c_2))$. (If the last condition is not satisfied, the situation is trivial.) Below, we consider computing $\overline{c}$ and try to find $\overline{\alpha}_1, \overline{\alpha}_2 \in \mathbb{K}[\boldsymbol{u}']$ satisfying $\overline{\alpha}_1\, c_1 + \overline{\alpha}_2\, c_2 = \overline{c}$ (this turns out to be impossible).

We compute $\overline{c}$ efficiently by the EZGCD algorithm [8]. Since $\check{c}_1 := c_1/\overline{c}$ and $\check{c}_2 := c_2/\overline{c}$ are in $\mathbb{K}[\boldsymbol{u}']$ and relatively prime, we can eliminate u_2 of system $\{\check{c}_1, \check{c}_2\}$ by the PRS method. Thus, we obtain $\check{c} := \mathrm{nmlastPRS}_{u_2}(\check{c}_1, \check{c}_2) \in \mathbb{K}[\boldsymbol{u}'']$ and its cofactors $\check{\alpha}_1, \check{\alpha}_2 \in \mathbb{K}[\boldsymbol{u}']$, satisfying $\check{c} = \check{\alpha}_1 \check{c}_1 + \check{\alpha}_2 \check{c}_2$. This equality gives us $\overline{c} = (\check{\alpha}_1/\check{c}) \times c_1 + (\check{\alpha}_2/\check{c}) \times c_2$. Thus, unless $\check{c} \in \mathbb{K}$, we must introduce rational functions of denominator $\check{c}$. On the other hand, it gives the following proposition at once.

Proposition 4
Let $W_1, W_2 \in \mathbb{K}[x_m, \boldsymbol{u}]$ be LCtoW polynomials of c_1 and c_2, respectively. Computing $\mathrm{LCtoW}(\overline{c})$ as

$$
\mathrm{LCtoW}(\overline{c}) := \check{c} \times (\check{\alpha}_1\, W_1 + \check{\alpha}_2\, W_2), \tag{22}
$$

we obtain $\mathrm{LCtoW}(\overline{c})$ in $\mathbb{K}[x_m, \boldsymbol{u}]$. □

6.2 On enhancing PRS and extended PRS algorithms

In our method, the most expensive operation is the computation of resultants and their cofactors. We have so far developed an efficient PRS algorithm by utilizing the power-series [9], however, its efficiency is never satisfiable. We are now developing several other methods.

Here, we present a tiny idea. In **5.1**, we have faced very large polynomials, $\widetilde{\widetilde{W}}{}_1'$ in (15) and $\overline{W}''$ in (16), etc. They were generated by eliminating variable u from $C_1', C_2', C_3' \in \mathbb{Z}_p[u, w]$, where each C_j' is of degree 6 w.r.t. u; see R_1' in (6), where $C_1' = \mathrm{lcf}_y(R_1')$. However, these polynomials were made quite small by Mreductions by G_{10} (and G_9). Then, the u-elimination process will be enhanced much if we apply the Mreductions each time the elimination decreases the degree of u by 1.

6.3 On treatment of systems of many main-variables

Our current scheme eliminates the main variables $x_1, \ldots, x_m$ at once. This will give m very big resultants. If $m \geq 3$, we should employ "divide-conquer elimination" which we have proposed in [10].

6.4 On treatment of non-healthy systems

One may think that the treatment of non-healthy systems will be difficult, which is wrong, although the implementation will be complicated. Non-healthy systems cause only branching of the control of computation. The scheme of our computation is based on the PRS, and the PRS computation branches off by whether its arguments are relatively prime or not. The resultant of PRS branches off by whether the case iii) specified in **1** occurs or not.

Acknowledgements

This work was supported by Japan Society for Promotion of Science (Grant number 18K03389), and partly by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

References

[1] W.S. Brown: On Euclid's algorithm and the computation of polynomial greatest common divisors. JACM **18**(4), 478-504 (1971).

[2] W.S. Brown and J.F. Traub: On Euclid's algorithm and the theory of subresultants. JACM **18**(4), 505-515 (1971).

[3] W.S. Brown: The subresultant PRS algorithm. ACM TOMS **4**, 237-249 (1978).

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

[5] B. Buchberger: Gröbner bases: an algorithmic methods in polynomial ideal theory. *Multidimensional Systems Theory*, Chap. 6. Reidel Publishing (1985).

[6] G.E. Collins: Subresultants and reduced polynomial remainder sequences. JACM **14** 128-142 (1967).

[7] D. Kapur: Algebraic elimination methods. Tutorial paper to ISSAC '95. Mail to kapur@cs.albany-edu.

[8] J. Moses and D.Y.Y. Yun. The EZ GCD algorithm. Proc. 1973 ACM Annual Conference, 159-166, ACM (1973).

[9] T. Sasaki: A theory and an algorithm for computing sparse multivariate polynomial remainder sequence. In: Computer Algebra in Scientific Computing, Springer LNCS **11077**, 345-360 (2018).

[10] T. Sasaki: An attempt to enhance Buchberger's algorithm by using remainder sequences and GCD operation. In: SYNASC 2019, IEEE Conference Publishing Services, 27-34 (2020).

[11] T. Sasaki and D. Inaba: Simple relation between the lowest-order element of ideal $\langle G, H \rangle$ and the last element of polynomial remainder sequence. In: SYNASC 2017, IEEE Conference Publishing Services, 55-62 (2018).

[12] T. Sasaki and D. Inaba: Computing the lowest order element of the elimination ideal of multivariate polynomial system by using remainder sequence. In: SYNASC 2018, IEEE Conference Publishing Services, 37-44 (2019).