A Bridge between Euclid and Buchberger

(An attempt to enhance Gröbner basis algorithm by PRSs (Poly.Rem.Seq.) and GCDs (Great.Com.Div.))

Tateaki Sasaki (Univ. Tsukuba, Japan)

Outline of Talk

1) Variable Elimination **:** **PRS-method** vs **GB-method** (lexico.-order Gröbner Basis)

2) **2**-polynomial system **:** PRS-method ⇒ **lowest**$(\langle G, H\rangle)$

3) $\boldsymbol{n}$-polynomial system **:** **healthy** system ⇒ **Theorem 2**

4) **rectangular PRSs** ⇒ **extraneous factor** removal

5) Elimination of Lead.Coeff-vars ⇒ **LCtoW** polynomial

By Euclid, we mean following Two

- **Euclidean** Method for $\boldsymbol{G}, \boldsymbol{H} \in \mathbb{K}[x, \boldsymbol{u} = u_1, \ldots, u_n]$

  $P_1 := G,\ P_2 := H$, where $\deg_x(G) \geq \deg_x(H) \geq 1$,

  $\boldsymbol{P_{i+1} := (\alpha_i P_{i-1} - Q_i P_i)/\beta_i}$, $\boldsymbol{\alpha_i, \beta_i} \in \mathbb{K}[\boldsymbol{u}]$,

  $\deg_x(P_{i+1}) < \deg_x(P_i),\ P_k \neq 0,\ P_{k+1} = 0$,

  $\boldsymbol{\alpha_i, \beta_i}$ are so chosen that $\boldsymbol{P_{i+1}} \in \mathbb{K}[x, \boldsymbol{u}]$.

- **Extended** Euclidean algorithm for $\boldsymbol{A_i}, \boldsymbol{B_i} \in \mathbb{K}[x, \boldsymbol{u}]$,

  satisfying $\boldsymbol{A_i G + B_i H = P_i}$, $(i = 2, 3, \ldots, k-1)$,

  $\boldsymbol{A_{i+1} := (\alpha_i A_{i-1} - Q_i A_i)/\beta_i}$, $A_1 = 1,\ A_2 = 0$,

  $\boldsymbol{B_{i+1} := (\alpha_i B_{i-1} - Q_i B_i)/\beta_i}$, $B_1 = 0,\ B_2 = 1$.

  $\boldsymbol{(A_i, B_i)}$ is **uniquely determined** if we fix $\boldsymbol{P_i}$.

Histrory of Variable Elimination

(Sasaki's personal view)

(Given $\{F_1, \ldots, F_{m+1}\} \in \mathbb{K}[x = x_1, .., x_m, u]$, eliminate $x_1, .., x_m$ of $\{F_1, \ldots, F_{m+1}\}$, if possible)

Takakazu Seki (Japan) : multivariate **resultant,determinant** (with Tanaka et al.) (1674∼1685) **discriminant** (with Tatebe) (∼1685)

I. Newton, L. Euler : elimination method for 2-polynomial system (Newton:1707, Euler:1748)

E. Bézout : variable elimination method (1764) similar to that by Seki et al.

J.J. Sylvester : determinant for uni-var elimi. (1840)

F.S. Macaulay, A.L. Dixon et al. : determinants for m-var elimination (Macaulay:1902,16, Dixson:1908) <u>monomials in x</u>, <u>polynoms. in u</u> encounter **extraneous factors**

B. Buchberger (1965) : theory & algorithm of Gröbner basis ∴ <u>monomials in both x and u</u> ♠ gives **lowest-order resultant**

J.E. Collins, W.S. Brown : subresultant PRS algorithm**:** elimi. main var. (Collins:1967,Brown:1978) & extended PRS**:** $A_k G + B_k H = P_k$

D. Lazard ('83) : matrix: <u>all possible monos in column</u> apply Gaussian elimination to it

D. Kapur et al. (1990s) : revival of **sparse resultants** of Mcaulay, Dixon, et al. <u>**extraneous factors** still remain</u>

Lead.-Mono. vs Lead.-Term Eliminations

(Ref. Knuth-Bendix (1967))

(**Mono**mial)

GB : **Mono Repr**esentat. & **Lead.-mono Elim**ination

$$\boldsymbol{F(x) = c_1 M_1(x) + \cdots + c_m M_m(x)}$$

$$\boldsymbol{M(x) = x_1^{e_1} \cdots x_n^{e_n}}, \ M_1 \succ \cdots \succ M_m$$

$$\mathbf{Spol}(\boldsymbol{F, F'}) = \boldsymbol{(c'_1 M'_1 / C)\, F - (c_1 M_1 / C)\, F'}$$

where $\boldsymbol{C} = \mathbf{gcd}(\boldsymbol{c_1 M_1, c'_1 M'_1})$

(**Recur**sive)

PRS : **Recu. Repr**esentat. & **Lead.-term Elim**ination

$$\boldsymbol{F(X, u) := f_d(u) X^d + \cdots + f_0(u) X^0}$$

$$\mathbf{Elim}(\boldsymbol{F, F'}) := \boldsymbol{(f'_{d'} / \gamma)\, F - X^{d-d'} (f_d / \gamma) F'}$$

where $d \geq d'$, $\quad \boldsymbol{\gamma} = \mathbf{gcd}(\boldsymbol{f_d(u), f'_{d'}(u)})$

Coefficients of Generators (new name)

PRS: $\boldsymbol{P_k} := \mathbf{lastPRS}_x(G, H) = \boldsymbol{A_k} G + \boldsymbol{B_k} H$ **:**

$$P_k \in \mathbb{K}[\boldsymbol{u}] \Rightarrow \begin{cases} \mathbf{deg}_{\boldsymbol{x}}(\boldsymbol{A_k}) < \mathbf{deg}_{\boldsymbol{x}}(\boldsymbol{H}) \\ \mathbf{deg}_{\boldsymbol{x}}(\boldsymbol{B_k}) < \mathbf{deg}_{\boldsymbol{x}}(\boldsymbol{G}) \end{cases}$$

GB: $\boldsymbol{\widehat{S}} :=$ **lowest** element of **GB**$(\{G, H\})$

$$= \boldsymbol{\widetilde{A}}\, G + \boldsymbol{\widetilde{B}}\, H \ \textbf{:}$$

$$\widehat{S} \in \mathbb{K}[\boldsymbol{u}] \Rightarrow \begin{cases} \mathbf{deg}_{\boldsymbol{x}}(\boldsymbol{\widetilde{A}}) \not< \mathbf{deg}_{\boldsymbol{x}}(\boldsymbol{H}) \\ \mathbf{deg}_{\boldsymbol{x}}(\boldsymbol{\widetilde{B}}) \not< \mathbf{deg}_{\boldsymbol{x}}(\boldsymbol{G}) \end{cases}$$

GB: **in general**, for **GB**$(\{F_1, \ldots, F_{m+1}\})$ **:**

$$\widehat{S} = \boldsymbol{\widetilde{A}_1} F_1 + \cdots + \boldsymbol{\widetilde{A}_{m+1}} F_{m+1}$$

2-Pol. System : Compare GB vs PRS

(GBmethod(**Mathematica**) vs **PRS**method(**GAL**))
(data by **Inaba**) (in **Sasaki** Lab.)

Ex2017:
$$\begin{cases} G &= X^6\,(u+2v+w) + X^4\,(u-2x-z) \\ &\quad + X^2\,(v+3y-z) + (v+2w+y), \\ H &= X^6\,(v-w+2x) - X^4\,(v+y-2z) \\ &\quad + X^2\,(w-2x+y) + (u-v+2z). \end{cases}$$

Ex-6: $(G_6, H_6) := (G, H)$,
Ex-5: $(G_5, H_5) :=$ replace (z) by (w) in (G, H)
Ex-4: $(G_4, H_4) :=$ replace (y, z) by (v, w) in (G, H)
Ex-3: $(G_3, H_3) :=$ replace (x, y, z) by (u, v, w) in (G, H)

♠ GB vs PRS : Lowest$(\langle G, H\rangle) \Leftrightarrow P_k$

(Table from S&Inaba (2017))

	GB(lex) time (**msec**)	**sparsePRS** with A'_k & B'_k M-time	G-time	#(P'_k)	#(P_k)
Ex-3	46.33	78.0	5.27	**65**	**28**
Ex-4	12040.	218.	18.64	**279**	**81**
Ex-5	>90 min	749.	65.47	**961**	**201**
Ex-6	>90 min	2246.	224.8	**2815**	**445**

GB(lex) : reduced **G**röbner **B**asis (lex. term-order)
M-time : ⇐ programed in Mathematica language
G-time : ⇐ programed in LISP language of GAL
#(P'_k, P_k) : **#mono**(**with,without**) extran.-factor

A Relation between Two Eliminations

(assume $\mathbf{ltm}(\boldsymbol{H}) \nmid \mathbf{ltm}(\boldsymbol{G})$)

Lemma 1

Let $\deg(G) \geq \deg(H) \geq 1$. Let $\boldsymbol{E}_1$ be $\underline{\mathrm{LtmElim}(G,H)}$. Let $\widehat{\boldsymbol{E}}_1$ be the **lowest** polynom., obtained by decreasing **degree** of G to $\deg(E_1)$ by $\underline{\text{leading-monomial eliminatn}}$, where only $\mathbf{ltm}(\boldsymbol{G})$ & $\mathbf{ltm}(\boldsymbol{H})$ are used in elimination. Then, $\boldsymbol{E}_1$ is **a constant multiple** of $\widehat{\boldsymbol{E}}_1$.

Proof Both are lowest-order polynomials and unique. □

We show a simple example

$$\begin{cases} G = \underline{x^4\cdot(y+u)} + x^2\cdot(y-2w) + (2u+w), \\ H = \underline{x^4\cdot(y-w)} + x^2\cdot(2y+u) + (u-2w). \end{cases}$$

$\mathbf{LtmElim}(\boldsymbol{G},\boldsymbol{H})$ gives $\boldsymbol{E}_1$ as follows :

$\mathrm{lcf}(G) = y+u,\ \ \mathrm{lcf}(H) = y-w,\ \ \gamma = \gcd(y+u, y-w) = 1,$

$\mathbf{LtmElim}(\boldsymbol{G},\boldsymbol{H}) = \underline{(y-w)}\times G - \underline{(y+u)}\times H \implies \boldsymbol{E}_1 :=$

$\quad \underline{(y-w)}[x^2\,(y-2w) + (2u+w)] - \underline{(y+u)}[x^2\,(2y+u) + (u-2w)]$

Leading-mono eliminations give $\widehat{\boldsymbol{E}}_1$ as follows :

(we put $\boldsymbol{R_G} := \mathbf{rest}(\boldsymbol{G})$ and $\boldsymbol{R_H} := \mathbf{rest}(\boldsymbol{H})$)

$\boldsymbol{G} = \underline{x^4y} + \underline{x^4u} + R_G, \qquad \boldsymbol{H} = \underline{x^4y} - \underline{x^4w} + R_H,$

$\mathbf{Spol}(\boldsymbol{G},\boldsymbol{H}) = G - H = \underline{x^4u} + \underline{x^4w} + R_G - R_H \ \Rightarrow\ \boldsymbol{G}_3,$

$\mathbf{Spol}(\boldsymbol{G},\boldsymbol{G}_3) = -\underline{x^4yw} + \underline{x^4u^2} - (y-u)\,R_G + (y+w)\,R_H$

$\qquad \xrightarrow{H} \underline{x^4u^2} - \underline{x^4w^2} - (y-u)\,R_G + (y+w)\,R_H$

$\qquad \xrightarrow{G_3}\!\!\to\ -(y-w)\,R_G + (y+u)\,R_H \ \Rightarrow\ \widehat{\boldsymbol{E}}_1,$

$\mathbf{Spol}(\boldsymbol{H},\boldsymbol{G}_3) = \cdots \xrightarrow{G}\ -(y-w)\,R_G + (y+u)\,R_H = \widehat{\boldsymbol{E}}_1.$

PRS-method Computes lowest($\langle G, H \rangle$) without Computing any S-polynomial

Theorem 1 (S&I 2017)

Let $G, H \in \mathbb{K}[X, u]$ be relatively prime, $P_k \in \mathbb{K}[u]$ be the last element of PRS(G, H), $A_k, B_k \in \mathbb{K}[X, u]$ satisfy $A_k G + B_k H = P_k$ & **degree conditions** $\deg(A_k) < \deg(H), \deg(B_k) < \deg(G)$. Then, we have $P_k \,/\, \mathrm{gcd}(\mathrm{cont}_X(A_k), \mathrm{cont}_X(B_k)) = c\,\widehat{S}$, $c \in \mathbb{K}$, where, $\widehat{S}$ is the lowest element of $\mathrm{GB}(\{G, H\})$.

$*$) $\mathrm{cont}(F) = \mathrm{gcd}(f_d, \ldots, f_0)$ for $F = f_d X^d + \cdots + f_0$

Outline of Proof

1) Let $\widetilde{A}G + \widetilde{B}H = \widehat{S} \Longleftarrow$ Buchberger's method,
$\deg(\widetilde{A}) > \deg(H)$, $\deg(\widetilde{B}) > \deg(G)$, in general.

2) **Show** that we **can decrease** $\deg(\widetilde{A})$ and $\deg(\widetilde{B})$.
Easy when $\gamma := \mathrm{gcd}(\mathrm{lcf}(G), \mathrm{lcf}(H)) = 1$
$\Rightarrow$ **next screen** ($\mathrm{lcf}(F)$: leading-coefficient)

3) **else Show** that factors of γ **move** to $\widetilde{A}, \widetilde{B}$ as x_1**-elimination** proceeds $\Rightarrow$ **2-next screen**
(Lemma 1 $\Rightarrow$ we treat A_i, B_i $(i \le k)$ instead of $\widetilde{A}_i, \widetilde{B}_i$)

Detail of Proof : Case of $\gamma = 1$

(for $\widetilde{A}_{k+j}, \widetilde{B}_{k+j}$ $(j \geq 1)$)

Assuming $\mathbf{deg}(\widetilde{A}G) = \mathbf{deg}(\widetilde{B}H) \geq \mathbf{deg}(GH)$, consider **ltm** (= **leading-term**) of l.h.s. of $(*)$ $\widetilde{A}G + \widetilde{B}H = \widehat{S}$.
$\gamma = 1 \;\Rightarrow\; q_A := \mathrm{ltm}(\widetilde{A})/\mathrm{ltm}(H), q_B := \mathrm{ltm}(\widetilde{B})/\mathrm{ltm}(G)$ are polynoms. Put $\widetilde{A} = q_A H + \widetilde{A}'$, $\widetilde{B} = q_B G + \widetilde{B}'$, where $\widetilde{A}' = \mathrm{rest}(\widetilde{A}) - q_A \,\mathrm{rest}(H)$ & $\widetilde{B}' = (\cdots)$, we see $q_A + q_B = 0$, $\mathbf{deg}(\widetilde{A}') < \deg(\widetilde{A})$, $\mathbf{deg}(\widetilde{B}') < \deg(\widetilde{B})$.
Substituting these into $(*)$, we get $\widetilde{A}'G + \widetilde{B}'H = \widehat{S}$.
Repeating this, we attain the proof. $\square$

Detail of Proof : Case of $\gamma \neq 1$

(for A_i, B_i $(i \leq k)$ rare detail is omitted)

Consider the formulas on **PRS** and related A_i (& B_i) **:**

$$P_{i+1} := (c_i/\gamma_i)P_{i-1} - (c_{i-1}/\gamma_i)X^{d_i}P_i, \quad i = 2, 3, \cdots$$
$$A_{i+1} := (c_i/\gamma_i)A_{i-1} - \underline{(c_{i-1}/\gamma_i)X^{d_i}A_i}, \quad A_1 = 1, A_2 = 0$$
$$\gamma_i = \mathbf{gcd}(c_{i-1}, c_i),\; c_i = \mathbf{lcf}(P_i),\; d_i = \mathbf{deg}(P_{i-1}) - \mathbf{deg}(P_i)$$

Let $\hat{\gamma}$ be a factor of γ, and consider that $\hat{\gamma}$ is **contained** in c_{i-1} but **not** in c_i $\Rightarrow$ (c_{i-1}/γ_i) **contains** $\hat{\gamma}$.
This means that $\hat{\gamma}$ is **moved** to the leading-term of A_{i+1}, because $\mathbf{ltm}(A_{i+1}) = -\mathbf{ltm}((c_{i-1}/\gamma_i)X^{d_i}A_i)$.
Since $\hat{\gamma} \to 1$ as $i \to k$, we attain the proof. $\square$

Main Target : Many-Polynom. System

$$\mathcal{F} := \{F_1(\boldsymbol{x},\boldsymbol{u}), \cdots, F_{m+1}(\boldsymbol{x},\boldsymbol{u})\}, \quad m \geq 2$$
$$(\boldsymbol{x}) = (x_1, \ldots, x_m), \quad (\boldsymbol{u}) = (u_1, \ldots, u_n)$$
$$x_1 \succ \cdots \succ x_m \;\succ\; u_1 \succ \cdots \succ u_n$$

Coefficients of Generators (CofG in short)

$A_1, \ldots, A_{m+1} \in \mathbb{K}[\boldsymbol{x},\boldsymbol{u}]$, satisying,

$$A_1F_1 + \cdots + A_{m+1}F_{m+1} = R \in \mathbb{K}[\boldsymbol{u}]$$

Coefficients of Generators in $\boldsymbol{u}$ (CofG$\boldsymbol{u}$)

$$(a_1, \ldots, a_{m+1}) = (A_1, \ldots, A_{m+1})|_{\boldsymbol{x}\,=\,\boldsymbol{0}}$$

Many-Pol. Systems are Complicated

- **ALL variables** ($\boldsymbol{x}$ & $\boldsymbol{u}$) are eliminated
  if $F_i = F_j + 1$ for some $i \neq j$
- **NONE** of $x_1, \ldots, x_m$ is eliminated
  if $F_i = G(x)F_i'$ for $\forall i$
- At least one of $x_1, \ldots, x_m$ is **NOT** eliminated
  if $F_i = aF_j + bF_k \quad (i \neq j \neq k)$
- and so on

We want to treat these systems **simply**
Pathological systems $\Rightarrow$ **exceptional** cases.

Check Extran. Factor by Example

(we will use this **EXAMPLE** often)

$$\mathcal{F}_{2018} = \begin{cases} F_1 &= x^4\cdot(y+u) + x^2\cdot(y-2w) + (2u+w), \\ F_2 &= x^4\cdot(\,y\,u\,) \;+ x^2\cdot(y+2w) + (3u-w), \\ F_3 &= x^4\cdot(y-u) + x^2\cdot(2y+u) + (u-2w). \end{cases}$$

$$\begin{aligned} \widehat{S} \; = \; & 33\,\boldsymbol{u^7} + 23\,u^6w - 126\,u^6 - 55\,u^5w^2 - 343\,u^5w + 316\,u^5 - 12\,u^4w^3 \\ & - 130\,u^4w^2 + 544\,u^4w - 202\,u^4 + 32\,u^3w^4 + 218\,u^3w^3 + 548\,u^3w^2 \\ & - 128\,u^3w - 144\,u^2w^4 + 428\,u^2w^3 - 420\,u^2w^2 + 144\,uw^4 - 256\,uw^3 \\ & - 32\,w^4. \end{aligned}$$

Is Theorem 1 EFFECTIVE for $\mathcal{F}$?

$\widehat{\spadesuit}$: Wow, Extraneous Factor is Big!

$$G_2 := \mathbf{res}_{\boldsymbol{x}}(F_1, F_2),\; G_3 := \mathbf{res}_{\boldsymbol{x}}(F_1, F_3) \quad (\Leftarrow \textbf{eliminate } \boldsymbol{x})$$

$$\Rightarrow \quad H_3 := \mathbf{res}_{\boldsymbol{y}}(G_2, G_3) \quad (\Leftarrow \textbf{eliminate } \boldsymbol{y})$$

$$\boldsymbol{H_3} = \widehat{\boldsymbol{S}} \times \boldsymbol{u^2} \times \boldsymbol{E_3}, \quad \text{where}$$

$$\begin{aligned} \boldsymbol{E_3} \; = \; & 704\,u^{12} + 1664\,u^{11}w - 3568\,u^{11} + 720\,u^{10}w^2 - 2624\,u^{10}w + 6932\,u^{10} - 1136\,u^9w^3 \\ & + 16200\,u^9w^2 - 8\,u^9w - 6579\,u^9 - 1084\,u^8w^4 + 22504\,u^8w^3 - 39387\,u^8w^2 \\ & - 12208\,u^8w + 192\,u^7w^5 - 983\,u^7w^4 - 11531\,u^7w^3 - 6351\,u^7w^2 + 667\,u^6w^6 \\ & - 12854\,u^6w^5 + 77287\,u^6w^4 - 28467\,u^6w^3 + 365\,u^5w^7 - 2337\,u^5w^6 + 58336\,u^5w^5 \\ & - 49039\,u^5w^4 + 87\,u^4w^8 + 4225\,u^4w^7 - 7134\,u^4w^6 - 22022\,u^4w^5 + 8\,u^3w^9 \\ & + 2267\,u^3w^8 - 1286\,u^3w^7 - 8044\,u^3w^6 + 336\,u^2w^9 + 10982\,u^2w^8 + 8882\,u^2w^7 \\ & + 3576\,uw^9 + 23744\,uw^8 + 6448\,w^9. \end{aligned}$$

extraneous factor is $\boldsymbol{u^2} \times \boldsymbol{E_3}$

♠ : Introduction of Healthy System

System $\mathcal{F}$ is **Healthy** **if**

1) **All** the $x_1, \ldots, x_m$ can be **eliminated**
2) **None** of $u_1, \ldots, u_n$ can be **eliminated**
3) Such cases do **NOT occur** that
 $\mathrm{GB}(\mathcal{F}) \cap \mathbb{K}[u] = \{G_1, \ldots, G_{l \geq 2}\}$, satisfying
 $\mathbf{LMvars}(G_i) \cap \mathbf{LMvars}(G_j) = \emptyset$ for $\forall (i \neq j)$;
 ($\mathbf{LMvars}(G)$ = all variables in Lead-Monomial of G)
 ($\Leftrightarrow$ $u_1, \ldots, u_n$ are **distributed** into $G_1, \ldots, G_l$)

Main Theorem for Many-Pol. Systems

Theorem 2 (S&I 2018)

If $\mathcal{F}$ **is healty** then $\mathrm{GB}(\mathcal{F}) \cap \mathbb{K}[u] = \{\widehat{S}\}$

Outline of Proof

Suppose $\mathrm{GB}(\mathcal{F}) \cap \mathbb{K}[u] = \{S_1, \ldots, S_{l \geq 2}\}, S_1 \prec \cdots \prec S_l$.
First, treat the case that each S_i satisfies Condition 2).
Then, $\mathrm{Spol}(S_1, S_2)$ is not zero, and of lower order than S_2, contradicting the **reducedness** of $\mathbf{GB}(\mathcal{F})$.

$u_1, \ldots, u_n$ may be **distributed** among $S_1, \ldots, S_l$.
This case is not healthy by **Condition 3)**.

$\overset{\bowtie}{\spadesuit}$: Introduction of RectAngular PRSs

(rectPRSs, in short)

Triangular PRSs (conventional)

$$
\begin{array}{llll}
\boldsymbol{G_i} := \mathrm{lastPRS}_{\boldsymbol{x_1}}(\boldsymbol{F_1}, \boldsymbol{F_i}), & \cdots, & \cdots & (\,\boldsymbol{i \geq 2}\,) \\
& \boldsymbol{G'_i} := \mathrm{lastPRS}_{\boldsymbol{x_2}}(\boldsymbol{G_2}, \boldsymbol{G_i}), & \cdots & (\,\boldsymbol{i \geq 3}\,) \\
& \ddots & \ddots & \\
& & \boldsymbol{G'''_{m+1}} := \mathrm{lastPRS}_{\boldsymbol{x_m}}(\boldsymbol{G''_m}, \boldsymbol{G''_{m+1}}) &
\end{array}
$$

Rectangular PRSs (our method)

$$
\begin{array}{lll}
\boldsymbol{G_1} := \mathrm{lastPRS}_{\boldsymbol{x_1}}(F_1, F_2), & \cdots & \boldsymbol{G_{m+1}} := \mathrm{lastPRS}_{\boldsymbol{x_1}}(F_{m+1}, F_1) \\
\boldsymbol{G'_1} := \mathrm{lastPRS}_{\boldsymbol{x_2}}(G_1, G_2), & \cdots, & \boldsymbol{G'_{m+1}} := \mathrm{lastPRS}_{\boldsymbol{x_2}}(G_{m+1}, G_1) \\
\vdots & \vdots & \vdots \\
\boldsymbol{G'''_1} := \mathrm{lastPRS}_{\boldsymbol{x_m}}(G''_1, G''_2), & \cdots, & \boldsymbol{G'''_{m+1}} := \mathrm{lastPRS}_{\boldsymbol{x_m}}(G''_{m+1}, G''_1)
\end{array}
$$

$\overset{\cdots}{\spadesuit}$: Remove Extrn.Factr by RectPRSs

(Eliminate $\boldsymbol{x, y} \Rightarrow$ **RectAngular** PRSs)

$$(F_1, F_2, F_3) \;\Rightarrow\; (G_1, G_2, G_3) \;\Rightarrow\; (H_1, H_2, H_3)$$

Theorem 2 $\Rightarrow$ Each $\boldsymbol{H_i}$ is a multiple of $\boldsymbol{\widehat{S}}$

gcd($\boldsymbol{H_1, H_2, H_3}$) will be a **small** multiple of $\boldsymbol{\widehat{S}}$

$$\Downarrow$$

$$
\begin{aligned}
\boldsymbol{H_1} &= 382239\,\boldsymbol{u^{22}} - 313632\,u^{21}w - 3218292\,u^{21} - 172611\,u^{20}w^2 + \cdots, \\
\boldsymbol{H_2} &= 363\,\boldsymbol{u^{21}} - 4334\,u^{20}w - 14190\,u^{20} + 20453\,u^{19}w^2 + \cdots, \\
\boldsymbol{H_3} &= -23232\,\boldsymbol{u^{21}} - 71104\,u^{20}w + 206448\,u^{20} - 23312\,u^{19}w^2 + \cdots.
\end{aligned}
$$

$$\boldsymbol{\overline{H} := \mathrm{gcd}(H_1, H_2, H_3) = u^2\widehat{S}}$$

We want to remove u^2 further

$$(f_1^{(0)}, \ldots, f_{m+1}^{(0)}) := (F_1(\mathbf{0}, \boldsymbol{u}), \ldots, F_{m+1}(\mathbf{0}, \boldsymbol{u}))$$

(if some $f_i^{(0)} = 0$ then move **origin** of $\boldsymbol{u}$)

$(a_1, \ldots, a_{m+1})$: CofGs of H_i in $\boldsymbol{u}$

Proposition 1 (S& I 2018)

1) If $\overline{f} := \gcd(f_1^{(0)}, \ldots, f_{m+1}^{(0)}) \notin \mathbb{K}$ then $\widehat{S}$ = lowest(GB($\mathcal{F}$)) **has** $\overline{f}$ as a factor.
2) If $\overline{a} := \gcd(a_1, \ldots, a_{m+1}) \notin \mathbb{K}$ then $\overline{a}$ is an **extraneous factor** of H_i.

Hint for the Proof

Consider $\overline{H_i} = a_1 F_1 + \cdots + a_{m+1} F_{m+1}$ ($\in \langle \mathcal{F} \rangle$)

Proposition 1 removes u^2 extraneous factor **:**

Prop. 1 tells that H_1, H_2, H_3 contain u^2, u^1, u^1 extran. factors, respectively. while each H_i is not divisible by u^3.

$\Rightarrow$ $\overline{H}/u^2$ is <u>irreducible</u> $\Rightarrow$ $\overline{H}/u^2 = \widehat{S}$

HOW to Enhance Buchberger's Method

Let $\mathbf{GB}(\mathcal{F}) = \{\widehat{G}_1, \widehat{G}_2, \cdots\}$, where $\widehat{G}_1 \prec \widehat{G}_2 \prec \cdots$

Let $\widetilde{G}_i$ be either a small multiple or LM-multiple of $\widehat{G}_i$

(**LM-multiple** : $\mathrm{lmn}(\widetilde{G}_i)$ is a multiple of $\mathrm{lmn}(\widehat{G}_i)$)

=== **Plan** ===

1) Eliminate variables $x_1, \ldots, x_m \Longrightarrow$ obtain **rectPRSs**
(Each element of rectPRSs $\in \langle \mathcal{F} \rangle$)

2) Remove extran.factor of **last Res** by Prop. 1 $\Longrightarrow \widetilde{G}_1$

3) Trace rectPRSs **backwardly** $\Longrightarrow$ **calc.** $\widetilde{G}_2, \widetilde{G}_3, \cdots$
(How to **calc?** $\Longrightarrow$ **next screen**)

4) Apply Buchberger's procedure to $\mathcal{F} \cup \{\widetilde{G}_1, \widetilde{G}_2, \cdots\}$

Compare RectPRSs with GB($\mathcal{F}_{2018}$)

$R_{3:(1,2)} = x^2y^2u + \cdots$	$\widehat{G}_6 = 27\,\mathrm{digitsCoef}\; x^2uw + \cdots$
	$\widehat{G}_5 = 26\,\mathrm{digitsCoef}\; x^2w^2 + \cdots$
$R_{3:(1,2,3)} = 39\, y^2u^6 + \cdots$	$\widehat{G}_4 = 24\,\mathrm{digitsCoef}\; y^2w + \cdots$
	$\widehat{G}_3 = 27\,\mathrm{digitsCoef}\; yu + \cdots$
$R_{4:(1,2,3)} = 1872\, yu^{14} + \cdots$	$\widehat{G}_2 = \mathbf{48000}\, yw^8 - \cdots + \cdots$
$R_{5:(1,2,3)} = 382239\, u^{22} + \cdots$	$\widehat{G}_1 = \mathbf{33}\, u^7 + 23\, u^6w + \cdots$

(notice the **coefficient** sizes)

$\Downarrow$

Tactics at Step-3 above

$\overset{\bowtie}{\spadesuit}$: **Eliminate Variables** in **LeadCoef**ficients(R_{***})

Elimination of Similar Lead. Coeffs.

given : $\boldsymbol{R_1, \ldots, R_l} \in \mathbb{K}[\boldsymbol{x_m}, \boldsymbol{u}] \quad (l \geq 3)$

i) Let $\boldsymbol{C_i} := \textbf{LeadCoeff}(\boldsymbol{R_i}),\ \boldsymbol{C_1, \ldots, C_l} \in \mathbb{K}[\boldsymbol{u}]$

ii) Let $\boldsymbol{c_i} := \textbf{lastPRS}_{\boldsymbol{u_1}}(\boldsymbol{C_i}, \boldsymbol{C_{i+1}}) \in \mathbb{K}[\boldsymbol{u_2}, \ldots, n_n]$

(**lastPRS** = last element of PRS)

iii) Finally, let $\overline{\boldsymbol{c}} \simeq \textbf{gcd}(\boldsymbol{c_1, \ldots, c_l}) \in \mathbb{K}[\boldsymbol{u_2}, \ldots, n_n]$

We have seen **:** $\#\textbf{mn}(\overline{\boldsymbol{H}}) \ll \#\textbf{mn}(\boldsymbol{H_1}), \ldots, \#\textbf{mn}(\boldsymbol{H_3})$

We will see **:** $\#\textbf{mn}(\overline{\boldsymbol{c}}) \ll \#\textbf{mn}(\boldsymbol{c_1}), \ldots, \#\textbf{mn}(\boldsymbol{c_3})$

($\#\textbf{mn}(P) = \#$ of monomials in P)

Important NOTE on $\overline{\boldsymbol{c}}$

(often $\textbf{gcd}(\boldsymbol{c_1, \ldots, c_l}) \notin \langle \mathcal{F} \rangle$)

Let $\overline{\boldsymbol{c}} = \boldsymbol{\alpha_1} c_1 + \cdots + \boldsymbol{\alpha_l} c_l,\ \boldsymbol{\alpha_j} \in \mathbb{K}[\underline{u_2, \ldots, u_n}]$.

We compute $\overline{\boldsymbol{c}}$ as $\overline{\boldsymbol{c}} = \widehat{\boldsymbol{c}}\, \textbf{gcd}(\boldsymbol{c_1, \ldots, c_l})$,

where $\widehat{\boldsymbol{c}} \in \mathbb{K}[\underline{\boldsymbol{u_3, \ldots, u_n}}]$ is determined

to make polynomials $\boldsymbol{\alpha_1, \ldots, \alpha_l}$ a.**s**.a.p.

Anyway, $\overline{\boldsymbol{c}} \notin \langle \boldsymbol{\mathcal{F}} \rangle$ **: How to Use $\overline{\boldsymbol{c}}$?**

$\overset{\bowtie}{\spadesuit}$: from $c_j, \overline{c}$ to Polynomials in $\langle \mathcal{F} \rangle$

Let $c_i = a_i C_i + b_i C_{i+1}$, $a_i, b_i \in \mathbb{K}[u]$ ($\Leftarrow$ Elim u_1)

Let $\overline{c} = \alpha_1 c_1 + \cdots + \alpha_l c_l$, $\alpha_1, \cdots, \alpha_l \in \mathbb{K}[u_2, .., u_n]$

We define $\mathbf{LCtoW}(c_i) = W_i \overset{\text{def}}{=} a_i R_i + b_i R_{i+1}$:
(**LC** to **Whole**-polynomial)

$\mathbf{LCtoW}(c_i) \in \langle \mathcal{F} \rangle$, s.t. **LeadCoef**(LCtoW(c_i)) $= c_i$

We define $\overline{\mathbf{LCtoW}}(\overline{c}) \overset{\text{def}}{=} \alpha_1 W_1 + \cdots + \alpha_l W_l$:

$\overline{\mathbf{LCtoW}}(\overline{c}) \in \langle \mathcal{F} \rangle$, s.t. **LeadCoef**($\overline{\text{LCtoW}}(\overline{c})$) $= \overline{c}$

Let's Test above Scheme by $\mathcal{F}_{2018}$

As mentioned, we use **Spol** only in Buchberger-step

However, we use **Mreduction** indispensably
(**Mono**mial reduction)

Mreduce(F, G) : Mreduce F **fully** by G, i.e.,

$F \xrightarrow{G}\!\!\!\!\to R$: each term of R is **Mirred**ucible by G

$F = QG + R$: `quopol`$(F, G) = Q$, `rempol`$(F, G) = R$

==== **in Testing** ===

1) : **Use** $\mathbb{F}_p$, $p = 1073738848$, to simplify coefficients

2) : **Mreduce** $\{R_1, R_2, R_3\}$ ($\{C_1, C_2, C_3\}$, too) by G_1

$R_i \xrightarrow{G_1}\!\!\!\!\to R'_i$, $C_i \xrightarrow{G_1}\!\!\!\!\to C'_i$ ($'$ means Mred by G_1)

Computation of Second-Lowest $\widetilde{G}_2$

given $R'_1, R'_2, R'_3 \in \mathbb{F}_p[y,u,w]$, $\mathbf{deg}_y(R'_i) = 1\ (\forall i)$

$C'_i := \mathbf{leadCoef}(R'_i) \in \mathbb{F}_p[u,w]$, $\mathbf{deg}_u(C'_i) = 6$

$\widetilde{c}'_j := \mathbf{lastPRS}_u(C'_j, C'_{j+1}) \in \mathbb{F}_p[w]$

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

$\overline{c}' := \mathbf{gcd}(c'_1, c'_2, c'_3) \quad (= \gcd(c'_{j_1}, c'_{j_2 \neq j_1}))$

$$\overline{c}' = w^{17} - 56371298\,w^{16} + 138243860\,w^{15} - 521121094\,w^{14} - 96457750\,w^{13} - 382429906\,w^{12} - 247496825\,w^{11}.$$

$\mathbf{LCtoW}(c'_j)$ and $\overline{\mathbf{LCtoW}}(\overline{c})$ for $\widetilde{G}_2$

$c'_i = a_i C'_1 + b_i C'_{i+1} \Rightarrow W'_i := \mathrm{LCtoW}(c'_i)$ **:** $\#\mathrm{mn}(W'_i) = \mathbf{1016}$

$\overline{c} = \alpha_i\, c'_i + \beta_i\, c'_{i+1} \Rightarrow \overline{W}' := \overline{\mathrm{LCtoW}}(\,\overline{c}\,)$ **:** $\#\mathrm{mn}(\overline{W}') = \mathbf{1686}$

We get $\overline{W}'' := \mathbf{Mreduce}(\overline{W}', \widehat{G}_1) \implies$ **:** $\#\mathrm{mn}(\overline{W}'') = \mathbf{61}$

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

We see $\overline{W}'' = w^9 \widehat{G}_2$, $\;w^9$ is extraneous.

How can we remove w^9 in $\overline{W}''$?

=== **We found that** ===

Although we have $a'_j R'_j + b'_j R'_{j+1} \propto w^9$, we have

$$\texttt{redpol}(a'_j R'_j, w^9) \;=\; -\,\texttt{redpol}(b'_j R'_{j+1}, w^9)$$

both sides contain $w^0,\ w^1, \cdots, w^7, w^8$-terms

Proposition 2 (SSIK2020)

The w^j-terms ($\forall j \leq 8$) in the CofGs in u, of $\overline{W}'_j$ and $\overline{W}''_j$ can be cut off.

Proof of Proposition 2

$\overline{W}'_j$ is expressed by CofGs $a'_{j,1}, a'_{j,2}, a'_{j,3}$ as $\overline{W}'_j =$ $C_{\rm ofG}(\%P[1], \%P[2], \%P[3]) := a'_{j,1}\%P[1] + a'_{j,2}\%P[2] + a'_{j,3}\%P[3]$, where $\%P[i]$ is a system variable representing F_i. Each $F_i(0, u, w)$ has a nonzero w^0-term, hence if we substitute $F_i(\mathbf{0}, u, w)$ for $\%P[i]$, $i \in \{1, 2, 3\}$, all the w^e-terms, $0 \leq \forall e \leq 8$, of $a'_{j,1}, a'_{j,2}, a'_{j,3}$ cancel. Since $\overline{W}'_j = C_{\rm ofG}(F_1(\mathbf{0}, u, w), F_2(\mathbf{0}, u, w), F_3(\mathbf{0}, u, w))$, this cancellation does **not** change $\overline{W}'_j$ itself. (The same reasoning is applicable to $\overline{W}''_j$, too.) □

Another Useful Technique

$$\left(\begin{array}{l}\text{We show technique by computing } \widetilde{G}_4 \\ \text{where } \widehat{G}_4 = 17615 \cdots y^2 \underline{\underline{w}} + \cdots \end{array}\right)$$

given $R'_1, R'_2, R'_3 \in \mathbb{F}_p[y, u, w]$, $\mathbf{deg}_y(R'_i) = 2$,
$\widetilde{c}'_j := \mathbf{lastPRS}_u(C'_j, C'_{j+1})$, $C'_j := \mathbf{LCoef}(R'_j)$,
compute $\overline{c}' := \mathbf{gcd}(\widetilde{c}'_1, \widetilde{c}'_2, \widetilde{c}'_3)$, then we obtained
$\overline{c}' = -\,14400000\,\underline{\underline{w^{14}}} + \cdots + 51678000\,\underline{\underline{w^5}}$
$\overline{c}'$ is too higher-order than $\mathbf{LCoef}_y(\widehat{G}_4) = c\,w$.

We can decrease $\texttt{order}(\overline{c}')$ easily

Our Method **:** $\widetilde{c}'_4 := \mathbf{gcd}(\overline{c}', \mathbf{LCoef}_y(\widetilde{G}_2))$
$\Rightarrow \widetilde{G}'_4 := \mathbf{LCtoW}(\widetilde{c}'_4) = \alpha_4 \overline{W}'_4 + \beta_4\, \underline{\underline{y\, \widetilde{G}_2}}$
$\Rightarrow \widetilde{G}_4 := \texttt{Mreduce}(\widetilde{G}'_4, \widetilde{G}_2, \widetilde{G}_1)$, then

$$\begin{array}{rl}\widetilde{G}_4 = & y^2 \times (\;\; 260166204\, w^2 \;) \\ + & y^1 \times [\; u^6 \times (\;\; 890901532\, w^{16} + \cdots + 736495066\, w - 263471195 \;) \\ & \quad + u^5 \times (-360952533\, w^{17} + \cdots - 539864510\, w - 470888958 \;) \\ & \quad \vdots \qquad\qquad \vdots \qquad\qquad\qquad \vdots \qquad\qquad\qquad] \\ + & y^0 \times [\; u^6 \times (\;\; 890901532\, w^{16} + \cdots + 736495066\, w - 263471195 \;) \\ & \quad + u^5 \times (-360952533\, w^{17} + \cdots - 539864510\, w - 470888958 \;) \\ & \quad \vdots \qquad\qquad \vdots \qquad\qquad\qquad \vdots \qquad\qquad\qquad]. \end{array}$$

How to Treat $m \gg 1$ case?

(**mixed-tri&rectAngular Elimination**)

$\{F_1, F_2, \cdots, F_{m+1}\} \subset \mathbb{K}[x_1, \ldots, x_m, u] \;\Rightarrow$
$\{F_1, F_2, F_3\} \cup \{F_1, F_2, F_4\} \cup \cdots \cup \{F_1, F_2, F_{m+1}\}$

$\Rightarrow$ $\mathrm{rectPRS}_{x_1,x_2}(F_1, F_2, F_i)$ $\quad$ (x_1, x_2 eliminated)
$\quad \Rightarrow \{G_{i,1}, G_{i,2}, G_{i,i}\} \subset \mathbb{K}[x_3, .., x_m, u]$
$\quad \Rightarrow \widehat{G}_i := \mathrm{gcd}(G_{i,1}, G_{i,2}, G_{i,i})$ $\;(i = 3, \ldots, m{+}1)$

$\Rightarrow \{\widehat{G}_3, \widehat{G}_4, \ldots, \widehat{G}_{m+1}\} \subset \mathbb{K}[x_3, .., x_m, u]$

Continue the above elimination

(We have NOT tested yet)

How to Treat Non-Healthy systems?

(various **Computation-Branchings** occur)

♠ **2-Polynomial (sub-)Systems**

- **if** $(G, H) = (DG', DH')$, $D \notin \mathbb{K}$
  then $\mathrm{GB}(\{G, H\}) = D \times \mathrm{GB}(\{G', H'\})$

♣ **$(m+1)$-Polynomial Systems**

- **separate** $\{F_1, \ldots, F_{m+1}\}$ into
  mutually disconnected systems
- **separate** $GB(G'(u')\, G''(u''))$ into
  $GB(G'(u'))$ & $GB(G''(u''))$, where
  $\mathrm{LMvars}(G') \cap \mathrm{LMvars}(G'') = \emptyset$ **:** NOT yet

What is Bridge between E & B ?

Bridge = Coefficients of Generators

$\Downarrow$

PRS : LCtoW-polynomial

GB : Mreduce-operation

♠ : **collaboration** is **UNbelievably NICE**

What is the NEXT Work ?

Develop Computational Techniques
for **big PRSs** & **Coef-of-Generators**

THANK YOU VERY MUCH for YOUR ATTENTION

Acknowledgements

The speaker thanks F.Kako, D.Inaba, and M.Sanuki for helping him in maintaining his research environment.

Thanks are also to Japan Soc. for Promotion of Science & Res. Inst. for Math. Sci., for their financial supports.