A Bridge between Euclid and Buchberger *

(An Attempt to Enhance Gröbner Basis Algorithm by PRSs and GCDs)

Tateaki Sasaki

Professor emeritus, University of Tsukuba
Tsukuba-shi, Ibaraki 305-8571, Japan
sasaki@math.tsukuba.ac.jp

Abstract

By Euclid we mean the Euclidean and extended Euclidean algorithms for multivariate polynomials. From the viewpoint of variable elimination, the PRS (polynomial remainder sequence) method is very fast but the resultant obtained by this method contains mostly a big extraneous factor. The lowest-order resultant is obtained by computing the reduced Gröbner basis w.r.t. the lexicographic order, abbreviated to GB below, but the GB method is very slow, in particular, when the number of variables is many. Very many attempts were done to remove the extraneous factors and to enhance the GB computation greatly, such as the sparse resultant theory, but the current status is far from satisfaction.

Recently, the author and his collaborators are studying a new method; see Refs below. Let $\mathcal{F} := \{F_1, \dots, F_{m+1}\} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{u}]$ be a given system, where $(\boldsymbol{x}) = (x_1, \dots, x_m)$ and $(\boldsymbol{u}) = (u_1, \dots, u_n)$, with $\forall x_i \succ \forall u_j$. We want to compute $\mathrm{GB}(\mathcal{F})$, the GB of the ideal $\langle \mathcal{F} \rangle$. Our method is to apply Buchberger's algorithm to the system $\mathcal{F} \cup \mathcal{G}'$, where $\mathcal{G}'$ is a set of small multiples (multiplier is 1 sometimes) of important elements of $\mathrm{GB}(\mathcal{F})$. We compute $\mathcal{G}'$ by the PRSs and GCDs. As for relatively prime polynomials $G, H \in \mathbb{Q}[x, \boldsymbol{u}]$, we found a theorem which gives us the lowest-order polynomial $\widehat{S}(\boldsymbol{u})$ of $\mathrm{GB}(\{G, H\})$ by a PRS and GCDs. As for $\mathcal{F}$, with $m + 1 \geq 3$, we introduced a concept "healthy": $\mathcal{F}$ is healthy if i) all the $x_1, \dots, x_m$ are eliminable, ii) none of $u_1, \dots, u_n$ is eliminable, and iii) the $u_1, \dots, u_n$ are *not* divided into two or more "mutually non-overlapping" GBs. Then, we obtained a theorem: *If* $\mathcal{F}$ *is healthy then* $\mathrm{GB}(\mathcal{F}) \cap \mathbb{Q}[\boldsymbol{u}] = \{\widehat{S}(\boldsymbol{u})\}$. By eliminating $x_1, \dots, x_m$ of healthy $\mathcal{F}$ with the PRS method through several routes, we obtain several resultants each of which is a multiple of $\widehat{S}$, so the GCD of them must be a small multiple of $\widehat{S}$; actually, a very small multiple of $\widehat{S}$. (Non-healthy systems cause branching of the elimination). As for other elements of $\mathrm{GB}(\mathcal{F})$, we use intermediate elements of the PRSs, and obtain small multiples of elements of $\mathrm{GB}(\mathcal{F})$ by eliminating variables in their leading coefficients. (Our research is now on-going, so we cannot give final timing data now).

References

[1] 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).

[2] 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).

[3] 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).

[4] T. Sasaki, M. Sanuki, D. Inaba, F. Kako: An attempt to enhance Buchberger's algorithm by using remainder sequences and GCDs (II). *RIMS Kôkyûroku (Research Reports of Research-Inst.-for-Mathematical-Sciences, Kyoto Univ.) 2185*, 71–80 (2021).

*Work supported by Japan Society for Promotion of Science KAKENHI Grant number 18K03389, and in part by The Research Institute for Mathematical Sciences in Kyoto University.