Attempts at Computing Gröbner Bases without $S$-polynomials whenever Possible

Alkiviadis G. Akritas$^1$, Gennadi Malaschonok$^2$

$^1$Department of Electrical and Computer Engineering, University of Thessaly, GR-38221, Volos, Greece
$^2$Tambov State University, Internatsionalnaya, 33, Tambov, Russia

e-mail: akritas@uth.gr AND malaschonok@gmail.com

Abstract

In this note we lay down some thoughts on computing Gröbner bases using subresultant polynomial remainder sequences (prs's) to eliminate variables.

In this way we try to minimise $S$-polynomial computations and, if possible, to completely avoid them.

A personal note to us by Bruno Buchberger — at the Polynomial Computer Algebra conference (PCA-2015) in St. Petersburg, Russia — served as the motivation for our effort.

Outline of our Algorithm

In order to understand our method, we first give a brief presentation of Buchberger's original algorithm for computing the Gröbner basis of a system of polynomials equations in many variables with rational coefficients.

Buchberger's Original Algorithm

• for each pair of polynomials compute the $S$-polynomial,

• reduce each polynomial by all others,

• the process terminates when no new $S$-polynomials appear.

Our Algorithm — working version

1. for each pair of polynomials $A, B$ compute $C$, the last member of the subresultant prs of $A, B$,
   
   (a) if $\text{lc}(B) = 1$, then we replace the pair $A, B$ by the pair $B, C$,
   
   (b) if $\text{lc}(B) \neq 1$, then we replace the pair $A, B$ by the triplet $A, B, C$,
2. reduce each polynomial by all others,
3. the process terminates when no new polynomials $C$ appear.

Acknowledgments

Second author is partially supported by RFBR grant No 16-07-00420.

References