Gröbner Bases and Generalized Sylvester Matrices

Manuela Wiesinger-Widi*
Doctoral Program Computational Mathematics
Johannes Kepler University Linz
4040 Linz, Austria
manuela.wiesinger@dk-compmath.jku.at

In his PhD thesis [1], Buchberger introduced the notion of Gröbner bases and gave the first algorithm for computing them. Since then, extensive research has been done in order to reduce the complexity of the computation. But nevertheless, even for small examples the computation sometimes does not terminate in reasonable time.

There are basically two approaches for computing a Gröbner basis. The first is the one pursued by the Buchberger algorithm: We start from the initial set F, execute certain reduction steps (consisting of multiplication of polynomials by terms — called shifts — and subtraction of polynomials) and due to Buchberger's theorem, which says that the computation is finished if all the s-polynomials reduce to zero, we know that after finitely many iterations of this procedure we obtain a Gröbner basis of the ideal generated by F. The second approach is to start from F, execute certain shifts of the initial polynomials in F, arrange them as rows in a matrix, triangularize this matrix and from the resulting matrix extract a Gröbner basis.

In project DK1 of the Doctoral Program, which was proposed by Buchberger, we pursue the second approach and seek to improve the theory in order to speed up the Gröbner bases computation. This approach has been studied a couple of times in the past, but never thoroughly. The immediate question is: Does there exist a finite set of shifts such that a triangularization of the matrix built by these shifts yields a Gröbner basis and, if so, how can we construct these shifts? We give first results in answering this question. In the following, let K be a field.

In the univariate case, Gröbner bases computation specializes to gcd computation. In [3] (see also [4] for a good overview on this topic), Habicht establishes a connection between the computation of polynomial remainder sequences and linear algebra. More specifically, the problem of finding a gcd of two polynomials $f, g \in K[x]$ with degrees m and n, respectively, where $m \geq n$, can be solved by triangularizing the matrix

$$M = \mathrm{mat}(x^{n-1}f, x^{n-2}f, \ldots, f, x^{m-1}g, x^{m-2}g, \ldots, g),$$

i.e. the Sylvester matrix of f and g. If the resulting triangularized matrix is arranged as a right upper triangular matrix, the bottom most non-zero row corresponds to a gcd of the polynomials f and g.

As a first step we generalize this method to the case of r univariate polynomials with $r \geq 2$. Such generalizations have been done before (see [5],[2]). Those, however, resulted in bigger matrices.

Theorem 1 *Let $F = \{f_1, \ldots, f_r\} \subset K[x] \setminus \{0\}$ with $r \geq 2$ and with f_r having minimal degree $n \geq 1$ among the polynomials in F. Let m be the maximal degree of the polynomials in F. Let $M := \mathrm{mat}(x^{n-1}f_1, x^{n-2}f_1, \ldots, f_1, \ldots, x^{n-1}f_{r-1}, x^{n-2}f_{r-1}, \ldots, f_{r-1}, x^{m-1}f_r, x^{m-2}f_r, \ldots, f_r)$ and let M' be a matrix obtained by triangularizing M.*
Then the polynomial corresponding to the non-zero row of lowest degree in M' is a gcd *of the polynomials in F.*

*This project is funded by the Austrian Science Fund (FWF) under grant W1214/DK1.

For the proof of Theorem 1 see [6].

In the multivariate case the problem is much more difficult. We show that by carefully tracing the computations in the Gröbner bases algorithm we can in an inductive way come up with shifts sufficient for computing a Gröbner basis of input set F by matrix triangularization. These shifts are collected in the history tuple $\mathrm{hist}(F)$. The details can be found in [7].

For a history tuple s the matrix $\mathrm{matrix}(s)$ is built by representing the polynomials occurring in s as vectors (indexed by terms) and arranging them as its rows in some order.

Let M be a triangular matrix of polynomials over K. We define

$$\mathrm{contour}(M) := \{f \text{ in } M : f \neq 0 \wedge \underset{\substack{g \text{ in } M \\ g \neq 0 \wedge g \neq f}}{\forall} \mathrm{lt}(g) \nmid \mathrm{lt}(f)\}.$$

The following theorem states that for every finite input set F of non-zero polynomials there exists a finite set of shifts of the polynomials in F such that a triangularization of the matrix built by these shifts provides a Gröbner basis.

Theorem 2 *Let $F \subseteq K[x_1, \ldots, x_n] \setminus \{0\}$ be finite, $|F| > 1$. Then for all M, which can be obtained by triangularizing* $\mathrm{matrix}(\mathrm{hist}(F))$, $\mathrm{contour}(M)$ *is a Gröbner basis of* $\mathrm{Ideal}(F)$.

Theorem 2 gives a construction of such a matrix, but since we need a Gröbner bases computation to get the necessary shifts, this is of course only one step in answering the question of how to get such shifts a priori, without previous Gröbner bases computation.

We are working on obtaining the initial matrix of necessary shifts without having a previous Gröbner bases computation.

References

[1] Bruno Buchberger. An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal (german). Mathematical Institute, University of Innsbruck, Austria. PhD Thesis. 1965. English translation in *J. of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science: Interactions*. Vol. 41, Number 3-4, pages 475–511, 2006.

[2] Stavros Fatouros and Nicos Karcanias. Resultant Properties of GCD of Many Polynomials and a Factorization Representation of GCD. *International Journal of Control*, Vol. 76, Issue 16, pp. 1666–1683, 2003.

[3] Walter Habicht. Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens. *Comm. Math. Helvetici* 21, pp. 99–116, 1948.

[4] Rüdiger Loos. Generalized Polynomial Remainder Sequences. In *Computer Algebra: Symbolic and Algebraic Computation*, pp. 115–137, Springer-Verlag, 1982.

[5] A.I.G. Vardulakis and P.N.R. Stoyle. Generalized Resultant Theorem. *IMA Journal of Applied Mathematics*, Vol. 22, Issue 3, pp. 331–335, 1978.

[6] Manuela Wiesinger-Widi. Sylvester Matrix and GCD for Several Univariate Polynomials. Technical report, DK Computational Mathematics, JKU, Linz, Austria, 2011. In preparation.

[7] Manuela Wiesinger-Widi. Towards Computing a Gröbner Basis of a Polynomial Ideal Over a Field by Using Matrix Triangularization. Technical report, DK Computational Mathematics, JKU, Linz, Austria, 2011. In preparation.