Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Signature-based Criteria for Computing Weak Gröbner Bases over PIDs

Thibaut Verron[1], **Maria Francis**[1]

The theory of Gröbner bases was introduced by Buchberger in 1965 [2] and has since become a fundamental algorithmic tool in computer algebra. Over the past decades, many algorithms have been developed to compute Gröbner bases more and more efficiently. The latest iteration of such algorithms is the class of signature-based algorithms, which introduce the notion of signatures and use it to detect and prevent unnecessary or redundant reductions. This technique was first introduced for Algorithm F5 [5], and there have been many research works in this direction [3].

All these algorithms are for ideals in polynomial rings over fields. Gröbner bases can be defined and computed over commutative rings [1, Ch. 4], and can be used in many applications [7]. An important particular case is that where the coefficient ring is a Principal Ideal Domain (PID), for example $\mathbb{Z}$ or the ring of univariate polynomials over a field.

If the coefficient ring is not a field, there are two ways to define Gröbner bases, namely weak and strong bases. Strong Gröbner bases ensure that normal forms can be computed as in the case of fields. But computing a strong Gröbner basis is more expensive than a weak one, and if the base ring is not a Principal Ideal Domain (PID), then some ideals exist which do not admit a strong Gröbner basis. On the other hand, weak Gröbner bases, or simply Gröbner bases, always exist for polynomial ideals over a Noetherian commutative ring. They do not necessarily define a unique normal form, but they can be used to decide ideal membership.

Recent works have focused on generalizing signature-based techniques to Gröbner basis algorithms over rings. First steps in this direction, adding signatures to a modified version of Buchberger's algorithm for strong Gröbner bases over Euclidean rings [6], were presented in [4]. The paper proves that a signature-based Buchberger's algorithm for strong Gröbner bases cannot ensure correctness of the result after encountering a "signature-drop", but can nonetheless be used as a prereduction step in order to significantly speed up the computations.

Here we consider the problem of computing a weak Gröbner basis of a polynomial ideal with coefficients in a PID, using signature-based techniques. The proof-of-concept algorithm that we present is adapted from that the general algorithm due to Möller [8], which considers combinations and reductions by multiple polynomials at once. The way the signatures are ordered ensures that no reductions leading to signature-drops can happen. In particular, we could prove that the algorithm terminates and computes a signature Gröbner basis with elements ordered with non-decreasing signatures. This property allows us to examine classic signature-based criteria, such as the syzygy criterion, the F5 criterion and the singular criterion, and show how they can be adapted to the case of PIDs. In particular, when the input forms a regular sequence, the algorithm performs no reductions to zero.

We have written a toy implementation in Magma of the algorithms presented, with the F5 and singular criteria. Möller's algorithm, without signatures, works for polynomial systems over any Noetherian commutative ring. The signature-based algorithm is only proved to be correct and to terminate for PIDs, but with minimal changes, it can be made to accomodate inputs with coefficients in a more general ring. Interestingly, early experimental data with

coefficients in a multivariate polynomial ring (a Unique Factorization Domain which is not a PID) suggest that the signature-based algorithm might work over more general rings than just PIDs.

Keywords: Gröbner bases, Signature-based algorithms, Principal Ideal Domains

References

[1] ADAMS, W. & LOUSTAUNAU, P. (1994). *An Introduction to Gröbner Bases*. American Mathematical Society.

[2] BUCHBERGER, B. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. Ph.D. thesis, University of Innsbruck, Austria.

[3] EDER, C. & FAUGÈRE, J.-C. (2017). A Survey on Signature-based Algorithms for Computing Gröbner Bases. *Journal of Symbolic Computation* **80**, 719–784.

[4] EDER, C., PFISTER, G. & POPESCU, A. (2017). On Signature-Based Gröbner Bases over Euclidean Rings. In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17. New York, NY, USA: ACM.

[5] FAUGÈRE, J. C. (2002). A New Efficient Algorithm for Computing GrÖbner Bases without Reduction to Zero (F5). In: *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02. New York, NY, USA: ACM.

[6] LICHTBLAU, D. (2012). Effective Computation of Strong Gröbner Bases over Euclidean Domains. *Illinois J. Math.* **56**(1), 177–194 (2013).

[7] LICHTBLAU, D. (2013). Applications of Strong Gröbner Bases over Euclidean Domains. *Int. J. Algebra* **7**(5-8), 369–390.

[8] MÖLLER, H. M. (1988). On the Construction of Gröbner Bases using Syzygies. *Journal of Symbolic Computation* **6**(2-3), 345–359.

[1]Institute for Algebra
Johannes Kepler University
4040 Linz, Austria
thibaut.verron@jku.at
maria.francis@jku.at