Groebner Rings and Modules

Extended Abstract

Bruno Buchberger
RISC (Research Institute for Symbolic Computation)
Johannes Kepler University, Linz, A4232, Schloss Hagenberg, Austria
Bruno.Buchberger@RISC.Uni-Linz.ac.at

Acknowledgement: The research described in this paper is sponsored by the Austrian NSF (FWF, Österreichischer Fonds zur Förderung der wissenschaftlichen Forschung) in the SFB-Project "Scientific Computing", SFB 1302. The paper was written during a stay at Texas A&M, Math. Dept. withing the "Frontiers of Mathematics" program. My special thanks to Dr. Beth Arnold for having organized this visit for me.

■ Motivation

Originally, the theory of Groebner bases has been introduced, in [Buchberger 1970], for the case of commutative polynomials over coefficient fields. Since then, several generalizations of the theory for more general classes of rings have been proposed in the literature. Most of these generalizations prove theorems of the following kind: If Groebner bases can be constructed in a certain (commutative) ring R then Groebner bases can also be constructed in the polynomial ring over R. In [Buchberger 1984] I proposed a different approach for generalizing Groebner bases theory which I think is more natural and more useful: I formulated axioms for a ring R that guarantee that one can construct Groebner bases in R ("Construction Theorem") and then I proved that, if R satisfies these axioms, then also the polynomial ring over R satisfies these axioms ("Conservation Theorem"). S. Stifter, a PhD student of mine, later proved that conservation theorems can also be proved for other ring constructions, e.g. the construction of direct products of rings, see [Stifter 1987].

The axioms I proposed were, however, quite involved. In particular, I had to introduce a "set of multipliers" in R. In this talk, I would like to propose a new approach to the axiomatization of Groebner bases theory, which is still along the lines of [Buchberger 1984] but avoids speaking about sets of multipliers. In the talk, I will report on the current state of formulating the appropriate axioms in the new approach and proving the corresponding construction and conservation theorems. I will give the necessary definitions in the next section and then, in the third section, state the research problem.

■ Definitions

Let R be a commutative ring with algorithmic operations +, 0, -, and *. We now suppose that, In addition to +, 0, -, we have an algorithmic binary relation < ("lesss"), and two more algorithmic binary functions / ("ring quotient") and ↑ ("least common reducible") in R. Unless stated otherwise, all quantifiers range over the elements of R.

Definition:

r is reducible modulo s iff $\underset{q}{\exists}\; r - q * s < r$.

Axiom (Reducibility):

$\underset{r,s}{\forall}$ (r is reducible modulo $s \Longrightarrow r - (r/s) * s < r$).

Note that, if the reducibility axiom holds, the reducibility is algorithmic because then, in fact,

$\underset{r,s}{\forall}$ (r is reducible modulo $s \Longleftrightarrow r - (r/s) * s < r$)

and the operations -, *, <, and / are supposed to be algorithmic.

Let now S range over finite sets of elements in R.

Definition:

$$\mathrm{rd}[r,S] := \begin{cases} \mathrm{rd}[r - (r/s) * s,\ S], & \Leftarrow \underset{s \in S}{\exists} (r \text{ is reducible modulo } s) \\ \quad \text{where } s \in S \text{ is such that } r \text{ is reducible modulo } s & \\ r & \Leftarrow \text{otherwise} \end{cases}$$

Note that, if the reducibility axiom holds, rd is an algorithmic partial function: Because of the finiteness of S and the reducibility axiom, the condition

$\underset{s \in S}{\exists}$ (r is reducible modulo s)

is algorithmic and the operations-, *,and / are algorithmic by assumption.

If, in addition, the following Noetherianity axiom holds, then rd is an algorithmic total function because the sequence of intermediate elements $r_0 := r$, $r_1 := r_0 - (r_0/s_1) * s_1$, $r_2 := r_1 - (r_1/s_1) * s_2$, ... will then be always finite.

Axiom (Noetherianity):

< is a Noetherian partial ordering.

Now we define, as usual, the ideal generated by a (finite) set S.

Definition:

$$\text{ideal}[S] := \left\{ \sum_{i=1,\ldots,m} r_i * s_i \;\middle|\; m \in \mathbb{N},\, r_i \in R,\, s_i \in S \right\}$$

With the above reduction function, we can now also define the notion of Groebner basis:

Definition:

S is a Groebner basis iff $\underset{r \in \text{ideal}[S]}{\forall} \text{rd}[r, S] = 0$.

Now, we define the function sp ("S-polynomial") in terms of the function ↑. Of course, in the case of general rings, this function should be called "difference of least common multiples" rather than "S-polynomial".

Definition:

$$\text{sp}[s,t] := (u - (u/s) * s) - (u - (u/t) * t) \;\; (= -(u/s) * s + (u/t) * t),$$
$$\text{where } u := s \uparrow t.$$

It is clear that sp[s,t]∈ideal[{s,t}]. Also, sp is an algorithmic function.

Now we are able to specify the usual Groebner basis algorithm of [Buchberger 1970] in this abstract setting:

Definition:

$$\text{GB}[S] := \text{GB}[S, \{\{s, t\} \mid s, t \in S\}]$$

$$\text{GB}[S,P] := \begin{cases} S & \Leftarrow \;\; P = \emptyset \\ \begin{cases} \text{GB}[S,\, P - \{\{s, t\}\}] & \Leftarrow \;\; h = 0 \\ \text{GB}[S \cup \{h\},\, P - \{\{s, t\}\} \cup \{\{s, h\} \mid s \in S\}] & \Leftarrow \;\; \text{otherwise} \\ \quad\quad \text{where } \{s, t\} \in P,\, h := \text{sp}[s, t] & \end{cases} & \Leftarrow \;\; \text{otherwise} \end{cases}$$

GB is an always an algorithmic partial function. It will always conserve the ideal generated by the initial set S. However, GB may not be total and, of course, it may not always yield a Groebner basis. Let us now characterize *Groebner rings* by requiring that GB is total and constructs, in fact, Groebner bases:

Definition: R (with <, /, ↑) is a Groebner ring iff GB is total and

$\underset{S}{\forall}$ ideal[S] = ideal[GB[S]] and GB[S] is a Groebner basis.

A similar setting and a similar definition could be given for modules.

■ Research Problem

The problem now is to formulate "easy" axioms for the ring operations and the operations <, /, and ↑ in *R* such that one can prove that, under the assumption of these axioms, *R* is a Groebner ring and, in addition, it can be proved that the property of being a Groebner ring is conserved under going over to polynomial rings, direct products of rings, etc.

The axioms given in [Buchberger 1984] are a natural starting point for this research. However, they have to be reformulated (and will hopefully become simpler) in the new setting. For example, a natural axiom for the ↑ function would be the following axiom

Axiom (Least Common Reducible):

$$\underset{s,t}{\forall}\Big(s\uparrow t \text{ is a common reducible of } s \text{ and } t \bigwedge$$
$$\underset{u}{\forall}\ (u \text{ is a common reducible of } s \text{ and } t \Longrightarrow s\uparrow t \le u)\Big)$$

with the definition

Definition:

$$u \text{ is a common reducible of } s \text{ and } t \text{ iff } (u \text{ is reducible modulo } s \ \wedge\ u \text{ is reducible modulo } t).$$

In fact, weaker variants are conceivable (and will enhance the applicability of the theory), see [Buchberger 1984].

■ References

[Buchberger 1970] B. Buchberger. An Algorithmic Criterion for the Solvability of Algebraic Systems of Equations (German). *Aequationes mathematicae* 4/3, 374-383, 1970. (Published version of the author's PhD thesis, 1965, University of Innsbruck. English translation in: B. Buchberger, F. Winkler (eds.). *Gröbner Bases and Applications*. Proc. of the International Conference "33 Years of Groebner Bases", London Mathematical Society Lecture Note Series, 251, Cambridge University Press, pages 1-29.

[Buchberger 1984] B. Buchberger. A Critical-Pair/Completion Algorithm for Finitely Generated Ideals in Rings. Symposium "Rekursive Kombinatorik", Münster (FRG), May 1983, *Lecture Notes in Computer Science* 171, Springer, 1984, pp. 137-161.

[Stifter 1984] S. Stifter. Reduction Rings. *Journal of Symbolic Computation*, 1987.