Journal of Algebra, Number Theory: Advances and Applications
Volume 4, Number 1, 2010, Pages 41-48

TWO-ELEMENT GRÖBNER BASES OVER NOETHERIAN COMMUTATIVE RINGS

HAMID KULOSMAN and STEPHANIE BRITT

Department of Mathematics
University of Louisville
Louisville, KY 40292
U.S.A.
e-mail: h0kulo01@louisville.edu

Abstract

We find a necessary and sufficient condition for a set $G = \{f, g\}$ of two polynomials (of special form) in n-variables over a Noetherian commutative ring to be a Gröbner basis of the ideal $I = < f, g >$. That can eventually be used to obtain faster versions of the Insa-Pauer criterion (an analogue of Buchberger's criterion in the case of rings).

1. Notations and Preliminaries

The theory of Gröbner bases was developed by Buchberger in 1960s for the polynomial ideals over fields. One of the key results in his theory is nowdays called the *Buchberger's criterion*. It gives a procedure for testing whether a given finite set of polynomials is a Gröbner basis of the ideal they generate. The criterion uses the so-called *S-polynomials*.

Soon after Buchberger's theory was published, it became apparent that there is a need to generalize it to the case of rings. That process is

2010 Mathematics Subject Classification: Primary 13P10; Secondary 13B25.

Keywords and phrases: Gröbner basis, Buchberger's criterion, Insa-Pauer's criterion, polynomials over Noetherian commutative rings.

Received September 20, 2010

still going on (see [1], [2], [3], and [4] for some history and results in that direction). In this note, we will consider the polynomials over a commutative Noetherian ring. We will use a generalization of Buchberger's criterion to this context, developed by Insa and Pauer (see [3] and [4]), and we will call it the *Insa-Pauer,s criterion*. In it, it is not enough to use the S-polynomials, but they are replaced by the certain set of polynomials constructed by using the module of all the syzygies of the leading coefficients of the polynomials that are tested.

Here is an explanation of our notation. (For all notions or facts that are used, but not defined or stated here, the reader can consult [2].) $\mathbb{N}$ denotes the set $\{0, 1, 2, \ldots\}$ of natural numbers. For two elements $\mu = (\mu_1, \ldots, \mu_n)$ and $\nu = (\nu_1, \ldots, \nu_n)$ of $\mathbb{N}^n$, we say that $\mu \geq_{\text{coord}} \nu$, if $\mu_i \geq \nu_i$ in the standard order on $\mathbb{N}$ for every $i = 1, 2, \ldots, n$. R will always denote a Noetherian commutative ring such that (see [4]):

(i) for all $z \in R$ and for all finite subsets $S \subseteq R$, we can decide if z belongs to the ideal $< S >$ generated by S and if it does, we can compute a family $(d_s)_{s \in S}$ such that $z = \sum_{s \in S} d_s s$;

(ii) for every finite subset $S \subseteq R$, we can compute a finite system of generators of the R-module

$$\{(c_s)_{s \in S} \in R^S \mid \sum_{s \in S} c_s s = 0\}$$

of its syzygies.

$A = R[X_1, \ldots, X_n]$ denotes the ring of polynomials over R in n commuting variables $X_1, \ldots, X_n$. We assume that we have a fixed *monomial order*, denoted by $\geq_T$, on the set of monomials of A. For a nonzero element f of A, we define *the leading coefficient* $\text{lc}(f)$, *the leading monomial* $\text{lm}(f)$, *the leading term it* (f), and *the degree* $\deg(f) \in \mathbb{N}^n$ as in [2]. We define a *Gröbner basis* of an ideal I of A as a finite set G of polynomials such that, the set of the leading terms of elements of G generates in A the same ideal as the set of the leading terms of all the elements of I (see [4], page 1007).

Definition 1.1. Let E be a finite subset of $A \setminus \{0\}$. Then

$$m(E) := (\max_{e\in E} \deg(e)_1, \ldots, \max_{e\in E} \deg(e)_n) \in \mathbb{N}^n.$$

The next proposition is *the Insa-Pauer criterion*.

Proposition 1.2 ([3], [4])**.** *Let G be a finite subset of $A \setminus \{0\}$ and let I be the left ideal generated by G. For any nonempty subset $E \subseteq G$, let S_E be a finite set of generators of the R-module*

$$\{(c_e)_{e\in E} \mid \sum_{e\in E} c_e \mathrm{lc}(e) = 0\}$$

of syzygies of the family $(\mathrm{lc}(e))_{e\in E}$. Then, the following assertions are equivalent:

(i) *G is a Gröbner basis of I*;

(ii) *for all $E \subseteq G$ and for all $(\mathrm{lc}(e))_{e\in E} \in S_E$, a remainder of*

$$\sum_{e\in E} c_e X^{m(E)-\deg(e)} e,$$

after division by G, is zero.

In the case of polynomials over a field, it is important to know whether a set $G = \{f, g\}$, consisting of two polynomials, is a Gröbner basis of the ideal $I = < f, g >$ since that can be used for faster versions of the Buchberger's criterion (see [1], page 125). The following proposition gives a simple test for that.

Proposition 1.3 ([1], Lemma 3.3.1)**.** *Let $f, g \in K[X_1, \ldots, X_n]$. Then $G = \{f, g\}$ is a Gröbner basis of $I = < f, g >$, if and only if $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$ are relatively prime.*

In the case of general Noetherian commutative rings, knowing when a set $G = \{f, g\}$ is a Gröbner basis of $I = < f, g >$ is also a part of possible analogous improvements. However, it is much more complicated

to find conditions when that happens. The purpose of this note is to give necessary and sufficient conditions for a set $G = \{f, g\}$ to be a Gröbner basis of $I = < f, g >$ in a special situation. The general characterization is a *question* that we raise here.

2. Two-Element Gröbner Bases Over Noetherian Commutative Rings

Theorem 2.1. *Let* $f = c_{\mu(1)}X^{\mu(1)} + c_{\mu(2)}X^{\mu(2)}$ *and* $g = d_\nu X^\nu$ *be two elements of* $A = R[X_1, \ldots, X_n]$ *such that*

$$< d_\nu >: c_{\mu(1)} \subseteq < d_\nu >: c_{\mu(2)}. \tag{1}$$

Let $G = \{f, g\}$ *and* $I = < f, g >$. *Then G is a Gröbner basis of I, if and only if one of the following two cases, excluding each other, occurs*:

(a) *a stronger condition*

$$< d_\nu >: c_{\mu(1)} \subseteq \mathrm{Ann}(c_{\mu(2)}) \tag{2}$$

holds;

(b) (3) *and* ((4) *or* (5)) *hold, where*

$$< d_\nu >: c_{\mu(1)} \not\subseteq \mathrm{Ann}(c_{\mu(2)}), \tag{3}$$

$$\mathrm{Ann}(c_{\mu(1)}) \subseteq \mathrm{Ann}(c_{\mu(2)}), \tag{4}$$

$$\mu(2) \geq_{\mathrm{coord}} \nu. \tag{5}$$

Proof. In the proof, we use the Insa-Pauer criterion (Proposition 1.2).

Suppose G is a Gröbner basis of I.

Let $E = \{f\}$. Let (h) be a generating homogeneous syzygy of $(\mathrm{lt}(f))$. It has the form $h = a \in R$, where $a \in \mathrm{Ann}(c_{\mu(1)})$. The polynomial

$$s = hf = ac_{\mu(2)}X^{\mu(2)},$$

has 0 as a remainder when divided by G. Hence either $a \in \mathrm{Ann}(c_{\mu(2)})$, or, otherwise, $a \notin \mathrm{Ann}(c_{\mu(2)})$, and

$$ac_{\mu(2)}X^{\mu(2)} = l_1(c_{\mu(1)}X^{\mu(1)} + c_{\mu(2)}X^{\mu(2)}) + l_2 \cdot d_\nu X^\nu,$$

where $l_1, l_2 \in A$ are such that

$$X^{\mu(2)} = \max_{\geq T}(\mathrm{lm}(l_1)X^{\mu(1)}, \mathrm{lm}(l_2)X^\nu).$$

Hence $l_1 = 0$ and so $X^\nu | X^{\mu(2)}$. In other words,

$$\mu(2) \geq_{\mathrm{coord}} \nu.$$

Then $l_2 = eX^{\mu(2)-\nu}$, where $e \in R$ is such that

$$ac_{\mu(2)} = ed_\nu,$$

i.e.,

$$a \in < d_\nu >: c_{\mu(2)}.$$

To summarize, we have the following two options, excluding each other: The option (i) described by the condition (4) and the option (ii) described by the conditions:

$$\mathrm{Ann}(c_{\mu(1)}) \not\subseteq \mathrm{Ann}(c_{\mu(2)}), \tag{6}$$

$$\mathrm{Ann}(c_{\mu(1)}) \subseteq < d_\nu >: c_{\mu(2)}, \tag{7}$$

and the condition (5). Note that (7) is redundant since it follows from (1).

The case $E = \{g\}$ does not give any conditions.

Let $E = \{f, g\}$. Let (h_1, h_2) be a generating homogeneous syzygy of $(\mathrm{lt}(f), \mathrm{lt}(g))$. It has the form

$$(h_1, h_2) = (aX^\nu, bX^{\mu(1)}),$$

for some $a, b \in R$ such that

$$ac_{\mu(1)} + bd_{\nu} = 0.$$

The polynomial

$$s = h_1 f + h_2 g = ac_{\mu(2)} X^{\nu+\mu(2)},$$

has 0 as a remainder when divided by G. Hence either $a \in \mathrm{Ann}(c_{\mu(2)})$, or, otherwise, $a \notin \mathrm{Ann}(c_{\mu(2)})$, and

$$ac_{\mu(2)} X^{\nu+\mu(2)} = l_1 (c_{\mu(1)} X^{\nu(1)} + c_{\mu(2)} X^{\mu(2)}) + l_2 \cdot d_{\nu} X^{\nu}, \tag{8}$$

for some $l_1, l_2 \in A$ such that

$$X^{\nu+\mu(2)} = \max_{\geq T}(\mathrm{lm}(l_1) X^{\mu(1)}, \mathrm{lm}(l_2) X^{\nu}). \tag{9}$$

So, to the previously described options (i) and (ii), we add one of the following two conditions (which exclude each other):

$$(\forall (a, b) \in \mathrm{Syz}(c_{\mu(1)}, d_{\nu})) \quad a \in \mathrm{Ann}(c_{\mu(2)}), \tag{10}$$

$$(\exists (a, b) \in \mathrm{Syz}(c_{\mu(1)}, d_{\nu})) \quad a \notin \mathrm{Ann}(c_{\mu(2)}), \tag{11}$$

that can also be formulated as (2) (which is equivalent to (10)), or (3) and

$$(\forall a \in (\, < d_{\nu} >: c_{\mu(1)}) \setminus \mathrm{Ann}(c_{\mu(2)})) \text{ (8) and (9) hold} \tag{12}$$

(where (3) and (12) are equivalent to (11)).

The option (i), with the condition (2) added, gives sufficient conditions for G to be a Gröbner basis. Since the condition (4) is weaker than the condition (2), this option is characterized just by the condition (2). The option (ii), with the condition (2) added, has two contradicting conditions, so it is not possible.

Now, we analyze each of the options (i) and (ii) with the condition (3) added. We will call them the options (iii) and (iv), respectively.

First, we analyze the option (iii). So far, we have the conditions (4), (3), and (12) describing it. It follows from (1) that the condition

$$(< d_\nu >: c_{\mu(1)}) \setminus \mathrm{Ann}(c_{\mu(2)}) \subseteq < d_\nu >: c_{\mu(2)} \tag{13}$$

holds. The condition (13) implies the condition (12). Indeed, it implies that $ac_{\mu(2)} \in < d_\nu >$, hence $ac_{\mu(2)} = ed_\nu$, where $ed_\nu \neq 0$. So, if we put $l_1 = 0$ and $l_2 = eX^{\mu(2)}$, we have the Equations (8) and (9) satisfied. Hence, the conditions (4) and (3) are sufficient condition for G to be a Gröbner basis.

Now, we analyze the option (iv). So far, we have the conditions (6), (5), (3), and (12) (the first of which is redundant) describing it. It follows from (1) that the condition (13) holds and, as before, the condition (13) implies the condition (12). Hence, the conditions (5) and (3) are sufficient conditions for G to be a Gröbner basis. Now combining the options (iii) and (iv), we get the case (b) from the statement and the option (i) is the case (a). These two cases are sufficient for G to be a Gröbner basis.

It follows from the proof that they are also necessary.

This finishes the proof of the theorem. □

Example 2.2. (i) $f = \overline{2}X^2Y^3 + \overline{4}XY^4$, $g = \overline{3}X^3Y \in \mathbb{Z}_6[X, Y]$. Here, the condition (2) holds, so $\{f, g\}$ is a Gröbner basis of $< f, g >$.

(ii) $f = \overline{2}X^3Y^3 + \overline{4}XY^4$, $g = \overline{2}X^2Y^2 \in \mathbb{Z}_6[X, Y]$. Here, the conditions (1), (3), and (4) hold, so $\{f, g\}$ is a Gröbner basis of $< f, g >$.

(iii) $f = \overline{3}X^4Y + \overline{4}X^2Y^3$, $g = \overline{2}XY^2 \in \mathbb{Z}_6[X, Y]$. Here, the conditions (1), (3), and (5) hold, so $\{f, g\}$ is a Gröbner basis of $< f, g >$.

(iv) $f = \overline{3}X^4Y + \overline{4}X^2Y^3$, $g = \overline{2}XY^4 \in \mathbb{Z}_6[X, Y]$. Here, the conditions (1) and (3) hold, but neither (4) nor (5) holds, so $\{f, g\}$ is not a Gröbner basis of $< f, g >$.

References

[1] W. W. Adams and P. Loustaunau, An Introduction to Gröbner Bases, Graduate Studies in Mathematics, Vol. 3, AMS, Providence, R.I., 1994.

[2] D. Cox, J. Little and D. O'Shea, Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer, 2007.

[3] M. Insa and F. Pauer, Gröbner Bases in Rings of Differential Operators, B. Buchberger and F. Winkler, Gröbner Bases and Applications, London Mathematical Society Lecture Notes Series, Vol. 151, Cambridge University Press, (1988), 367-380.

[4] F. Pauer, Gröbner bases with coefficients in rings, J. Symbolic Comput. 42 (2007), 1003-1011.

■