A dynamical solution to Kronecker's problem

Ihsen Yengui ([1])

October 14, 2005

Abstract

In this paper, I present a new decision procedure for the ideal membership problem for polynomial rings over principal domains using discrete valuation domains. As a particular case, I solve a fundamental algorithmic question in the theory of multivariate polynomials over the integers called "Kronecker's problem", that is the problem of finding a decision procedure for the ideal membership problem for $\mathbb{Z}[X_1, \ldots, X_n]$. The techniques utilized are easily generalizable to Dedekind domains. In order to avoid the expensive complete factorization in the basic principal ring, I introduce the notion of "dynamical Gröbner bases" of polynomial ideals over a principal domain. As application, I give an alternative dynamical solution to "Kronecker's problem".

Key words : Dynamical Gröbner basis, ideal membership problem, principal domains.

Introduction

The concept of Gröbner basis was originally introduced by Buchberger in his Ph.D. thesis (1965) in order to solve the ideal membership problem for polynomial rings over a field [4]. The ideal membership problem has received considerable attention from the constructive algebra community resulting in algorithms that generalize the work of Buchberger. Our goal is to use dynamical methods in order to give a decision procedure for the ideal membership problem for polynomial rings over a principal domain. The case where the basic ring is $\mathbb{Z}$ is called "Kronecker's problem" and has been treated by many authors [1, 2, 8, 9, 11].

Recall that the notion of "dynamical proofs" comes from the work of Coste, Lombardi, and Roy in [5] and was inspired by the notion of dynamical evaluation introduced in computer algebra by Duval and Reynaud [7].

Our starting point is the method explained in [1, 11]. Let us recall the strategy of this method. Begin by noting that for a principal domain $\mathbf{R}$ with field of fractions $\mathbf{F}$, a necessary condition so that $f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{R}[X_1, \ldots, X_n]$ is: $f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{F}[X_1, \ldots, X_n]$.
Suppose that this condition is fulfilled, that is there exists $d \in \mathbf{R} \setminus \{0\}$ such that

$$d\, f \in \langle f_1, \ldots, f_s \rangle \text{ in } \mathbf{R}[X_1, \ldots, X_n]. \quad (0)$$

Since the basic ring $\mathbf{R}$ is principal and a fortiori factorial, we can write $d = u p_1^{n_1} \cdots p_\ell^{n_\ell}$, where the p_i are distinct irreducible elements in $\mathbf{R}$, u is invertible in $\mathbf{R}$, and $n_i \in \mathbb{N}$. Another necessary condition so that $f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{R}[X_1, \ldots, X_n]$ is: $f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{R}_{p_i\mathbf{R}}[X_1, \ldots, X_n]$ for each $1 \leq i \leq \ell$.
Write:

$$d_i\, f \in \langle f_1, \ldots, f_s \rangle \text{ in } \mathbf{R}[X_1, \ldots, X_n] \text{ for some } d_i \in \mathbf{R} \setminus p_i\mathbf{R}. \quad (i)$$

Since $\gcd(d, d_1, \ldots, d_\ell) = 1$, by combining equalities asserting $(0), (1), \ldots, (\ell)$ using a Bezout identity between $d, d_1, \ldots, d_\ell$, we can find an equality asserting that $f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{R}[X_1, \ldots, X_n]$. Thus, the necessary conditions are sufficient and it suffices to treat the problem in case the basic ring is a

[1] Departement of Mathematics, Faculty of Sciences of Sfax, 3018 Sfax, Tunisia. Email: ihsen.yengui@fss.rnu.tn

discrete valuation domain. The notions of Gröbner basis and S-polynomials, originally introduced by Buchberger, have been adapted in [11] to discrete valuation domains.

This method raises the following question:

How to avoid the expensive problem of factorizing an element in a factorial domain into a finite product of irreducible elements ?

The fact that the method developed in [11] is based on gluing "local realizability" appeals to the use of dynamical methods and more precisely, as will be explained later in this paper, the use of a new notion of Gröbner basis, namely the notion of "dynamical Gröbner basis" [12]. Our goal is to mimic dynamically as much as we can the method used in [11]. A key fact is that for any two nonzero elements a and b in a principal domain $\mathbf{R}$, writing $a = (a \wedge b)a'$, $b = (a \wedge b)b'$, with $a' \wedge b' = 1$, then a divides b in $\mathbf{R}_{a'}$ and b divides a in $\mathbf{R}_{b'}$, where for any nonzero $x \in \mathbf{R}$, R_x denotes the localization of $\mathbf{R}$ at the multiplicative subset S_x generated by x. Moreover, note that the two multiplicative subsets $S_{a'}$ and $S_{b'}$ are comaximal, that is, for any $x \in S_{a'}$ and $y \in S_{b'}$, the ideal $\langle x, y\rangle$ contains 1. Of course, this precious fact will enable us to go back from the leaves to the root of the evaluation tree produced by our dynamical method. In other words, this will make the gluing of "local realizability" possible.

The undefined terminology is standard as in [6] and [10].

1 Gröbner basis over a valuation domain

Definitions 1. Let $\mathbf{R}$ be a ring, $f = \sum_\alpha a_\alpha X^\alpha$ a nonzero polynomial in $\mathbf{R}[X_1, \dots, X_n]$, E a non empty subset of $\mathbf{R}[X_1, \dots, X_n]$, and $>$ a monomial order.

(i) The X^α (resp. the $a_\alpha X^\alpha$) are called the monomials (resp. the terms) of f.
(ii) The multidegree of f is $\mathrm{mdeg}(f) := \max\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}$.
(iii) The leading coefficient of f is $\mathrm{LC}(f) := a_{\mathrm{mdeg}(f)} \in \mathbf{R}$.
(iv) The leading monomial of f is $\mathrm{LM}(f) := X^{\mathrm{mdeg}(f)}$.
(v) The leading term of f is $\mathrm{LT}(f) := \mathrm{LC}(f)\,\mathrm{LM}(f)$.
(vi) $\mathrm{LT}(E) := \{\mathrm{LT}(g), g \in E\}$.
(vii) $\langle \mathrm{LT}(E)\rangle := \langle \mathrm{LT}(g), g \in E\rangle$ (ideal of $\mathbf{R}[X_1, \dots, X_n]$).

Definitions 2. Let $\mathbf{R}$ be a valuation domain, $f, g \in \mathbf{R}[X_1, \dots, X_n] \setminus \{0\}$, $I = \langle f_1, \dots, f_s\rangle$ a nonzero finitely generated ideal of $\mathbf{R}[X_1, \dots, X_n]$, and $>$ a monomial order.

(i) If $\mathrm{mdeg}(f) = \alpha$ and $\mathrm{mdeg}(g) = \beta$ then let $\gamma = (\gamma_1, \dots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. The S-polynomial of f and g is the combination:

$S(f, g) = \frac{X^\gamma}{\mathrm{LM}(f)} f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \frac{X^\gamma}{\mathrm{LM}(g)} g$ if $\mathrm{LC}(g)$ divides $\mathrm{LC}(f)$.

$S(f, g) = \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} \frac{X^\gamma}{\mathrm{LM}(f)} f - \frac{X^\gamma}{\mathrm{LM}(g)} g$ if $\mathrm{LC}(f)$ divides $\mathrm{LC}(g)$ and $\mathrm{LC}(g)$ does not divide $\mathrm{LC}(f)$.

(ii) $G = \{f_1, \dots, f_s\}$ is said to be a Gröbner basis for I if $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(f_1), \dots, \mathrm{LT}(f_s)\rangle$.

(iii) As in the classical division algorithm in $\mathbf{F}[X_1, \dots, X_n]$ ($\mathbf{F}$ field) (see [6], page 61), for each polynomials $h, h_1, \dots, h_m \in \mathbf{R}[X_1, \dots, X_n]$, there exist $q_1, \dots, q_m, r \in \mathbf{R}[X_1, \dots, X_n]$ such that

$$h = q_1 h_1, + \cdots + q_m h_m + r,$$

where either $r = 0$ or r is a sum of terms none of which is divisible by any of $\mathrm{LT}(h_1), \dots, \mathrm{LT}(h_m)$. The polynomial r is called a remainder of h on division by $H = \{h_1, \dots, h_m\}$ and denoted $r = \overline{h}^H$.

Lemma 1. *Let $\mathbf{R}$ be a valuation domain and $I = \langle a_\alpha X^\alpha, \alpha \in A\rangle$ an ideal of $\mathbf{R}[X_1, \dots, X_n]$ generated by a collection of terms. Then a term bX^β lies in I if and only if X^β is divisible by X^α and b is divisible by a_α for some $\alpha \in A$.*

Lemma 2 (Dickson's Lemma for discrete valuation domains). *Let* $\mathbf{R}$ *be a discrete valuation domain and* $I = \langle a_\alpha X^\alpha, \alpha \in A\rangle$ *an ideal of* $\mathbf{R}[X_1, \ldots, X_n]$ *generated by a collection of terms. Then there exist* $\alpha_1, \ldots, \alpha_s \in A$ *such that* $I = \langle a_{\alpha_1} X^{\alpha_1}, \ldots, a_{\alpha_s} X^{\alpha_s}\rangle$.

Using Lemma 1 and Lemma 2, we generalize some classical results about the existence of Gröbner basis for ideals in polynomial rings over discrete valuations domains.

Theorem 1. *Let* $\mathbf{R}$ *be a discrete valuation domain,* I *a nonzero ideal of* $\mathbf{R}[X_1, \ldots, X_n]$*, and fix a monomial order* $>$*. Then,* I *has a Gröbner basis* G*, and for each* $f \in \mathbf{R}[X_1, \ldots, X_n]$*,* $f \in I$ *if and only if the remainder on division of* f *by* G *is zero.*

The following lemma will be of big utility since it is the missing key for the characterization of Gröbner bases by means of S-polynomials (see [6], page 82).

Lemma 3. *Let* $\mathbf{R}$ *be a valuation domain,* $>$ *a monomial order, and* $f_1, \ldots, f_s \in \mathbf{R}[X_1, \ldots, X_n]$ *such that* $\mathrm{mdeg}(f_i) = \gamma$ *for each* $1 \leq i \leq s$*. If* $\mathrm{mdeg}(\sum_{i=1}^{s} a_i f_i) < \gamma$ *for some* $a_1, \ldots, a_s \in \mathbf{R}$*, then* $\sum_{i=1}^{s} a_i f_i$ *is a linear combination with coefficients in* $\mathbf{R}$ *of the S-polynomials* $S(f_i, f_j)$ *for* $1 \leq i, j \leq s$*. Furthermore, each* $S(f_i, f_j)$ *has multidegree* $< \gamma$*.*

Theorem 2. *Let* $\mathbf{R}$ *be a valuation domain ,* $I = \langle g_1, \ldots, g_s\rangle$ *an ideal of* $\mathbf{R}[X_1, \ldots, X_n]$*, and fix a monomial order* $>$*. Then,* $G = \{g_1, \ldots, g_s\}$ *is a Gröbner basis for* I *if and only if for all pairs* $i \neq j$*, the remainder on division of* $S(g_i, g_j)$ *by* G *is zero.*

Buchberger's Algorithm for discrete valuation domains. *Let* $\mathbf{R}$ *be a discrete valuation domain,* $I = \langle g_1, \ldots, g_s\rangle$ *a nonzero ideal of* $\mathbf{R}[X_1, \ldots, X_n]$*, and fix a monomial order* $>$*. Then, a Gröbner basis for* I *can be computed in a finite number of steps by the following algorithm:*

```
Input: $g_1, \ldots, g_s$
Output: a Gröbner basis $G$ for $\langle g_1, \ldots, g_s\rangle$ with $\{g_1, \ldots, g_s\} \subseteq G$

$G := \{g_1, \ldots, g_s\}$
REPEAT
$G' := G$
For each pair $f \neq g$ in $G'$ DO
    $S := \overline{S(f,g)}^{G'}$
    If $S \neq 0$ THEN $G := G' \cup \{S\}$
UNTIL $G = G'$
```

A natural question arising is :

For a valuation domain $\mathbf{R}$*, is it always possible to compute a Gröbner basis for each finitely generated nonzero ideal of* $\mathbf{R}[X_1, \ldots, X_n]$ *by Buchberger's Algorithm in a finite number of steps ?*

In fact, for a discrete valuation domain, what makes Buchberger's Algorithm work in a finite number of steps is the fact that the totally ordered group ($= \mathbb{Z}$) corresponding to this valuation is well-ordered (note that, conversely, a well-ordered group is isomorphic to $\mathbb{Z}$). Unfortunately, if the totally ordered group corresponding to the valuation is not archimedian, Buchberger's Algorithm does not always work in a finite number of steps as can be seen by the following example.

Example 1. Let $\mathbf{V}$ be a valuation domain with a corresponding valuation v and group G. Suppose that G is not archimedian, that is there exist $a, b \in \mathbf{V}$ such that:

$$v(a) > 0, \text{ and } \forall\, n \in \mathbb{N}^*,\ v(b) > n\, v(a).$$

Denote by I the ideal of $\mathbf{V}[X]$ generated by $g_1 = aX + 1$ and $g_2 = b$.

Since $S(g_1, g_2) = (\frac{b}{a})g_1 - Xg_2 = \frac{b}{a}$ and $\frac{b}{a}$ is not divisible by b, then one must add $g_3 = \frac{b}{a}$ when executing Buchberger's Algorithm .
In the same way, $S(g_1, g_3) = (\frac{b}{a^2})g_1 - Xg_3 = \frac{b}{a^2}$ and $\frac{b}{a^2}$ is not divisible by b nor by $\frac{b}{a}$. Thus, one must add $g_4 = \frac{b}{a^2}$, and so on, we observe that Buchberger's Algorithm does not terminate.

Taking the particular case $G = \mathbb{Z} \times \mathbb{Z}$ equipped with the lexicographic order, $a = (0, 1)$, and $b = (1, 0)$. We can prove $\langle \mathrm{LT}(I) \rangle$ is not finitely generated despite that I is finitely generated and that clearly $\langle \mathrm{LC}(I) \rangle = \langle a \rangle$ (there is no such example in the literature).

As a consequence of this example, keeping the notations above, we know that a necessary condition so that Buchberger's Algorithm terminates is that the group G is archimedian (this is in fact equivalent to $\dim \mathbf{V} \leq 1$, see for example Proposition 8 page 116 in [3]). Moreover, we already know that a sufficient condition is that G is well-ordered (this is in fact equivalent to that $\mathbf{V}$ is a discrete valuation domain). This encourages us to set the following three conjectures :

Conjecture 1. *Let $\mathbf{V}$ be a valuation domain with corresponding valuation group G, $n \in \mathbb{N}^*$, and fix a monomial order $>$ in $\mathbf{V}[X_1, \ldots, X_n]$. Then the following assertions are equivalent:*

(i) It is always possible to compute a Gröbner basis for each finitely generated nonzero ideal of $\mathbf{V}[X_1, \ldots, X_n]$ by the generalized version of Buchberger's Algorithm for valuation domains in a finite number of steps.

(ii) G is archimedian ($\Leftrightarrow$ $\dim \mathbf{V} \leq 1$).

Conjecture 2. *Let $\mathbf{V}$ be a valuation domain (Prüfer domain) with a corresponding valuation group G, $n \in \mathbb{N}^*$, and fix a monomial order $>$ in $\mathbf{V}[X_1, \ldots, X_n]$. Then the following assertions are equivalent:*

(ii) $\dim \mathbf{V} \leq 1$ ($\Leftrightarrow$ G is archimedian).

(iii) For each finitely generated ideal I of $\mathbf{V}[X_1, \ldots, X_n]$, the ideal $\{\mathrm{LT}(f), f \in I\}$ of $\mathbf{V}[X_1, \ldots, X_n]$ is finitely generated.

Conjecture 3. *Let $\mathbf{V}$ be a valuation domain (Prüfer domain), $n \in \mathbb{N}^*$, and fix a monomial order $>$ in $\mathbf{V}[X_1, \ldots, X_n]$. Then for each finitely generated ideal I of $\mathbf{V}[X_1, \ldots, X_n]$, the ideal $\{\mathrm{LC}(f), f \in I\}$ of $\mathbf{V}$ is finitely generated.*

2 The ideal membership problem and Gröbner basis over a principal domain

2.1 The ideal membership problem over a principal domain

As explained in the introduction, if $\mathbf{R}$ is a principal domain with field of fractions $\mathbf{F}$, to answer the question $\mathbf{Q}$:

$$f \in ?\ \langle f_1, \ldots, f_s \rangle \text{ in } \mathbf{R}[X_1, \ldots, X_n],$$

one should first answer the question $\mathbf{Q}_0$:

$$f \in ?\ \langle f_1, \ldots, f_s \rangle \text{ in } \mathbf{F}[X_1, \ldots, X_n].$$

If the answer to $\mathbf{Q}_0$ is negative then so is the answer to $\mathbf{Q}$. If positive, there exists $d \in \mathbf{R} \setminus \{0\}$ such that

$$d\, f \in \langle f_1, \ldots, f_s \rangle \ \text{ in } \mathbf{R}[X_1, \ldots, X_n]. \quad (0)$$

Since the basic ring is principal and a fortiori factorial, we can write $d = up_1^{n_1} \cdots p_\ell^{n_\ell}$, where the p_i are distinct irreducible elements in $\mathbf{R}$, u is invertible in $\mathbf{R}$, and $n_i \in \mathbb{N}$. The answer to the question $\mathbf{Q}$ is positive if and only if for all $1 \leq i \leq \ell$, the answer to the question $\mathbf{Q}_{p_i}$:

$$f \in ?\ \langle f_1, \ldots, f_s \rangle \text{ in } \mathbf{R}_{p_i\mathbf{R}}[X_1, \ldots, X_n],$$

is positive.

In case of positive answers, for each $1 \leq i \leq \ell$, write:

$$d_i\, f \in \langle f_1, \dots, f_s \rangle \text{ in } \mathbf{R}[X_1, \dots, X_n] \text{ for some } d_i \in \mathbf{R} \setminus p_i\mathbf{R}. \quad (i)$$

Since $\gcd(d, d_1, \dots, d_\ell) = 1$, by combining equalities asserting $(0), (1), \dots, (\ell)$ using a Bezout identity between $d, d_1, \dots, d_\ell$, we can find an equality asserting that $f \in \langle f_1, \dots, f_s \rangle$ in $\mathbf{R}[X_1, \dots, X_n]$.

As a conclusion, solving the ideal membership problem $\mathbf{Q}$ amounts to the resolution of a finite number of ideal membership problems $\mathbf{Q}_0$,$\mathbf{Q}_{p_1}$, . . . , $\mathbf{Q}_{p_\ell}$ over localizations of the basic ring $\mathbf{R}$.

2.2 What is a Gröbner basis over a principal domain ?

Let $\mathbf{R}$ be a principal domain with field of fractions $\mathbf{F}$, and $I = \langle f_1, \dots, f_s \rangle$ an ideal of $\mathbf{R}[X_1, \dots, X_n]$. We have seen that the first step to solve the ideal membership problem over $\mathbf{R}[X_1, \dots, X_n]$ is to solve it over $\mathbf{F}[X_1, \dots, X_n]$.

Let $G_0 = \{g_1, \dots, g_m\}$ be a Gröbner basis for $\langle f_1, \dots, f_s \rangle$ in $\mathbf{F}[X_1, \dots, X_n]$. For each $1 \leq j \leq m$, write $g_j = \frac{h_j}{c}$ and $\mathrm{LC}(g_j) = \frac{c_j}{c}$, where $c, c_j \in \mathbf{R} \setminus \{0\}$ and $h_j \in \mathbf{R}[X_1, \dots, X_n]$. Denoting by $p_1, \dots, p_\ell$ the distinct irreducible elements in $\mathbf{R}$ dividing one of $c, c_1, \dots, c_m$, it is easy to see $p_1, \dots, p_\ell$ are the only irreducible elements in $\mathbf{R}$ that may appear as factors of the denominators of the quotients of the division of a polynomial in $\mathbf{R}[X_1, \dots, X_n]$ by G_0. Let $G_{p_1}, \dots, G_{p_\ell}$ be Gröbner bases for $\langle f_1, \dots, f_s \rangle$ respectively in $\mathbf{R}_{p_i\mathbf{R}}[X_1, \dots, X_n]$, $1 \leq i \leq \ell$, as explained in the first section. From the survey made previously, it is natural to suggest that the finite set $G = \{G_0, G_{p_1}, \dots, G_{p_\ell}\}$ will be called a Gröbner basis for $I = \langle f_1, \dots, f_s \rangle$ in $\mathbf{R}[X_1, \dots, X_n]$. An element $f \in \mathbf{R}[X_1, \dots, X_n]$ belongs to I if and only if all the remainders $r_0, r_1, \dots, r_\ell$ on division of f respectively by $G_0, G_{p_1}, \dots, G_{p_\ell}$ are zero (the set $r = \{r_0, r_1, \dots, r_\ell\}$ will be called the remainder on division of f by G).

2.3 An example

Example 2. This example illustrates the simplicity of our method. Let consider the ideal membership problem

$$f = 5X^3Y + 2X^2 + 3XY^2 + 4Y - 7 \quad \in ? \ \langle f_1 = 3XY + 4, f_2 = 2X^2 + 3 \rangle \text{ in } \mathbb{Z}[X, Y].$$

Let fix the lexicographic order as monomial order with $X > Y$. By executing Buchberger's Algorithm in $\mathbb{Q}[X, Y]$, $G_0 = \{f_1, f_2, \frac{4}{3}X - \frac{3}{2}Y, \frac{9}{8}Y^2 + \frac{4}{3}\}$ is a Gröbner basis for $\langle f_1, f_2 \rangle$. The response to the ideal membership problem in $\mathbb{Q}[X, Y]$ is positive. One obtains:

$$f = (\frac{5}{3}X^2 + Y)f_1 - \frac{7}{3}f_2.$$

By clearing the denominators, one gets:

$$3f = (5X^2 + 3Y)f_1 - 7f_2. \quad (1)$$

It remains only to execute Buchberger's Algorithm in $\mathbb{Z}_{(3)}[X, Y]$ as explained in this paper. One obtains $G_3 = \{f_1, f_2, 4X - \frac{9}{2}Y, \frac{27}{8}Y^2 + 4\}$ as a Gröbner basis for $\langle f_1, f_2 \rangle$ in $\mathbb{Z}_{(3)}[X, Y]$.

Thus, $G = \{\{f_1, f_2, \frac{4}{3}X - \frac{3}{2}Y, \frac{9}{8}Y^2 + \frac{4}{3}\}, \{f_1, f_2, 4X - \frac{9}{2}Y, \frac{27}{8}Y^2 + 4\}\}$ is a Gröbner basis for $I = \langle f_1, f_2 \rangle$ in $\mathbb{Z}[X, Y]$.

The response to the ideal membership problem in $\mathbb{Z}_{(3)}[X, Y]$ is positive. One obtains:

$$f = (Y - \frac{5}{2})f_1 + (\frac{5}{2}XY + 1)f_2.$$

By clearing the denominators, one gets:

$$2f = (2Y-5)f_1 + (5XY+2)f_2. \quad (2)$$

A Bezout identity between 2 and 3 is

$$3-2=1.$$

Thus, (1) − (2) $\Rightarrow$ $f = (5X^2+Y+5)f_1 + (-5XY-9)f_2$, a complete positive answer.

3 The ideal membership problem and Gröbner basis over a Dedekind domain

All what is made in this paper for principal domains can easily be generalized to Dedekind domains (see [10] for a constructive study of Dedekind domains).
In order to avoid repetition, we keep the notations of the introduction, just suppose that $\mathbf{R}$ is a Dedekind domain. The factorization $d = p_1^{n_1}\cdots p_\ell^{n_\ell}$, is replaced by a decomposition of the principal ideal $\langle d\rangle$ into a finite product of nonzero prime ideals $\mathfrak{p}_i$ of $\mathbf{R}$, say

$$\langle d\rangle = \prod_{i=1}^{\ell} \mathfrak{p}_i^{n_i}.$$

Of course, all the rings $\mathbf{R}_{\mathfrak{p}_i}$ are discrete valuation domains in which the techniques of Section 1 apply. In case of positive answers in the rings $\mathbf{R}_{\mathfrak{p}_i}$, for each $1\le i\le \ell$, one can find $d_i \in \mathbf{R}\setminus \mathfrak{p}_i$ such that

$$d_i\, f \in \langle f_1,\ldots,f_s\rangle \text{ in } \mathbf{R}[X_1,\ldots,X_n].$$

Since no prime of $\mathbf{R}$ contains the ideal $\langle d, d_1,\ldots,d_\ell\rangle$, we infer that $1\in\langle d,d_1,\ldots,d_\ell\rangle$. Moreover, since all the ideals of $\mathbf{R}$ are detachable (see [10], page 331), we can find explicitly an equality $\alpha d + \alpha_1 d_1 + \cdots + \alpha_\ell d_\ell = 1$, $\alpha_i \in \mathbf{R}$, asserting that $1\in\langle d,d_1,\ldots,d_\ell\rangle$, and so on exactly as in the principal domain case.

For the notion of Gröbner basis for an ideal in polynomial ring over a discrete Dedekind domain, it is the same as in the principal domain case, just for an element $a\in\mathbf{R}\setminus\{0\}$, replace the irreducible factors of a by the prime ideals of $\mathbf{R}$ appearing in the decomposition of the principal ideal $\langle a\rangle$ into a finite product of nonzero prime ideals of $\mathbf{R}$.

4 Dynamical Gröbner basis over a principal domain

Definition 1 *Let $\mathbf{R}$ be an integral ring, $f,g\in\mathbf{R}[X_1,\ldots,X_n]$, $f\neq 0$, $f\neq 0$, $I=\langle f_1,\ldots,f_s\rangle$ a nonzero finitely generated ideal of $\mathbf{R}[X_1,\ldots,X_n]$, and $>$ a monomial order.*

1) If $\mathrm{mdeg}(f)=\alpha$ and $\mathrm{mdeg}(g)=\beta$ then let $\gamma=(\gamma_1,\ldots,\gamma_n)$, where $\gamma_i=\max(\alpha_i,\beta_i)$ for each i.
If $\mathrm{LC}(g)$ divides $\mathrm{LC}(f)$ or $\mathrm{LC}(f)$ divides $\mathrm{LC}(g)$, the S-polynomial of f and g is the combination:

$S(f,g) = \frac{X^\gamma}{\mathrm{LM}(f)}f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)}\frac{X^\gamma}{\mathrm{LM}(g)}g$ *if* $\mathrm{LC}(g)$ *divides* $\mathrm{LC}(f)$.

$S(f,g) = \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)}\frac{X^\gamma}{\mathrm{LM}(f)}f - \frac{X^\gamma}{\mathrm{LM}(g)}g$ *if* $\mathrm{LC}(f)$ *divides* $\mathrm{LC}(g)$ *and* $\mathrm{LC}(g)$ *does not divide* $\mathrm{LC}(f)$.

2) As in the classical division algorithm in $\mathbf{F}[X_1,\ldots,X_n]$ ($\mathbf{F}$ field) (see [6], page 61), for each polynomials $h,h_1,\ldots,h_m\in\mathbf{R}[X_1,\ldots,X_n]$, there exist $q_1,\ldots,q_m,r\in\mathbf{R}[X_1,\ldots,X_n]$ such that

$$h = q_1h_1, + \cdots + q_mh_m + r,$$

where either $r=0$ or r is a sum of terms none of which is divisible by any of $\mathrm{LT}(h_1),\ldots,\mathrm{LT}(h_m)$. The polynomial r is called a remainder of h on division by $H=\{h_1,\ldots,h_m\}$ and denoted $r=\overline{h}^H$.

3) For $g_1, \dots, g_t \in \mathbf{R}[X_1, \dots, X_n]$, $G = \{g_1, \dots, g_t\}$ is said to be a Gröbner basis for I if $I = \langle g_1, \dots, g_t\rangle$, the set $\{\mathrm{LC}(g_1), \dots, \mathrm{LC}(g_t)\}$ is totally ordered under division, and for each $i \neq j$, $\overline{S(g_i, g_j)}^G = 0$.

4) S is said to be a multiplicative subset of a ring $\mathbf{R}$ if

$$S \subset \mathbf{R}, 1 \in S \text{ and } \forall x, y \in S, xy \in S.$$

If S is a multiplicative subset of a ring $\mathbf{R}$, the localization of $\mathbf{R}$ at S is the ring $S^{-1}\mathbf{R} = \{\frac{x}{s}, x \in \mathbf{R}, s \in S\}$ in which the elements of S are forced into being invertible.
If $S_1, \dots, S_k$ are multiplicative subsets of $\mathbf{R}$, we say that $S_1, \dots, S_k$ are comaximal if

$$\forall s_1 \in S_1, \dots, s_n \in S_n,\ \exists\, a_1, \dots, a_n \in \mathbf{R} \text{ such that} \sum_{i=1}^{n} a_i s_i = 1.$$

5) If $x \in \mathbf{R}$, the localization of $\mathbf{R}$ at the multiplicative subset $S_x = \{x^k, k \in \mathbb{N}\}$ generated by x is denoted by $\mathbf{R}_x$. Moreover, by induction, for each $x_1, \dots, x_k \in \mathbf{R}$, we define $\mathbf{R}_{x_1.x_2.\dots.x_k} := (\mathbf{R}_{x_1.x_2.\dots.x_{k-1}})_{x_k}$.
For $x_1, \dots, x_k \in \mathbf{R}$, the notation $G_{x_1.x_2.\dots.x_k}(I)$, or simply $G_{x_1.x_2.\dots.x_k}$, will be utilized to denote a Gröbner basis for $\langle f_1, \dots, f_s\rangle$ in $\mathbf{R}_{x_1.x_2.\dots.x_k}$.
For $f, g \in \mathbf{R}_{x_1.x_2.\dots.x_k}[X_1, \dots, X_n]$, the notation $S^{(x_1.x_2.\dots.x_k)}(f, g)$ instead of $S(f, g)$ means that $S(f, g)$ is first computed in $\mathbf{R}_{x_1.x_2.\dots.x_k}[X_1, \dots, X_n]$. If its remainder r on division by the already constructed part of the Gröbner basis is nonzero, we must add it and it will be denoted by $r^{(x_1.x_2.\dots.x_k)}$.

6) $G = \{G_1, \dots, G_k\}$, where $G_i = \{g_{1,i}, \dots, g_{n_i,i}\}$ and $g_{j,i} \in \mathbf{R}[X_1, \dots, X_n]$, is said to be a dynamical Gröbner basis for I if there exist $S_1, \dots, S_k$ multiplicative comaximal subsets of $\mathbf{R}$ such that in each localization $(S_i^{-1}\mathbf{R})[X_1, \dots, X_n]$, G_i is a Gröbner basis for $\langle f_1, \dots, f_s\rangle$.

Proposition 2
Let $\mathbf{R}$ be a principal domain, $I = \langle f_1, \dots, f_s\rangle$ a nonzero finitely-generated ideal of $\mathbf{R}[X_1, \dots, X_n]$, $f \in \mathbf{R}[X_1, \dots, X_n]$, and fix a monomial order. Suppose that $G = \{g_1, \dots, g_t\}$ is a Gröbner basis for I in $\mathbf{R}[X_1, \dots, X_n]$. Then, $f \in I$ if and only if $\overline{f}^G = 0$.

Theorem 3 (Dynamical gluing)
Let $\mathbf{R}$ be a principal domain, $I = \langle f_1, \dots, f_s\rangle$ a nonzero finitely-generated ideal of $\mathbf{R}[X_1, \dots, X_n]$, $f \in \mathbf{R}[X_1, \dots, X_n]$, and fix a monomial order. Suppose that $G = \{G_1, \dots, G_k\}$ is a dynamical Gröbner basis for I in $\mathbf{R}[X_1, \dots, X_n]$, where each G_i is a Gröbner basis for $\langle f_1, \dots, f_s\rangle$ in a localization $(S_i^{-1}\mathbf{R})[X_1, \dots, X_n]$. Then, $f \in I$ if and only if $\overline{f}^{G_i} = 0$ in $(S_i^{-1}\mathbf{R})[X_1, \dots, X_n]$ for each $1 \leq i \leq k$.

4.1 How to construct a dynamical Gröbner basis ?

Let $\mathbf{R}$ be a principal domain, $I = \langle f_1, \dots, f_s\rangle$ a nonzero finitely-generated ideal of $\mathbf{R}[X_1, \dots, X_n]$, and fix a monomial order $>$. The purpose is to construct a dynamical Gröbner basis G for I.

Dynamical version of Buchberger's Algorithm

This algorithm works like Buchberger's Algorithm for discrete valuation domains. The only difference is that it may be blocked if it has to handle two non comparable (under division) elements a, b in $\mathbf{R}$. In this situation, one should compute $d = a \wedge b$, factorize $a = da'$, $b = db'$, with $a' \wedge b' = 1$, and then open two branches : the computations are pursued in $\mathbf{R}_{a'}$ and $\mathbf{R}_{b'}$.

Comments

1) Of course, any localization of a principal domain is a principal domain.

2) This algorithm must terminate after a finite number of steps since so does Buchberger's Algorithm for discrete valuation domains [11].

3) At the end of this tree, all the obtained bases are in localizations of $\mathbf{R}$ of type $\mathbf{R}_{x_1.x_2.....x_k}$, $x_1, \dots, x_k \in \mathbf{R}$. Of course, together, all the considered multiplicative subsets of $\mathbf{R}$ are comaximal (this is due to the fact that if one needs to break the current ring $\mathbf{R}_i$, this is done by considering the rings $(\mathbf{R}_i)_{a'}$ and $(\mathbf{R}_i)_{b'}$, with $a' \wedge b' = 1$). Thus, by Theorem 3, all the obtained Gröbner bases at the leaves of the constructed "evaluation tree" form together a dynamical Gröbner basis for $\langle f_1, \dots, f_s\rangle$ in $\mathbf{R}[X_1, \dots, X_n]$.

4) This algorithm may produce many redundancies due to the fact that if G_i is a Gröbner basis for $\langle f_1, \dots, f_s\rangle$ in $\mathbf{R}_{x_1.x_2.....x_k}[X_1, \dots, X_n]$, then it is also a Gröbner basis for $\langle f_1, \dots, f_s\rangle$ in $\mathbf{R}_{y_1 x_{\sigma(1)} \cdot y_2 x_{\sigma(2)} \cdot .... \cdot y_k x_{\sigma(k)}}[X_1, \dots, X_n]$ for each permutation σ of $\{1, \dots, k\}$ and $y_1, \dots, y_k \in \mathbf{R}$.

5) The condition in Definition 1.2) that for a Gröbner basis $G_i = \{g_1, \dots, g_t\}$ for $\langle f_1, \dots, f_s\rangle$ in $\mathbf{R}_{x_1.x_2.....x_k}[X_1, \dots, X_n]$, the set $\{\mathrm{LC}(g_1), \dots, \mathrm{LC}(g_t)\}$ must be totally ordered under division can be managed at the end of the algorithm by adding artificially new branches to the ring $\mathbf{R}_{x_1.x_2.....x_k}$ and keeping the same Gröbner basis G_i for each new branch. In fact, this is not really necessary, since if one faces the situation treated in the proof of Proposition 2 when considering an ideal membership problem $f \in ? \langle f_1, \dots, f_s\rangle$, he can then open just the necessary new branches with the same Gröbner basis kept at each new branch.

6) Of course, it may exist a shortcut when constructing a dynamical Gröbner basis. For example if one computes a finite number of Gröbner bases over localizations of the basic ring at multiplicative subsets which are comaximal without dealing with all the leaves of the evaluation tree.

4.2 An example

a) Suppose that we want to construct a dynamical Gröbner basis for $I = \langle f_1 = 10XY + 1, f_2 = 6X^2 + 3\rangle$ in $\mathbb{Z}[X, Y]$.

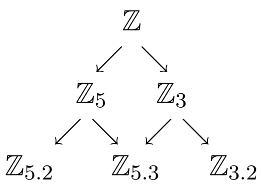
Let fix the lexicographic order as monomial order with $X > Y$. By executing by hand the dynamical version of Buchberger's Algorithm in $\mathbb{Z}[X, Y]$, we find as a dynamical Gröbner basis for I:

$$G = \{G^{5.2}, G^{5.3}, G^{3.2}\},$$

where

$$G^{5.2} = \{f_1, f_2, f_3^{(5)} = \tfrac{3}{5}X - 3Y, f_4^{(5.2)} = 3Y^2 + \tfrac{3}{50}\},$$
$$G^{5.3} = \{f_1, f_2, f_3^{(5)} = \tfrac{3}{5}X - 3Y, f_4^{(5.3)} = 2Y^2 + \tfrac{1}{25}, f_5^{(5.3)} = -\tfrac{3}{25}X^2 + 3Y^2\},$$
$$G^{3.2} = \{f_1, f_2, f_3^{(3)} = X - 5Y, f_4^{(3)} = 50Y^2 + 1, f_5^{(3.2)} = 25Y^2 + \tfrac{1}{2}\}.$$

The dynamical evaluation of the problem of constructing a Gröbner basis for I produces the following evaluation tree:



b) Suppose that we have to deal with the ideal membership problem:

$$f = 62X^3Y + 11X^2 + 10XY^2 + 56XY + Y + 8 \ \in ? \ \langle 10XY + 1, 6X^2 + 3\rangle \,\mathrm{in}\, \mathbb{Z}[X, Y].$$

The responses to this ideal membership problem in the rings $\mathbb{Z}_{5.2}[X, Y], \mathbb{Z}_{5.3}[X, Y], \mathbb{Z}_{3.2}[X, Y]$ are all positive. One obtains:

$5f = (31X^2 + 5Y + 28)f_1 + 4f_2$, and

$6f = (6Y + 15)f_1 + (62XY + 11)f_2$.

Together with the Bezout identity $6-5=1$, one obtains:

$f=(-31X^2+Y-13)f_1+(62XY+7)f_2$, a complete positive answer.

References

[1] M. Aschenbrenner, Ideal membership in polynomial rings over the integers, J. Amer. Math. Soc. **17** (2004), 407-441.

[2] C. Ayoub, On constructing bases for ideals in polynomial rings over the integers, J. Number theory **17** (1983), no. 2, 204-225.

[3] N. Bourbaki, " Algèbre commutative", Chapitres 5-6, Masson, Paris, 1985.

[4] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen polynomideal. Ph.D. thesis, University of Innsbruck, Austria, 1965.

[5] M. Coste, H. Lombardi, M.-F. Roy Dynamical method in algebra: Effective Nullstellensätze, Annals of Pure and Applied Logic **111** (2001), 203–256.

[6] D. Cox, J. Little and D. O'Shea, Ideals, varieties and algorithms, 2^{nd} edition, New York, Springer-Verlag, 1997.

[7] D. Duval and J-C. Reynaud, Sketches and computation (Part II) Dynamic evaluation and applications. Mathematical Structures in computer Sciences **4** (1994), 239–271.

(see http://www.Imc.imag.fr/Imc-cf/Dominique.Duval/evdyn.html)

[8] G. Gallo and B. Mishra, A solution to Kronecker's problem, Appl. Algebra in Engrg. Comm. Comput. **5** (1994), no. 6, 343-370.

[9] A. Kandry-Rody and D. Kapur, Computing a Gröbner basis of a polynomial ideal over a Euclidean domain, J. Symbolic Comput. **6** (1988), no. 1, 37-57.

[10] R. Mines, F. Richman, W. Ruitenburg, A Course in Constructive Algebra, Universitext, Springer-Verlag, 1988.

[11] I. Yengui, Computing a Gröbner basis of a polynomial ideal over a principal domain. Preprint (2004).

[12] I. Yengui, Dynamical Gröbner bases. Preprint (2004).