Abstract

In this paper, we introduce the notion of "dynamical Gröbner bases" of polynomial ideals over a principal domain. As application, we solve dynamically 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 $\mathbb{Z}[X_1, \ldots, X_n]$.

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 [3]. 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, 7, 8, 10].

Recall that the notion of “dynamical proofs” comes from the work of Coste, Lombardi, and Roy in [4] and was inspired by the notion of dynamical evaluation introduced in computer algebra by Duval and Reynaud [6].

Our starting point is the method explained in [1, 10]. Let us recall the strategy of this method. Begin by noting that for a principal domain $R$ with field of fractions $F$, a necessary condition so that $f \in \langle f_1, \ldots, f_s \rangle$ in $R[X_1, \ldots, X_n]$ is: $f \in \langle f_1, \ldots, f_s \rangle$ in $F[X_1, \ldots, X_n]$. Suppose that this condition is fulfilled, that is there exists $d \in R \setminus \{0\}$ such that $\forall j \leq \ell$.

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

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

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

Since $\gcd(d, d_1, \ldots, d_i) = 1$, by combining equalities asserting (0), (1), $\ldots$, (i) using a Bezout identity between $d, d_1, \ldots, d_i$, we can find an equality asserting that $f \in \langle f_1, \ldots, f_s \rangle$ in $R[X_1, \ldots, X_n]$. Thus, the necessary conditions are sufficient and it suffices to treat the problem in case the basic ring is a discrete valuation domain. The notions of Gröbner basis and S-polynomials, originally introduced by Buchberger, have been adapted in [10] 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 [10] 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”. Our goal is to mimic dynamically as much as we can the method used in [10]. A key fact is that for any two nonzero elements \( a \) and \( b \) in a principal domain \( R \), writing \( a = (a \wedge b)a' \), \( b = (a \wedge b)b' \), with \( a' \wedge b' = 1 \), then \( a \) divides \( b \) in \( R_{a'} \) and \( b \) divides \( a \) in \( R_{b'} \), where for any nonzero \( x \in R \), \( R_x \) denotes the localization of \( R \) at the multiplicative subset \( M(x) \) generated by \( x \). Moreover, note that the two multiplicative subsets \( M(a') \) and \( M(b') \) are comaximal, that is, for any \( x \in M(a') \) and \( y \in M(b') \), 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 [5] and [9].

1 Dynamical Gröbner basis over a principal domain

**Definition 1**  
\( S \) is said to be a multiplicative subset of a ring \( R \) if 
\[
S \subseteq R, 1 \in S \text{ and } \forall x, y \in S, xy \in S.
\]

For \( x_1, \ldots, x_r \in R \), \( M(x_1, \ldots, x_r) \) will denote the multiplicative subset of \( R \) generated by \( x_1, \ldots, x_r \), that is,
\[
M(x_1, \ldots, x_r) = \{x_1^{n_1} \cdots x_r^{n_r}, n_i \in \mathbb{N}\}.
\]

Such a multiplicative subset is said to be finitely generated. If \( S \) is a multiplicative subset of a ring \( R \), the localization of \( R \) at \( S \) is the ring \( S^{-1}R = \{\frac{1}{x}, x \in R, s \in S\} \) in which the elements of \( S \) are forced into being invertible.

If \( x \in R \), the localization of \( R \) at the multiplicative subset \( M(x) \) will be denoted by \( R_x \). Moreover, by induction, for each \( x_1, \ldots, x_k \in R \), we define \( R_{x_1, x_2, \ldots, x_k} := (R_{x_1, x_2, \ldots, x_{k-1}})_{x_k} \). This notation which is not very practical will be used only in the example.

If \( S_1, \ldots, S_k \) are multiplicative subsets of \( R \), we say that \( S_1, \ldots, S_k \) are comaximal if
\[
\forall s_1 \in S_1, \ldots, s_n \in S_n, \exists a_1, \ldots, a_n \in R \text{ such that } \sum_{i=1}^n a_i s_i = 1.
\]

**Definition 2**  
Let \( R \) be a ring, \( f = \sum a_\alpha X^\alpha \) a nonzero polynomial in \( R[X_1, \ldots, X_n] \), \( E \) a nonempty subset of \( R[X_1, \ldots, X_n] \), and \( \succ \) a monomial order.

1) The \( X^\alpha \) (resp. the \( a_\alpha X^\alpha \)) are called the monomials (resp. the terms) of \( f \).
2) The multidegree of \( f \) is \( \text{mdeg}(f) := \max\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\} \).
3) The leading coefficient of \( f \) is \( \text{LC}(f) := a_{\text{mdeg}(f)} \in R \).
4) The leading monomial of \( f \) is \( \text{LM}(f) := X^{\text{mdeg}(f)} \).
5) The leading term of \( f \) is \( \text{LT}(f) := \text{LC}(f) \text{LM}(f) \).
6) \( \text{LT}(E) := \{\text{LT}(g), g \in E\} \).
7) \( \langle \text{LT}(E) \rangle := \langle \text{LT}(g), g \in E \rangle \) (ideal of \( R[X_1, \ldots, X_n] \)).
8) For \( g, h \in R[X_1, \ldots, X_n] \), we say that \( \text{LT}(g) \) divides \( \text{LT}(h) \) if \( \text{LM}(g) \) divides \( \text{LM}(h) \) and \( \text{LC}(g) \) divides \( \text{LC}(h) \).

**Definition 3**  
Let \( R \) be an integral ring, \( f, g \in R[X_1, \ldots, X_n] \) \( \setminus \{0\} \), \( I = \langle f_1, \ldots, f_n \rangle \) a nonzero finitely generated ideal of \( R[X_1, \ldots, X_n] \), and \( \succ \) a monomial order.

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

\[
S(f, g) = \frac{X_g}{LM(f)} f - \frac{LC(f)}{LM(g)} X_g g \quad \text{if} \quad LC(g) \text{ divides } LC(f).
\]

\[
S(f, g) = \frac{LC(g)}{LM(f)} X_f f - \frac{X_f}{LM(g)} g \quad \text{if} \quad LC(f) \text{ divides } LC(g) \text{ and } LC(g) \text{ does not divide } LC(f).
\]

2) As in the classical division algorithm in \( F[X_1, \ldots, X_n] \) (\( F \) field) (see [5], page 61), for each polynomials \( h, h_1, \ldots, h_m \in R[X_1, \ldots, X_n] \), there exist \( q_1, \ldots, q_m, r \in R[X_1, \ldots, X_n] \) 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 \( LT(h_1), \ldots, LT(h_m) \). The polynomial \( r \) is called a remainder of \( h \) on division by \( H = \{ h_1, \ldots, h_m \} \) and denoted \( r = \overline{r} \).

3) For \( g_1, \ldots, g_t \in R[X_1, \ldots, X_n] \), \( G = \{ g_1, \ldots, g_t \} \) is said to be a special Gröbner basis for \( I \) if \( I = \langle g_1, \ldots, g_t \rangle \), the set \( \{ LC(g_1), \ldots, LC(g_t) \} \) is totally ordered under division, and for each \( i \neq j \),

\[
S(g_i, g_j) = 0.
\]

Note that in case \( R \) is a field, this definition coincides with the classical definition of Gröbner bases [5]. Also, in case \( R \) is a valuation domain, we retrieve the same definition of Gröbner bases introduced in [10].

4) A set \( G = \{ (S_1, G_1), \ldots, (S_k, G_k) \} \) is said to be a dynamical Gröbner basis for \( I \) if \( S_1, \ldots, S_k \) are finitely generated comaximal multiplicative subsets of \( R \) and in each localization \( (S_i^{-1}R)[X_1, \ldots, X_n] \), \( G_i \) is a special Gröbner basis for \( \langle f_1, \ldots, f_s \rangle \).

**Proposition 4**

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

**Proof** Of course, if \( \overline{f}^G = 0 \) then \( f \in \langle g_1, \ldots, g_t \rangle = I. \) For the converse, suppose that \( f \in I \) and that the remainder \( r \) of \( f \) on division by \( G \) in \( R[X_1, \ldots, X_n] \) is nonzero. This means that \( LT(r) \) is not divisible by any of \( LT(g_1), \ldots, LT(g_t) \).

Let \( F \) be the field of fractions of \( R \) and observe that \( G \) is also a Gröbner basis for \( F[X_1, \ldots, X_n] \) and in \( R_p \) for each irreducible element \( p \in R \) (in fact the definitions of S-polynomial and division algorithm used in this paper are the same as in [10] for discrete valuation domains).

Since \( G \) is also a Gröbner basis for \( \langle f_1, \ldots, f_s \rangle \) in \( F[X_1, \ldots, X_n] \), then \( LM(r) \) is divisible by at least one of \( LM(g_1), \ldots, LM(g_t) \), but for each \( g_i \) such that \( LM(g_i) \) divides \( LM(r) \), \( LC(g_i) \) does not divide \( LM(r) \). Let \( g_1, \ldots, g_i \) be such polynomials and suppose that \( LC(g_1)/LC(g_2)/\cdots/LC(g_k) \) (by definition of a special Gröbner basis we can make this hypothesis). Since the basic ring is principal and a fortiori factorial, we can write \( LC(g_i) = u p_1^{\alpha_1} \cdots p_l^{\alpha_l} \) and \( LC(r) = p_1^{\beta_1} \cdots p_l^{\beta_l} \), where the \( p_i \) are distinct irreducible elements in \( R \), \( u, v \) are invertible in \( R \), and \( \alpha_i, \beta_i \in \mathbb{N} \). Necessarily, there exists \( 1 \leq i < \ell \) such that \( \alpha_i > \beta_i \). But this would imply that the problem persists in the ring \( R_{p_0} \) for each \( 1 \leq i \leq \ell \).

**Theorem 5** (Dynamical gluing)

Let \( R \) be a principal domain, \( I = \langle f_1, \ldots, f_s \rangle \) a nonzero finitely generated ideal of \( R[X_1, \ldots, X_n] \), \( f \in R[X_1, \ldots, X_n] \), and fix a monomial order. Suppose that \( G = \{ (S_1, G_1), \ldots, (S_k, G_k) \} \) is a dynamical Gröbner basis for \( I \) in \( R[X_1, \ldots, X_n] \). Then, \( f \in I \) if and only if \( \overline{f}^G = 0 \) in \( (S_i^{-1}R)[X_1, \ldots, X_n] \) for each \( 1 \leq i \leq k \).

**Proof** “⇒” This follows from Proposition 4.
"\( \Leftarrow \)" Since \( \overline{f}^{G_i} = 0 \), then \( f \in (f_1, \ldots, f_s) \) in \( (S_i^{-1} R)[X_1, \ldots, X_n] \), for each \( 1 \leq i \leq k \). This means that for each \( 1 \leq i \leq k \), there exist \( s_i \in S_i \) and \( h_{i,1}, \ldots, h_{i,s} \in R[X_1, \ldots, X_n] \) such that

\[
s_i f = h_{i,1} f_1 + \cdots + h_{i,s} f_s.
\]

Using the fact that \( S_1, \ldots, S_k \) are comaximal, there exist \( a_1, \ldots, a_k \in R \) such that \( \sum_{i=1}^k a_i s_i = 1 \). It follows that

\[
f = \left( \sum_{i=1}^k a_i h_{i,1} \right) f_1 + \cdots + \left( \sum_{i=1}^k a_i h_{i,s} \right) f_s \in I.
\]

\[\square\]

1.1 How to construct a dynamical Gröbner basis?

Let \( R \) be a principal domain, \( I = (f_1, \ldots, f_s) \) a nonzero finitely generated ideal of \( R[X_1, \ldots, X_n] \), and fix a monomial order \( \triangleright \). The purpose is to construct a dynamical Gröbner basis \( G \) for \( I \).

First recall the Algorithm given in [10] which generalizes Buchberger’s Algorithm to discrete valuation domains and uses new definitions of division of terms and \( S \)-polynomials:

**Buchberger’s Algorithm for discrete valuation domains**

Input: \( f_1, \ldots, f_s \)

Output: a Gröbner basis \( G \) for \( (f_1, \ldots, f_s) \) with \( \{f_1, \ldots, f_s\} \subseteq G \)

\[
G = \{f_1, \ldots, f_s\}
\]

REPEAT

\[
G' := G
\]

For each pair \( f \not\equiv g \) in \( G' \) DO

\[
S := \left( S(f, g)^G \right)^G
\]

If \( S \not\equiv 0 \) THEN \( G := G' \cup \{S\} \)

UNTIL \( G = G' \)

**Dynamical version of Buchberger’s Algorithm**

This algorithm works like Buchberger’s Algorithm for discrete valuation domains. The only difference is when it has to handle two incomparable (under division) elements \( a, b \) in \( R \). In this situation, one should compute \( d = a \wedge b \), factorize \( a = a' b' \), \( b = b' \), with \( a' \wedge b' = 1 \), and then open two branches: the computations are pursued in \( R_{a'} \) and \( R_{b'} \).

- First possibility: the two incomparable elements \( a \) and \( b \) are encountered when performing the division algorithm (analogous to the division algorithm in the discrete valuation case). Suppose that one has to divide a term \( aX^\alpha \) by another term \( bX^\beta \) with \( X^\beta \) divides \( X^\alpha \).

In the ring \( R_{b'} \): \( f = \frac{a'}{b'} X^\alpha + r \) (\( \text{mdeg}(r) < \text{mdeg}(f) \)) and the division is pursued with \( f \) replaced by \( r \).

In the ring \( R_{a'} \): \( L T(f) \) is not divisible by \( L T(g) \) and thus \( f = \overline{f}^{G} \).

- Second possibility: the two incomparable elements \( a \) and \( b \) are encountered when computing \( S(f, g) \) with \( L T(f) = aX^\alpha \) and \( L T(g) = bX^\beta \). Denote \( \gamma = (\gamma_1, \ldots, \gamma_n) \), with \( \gamma_i = \max(\alpha_i, \beta_i) \) for each \( i \).

In the ring \( R_{b'} \): \( S(f, g) = \frac{X^\gamma}{X^\alpha} f - \frac{a'}{b'} X^\gamma g \).

In the ring \( R_{a'} \): \( S(f, g) = \frac{b'}{a'} X^\gamma f - \frac{X^\gamma}{X^\alpha} g \).

At each new branch, if \( S = \overline{S(f, g)}^{G'} \not\equiv 0 \) where \( G' \) is the current Gröbner basis, then \( S \) must be added to \( G' \).

**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. Indeed, if it does not stop then this would be the coefficients’ fault and not the monomials’ fault since \( \mathbb{N}^{n} \) is well ordered (see Dickson’s Lemma [5], page 69). That is, the Dynamical version of Buchberger’s Algorithm would produce infinitely many polynomials \( g_i \) with the same multidegree such that \( \langle \text{LC}(g_1) \rangle \subset \langle \text{LC}(g_2) \rangle \subset \langle \text{LC}(g_2) \rangle \subset \cdots \) in contradiction with the fact that a principal domain is Noetherian.

3) At the end of this tree, all the obtained bases are in localizations of \( R \) at finitely generated multiplicative subsets of \( R \). Of course, all together, the considered multiplicative subsets of \( R \) are comaximal (this is due to the fact that if one needs to break the current ring \( R_i \), this is done by considering two rings of type \( (R_i)_{a'} \) and \( (R_i)_{b'} \), with \( a'b' = 1 \)). Thus, by Theorem 5, the obtained special Gröbner bases at the leaves of the constructed “evaluation tree” all together form a dynamical Gröbner basis for \( \langle f_1, \ldots, f_s \rangle \) in \( R[X_1, \ldots, X_n] \).

4) This algorithm may produce many redundancies of leaves due to the fact that one can obtain the same leaf in different ways.

5) The condition in Definition 3.3) that for a Gröbner basis \( G_i = \{g_1, \ldots, g_t\} \) for \( \langle f_1, \ldots, f_s \rangle \) in \( (S_i^{-1}R)[X_1, \ldots, X_n] \), the set \( \{\text{LC}(g_1), \ldots, \text{LC}(g_t)\} \) must be totally ordered under division can be managed at the end of the algorithm by adding artificially new branches to the ring \( S_i^{-1}R \) 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 4 when considering an ideal membership problem \( f \in? \langle f_1, \ldots, f_s \rangle \), 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.

1.2 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 \( X > Y \). We will execute by hand the dynamical version of Buchberger’s Algorithm in \( \mathbb{Z}[X,Y] \). We will give all the details of the computations only for one leaf.

Since \( 10 \land 6 = 2, 10 = 2 \times 5, \) and \( 6 = 2 \times 3, \) one has to open two branches:

\[
\begin{array}{c}
\mathbb{Z} \\
\downarrow \\
\mathbb{Z}_5 \\
\downarrow \\
\mathbb{Z}_3
\end{array}
\]

In \( \mathbb{Z}_5 \):

\[
S(f_1, f_2) = \frac{3}{5}X f_1 - Y f_2 = \frac{3}{5}X - 3Y := f_3. \]

But, there is a jam when computing \( S(f_1, f_3) \) since the leading coefficients of \( f_1 \) and \( f_3 \) are not comparable under division. Since \( 10 \land \frac{3}{5} = 2 \land 3 = 1 \), one has to open two new branches:

\[
\begin{array}{c}
\mathbb{Z}_5 \\
\downarrow \\
\mathbb{Z}_{5,2} \\
\downarrow \\
\mathbb{Z}_{5,3}
\end{array}
\]

In \( \mathbb{Z}_{5,2} \):

\[
S(f_1, f_3) = \frac{3}{10}f_1 - Y f_3 = 3Y^2 + \frac{3}{50} := f_4.
\]

\[
S(f_1, f_4) = \frac{3}{10} Y f_1 - X f_4 = -\frac{3}{50} X + \frac{3}{10} Y = -\frac{1}{10} f_3 \xrightarrow{f_3} 0 \text{ (reduction modulo } f_3).\]
Thus, $G_1 = \{10XY + 1, 6X^2 + 3, \frac{2}{5}X - 3Y, 3Y^2 + \frac{3}{50}\}$ is a special Gröbner basis for $\langle 10XY + 1, 6X^2 + 3 \rangle$ at the leaf $\mathcal{M}(5, 2)^{-1} \mathbb{Z} = \mathbb{Z}_{5,2}$.

At the leaf $\mathbb{Z}_{5,3}$, we find $G_2 = \{10XY + 1, 6X^2 + 3, \frac{2}{5}X - 3Y, 2Y^2 + \frac{1}{25}, -\frac{2}{25}X^2 + 3Y^2\}$ as a special Gröbner basis for $\langle 10XY + 1, 6X^2 + 3 \rangle$.

Let’s handle the right subtree:

At the leaf $\mathbb{Z}_{3,2}$, we find $G_3 = \{10XY + 1, 6X^2 + 3, X - 5Y, 50Y^2 + 1, 25Y^2 + \frac{1}{2}\}$ as a special Gröbner basis for $\langle 10XY + 1, 6X^2 + 3 \rangle$. Of course, at the leaf $\mathbb{Z}_{3,5} = \mathbb{Z}_{5,3}$, $G_1$ is a special Gröbner basis for $\langle 10XY + 1, 6X^2 + 3 \rangle$.

As a conclusion, the dynamical evaluation of the problem of constructing a Gröbner basis for $I$ produces the following evaluation tree:

The obtained dynamical Gröbner basis of $I$ is

$$G = \{ (\mathcal{M}(5, 2), G_1), (\mathcal{M}(5, 3), G_2), (\mathcal{M}(3, 2), G_3) \}.$$  

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

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

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:

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

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

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


(see http://www.lmc.imag.fr/lmc-ej/Dominique.Duval/evdyn.html)


