

A GENERALIZED APPROACH TO DYNAMICAL GRÖBNER BASES IN BOOLEAN STRUCTURES

HADJER RYMA MOUSSEDEK and FATIMA BOUDAUD

Abstract. In this paper, we compute “dynamical Gröbner Bases” over the ring $\mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle$, and resolve the delicate problem caused by zero-divisors appearing as leading coefficients and we focus on generalizing Buchberger’s algorithm for Boolean rings.

MSC 2020. 3F05, 13F30, 06E75, 13P10.

Key words. Dynamical Gröbner bases, Boolean ring, localization, annihilators.

1. INTRODUCTION

One main feature of the use of dynamical Gröbner bases [4] is that it enables to easily resolve the delicate problem caused by zero-divisors appearing as leading coefficients. Cai and Kapur concluded their paper [1] by mentioning the open question of “How to generalize Buchberger’s algorithm for Boolean rings”. As a typical example of a problematical situation, they studied the case where the base ring is $\mathbf{A} = \mathbb{F}_2[a_1, a_2] / \langle a_1^2 - a_1, a_2^2 - a_2 \rangle$. In that case, the method they proposed in [1] does not work due to the fact that an annihilator of $a_1a_2 + a_1 + a_2 + 1 \in \mathbf{A}$ can be either a_1 or a_2 and thus there may exist noncomparable multiannihilators for an element in $\mathbf{A}$. Dynamical Gröbner Bases allow to fairly overcome this difficulty in this precise case, as will be explained bellow.

We will be led to compute a dynamical Gröbner base made up of four Gröbner bases on localizations of $\mathbf{A}$. We will see that the problem Cai and Kapur pointed disappears completely at each leaf of the constructed binary tree. Thus, by systemizing the dynamical construction above, it is straightforward that dynamical Gröbner bases over Dedekind rings could be a satisfactory solution to this open problem.

The authors thank the members of the editorial board for the effort they made to find suitable reviewers for our manuscript, and we thank the referee for his helpful comments and suggestions.

Corresponding author: Hadjer Ryma Moussedek.

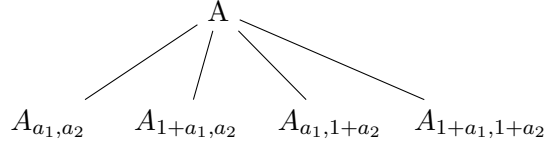
It is folklore that the presence of a nontrivial idempotent $\mathbf{e}$ in a ring $\mathbf{B}$ (i.e., $\mathbf{e}^2 = \mathbf{e}$ and $\mathbf{e} \notin \{0, 1\}$) splits $\mathbf{B}$ into two subrings as follows:

$$\mathbf{B} = \mathbf{eB} + (1 - \mathbf{e})\mathbf{B} \cong \mathbf{B} \times (1 - \mathbf{e})\mathbf{B} \cong \mathbf{B} / \langle 1 - \mathbf{e} \rangle \times \mathbf{B} / \langle \mathbf{e} \rangle \cong \mathbf{B} \left[\frac{1}{\mathbf{e}} \right] \times \mathbf{B} \left[\frac{1}{1 - \mathbf{e}} \right].$$

Let us consider the ring

$$\mathbf{A} = \mathbb{F}_2[a_1, a_2] / \langle a_1^2 - a_1, a_2^2 - a_2 \rangle = \mathbb{F}_2 a_1 a_2 + \mathbb{F}_2 a_1 + \mathbb{F}_2 a_2 + \mathbb{F}_2$$

with the relations $a_1^2 = a_1$ and $a_2^2 = a_2$. When working with the ring A , we know in advance that the binary tree we will construct when computing dynamically a Gröbner basis of an ideal of $A[X_1, \dots, X_n]$ is formed by only four leaves as follows:



where

$$\begin{aligned} A_{a_1, a_2} &:= A \left[\frac{1}{a_1}, \frac{1}{a_2} \right] \cong \mathbf{A} \text{ with } \begin{cases} a_1 = 1 \\ a_2 = 1 \end{cases} \cong \mathbb{F}_2, \\ A_{a_1, 1+a_2} &:= A \left[\frac{1}{a_1}, \frac{1}{1+a_2} \right] \cong \mathbf{A} \text{ with } \begin{cases} a_1 = 1 \\ a_2 = 0 \end{cases} \cong \mathbb{F}_2, \\ A_{1+a_1, a_2} &:= A \left[\frac{1}{1+a_1}, \frac{1}{a_2} \right] \cong \mathbf{A} \text{ with } \begin{cases} a_1 = 0 \\ a_2 = 1 \end{cases} \cong \mathbb{F}_2, \\ A_{1+a_1, 1+a_2} &:= A \left[\frac{1}{1+a_1}, \frac{1}{1+a_2} \right] \cong \mathbf{A} \text{ with } \begin{cases} a_1 = 0 \\ a_2 = 0 \end{cases} \cong \mathbb{F}_2. \end{aligned}$$

So computing a dynamical Gröbner basis over A amounts to computing four (classical) Gröbner over the field with two elements $\mathbb{F}_2$, which correspond to $(a_1, a_2) = (1, 1) = (1, 0) = (0, 1) = (0, 0)$.

Moreover, we define a ‘reduced dynamical Gröbner basis’ as a set

$$\{(G_1, a_1^{\mathbb{N}} a_2^{\mathbb{N}}), (G_2, a_1^{\mathbb{N}} (1 + a_2)^{\mathbb{N}}), (G_3, (1 + a_1)^{\mathbb{N}} a_2^{\mathbb{N}}), (G_4, (1 + a_1)^{\mathbb{N}} (1 + a_2)^{\mathbb{N}})\},$$

where each G_i is a reduced Gröbner basis over $\mathbb{F}_2$.

The paper is organized as follows: in the second section we recall basic definitions and propositions, in the third and last section we generalize Buchberger’s algorithm for such quotient rings by computing a dynamical Gröbner basis of a polynomial ideal where the leading coefficients could be from a ring with zero-divisors. The algorithm is illustrated using examples in the same section. We also take examples from the article [1] using our method.

2. PRELIMINARIES

DEFINITION 2.1. Let R be a ring, $f = \sum_{\alpha} a_{\alpha} X^{\alpha}$ a nonzero polynomial in $R[X_1, \dots, X_n]$, E a non-empty subset of $R[X_1, \dots, X_n]$, and $>$ a monomial order.

(1) The X^{α} 's (respectively the $a_{\alpha} X^{\alpha}$'s) are called the monomials (respectively the terms) of f .

(2) The multidegree of f is $\text{mdeg}(f) := \max\{\alpha \in N^n : a_{\alpha} \neq 0\}$.

(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 $R[X_1, \dots, X_n]$).

DEFINITION 2.2. (1) S is said to be a multiplicative subset of a ring R if $S \subseteq R$, $1 \in S$ and $\forall x, y \in S$, $xy \in S$.

(2) For $x_1, \dots, x_r \in R$, $M(x_1, \dots, x_r)$ will denote the multiplicative subset of R generated by $x_1, \dots, x_r$, that is, $M(x_1, \dots, x_r) = \{x_1^{n_1} \cdots x_r^{n_r}, n_i \in \mathbb{N}\}$. 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 constructed ring $S^{-1}R = \{\frac{x}{s}, x \in R, s \in S\}$ in which the elements of S are forced into being invertible.

(3) If $x \in R$, the localization of R at the multiplicative subset $M(x)$ will be denoted by R_x .

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

DEFINITION 2.3. Let R be an integral ring, $f, g \in R[X_1, \dots, X_n] \setminus \{0\}$, $I = \langle f_1, \dots, f_s \rangle$ a nonzero finitely generated ideal of $R[X_1, \dots, X_n]$, and $>$ a monomial order.

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

PROPOSITION 2.4. A non trivial idempotent e in a ring $\mathbf{B}$ (i.e., $e^2 = e$ and $e \notin \{0, 1\}$) splits $\mathbf{B}$ into two subrings as follows:

$$\mathbf{B} = e\mathbf{B} + (1-e)\mathbf{B} \cong \mathbf{B} \times (1-e)\mathbf{B} \cong \mathbf{B}/\langle 1-e \rangle \times \mathbf{B}/\langle e \rangle \cong \mathbf{B} \begin{bmatrix} 1 \\ e \end{bmatrix} \times \mathbf{B} \begin{bmatrix} 1 \\ 1-e \end{bmatrix}.$$

3. DYNAMICAL GRÖBNER BASES IN $\mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle$

3.1. COMPUTATION OF S-POLYNOMIALS

Let $f_i, f_j \in \mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle$ with $f_i = \sum_{\alpha_i} a_{\alpha_i} X^{\alpha_i}$ and $f_j = \sum_{\alpha_j} a_{\alpha_j} X^{\alpha_j}$ where $a_{\alpha_i}^2 = a_{\alpha_i}$ and $a_{\alpha_j}^2 = a_{\alpha_j}$ for $j = i + 1, \dots, n$.

Denote by $\text{mdeg}(f_i) = \alpha_i$, $\text{mdeg}(f_j) = \alpha_j$ and $\gamma = (\gamma_1, \dots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \alpha_j)$. Moreover, denote by $\text{LC}(f_i) = a_i$ and $\text{LC}(f_j) = a_j$.

As we have seen in introduction that it is straightforward that dynamical Gröbner bases over Dedekind rings could be a satisfactory solution to this open problem, so:

First, we have to find u, v, w such that:
$$\begin{cases} ua_j = va_i \\ wa_j = (1 - u)a_i \end{cases}.$$

Then if we take $u = a_i$, then we find
$$\begin{cases} v = u \frac{a_j}{a_i} = a_i \frac{a_j}{a_i} = a_j \\ w = (1 - u) \frac{a_i}{a_j} = (1 - a_i) \frac{a_i}{a_j} \end{cases} \quad \text{and}$$

we know in advance that $a_i = -a_i$.

Finally, we replace in S-polynomials of Dynamical Gröbner bases over Dedekind rings:

- In $R_u = R_{a_i}$: $S(f_i, f_j) = \frac{v}{u} \frac{x^\gamma}{x^{\alpha_i}} f_i - \frac{x^\gamma}{x^{\alpha_j}} f_j = \frac{a_j}{a_i} \frac{x^\gamma}{x^{\alpha_i}} f_i - \frac{x^\gamma}{x^{\alpha_j}} f_j$.
- In $R_{1-u} = R_{1+a_i}$: $S(f_i, f_j) = \frac{x^\gamma}{x^{\alpha_i}} f_i - \frac{w}{1-u} \frac{x^\gamma}{x^{\alpha_j}} f_j = \frac{x^\gamma}{x^{\alpha_i}} f_i - \frac{a_i}{a_j} \frac{x^\gamma}{x^{\alpha_j}} f_j$.

3.2. COMPUTATION OF S-POLYNOMIALS

PROPOSITION 3.1. *The annihilators in $\mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle$ are $a_1, \dots, a_n$ and:*

$$\begin{aligned} 1 + \prod_{i=1}^n a_i + \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} \\ + \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} + \dots + \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} + \sum_{i=1}^n a_i. \end{aligned}$$

Proof. Basic step. We must show that $P(n_0)$, that is, $P(2)$ is true.

The statement $P(2)$ is that in $\mathbb{F}_2[a_1, a_2] / \langle a_1^2 - a_1, a_2^2 - a_2 \rangle$ with the relations $a_1^2 = a_1$ and $a_2^2 = a_2$, the annihilators are: $a_1 a_2 + a_1 + a_2 + 1$, a_1 and a_2 , which is clearly true:

$$\begin{aligned} a_1(a_1 a_2 + a_1 + a_2 + 1) &= a_1^2 a_2 + a_1^2 + a_1 a_2 + a_1 \\ &= a_1 a_2 + a_1 + a_1 a_2 + a_1 \quad (\text{we have } a_1^2 = a_1) \\ &= 2a_1 a_2 + 2a_1 = 0 \quad (\text{because it is in } \mathbb{F}_2) \end{aligned}$$

and it is the same for a_2 : $a_2(a_1 a_2 + a_1 + a_2 + 1) = 0$.

Inductive step. We must show that $P(n+1)$ is true as a consequence of $P(n)$ being true, that is, we must show that the annihilators in

$$\mathbb{F}_2[a_1, \dots, a_{n+1}] / \langle a_1^2 - a_1, \dots, a_{n+1}^2 - a_{n+1} \rangle$$

are $a_1, \dots, a_{n+1}$ and:

$$\begin{aligned}
 (*) \quad & 1 + \prod_{i=1}^{n+1} a_i + \sum_{\substack{i_1=1 \\ i_n \succ \dots \succ i_1}}^{n+1} a_{i_n} a_{i_{n-1}} \dots a_{i_1} \\
 & + \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^{n+1} a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} + \dots + \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^{n+1} a_{i_2} a_{i_1} + \sum_{i=1}^{n+1} a_i
 \end{aligned}$$

is a consequence of the fact that the annihilators in

$$\mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle$$

are $a_1, \dots, a_n$ and:

$$\begin{aligned}
 (**) \quad & 1 + \prod_{i=1}^n a_i + \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} \\
 & + \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} + \dots + \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} + \sum_{i=1}^n a_i
 \end{aligned}$$

Now, we have:

$$\begin{aligned}
 (*) &= 1 + a_{n+1} \prod_{i=1}^n a_i + a_{n+1} \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} \\
 & + \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} + a_{n+1} \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} \\
 & + \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} + \dots + a_{n+1} \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} \\
 & + \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} + a_{n+1} + \sum_{i=1}^n a_i.
 \end{aligned}$$

When we multiply $(*)$ by a_{n+1} , we have:

$$a_{n+1} (*) = a_{n+1} + a_{n+1}^2 \prod_{i=1}^n a_i + a_{n+1}^2 \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1}$$

$$\begin{aligned}
& + a_{n+1} \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} + a_{n+1}^2 \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} \\
& + a_{n+1} \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} + \dots + a_{n+1}^2 \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} \\
& + a_{n+1} \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} + a_{n+1}^2 + a_{n+1} \sum_{i=1}^n a_i \\
a_{n+1}(\ast) & = a_{n+1} + a_{n+1} \prod_{i=1}^n a_i + a_{n+1} \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} \\
& + a_{n+1} \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} + a_{n+1} \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} \\
& + a_{n+1} \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} + \dots + a_{n+1} \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} \\
& + a_{n+1} \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} + a_{n+1} + a_{n+1} \sum_{i=1}^n a_i \quad (\text{because } a_{n+1}^2 = a_{n+1}) \\
a_{n+1}(\ast) & = 2a_{n+1} + 2a_{n+1} \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} \\
& + 2a_{n+1} \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} \\
& + \dots + 2a_{n+1} \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} + 2a_{n+1} \sum_{i=1}^n a_i \quad (\text{because it is in } \mathbb{F}_2) \\
& = 2a_{n+1} = 0
\end{aligned}$$

□

LEMMA 3.2. (1) *The number of elements in the annihilator*

$$1 + \prod_{i=1}^n a_i + \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1}$$

$$+ \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} + \dots + \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} + \sum_{i=1}^n a_i$$

is 2^n .

(2) The number of the annihilators in $\mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle$ is $n + 1$

EXAMPLE 3.3. For $n = 4$ the annihilators in

$$\mathbb{F}_2[a_1, a_2, a_3, a_4] / \langle a_1^2 - a_1, a_2^2 - a_2, a_3^2 - a_3, a_4^2 - a_4 \rangle$$

are a_1, a_2, a_3, a_4 and $1 + a_1 a_2 a_3 a_4 + a_1 a_2 a_3 + a_1 a_2 a_4 + a_1 a_3 a_4 + a_2 a_3 a_4 + a_1 a_2 + a_1 a_3 + a_1 a_4 + a_2 a_3 + a_2 a_4 + a_3 a_4 + a_1 + a_2 + a_3 + a_4$. The number of elements in this annihilator is $2^4 = 16$.

The number of annihilators in

$$\mathbb{F}_2[a_1, a_2, a_3, a_4] / \langle a_1^2 - a_1, a_2^2 - a_2, a_3^2 - a_3, a_4^2 - a_4 \rangle$$

is $4 + 1 = 5$.

3.3. COMPUTING DYNAMICAL GRÖBNER BASES OVER

$$\mathbb{F}_2[a_1, a_2, a_3] / \langle a_1^2 - a_1, a_2^2 - a_2, a_3^2 - a_3 \rangle$$

Let us consider the ring:

$$\begin{aligned} R &= \mathbb{F}_2[a_1, a_2, a_3] / \langle a_1^2 - a_1, a_2^2 - a_2, a_3^2 - a_3 \rangle \\ &= \mathbb{F}_2 + a_1 a_2 a_3 \mathbb{F}_2 + a_1 a_2 \mathbb{F}_2 + a_1 a_3 \mathbb{F}_2 + a_2 a_3 \mathbb{F}_2 + a_1 \mathbb{F}_2 + a_2 \mathbb{F}_2 + a_3 \mathbb{F}_2 \end{aligned}$$

with the relations $a_1^2 = a_1, a_2^2 = a_2$ and $a_3^2 = a_3$, where the annihilators are $1 + a_1 a_2 a_3 + a_1 a_2 + a_1 a_3 + a_2 a_3 + a_1 + a_2 + a_3, a_1, a_2$ and a_3 .

3.4. COMPUTING DYNAMICAL GRÖBNER BASES IN

$$\mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle$$

Let us consider the ring:

$$\begin{aligned} R &= \mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle \\ &= \mathbb{F}_2 + \mathbb{F}_2 \left(\prod_{i=1}^n a_i \right) + \mathbb{F}_2 \left(\sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} \right) \\ &\quad + \mathbb{F}_2 \left(\sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} \right) + \dots + \mathbb{F}_2 \left(\sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} \right) + \mathbb{F}_2 \left(\sum_{i=1}^n a_i \right) \end{aligned}$$

with the relations $a_1^2 = a_1, \dots, a_n^2 = a_n$.

We will give an algorithm for computing a dynamical Gröbner basis in

$$\mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle.$$

ALGORITHM 3.4. Input: $\langle f_1, \dots, f_n \rangle$ ideal of

$$\mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle,$$

where $\text{LC}(f_1) = a_1, \dots, \text{LC}(f_n) = a_n$

Output: A Gröbner basis G for $\langle f_1, \dots, f_n \rangle$ with respect to the lexicographic monomial order $>$, with $\{f_1, \dots, f_n\} \subseteq G$.

Start: Let $G := \{f_1, \dots, f_n\}$.

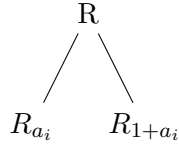
Repeat: Let $G' := G$.

Step 1. Calculate the annihilator:

$$\begin{aligned} 1 + \prod_{i=1}^n a_i + \sum_{\substack{i_1=1 \\ i_{n-1} \succ \dots \succ i_1}}^n a_{i_{n-1}} a_{i_{n-2}} \dots a_{i_1} \\ + \sum_{\substack{i_1=1 \\ i_{n-2} \succ \dots \succ i_1}}^n a_{i_{n-2}} a_{i_{n-3}} \dots a_{i_1} + \dots + \sum_{\substack{i_1=1 \\ i_2 \succ i_1}}^n a_{i_2} a_{i_1} + \sum_{i=1}^n a_i \end{aligned}$$

Step 2.

(1) For i from 1 to $n-1$



(2) For each pair f_i, f_j in G' for $j = i+1, \dots, n$ calculate:

In R_{a_i} :

$$S(f_i, f_j) = \frac{a_j}{a_i} \frac{x^\gamma}{x^{\alpha_i}} f_i - \frac{x^\gamma}{x^{\alpha_j}} f_j$$

In R_{1+a_i} :

$$S(f_i, f_j) = \frac{x^\gamma}{x^{\alpha_i}} f_i - \frac{a_i}{a_j} \frac{x^\gamma}{x^{\alpha_j}} f_j$$

Let $S := \overline{S(f_i, f_j)}^{G'}$.

If $S \neq 0$ then $G := G' \cup S$.

Until $G = G'$.

Step 3. For $j = i+1, \dots, n$

$$\begin{aligned} R &\mapsto R_{a_j}, \\ R &\mapsto R_{1+a_j}. \end{aligned}$$

Return to **Step 2**.

PROPOSITION 3.5. *Algorithm 3.4 terminates.*

Proof. The algorithm terminates because

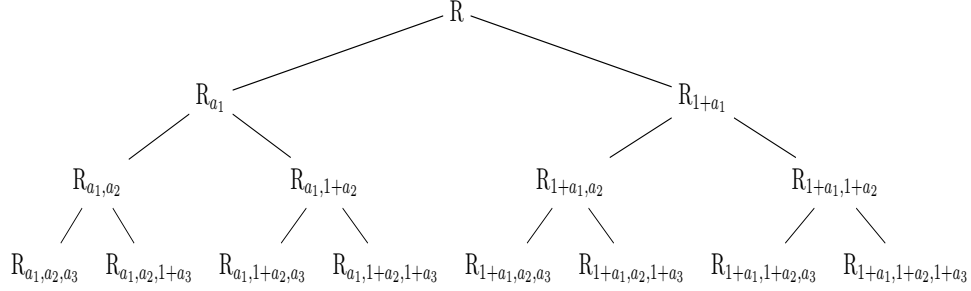
$$\mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle$$

is a Noetherian ring. $\square$

3.5. CONSTRUCTION OF DYNAMICAL GRÖBNER BASES IN

$$\mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle$$

When working with the ring R (with $n = 3$), we find that the binary tree we will construct when computing dynamically a Gröbner basis of an ideal $R[X_1, \dots, X_s]$ is formed as follows:



where the localizations at each leaf are:

$$R_{a_1, a_2, a_3} := R \left[\frac{1}{a_1}, \frac{1}{a_2}, \frac{1}{a_3} \right] \cong R \text{ with } \begin{cases} a_1 = 1 \\ a_2 = 1 \\ a_3 = 1 \end{cases} \cong \mathbb{F}_2,$$

$$R_{a_1, a_2, 1+a_3} := R \left[\frac{1}{a_1}, \frac{1}{a_2}, \frac{1}{1+a_3} \right] \cong R \text{ with } \begin{cases} a_1 = 1 \\ a_2 = 1 \\ a_3 = 0 \end{cases} \cong \mathbb{F}_2,$$

$$R_{a_1, 1+a_2, a_3} := R \left[\frac{1}{a_1}, \frac{1}{1+a_2}, \frac{1}{a_3} \right] \cong R \text{ with } \begin{cases} a_1 = 1 \\ a_2 = 0 \\ a_3 = 1 \end{cases} \cong \mathbb{F}_2,$$

$$R_{a_1, 1+a_2, 1+a_3} := R \left[\frac{1}{a_1}, \frac{1}{1+a_2}, \frac{1}{1+a_3} \right] \cong R \text{ with } \begin{cases} a_1 = 1 \\ a_2 = 0 \\ a_3 = 0 \end{cases} \cong \mathbb{F}_2,$$

$$R_{1+a_1, a_2, a_3} := R \left[\frac{1}{1+a_1}, \frac{1}{a_2}, \frac{1}{a_3} \right] \cong R \text{ with } \begin{cases} a_1 = 0 \\ a_2 = 1 \\ a_3 = 1 \end{cases} \cong \mathbb{F}_2,$$

$$R_{1+a_1, a_2, 1+a_3} := R \left[\frac{1}{1+a_1}, \frac{1}{a_2}, \frac{1}{1+a_3} \right] \cong R \text{ with } \begin{cases} a_1 = 0 \\ a_2 = 1 \\ a_3 = 0 \end{cases} \cong \mathbb{F}_2,$$

$$R_{1+a_1, 1+a_2, a_3} := R \left[\frac{1}{1+a_1}, \frac{1}{1+a_2}, \frac{1}{a_3} \right] \cong R \text{ with } \begin{cases} a_1 = 0 \\ a_2 = 0 \\ a_3 = 1 \end{cases} \cong \mathbb{F}_2,$$

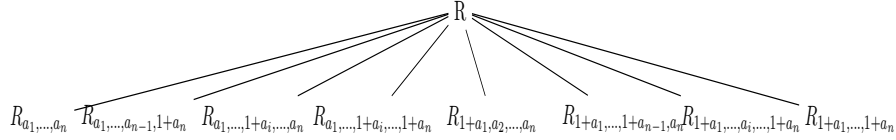
$$R_{1+a_1, 1+a_2, 1+a_3} := R \left[\frac{1}{1+a_1}, \frac{1}{1+a_2}, \frac{1}{1+a_3} \right] \cong R \text{ with } \begin{cases} a_1 = 0 \\ a_2 = 0 \\ a_3 = 0 \end{cases} \cong \mathbb{F}_2.$$

We can define a ‘reduced dynamical Gröbner Bases’ as a set

$$\{(G_1, a_1^{\mathbb{N}} a_2^{\mathbb{N}} a_3^{\mathbb{N}}), (G_2, a_1^{\mathbb{N}} a_2^{\mathbb{N}} (1+a_3)^{\mathbb{N}}), (G_3, a_1^{\mathbb{N}} (1+a_2)^{\mathbb{N}} a_3^{\mathbb{N}}), \\ (G_4, a_1^{\mathbb{N}} (1+a_2)^{\mathbb{N}} (1+a_3)^{\mathbb{N}}), (G_5, (1+a_1)^{\mathbb{N}} a_2^{\mathbb{N}} a_3^{\mathbb{N}}), (G_6, (1+a_1)^{\mathbb{N}} a_2^{\mathbb{N}} (1+a_3)^{\mathbb{N}}), \\ (G_7, (1+a_1)^{\mathbb{N}} (1+a_2)^{\mathbb{N}} a_3^{\mathbb{N}}), (G_8, (1+a_1)^{\mathbb{N}} (1+a_2)^{\mathbb{N}} (1+a_3)^{\mathbb{N}})\},$$

where each G_i is a Gröbner Bases over R .

By induction when we work with the ring R we find that the binary tree constructed when computing dynamically a Gröbner basis of an ideal $R[X_1, \dots, X_s]$ is formed as follows:



And the localizations at each leaf are:

$$R_{a_1, \dots, a_n} := R \left[\frac{1}{a_1}, \dots, \frac{1}{a_n} \right] \cong R \text{ with } \begin{cases} a_1 = 1 \\ \vdots \\ a_n = 1 \end{cases} \cong \mathbb{F}_2,$$

$$R_{a_1, \dots, a_{n-1}, 1+a_n} := R \left[\frac{1}{a_1}, \dots, \frac{1}{a_{n-1}}, \frac{1}{1+a_n} \right] \cong R \text{ with } \begin{cases} a_1 = 1 \\ \vdots \\ a_{n-1} = 1 \\ a_n = 0 \end{cases} \cong \mathbb{F}_2,$$

$$R_{a_1, \dots, 1+a_i, \dots, a_n} := R \left[\frac{1}{a_1}, \dots, \frac{1}{1+a_i}, \dots, \frac{1}{a_n} \right] \cong R \text{ with } \begin{cases} a_1 = 1 \\ a_i = 0 \\ a_n = 1 \end{cases} \cong \mathbb{F}_2,$$

$$R_{a_1, \dots, 1+a_i, \dots, 1+a_n} := R \left[\frac{1}{a_1}, \dots, \frac{1}{1+a_i}, \dots, \frac{1}{1+a_n} \right] \cong R \text{ with } \begin{cases} a_1 = 1 \\ a_i = 0 \\ a_n = 0 \end{cases} \cong \mathbb{F}_2,$$

$$R_{1+a_1, a_2, \dots, a_n} := R \left[\frac{1}{1+a_1}, \frac{1}{a_2}, \dots, \frac{1}{a_n} \right] \cong R \text{ with } \begin{cases} a_1 = 0 \\ a_2 = 1 \\ \vdots \\ a_n = 1 \end{cases} \cong \mathbb{F}_2,$$

$$\begin{aligned}
R_{1+a_1, \dots, 1+a_{n-1}, a_n} &:= R \left[\frac{1}{1+a_1}, \dots, \frac{1}{1+a_{n-1}}, \frac{1}{a_n} \right] \cong R \text{ with } \\
&\quad \begin{cases} a_1 = 0 \\ \vdots \\ a_{n-1} = 0 \\ a_n = 1 \end{cases} \cong \mathbb{F}_2, \\
R_{1+a_1, \dots, a_i, \dots, 1+a_n} &:= R \left[\frac{1}{1+a_1}, \dots, \frac{1}{a_i}, \dots, \frac{1}{1+a_n} \right] \cong R \text{ with } \begin{cases} a_1 = 0 \\ a_i = 1 \\ a_n = 0 \end{cases} \cong \mathbb{F}_2, \\
R_{1+a_1, \dots, 1+a_n} &:= R \left[\frac{1}{1+a_1}, \dots, \frac{1}{1+a_n} \right] \cong R \text{ with } \begin{cases} a_1 = 0 \\ \vdots \\ a_n = 0 \end{cases} \cong \mathbb{F}_2.
\end{aligned}$$

THEOREM 3.6. *Let $R = \mathbb{F}_2[a_1, \dots, a_n] / \langle a_1^2 - a_1, \dots, a_n^2 - a_n \rangle$ be a ring, $I = \{f_1, \dots, f_n\}$ an ideal of finite type of $R[X_1, \dots, X_s]$, and we fix a monomial order $>$. Then $G = \{f_1, \dots, f_n\}$ is a Gröbner bases for I if and only if $\overline{S(f_i, f_j)}^{G'} = 0$ for $1 \leq i \leq n-1$, $i+1 \leq j \leq n$.*

LEMMA 3.7. *The number of the leaves of the tree constructed when computing dynamically a Gröbner bases of an ideal $R[X_1, \dots, X_s]$ is 2^n .*

Proof. For $i = 2$ we have 4 leaves, that means 2^2 , so by induction from the tree for $i = n$ we find 2^n leaves. $\square$

4. EXAMPLES

EXAMPLE 4.1. Let us consider the ideal $I = \langle f = X + XY^2 + Y^2 + (1 + a_1 + a_2 + a_3 + a_4 + a_1a_2 + a_1a_3 + a_1a_4 + a_2a_3 + a_2a_4 + a_3a_4 + a_1a_2a_3 + a_1a_2a_4 + a_1a_3a_4 + a_2a_3a_4 + a_1a_2a_3a_4)X^2 \rangle$ of $A[X, Y]$ where $A = \mathbb{F}_2[a_1, a_2, a_3, a_4]$ with $a_1^2 = a_1, a_2^2 = a_2, a_3^2 = a_3$ and $a_4^2 = a_4$.

Let us fix the lexicographic order as monomial order with $X > Y$.

The reduced dynamical Gröbner basis of I is

$$\begin{aligned}
&\{(\{X + XY^2 + Y^2\}, a_1^{\mathbb{N}} a_2^{\mathbb{N}} a_3^{\mathbb{N}} a_4^{\mathbb{N}}), (\{X + XY^2 + Y^2\}, a_1^{\mathbb{N}} a_2^{\mathbb{N}} a_3^{\mathbb{N}} (1 + a_4)^{\mathbb{N}}), \\
&\quad (\{X + XY^2 + Y^2\}, a_1^{\mathbb{N}} a_2^{\mathbb{N}} (1 + a_3)^{\mathbb{N}} a_4^{\mathbb{N}}), \\
&\quad (\{X + XY^2 + Y^2\}, a_1^{\mathbb{N}} a_2^{\mathbb{N}} (1 + a_3)^{\mathbb{N}} (1 + a_4)^{\mathbb{N}}), \\
&\quad (\{X + XY^2 + Y^2\}, a_1^{\mathbb{N}} (1 + a_2)^{\mathbb{N}} a_3^{\mathbb{N}} a_4^{\mathbb{N}}), \\
&\quad (\{X + XY^2 + Y^2\}, a_1^{\mathbb{N}} (1 + a_2)^{\mathbb{N}} a_3^{\mathbb{N}} (1 + a_4)^{\mathbb{N}}), \\
&\quad (\{X + XY^2 + Y^2\}, a_1^{\mathbb{N}} (1 + a_2)^{\mathbb{N}} (1 + a_3)^{\mathbb{N}} a_4^{\mathbb{N}}), \\
&\quad (\{1\}, a_1^{\mathbb{N}} (1 + a_2)^{\mathbb{N}} (1 + a_3)^{\mathbb{N}} (1 + a_4)^{\mathbb{N}}), \\
&\quad (\{X + XY^2 + Y^2\}, (1 + a_1)^{\mathbb{N}} a_2^{\mathbb{N}} a_3^{\mathbb{N}} a_4^{\mathbb{N}})\}
\end{aligned}$$

$$\begin{aligned}
& (\{X + XY^2 + Y^2\}, (1 + a_1)^{\mathbb{N}} a_2^{\mathbb{N}} a_3^{\mathbb{N}} (1 + a_4)^{\mathbb{N}}), \\
& (\{X + XY^2 + Y^2\}, (1 + a_1)^{\mathbb{N}} a_2^{\mathbb{N}} (1 + a_3)^{\mathbb{N}} a_4^{\mathbb{N}}), \\
& (\{X + XY^2 + Y^2\}, (1 + a_1)^{\mathbb{N}} a_2^{\mathbb{N}} (1 + a_3)^{\mathbb{N}} (1 + a_4)^{\mathbb{N}}), \\
& (\{X + XY^2 + Y^2\}, (1 + a_1)^{\mathbb{N}} (1 + a_2)^{\mathbb{N}} a_3^{\mathbb{N}} a_4^{\mathbb{N}}), \\
& (\{X + XY^2 + Y^2\}, (1 + a_1)^{\mathbb{N}} (1 + a_2)^{\mathbb{N}} a_3^{\mathbb{N}} (1 + a_4)^{\mathbb{N}}), \\
& (\{X + XY^2 + Y^2\}, (1 + a_1)^{\mathbb{N}} (1 + a_2)^{\mathbb{N}} (1 + a_3)^{\mathbb{N}} a_4^{\mathbb{N}}), \\
& (\{X + XY^2 + Y^2 + X^2\}, (1 + a_1)^{\mathbb{N}} (1 + a_2)^{\mathbb{N}} (1 + a_3)^{\mathbb{N}} (1 + a_4)^{\mathbb{N}}).
\end{aligned}$$

EXAMPLE 4.2. Let us consider the ideal

$$I = \langle f = Y + (1 + 1 + 0 + 1 + 0 + 1 + 0 + 0)XY \rangle$$

of $A[X, Y]$ where $A = \mathbb{F}_2[a_1, a_2, a_3]$ with $a_1^2 = a_1$, $a_2^2 = a_2$ and $a_3^2 = a_3$.

Let us fix the lexicographic order as monomial order with $X > Y$.

The reduced dynamical Gröbner basis of I is

$$\{(\{Y\}, a_1^{\mathbb{N}} a_2^{\mathbb{N}} (1 + a_3)^{\mathbb{N}}), (\{Y\}, a_1^{\mathbb{N}} (1 + a_2)^{\mathbb{N}} a_3^{\mathbb{N}}), (\{Y\}, (1 + a_1)^{\mathbb{N}} a_2^{\mathbb{N}} a_3^{\mathbb{N}})\}.$$

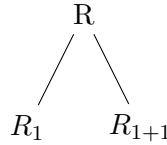
EXAMPLE 4.3. We suppose that we want to construct a dynamical Gröbner bases over $R = \mathbb{F}_2[a_1, a_2, a_3] / \langle a_1^2 - a_1, a_2^2 - a_2, a_3^2 - a_3 \rangle$ for

$$I = \left\langle f_1 = X + 1, f_2 = XY - 1, f_3 = \frac{1-i}{2}Y - 1 \right\rangle$$

with $a_1^2 = a_1$, $a_2^2 = a_2$ and $a_3^2 = a_3$.

Let us fix the lexicographic order as monomial order with $X > Y$. We will give all the details of the computations only for one leaf.

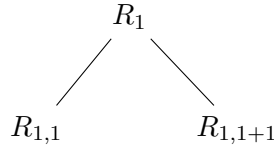
First we have to open two branches:



In R_1 :

$$S(f_1, f_2) = \frac{1}{1} \frac{XY}{X} (X + 1) - \frac{XY}{XY} (XY - 1) = Y + 1 := f_4,$$

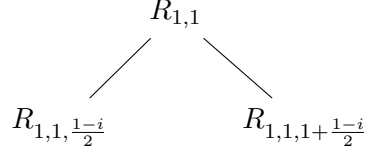
which is not divisible by f_1 and f_2 , one has to open two new branches:



In $R_{1,1}$:

$$S(f_1, f_4) = \frac{1}{1} \frac{XY}{X} (X+1) - \frac{XY}{Y} (Y+1) = -X + Y := f_5$$

which is not divisible by f_1 and f_4 , one has to open two new branches:



In $R_{1,1,\frac{1-i}{2}}$:

$$\begin{aligned} S(f_1, f_5) &= -Y - 1 \xrightarrow{f_4} 0 \\ S(f_2, f_4) &= -x - 1 \xrightarrow{f_1} 0 \\ S(f_2, f_5) &= -Y^2 + 1 \xrightarrow{f_4} 0 \\ S(f_1, f_3) &= \frac{1-i}{2}Y + X \xrightarrow{f_1, f_3} 0 \\ S(f_2, f_3) &= X - \frac{1-i}{2} \xrightarrow{f_2, f_6} 0 \\ S(f_3, f_4) &= \frac{i-3}{1-i} := f_6 \\ S(f_3, f_5) &= \frac{2}{1-i}X - Y^2 \xrightarrow{f_1, f_3, f_4} 0 \\ S(f_4, f_5) &= -X - Y^2 \xrightarrow{f_1, f_4} 0 \\ S(f_5, f_6) &= -\frac{i-3}{1-i}Y \xrightarrow{f_6} 0 \end{aligned}$$

Thus $G_1 = \left\{ X+1, XY-1, \frac{1-i}{2}Y-1, Y+1, -X+Y, \frac{i-3}{1-i} \right\}$ is a Gröbner basis for $\langle f_1, f_2, f_3 \rangle$ at the leaf $R_{1,1,\frac{1-i}{2}}$.

At the leaf $R_{1,1,1+\frac{1-i}{2}}$,

$$G_2 = \left\{ X+1, XY-1, \frac{1-i}{2}Y-1, Y+1, -X+Y, \frac{i-3}{2} \right\}.$$

At the leaf $R_{1,1+1,\frac{1-i}{2}}$,

$$G_3 = \left\{ X+1, XY-1, \frac{1-i}{2}Y-1, Y+1, -X+Y, \frac{i-3}{1-i} \right\}.$$

At the leaf $R_{1,1+1,1+\frac{1-i}{2}}$,

$$G_4 = \left\{ X+1, XY-1, \frac{1-i}{2}Y-1, Y+1, -X+Y, \frac{i-3}{2} \right\}.$$

At the leaf $R_{1+1,1,\frac{1-i}{2}}$,

$$G_5 = \left\{ X + 1, XY - 1, \frac{1-i}{2}Y - 1, Y + 1, -X + Y, \frac{i-3}{1-i} \right\}.$$

At the leaf $R_{1+1,1,1+\frac{1-i}{2}}$,

$$G_6 = \left\{ X + 1, XY - 1, \frac{1-i}{2}Y - 1, Y + 1, -X + Y, \frac{i-3}{2} \right\}.$$

At the leaf $R_{1+1,1+1,\frac{1-i}{2}}$,

$$G_7 = \left\{ X + 1, XY - 1, \frac{1-i}{2}Y - 1, Y + 1, -X + Y, \frac{i-3}{1-i} \right\}.$$

At the leaf $R_{1+1,1+1,1+\frac{1-i}{2}}$,

$$G_8 = \left\{ X + 1, XY - 1, \frac{1-i}{2}Y - 1, Y + 1, -X + Y, \frac{i-3}{2} \right\}.$$

REFERENCES

- [1] Y. Cai and D. Kapur, *An algorithm for computing a Gröbner basis of a polynomial ideal over a ring with zero divisors*, University of New Mexico, Technical Report, 2003.
- [2] A. Hadj Kacem and I. Yengui, *Dynamical Gröbner bases over Dedekind rings*, J. Algebra, **324** (2010), 12–24.
- [3] D. Kapur and P. Narendran, *An equational approach to theoretical proving in first-order predicate calculus*. In: *International Joint Conference on Artificial Intelligence* (1985), pp. 1146–1153.
- [4] I. Yengui, *Constructive commutative algebra*, Springer, 2015.
- [5] F. Pauer, *On lucky ideals for Grobner basis computations*, Symb. Comp. , **14** (1992) 471–482.
- [6] E. Arnold, *Modular algorithms for computing Grobner bases*, J. Symb. Comp., **35** (2003) 403–419.
- [7] M. Brickenstein, A. Dreyer, G. Greuel, M. Wedler and O. Wienand, *New developments in the theory of Groebner bases and applications to formal verification*, J. Pure Appl. Algebra, **213** (2009), 1612–1635.

Received November 1, 2024

Accepted February 13, 2025

University of Oran1

Department of Mathematics and Applications

Mathematics and Applications Laboratory

Oran, Algeria

E-mail: mouseddek.hadjer@edu.univ-oran1.dz

E-mail: mouseddekhadjerry@gmail.com

<https://orcid.org/0009-0007-4583-1923>

E-mail: fboudaoud@yahoo.fr

<https://orcid.org/0000-0003-4211-130X>