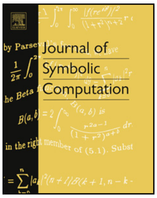
Journal of Symbolic Computation 86 (2018) 1–19

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc



On Gröbner bases and Krull dimension of residue class rings of polynomial rings over integral domains

Maria Francis, Ambedkar Dukkipati

Dept. of Computer Science & Automation, Indian Institute of Science, Bangalore 560012, India

ARTICLE INFO

Article history:
Received 20 July 2016
Accepted 3 March 2017
Available online 24 March 2017

Keywords:
Gröbner bases over commutative rings
Krull dimension of residue class rings of polynomial rings over rings
Independent sets modulo an ideal

ABSTRACT

Given an ideal $\mathfrak{a}$ in $A[x_1, \dots, x_n]$ where A is a Noetherian integral domain, we propose an approach to compute the Krull dimension of $A[x_1, \dots, x_n]/\mathfrak{a}$, when the residue class ring is a free A-module. When A is a field, the Krull dimension of $A[x_1, \dots, x_n]/\mathfrak{a}$ has several equivalent algorithmic definitions by which it can be computed. But this is not true in the case of arbitrary Noetherian rings. For a Noetherian integral domain A we introduce the notion of combinatorial dimension of $A[x_1, \dots, x_n]/\mathfrak{a}$ and give a Gröbner basis method to compute it for residue class rings that have a free A-module representation w.r.t. a lexicographic ordering. For such A-algebras, we derive a relation between Krull dimension and combinatorial dimension of $A[x_1, \dots, x_n]/\mathfrak{a}$. An immediate application of this relation is that it gives a uniform method, the first of its kind, to compute the dimension of $A[x_1, \dots, x_n]/\mathfrak{a}$ without having to consider individual properties of the ideal. For A-algebras that have a free A-module representation w.r.t. degree compatible monomial orderings, we introduce the concepts of Hilbert function, Hilbert series and Hilbert polynomials and show that Gröbner basis methods can be used to compute these quantities. We then proceed to show that the combinatorial dimension of such A-algebras is equal to the degree of the Hilbert polynomial. This enables us to extend the relation between Krull dimension and combinatorial dimension to A-algebras with a free A-module representation w.r.t. a degree compatible ordering as well.

E-mail addresses: mariaf@csa.iisc.ernet.in (M. Francis), ad@csa.iisc.ernet.in (A. Dukkipati).

http://dx.doi.org/10.1016/j.jsc.2017.03.003
0747-7171/© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

One of the fundamental problems in computational ideal theory is determining the dimension of an ideal, i.e. the Krull dimension of the $\mathbb{k}$-algebra, $\mathbb{k}[x_1, \dots, x_n]/\mathfrak{a}$. The dimension of an affine variety associated with an ideal $\mathfrak{a} \subseteq \mathbb{k}[x_1, \dots, x_n]$ is the Krull dimension of the affine $\mathbb{k}$-algebra $\mathbb{k}[x_1, \dots, x_n]/\mathfrak{a}$ for an algebraically closed field $\mathbb{k}$. Since the definition of Krull dimension does not lead to an algorithmic method to compute it, various alternate equivalent definitions have been proposed. The Krull dimension of an affine $\mathbb{k}$-algebra is equal to its transcendence degree, the degree of the Hilbert polynomial of $\mathfrak{a}$ and the largest number of elements among the maximal set of indeterminates independent mod $\mathfrak{a}$ (called the combinatorial dimension of $\mathbb{k}[x_1, \dots, x_n]/\mathfrak{a}$) (Kreuzer and Robbiano, 2005). Gröbner basis based algorithms have been proposed to compute the degree of the Hilbert polynomial of $\mathfrak{a}$ and the combinatorial dimension of $\mathbb{k}[x_1, \dots, x_n]/\mathfrak{a}$ (Mora and Möller, 1983; Kredel and Weispfenning, 1988), thus providing an algorithmic framework for determining the Krull dimension of the affine variety associated with $\mathfrak{a}$. This paper studies the question of whether one can give Gröbner basis methods to compute the Krull dimension of $A[x_1, \dots, x_n]/\mathfrak{a}$, where A is a Noetherian integral domain, given that it has a free A-module representation w.r.t. some monomial order.

For any Noetherian commutative ring A, a necessary and sufficient condition for a finitely generated A-module $A[x_1, \dots, x_n]/\mathfrak{a}$ to have a free A-module representation w.r.t. a monomial order has been studied in Francis and Dukkipati (2014). Here, we show that this characterization can be extended to $A[x_1, \dots, x_n]/\mathfrak{a}$ that need not be finitely generated as an A-module.

Given an integral domain A and an A-algebra with a free A-module representation w.r.t. some monomial order, we study alternate algorithmic definitions for Krull dimension. We first extend the concept of combinatorial dimension to A-algebras. For an A-algebra with a free A-module representation w.r.t. a lexicographic ordering, we give a Gröbner basis algorithm for computing its combinatorial dimension. In affine $\mathbb{k}$-algebras, the combinatorial dimension is equal to the Krull dimension. We derive a relation between Krull dimension and combinatorial dimension for A-algebras that have a free A-module representation w.r.t. a lexicographic order. We also show that the concepts of Hilbert functions, Hilbert series and Hilbert polynomial can be extended to A-algebras that have a free A-module representation w.r.t. a degree compatible ordering. We also give a Gröbner basis algorithm to compute these quantities. For degree compatible orderings, we show that the combinatorial dimension of $A[x_1, \dots, x_n]/\mathfrak{a}$ is equal to the degree of the Hilbert polynomial of $\mathfrak{a}$ and therefore we have a Gröbner basis algorithm to compute the combinatorial dimension. We also show how this can be used to derive a relation between the Krull dimension of $A[x_1, \dots, x_n]/\mathfrak{a}$ and the degree of the Hilbert polynomial of $\mathfrak{a}$. The concepts of combinatorial dimension and Hilbert polynomial are important because they give us a uniform method, independent of the ideal, to determine the Krull dimension of $A[x_1, \dots, x_n]/\mathfrak{a}$ that has a free A-module representation w.r.t. either a lexicographic or a degree compatible monomial ordering. More importantly, these concepts allow for an algorithmic interpretation of the algebraic concept of Krull dimension for certain A-algebras.

The rest of the paper is organized as follows. In Section 2, we discuss the notations used in the paper. In Section 3, we extend the necessary and sufficient condition for the quotient ring $A[x_1, \dots, x_n]/\mathfrak{a}$, where A is a Noetherian commutative ring, to have a free A-module representation w.r.t. a monomial order to the infinite case. After this section, the paper restricts its study to residue class rings of polynomial rings over Noetherian integral domains. In Section 4, we define combinatorial dimension for A-algebras, where A is a Noetherian integral domain. In Section 4.2, we give a Gröbner basis method to compute the combinatorial dimension of $A[x_1, \dots, x_n]/\mathfrak{a}$ that has a free A-module representation w.r.t. a lexicographic ordering. For such A-algebras, we derive a relation between combinatorial dimension and Krull dimension in Section 5. In Section 5.2, we illustrate with examples how this relation gives an algorithmic method to determine the Krull dimension. We define Hilbert function, Hilbert series and Hilbert polynomial for A-algebras that have a free A-module representation w.r.t. a degree compatible monomial order in Section 6. We also give a Gröbner basis algorithm to compute these quantities. We then show in Section 6.2 that the combinatorial dimension of A-algebras with a free A-module representation w.r.t. a degree compatible monomial order is equal to the degree of the Hilbert polynomial. This enables us to give a relation between the degree of the Hilbert polynomial and the Krull dimension of the corresponding residue class ring in Section 6.3.

2. Preliminaries

Throughout this paper, $\Bbbk$ denotes a field, $\mathbb{Z}$ the ring of integers and $\mathbb{N}$ the set of positive integers including zero. We use A to denote a Noetherian commutative ring. From Section 4 onwards, A is restricted to Noetherian integral domains. A polynomial ring in indeterminates $x_1, \dots, x_n$ over A is denoted as $A[x_1, \dots, x_n]$. At times, we represent the indeterminates collectively as a set X and the corresponding polynomial ring as $A[X]$. We represent a monomial in $x_1, \dots, x_n$ as x^α where $\alpha \in \mathbb{Z}^n_{\geq 0}$. The monoid isomorphism between the set of all monomials in indeterminates $x_1, \dots, x_n$ and $\mathbb{Z}^n_{\geq 0}$ allows us to denote the set of all monomials as $\mathbb{Z}^n_{\geq 0}$. A nonzero polynomial, f in $x_1, \dots, x_n$ with coefficients from A is given by

$$f = \sum_{\alpha \in \Lambda_f} a_\alpha x^\alpha,$$

where $\Lambda_f \subsetneq \mathbb{Z}^n_{\geq 0}$ is a finite set and $a_\alpha \in A \setminus \{0\}$. We denote all the monomials of a polynomial f as $\mathrm{Mon}(f)$. We assume that there is a monomial order $\prec$ on the monomials in the indeterminates $x_1, \dots, x_n$. With respect to this monomial order, we have the leading monomial ($\mathrm{lm}_\prec$), leading coefficient ($\mathrm{lc}_\prec$), leading term ($\mathrm{lt}_\prec$) and multidegree ($\mathrm{multideg}_\prec$) of a polynomial $f \in A[x_1, \dots, x_n]$, where $\mathrm{multideg}_\prec(f) = \max_\prec\{\alpha \in \Lambda_f\}$ and $\mathrm{lt}_\prec(f) = \mathrm{lc}_\prec(f)\mathrm{lm}_\prec(f)$ in $A[x_1, \dots, x_n]$. In certain scenarios, we also consider another concept of degree of a polynomial which we will denote as $\deg(f)$. The degree of a monomial x^α, $\deg(x^\alpha)$ is the sum of its exponents. The degree of a polynomial, f is the maximum degree of the monomials in f, i.e.

$$\deg(f) = \max\{\deg(x^\alpha) : x^\alpha \in \mathrm{Mon}(f)\}.$$

A degree compatible monomial ordering $\prec$ is a monomial ordering on $A[x_1, \dots, x_n]$ such that two monomials x^α, $x^{\alpha'}$ with $x^\alpha \prec x^{\alpha'}$ satisfy $\deg(x^\alpha) \leq \deg(x^{\alpha'})$. For a degree compatible monomial ordering, the leading monomial will be a monomial with maximum degree. The leading term ideal (or initial ideal) of a set $S \subseteq A[x_1, \dots, x_n]$, is $\langle \mathrm{lt}_\prec(S) \rangle = \langle \{\mathrm{lt}_\prec(f) \mid f \in S\} \rangle$. When there is no confusion regarding which monomial order to consider we omit the monomial order subscript $\prec$ from the notations. For a free A-module M, the minimum cardinality of a basis of A is called its free rank and is denoted by $\mathrm{FreeRank}_A(M)$.

3. Characterization of a free residue class ring of $A[x_1, \dots, x_n]$

Consider an ideal $\mathfrak{a}$ in $A[x_1, \dots, x_n]$ and let $G = \{g_i : i = 1, \dots, t\}$ be its Gröbner basis w.r.t. a monomial order $\prec$. For each monomial x^α, let $J_{x^\alpha} = \{i : \mathrm{lm}(g_i) \mid x^\alpha, g_i \in G\}$ and $I_{J_{x^\alpha}} = \langle \{\mathrm{lc}(g_i) : i \in J_{x^\alpha}\} \rangle$. We refer to $I_{J_{x^\alpha}}$ as the leading coefficient ideal w.r.t. G. Let $C_{J_{x^\alpha}}$ represent a set of coset representatives of the equivalence classes in $A/I_{J_{x^\alpha}}$. We use the same definitions as given in Adams and Loustaunau (1994). Given a polynomial $f \in A[x_1, \dots, x_n]$, let $f = \sum_{i=1}^{m} a_i x^{\alpha_i} \mod \langle G \rangle$, where $a_i \in A, i = 1, \dots, m$. If $A[x_1, \dots, x_n]/\langle G \rangle$ is an A-module finitely generated by m elements, then corresponding to the coset representatives, $C_{J_{x^{\alpha_1}}}, \dots, C_{J_{x^{\alpha_m}}}$, there exists an A-module isomorphism,

$$\begin{aligned} \phi : A[x_1, \dots, x_n]/\langle G \rangle &\longrightarrow A/I_{J_{x^{\alpha_1}}} \times \cdots \times A/I_{J_{x^{\alpha_m}}} \\ \sum_{i=1}^{m} a_i x^{\alpha_i} + \langle G \rangle &\longmapsto (c_1 + I_{J_{x^{\alpha_1}}}, \cdots, c_m + I_{J_{x^{\alpha_m}}}), \end{aligned} \tag{1}$$

where $c_i = a_i \mod I_{J_{x^{\alpha_i}}}$ and $c_i \in C_{J_{x^{\alpha_i}}}$.

We refer to $A/I_{J_{x^{\alpha_1}}} \times \cdots \times A/I_{J_{x^{\alpha_m}}}$ as the A-module representation of $A[x_1, \dots, x_n]/\mathfrak{a}$ w.r.t. G (or w.r.t. $\prec$). If $I_{J_{x^{\alpha_i}}} = \{0\}$, we have $C_{J_{x^{\alpha_i}}} = A$, for all $i = 1, \dots, m$. This implies $A[x_1, \dots, x_n]/\mathfrak{a} \cong A^m$, i.e.

$A[x_1,\dots,x_n]/\mathfrak{a}$ has an A-module basis and it is free. We say that $A[x_1,\dots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G (or w.r.t. $\prec$). If the A-module is infinitely generated, we say that it has a free A-module representation w.r.t. G (or equivalently w.r.t. $\prec$) if $I_{J_{x^\alpha}} = \{0\}$ for all $x^\alpha \notin \langle \mathrm{lm}(\mathfrak{a})\rangle$ and $I_{J_{x^\alpha}} = A$ for all $x^\alpha \in \langle \mathrm{lm}(\mathfrak{a})\rangle$.

The necessary and sufficient condition for an A-module $A[x_1,\dots,x_n]/\mathfrak{a}$ to have a free A-module representation w.r.t. G (or w.r.t. $\prec$) makes use of the concept of 'short reduced Gröbner basis' introduced in Francis and Dukkipati (2014) which we briefly describe below.

Definition 3.1. Let $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ be an ideal. Consider the isomorphism in (1). A reduced Gröbner basis (as defined in Pauer, 2007), G of $\mathfrak{a}$ is called a short reduced Gröbner basis if for each $x^\alpha \in \mathrm{lm}(G)$, the number of elements in the generating set of the leading coefficient ideal of x^α, $I_{J_{x^\alpha}}$ in (1) is minimal.

One can define reduced Gröbner bases over rings exactly as that of fields but it may not exist in all the cases. The definition of reduced Gröbner basis given by Pauer (2007) ensures the existence of such a basis for every ideal in the polynomial ring.

A necessary and sufficient condition for a finitely generated A-module $A[x_1,\dots,x_n]/\mathfrak{a}$ to have a free A-module representation w.r.t. G (or w.r.t. $\prec$) is given in Francis and Dukkipati (2014). One can easily extend this to residue class rings that are not finitely generated as shown below.

Lemma 3.2. *Let $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ be a non-zero ideal and let G be a short reduced Gröbner basis for $\mathfrak{a}$. All the leading coefficient ideals associated with G are either trivial or the entire ring A if and only if G is monic.*

Proof. The proof is along the lines of Francis and Dukkipati (2014, Lemma 3.10). □

We now prove the necessary condition.

Theorem 3.3. *Let $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ be a non-zero ideal and let G be a short reduced Gröbner basis of $\mathfrak{a}$. If $A[x_1,\dots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G (or w.r.t. $\prec$) then G is monic.*

Proof. By definition, if $A[x_1,\dots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G then $I_{J_{x^\alpha}} = \{0\}$ for all $x^\alpha \notin \langle \mathrm{lm}(\mathfrak{a})\rangle$ and $I_{J_{x^\alpha}} = \{1\}$ for all $x^\alpha \in \langle \mathrm{lm}(\mathfrak{a})\rangle$. That is, all the leading coefficient ideals associated with G are either trivial or the entire ring, A. Therefore by Lemma 3.2, G is monic. □

The sufficient condition is subsumed by Francis and Dukkipati (2014, Theorem 3.8). We state the characterization result as follows.

Proposition 3.4. *Let $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ be a nonzero ideal. Let G be a short reduced Gröbner basis for $\mathfrak{a}$ w.r.t. some monomial ordering $\prec$. Then, $A[x_1,\dots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G (or $\prec$) if and only if G is monic.*

Example 3.5. Let $G = \{3x, 5x\}$ be the Gröbner basis of an ideal $\mathfrak{a}$ in $\mathbb{Z}[x,y]$ w.r.t. a lexicographic ordering $\prec$ such that $x \prec y$. We have $I_{J_x} = \langle 3, 5\rangle = \langle 1\rangle$. Therefore, $\mathbb{Z}[x,y]/\langle 3x, 5x\rangle$ has a free A-module representation w.r.t. $\prec$. The short reduced Gröbner basis of $\mathfrak{a}$ is given by $G_{\mathrm{red}} = \{x\}$. It is monic and a $\mathbb{Z}$-module basis of $\mathbb{Z}[x,y]/\mathfrak{a}$ is given by $\{1 + \mathfrak{a}, y^n + \mathfrak{a}, n \in \mathbb{N} \setminus \{0\}\}$.

Note that if a Gröbner basis or reduced Gröbner basis of an ideal w.r.t. a monomial order $\prec$ is monic its short reduced Gröbner basis w.r.t. $\prec$ will also be monic, but not vice versa. Throughout this paper, we will assume that $A[x_1,\dots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a monomial order or equivalently, w.r.t. any Gröbner basis corresponding to that monomial order.

4. Combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$

In the rest of the paper we assume that A is a Noetherian integral domain. The Krull dimension of a ring is defined as the supremum of the lengths of all the chains of prime ideals in it. There are many alternate algorithmic definitions for the dimension of an affine $\Bbbk$-algebra. All of them can be shown to be equivalent. On the other hand, for A-algebras these definitions are either not equivalent or not valid.

We define combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$, denoted by $\operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$, in a manner analogous to the definition of combinatorial dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ (Kreuzer and Robbiano, 2005).

Definition 4.1. Given a Noetherian integral domain A, let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal. Let $X \subseteq \{x_1, \ldots, x_n\}$ be a set of indeterminates. The set X is said to be independent modulo $\mathfrak{a}$ or an independent set of indeterminates modulo $\mathfrak{a}$ if $\mathfrak{a} \cap A[X] = \{0\}$. The set X is called a maximal independent set modulo $\mathfrak{a}$ if X is independent modulo $\mathfrak{a}$ and there is no set $Y \subseteq \{x_1, \ldots, x_n\}$ independent modulo $\mathfrak{a}$ with $X \subsetneq Y$. The largest number of elements of a maximal independent set of indeterminates modulo $\mathfrak{a}$ is called the combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$, denoted as $\operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$.

4.1. Some properties of combinatorial dimension

The Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$, for an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$, is the maximal Krull dimension of an isolated prime ideal associated with $\mathfrak{a}$. Below we show that this result holds for combinatorial dimension as well.

Lemma 4.2. *Let A be a Noetherian integral domain and $\mathfrak{a}$ be an ideal in $A[x_1, \ldots, x_n]$. Then $\operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$ is the maximum of $\operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{p})$, where $\mathfrak{p}$ is an isolated prime ideal associated with $\mathfrak{a}$.*

Proof. We will denote $\operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$ as d. Let $\mathfrak{p}$ be an isolated prime ideal associated with $\mathfrak{a}$ and $S \subseteq X$ denote the maximal set of indeterminates that are independent modulo $\mathfrak{p}$. They are independent modulo $\mathfrak{a}$ and therefore, $d \geq |S|$. Conversely, let $S \subseteq X$ be a maximal independent set of indeterminates modulo $\mathfrak{a}$ such that $|S| = d$. Then $M = A[S] \setminus \{0\}$ is multiplicatively closed and disjoint from $\mathfrak{a}$. There exists a prime ideal $\mathfrak{P}$, that contains $\mathfrak{a}$ and does not meet M. Let $\mathfrak{p}' \subseteq \mathfrak{P}$ be the isolated prime ideal associated with $\mathfrak{a}$. S is independent modulo $\mathfrak{p}'$. This implies $\operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{p}') \geq d$. □

For a subset of indeterminates S, the set $\overline{S}$ represents the set of residue classes of S modulo the ideal $\mathfrak{a}$.

Proposition 4.3. *Given a Noetherian integral domain A, let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be a prime ideal. Then, all maximal sets of indeterminates independent modulo $\mathfrak{a}$ have the same cardinality.*

Proof. Since $\mathfrak{a}$ is a prime ideal, $A[x_1, \ldots, x_n]/\mathfrak{a}$ is an integral domain. Let $\operatorname{Quot}(A[x_1, \ldots, x_n]/\mathfrak{a})$ represent the quotient field of $A[x_1, \ldots, x_n]/\mathfrak{a}$. Let $X = \{x_1, \ldots, x_n\}$ and $S \subseteq X$ be a set of indeterminates. S is independent modulo $\mathfrak{a}$ if and only if $\overline{S}$ is algebraically independent in $\operatorname{Quot}(A[x_1, \ldots, x_n]/\mathfrak{a})$ over A. Assume that there are maximal independent sets modulo $\mathfrak{a}$ of different cardinalities. Let the two sets that are maximal independent modulo $\mathfrak{a}$ be $S \cup \{a\}$ and $S \cup \{b_1, b_2\}$. This implies $S \cup \{a, b_1\}$ and $S \cup \{a, b_2\}$ are dependent sets of indeterminates modulo $\mathfrak{a}$. Therefore, we have $\overline{b_1}$ is algebraic over $\operatorname{Quot}(A[\overline{S}])(\overline{a})$ and $\overline{a}$ is algebraic over $\operatorname{Quot}(A[\overline{S}])(\overline{b_2})$. Therefore, $\overline{b_1}$ is algebraic over $\operatorname{Quot}(A[\overline{S}])(\overline{b_2})$, which is a contradiction to the independence of $S \cup \{b_1, b_2\}$ modulo $\mathfrak{a}$. □

4.2. Gröbner basis method for computing combinatorial dimension for lexicographic orderings

We extend the concept of strongly independent indeterminates modulo $\mathfrak{a}$ introduced in Kredel and Weispfenning (1988) for ideals in $\mathbb{k}[x_1, \dots, x_n]$, to polynomial rings over A.

Definition 4.4. Let $S \subseteq X$ be a set of indeterminates and $\prec$ a monomial order in $A[x_1, \dots, x_n]$. Then, $A[S/(X \setminus S)]$ denotes the following set,

$$A[S/(X \setminus S)] = \{f \in A[x_1, \dots, x_n] : 0 \neq f \text{ and } \mathrm{lt}(f) \in A[S]\}.$$

We say that S is strongly independent modulo $\mathfrak{a}$ if $A[S/(X \setminus S)] \cap \mathfrak{a} = \emptyset$.

Clearly, if S is strongly independent modulo $\mathfrak{a}$, then it is independent modulo $\mathfrak{a}$. But the converse is not true.

Lemma 4.5. *Let $\mathfrak{a} \subseteq A[x_1, \dots, x_n]$ be a proper ideal and $\prec$ be a monomial order in $A[x_1, \dots, x_n]$. Let $S \subseteq X$ be a set of indeterminates.*

(i) *If S is strongly independent modulo $\mathfrak{a}$ w.r.t. $\prec$, then there exists an isolated prime ideal $\mathfrak{p}$ associated with $\mathfrak{a}$ such that S is also strongly independent modulo $\mathfrak{p}$ w.r.t. $\prec$.*

(ii) *Let $U = \{S \subseteq X : S$ is strongly independent modulo $\mathfrak{a}$ w.r.t. $\prec\}$ and $U' = \{S \subseteq X :$ there exists an isolated prime ideal $\mathfrak{p}$ associated with $\mathfrak{a}$ such that S is strongly independent modulo $\mathfrak{p}$ w.r.t. $\prec\}$, then $U = U'$.*

Proof.

(i) Let S be strongly independent modulo $\mathfrak{a}$. Let $M = A[S/(X \setminus S)] \setminus \{0\}$ be a multiplicatively closed subset of $A[x_1, \dots, x_n]$ disjoint to $\mathfrak{a}$. Then there exists a prime ideal $\mathfrak{P}$ such that $\mathfrak{a} \subseteq \mathfrak{P}$ and disjoint from M. Let $\mathfrak{p}' \subseteq \mathfrak{P}$ be an isolated prime ideal associated with $\mathfrak{a}$. Then S is strongly independent modulo $\mathfrak{p}'$. Also, if S is maximal strongly independent modulo $\mathfrak{a}$, then for any $S \subseteq S' \subseteq X$, where S' is strongly independent modulo $\mathfrak{p}'$, S' is strongly independent modulo $\mathfrak{a}$, so $S' = S$.

(ii) Clearly, $U' \subseteq U$ and by (i), $U \subseteq U'$. □

We recall the concept of inessential set of indeterminates from Kredel and Weispfenning (1988). Let $S \subseteq X$ be a set of indeterminates, $f \in A[x_1, \dots, x_n]$ be a polynomial and $\prec$ be a monomial order in $A[x_1, \dots, x_n]$. We denote f^S as the polynomial resulting from f by substituting 1 for all indeterminates from S in f. We say that S is inessential for f if for all terms t occurring in f, $t^S \preccurlyeq \mathrm{lt}(f)^S$.

Theorem 4.6. *Let $S \subseteq X$, $\mathfrak{a}$ be a prime ideal in $A[x_1, \dots, x_n]$ and let $\prec$ be a monomial order such that $A[x_1, \dots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. $\prec$. Assume that S is independent modulo $\mathfrak{a}$ and that for any $x \in X \setminus S$, there exists a polynomial $f_x \in A[S \cup \{x\}/X \setminus (S \cup \{x\})] \cap \mathfrak{a}$ such that S is inessential for f_x. Then S is maximal independent modulo $\mathfrak{a}$ and $|S| = \mathrm{cdim}(A[x_1, \dots, x_n]/\mathfrak{a})$.*

Proof. For $x \in X \setminus S$, let d_x be the degree of $\mathrm{lt}(f_x)$ in x. Then $d_x \gneq 0$, for otherwise $\mathrm{lt}(f_x)^S = 1$ and so $t^S = 1$ for all terms t occurring in f_x, which implies $f_x \in A[S]$ which contradicts the independence of S modulo $\mathfrak{a}$. Let T be the set of all $t \in \mathrm{Mon}(A[x_1, \dots, x_n])$ such that for every $x \in X \setminus S$, the degree of x in t is $\lneq d_x$.

Claim 1. *For every $t \in \mathrm{Mon}(A[x_1, \dots, x_n]) \setminus T$, there exists $0 \neq p, p_1, \dots, p_m \in A[S]$, $t_1, \dots, t_m \in T$ and $f \in \mathfrak{a}$ such that $pt = p_1 t_1 + \cdots + p_m t_m + f$.*

Proof of the claim. Assume the contradiction, that the claim fails for some $t \in \mathrm{Mon}(A[x_1, \dots, x_n]) \setminus T$ and that t is $\prec$-minimal among the monomials with this property. Choose $x \in X \setminus S$ such that the degree d of t in $x \geq d_x$ and let $u = tx^{-d} \in \mathrm{Mon}(A[x_1, \ldots, x_n])$. f_x can be written as $px^{d_x} - (p_1 t_1 + \cdots + p_m t_m)$ with $0 \neq p, p_1, \ldots, p_m \in A[S]$, $t_i \in \mathrm{Mon}(A[X \setminus S])$, $t_i \prec x^{d_x}$, $1 \leq i \leq m$. By multiplying with $x^{d-d_x}u$, we get

$$pt = x^{d-d_x}uf_x - (p_1 t_1 x^{d-d_x}u + \cdots + p_m t_m x^{d-d_x}u).$$

We have $x^{d-d_x}uf_x \in \mathfrak{a}$ and $t_i x^{d-d_x}u \prec x^{d_x}x^{d-d_x}u = t$ for $1 \leq i \leq m$. (Note that here we have two comparisons, one is the less than comparison, $<$ based on the degrees of a variable in the monomials and the other is the comparison based on the monomial order, $\prec$.) Since t is $\prec$-minimal among the monomials that violate the claim, the claim is valid for all $t_i x^{d-d_x}u, 1 \leq i \leq m$ and therefore Claim 1 is valid for t as well, a contradiction.

Let $\mathrm{Quot}(A)$ represent the quotient field of the integral domain, A. Since $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. $\prec$ we have $A \cap \mathfrak{a} = \{0\}$. This implies $\mathrm{Quot}(A) \subseteq \mathrm{Quot}(A)(\overline{S}) \subsetneq \mathrm{Quot}(A[x_1, \ldots, x_n]/\mathfrak{a})$. By Claim 1, $\mathrm{Quot}(A)[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated as a $\mathrm{Quot}(A)(\overline{S})$-vector space by $\overline{T}$. Each $\overline{x}$, $x \in X \setminus S$ is algebraic over $\mathrm{Quot}(A)(\overline{S})$. Since $A \cap \mathfrak{a} = \{0\}$, this implies that for each $x \in X \setminus S$ we can determine a $f \in A[S \cup \{x\}] \cap \mathfrak{a}$. Therefore, S is maximal independent modulo $\mathfrak{a}$ and since $\mathfrak{a}$ is a prime ideal, $\mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) = |S|$. □

Definition 4.7 *(Left Basic Set (LBS)).* Let $\prec$ be a monomial order in $A[x_1, \ldots, x_n]$ and $\mathfrak{a}$ be an ideal in $A[x_1, \ldots, x_n]$. Given the set of indeterminates X, we define $S_k \subseteq X$, $0 \leq k \leq n$ inductively as

$$S_0 = \emptyset$$
$$S_{k+1} = \begin{cases} S_k \cup \{x_k\} & \text{if } S_k \cup \{x_k\} \text{ is strongly independent} \\ & \text{modulo } \mathfrak{a} \text{ w.r.t. } \prec \\ S_k & \text{otherwise.} \end{cases}$$

The set S_n is called the left basic set of $\mathfrak{a}$ w.r.t. $\prec$.

S_n is maximal strongly independent modulo $\mathfrak{a}$ w.r.t. $\prec$. For lexicographic orderings, as a consequence of Theorem 4.6 we have the following result for prime ideals.

Corollary 4.8. *Let $\mathfrak{a}$ be a prime ideal in $A[x_1, \ldots, x_n]$ and $\prec$ be a lexicographic ordering such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. $\prec$. If S is the left basic set of $\mathfrak{a}$ w.r.t. $\prec$, then S is maximal independent modulo $\mathfrak{a}$ and so $|S| = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$.*

Proof. Since S is maximal strongly independent modulo $\mathfrak{a}$, for every $x \in X \setminus S$, there exists a polynomial $f_x \in A[S \cup \{x\}/X \setminus (S \cup \{x\})] \cap \mathfrak{a}$. f_x contains no $y \in X$ such that $x \prec y$ since $\prec$ is a lexicographic order. Also for every monomial $t \in \mathrm{Mon}(f_x)$, the degree of t in x is less than or equal to the degree of the leading term of f_x in x. Therefore, $\mathrm{lt}(f_x)^S \geq t^S$ for all terms in f_x. Therefore, S is inessential for f_x and we can apply Theorem 4.6 and $|S| = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$. □

The idea can be extended to other proper ideals in $A[x_1, \ldots, x_n]$.

Theorem 4.9. *Let $\mathfrak{a}$ be a proper ideal in $A[x_1, \ldots, x_n]$ and $\prec$ be a lexicographic monomial order such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. $\prec$. Let*

$$d = \max\{|S| : S \subseteq X, S \textit{ is maximal strongly independent modulo } \mathfrak{a} \textit{ w.r.t. } \prec\}.$$

Then, $d = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$.

Proof. Since each S that is maximal strongly independent modulo $\mathfrak{a}$ is independent modulo $\mathfrak{a}$ we have $\mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) \geq d$. Pick an isolated prime ideal $\mathfrak{p}$ associated with $\mathfrak{a}$ such that

$$\mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{p}) = \mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a}).$$

Let S be the LBS of $\mathfrak{p}$. Then,

$$|S| = \mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{p}) = \mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a})$$

and S is strongly independent modulo $\mathfrak{p}$ and therefore $\mathfrak{a}$ and so $d \geq \mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a})$. □

Since strongly independent modulo $\mathfrak{a}$ depends on the leading terms of an ideal, we explore its connections with Gröbner basis.

Theorem 4.10. *Let $\prec$ be a monomial ordering in $A[x_1,\dots,x_n]$ and $S \subseteq X$ be a set of indeterminates. Let G be a Gröbner basis of an ideal, $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ w.r.t. $\prec$. Then S is strongly independent modulo $\mathfrak{a}$ w.r.t. $\prec$ if and only if $A[S] \cap \mathrm{lt}(G) = \emptyset$.*

Proof. If for some $g \in G$, $\mathrm{lt}(g) \in A[S]$, then $g \in A[S/(X \setminus S)] \cap \mathfrak{a}$ and therefore S is not strongly independent modulo $\mathfrak{a}$. Conversely, assume there exists $f \in A[S/(X \setminus S)] \cap \mathfrak{a}$, then there exists at least one $g \in G$ such that $\mathrm{lm}(g) \mid \mathrm{lm}(f)$. Since $\mathrm{lt}(f) \in A[S]$, $\mathrm{lm}(g) \in A[S]$. □

We can construct the LBS of $\mathfrak{a}$ w.r.t. $\prec$ from G by the following algorithm which is analogous to Kredel and Weispfenning (1988, Corollary 2.2).

Corollary 4.11. *Let $\prec$ be a monomial order in $A[x_1,\dots,x_n]$ and G be a Gröbner basis w.r.t. $\prec$ for an ideal $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$. Algorithm 1 determines the left basic set of $\mathfrak{a}$ w.r.t. $\prec$.*

Algorithm 1 Finding the Left Basic Set of an ideal $\mathfrak{a}$ in $A[x_1,\dots,x_n]$.

```
Input $G$, Gröbner basis of $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ w.r.t. $\prec$
Output $S$, Left Basic Set of $\mathfrak{a}$ w.r.t. $\prec$.
$S = \emptyset$, $U = \{x_1,\dots,x_n\}$
while $U \neq \emptyset$ do
  Select $x$ from $U$.
  $U = U \setminus \{x\}$
  if $\mathrm{Mon}(A[S] \cup \{x\}) \cap \mathrm{lt}(G) = \emptyset$ then
    $S = S \cup \{x\}$
  end if
end while
```

Corollary 4.12. *Let $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ be an ideal such that $A[x_1,\dots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. some lexicographic ordering, $\prec$ and G be its monic short reduced Gröbner basis w.r.t. $\prec$. Let $S \subseteq X$ be a set of indeterminates such that*

$$\mathrm{Mon}(A[S]) \cap \mathrm{lt}(G) = \emptyset,$$

and S has the largest number of elements among all subsets of X that satisfy the above equation. Then S is maximal independent modulo $\mathfrak{a}$ and $|S| = \mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a})$.

Proof. This result is a direct consequence of Theorem 4.10 and Theorem 4.9. □

The above result gives us an algorithmic technique to determine the combinatorial dimension of $A[x_1,\dots,x_n]/\mathfrak{a}$. It involves computing a Gröbner basis w.r.t. a lexicographic ordering. Given a Noetherian integral domain A, we give below an explicit description of the algorithm to compute the combinatorial dimension of A-algebras $A[x_1,\dots,x_n]/\mathfrak{a}$, that have a free A-module representation w.r.t. a lexicographic ordering. The correctness of the algorithm follows from Corollary 4.12. It consists of two routines, Algorithm 2 and Algorithm 3, the latter of which is recursive. Algorithm 3 also determines the maximal independent set of indeterminates modulo $\mathfrak{a}$. This algorithm is along the lines of the algorithm described in Kredel and Weispfenning (1988, Section 3).

Algorithm 2 Algorithm for finding the combinatorial dimension of $A[x_1,\ldots,x_n]/\mathfrak{a}$ for lexicographic orderings.

```
Input $G$, short reduced Gröbner basis of $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$ w.r.t. a lexicographic ordering $\prec$,
$X = \{x_1,\ldots,x_n\}$
Output $c$, combinatorial dimension of $A[x_1,\ldots,x_n]/\mathfrak{a}$
$\mathcal{S}$, the maximal set of indeterminates independent modulo $\mathfrak{a}$.
if $G$ is not monic then
  Exit
end if
$c = 0$, $S = \emptyset$, $U = X$, $\mathcal{M} = \emptyset$
{Calls the recursive algorithm}
$\mathcal{M} =$ Algorithm 3$(G, S, U, \mathcal{M})$
$\mathcal{S} = \mathcal{M}$
while $\mathcal{M} \neq \emptyset$ do
  Select any $M$ from $\mathcal{M}$
  $\mathcal{M} = \mathcal{M} \setminus \{M\}$
  if $c \leq |M|$ then
    $c = |M|$
  end if
end while
```

Algorithm 3 Recursive algorithm for finding the maximal set of indeterminates independent modulo the ideal $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$ for lexicographic orderings.

```
Input $G$, Gröbner basis of $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$ w.r.t. a lexicographic ordering $\prec$,
$S$, set of indeterminates such that $\mathrm{Mon}(S) \cap \mathrm{lt}(G) = \emptyset$,
$U$, a subset of the indeterminates set $X$,
$\mathcal{M}$, a set of already computed maximal sets $S'$ with $\mathrm{Mon}(S') \cap \mathrm{lt}(G) = \emptyset$.
Output $\mathcal{M}'$, the updated set of maximal set of indeterminates $S'$ with $\mathrm{Mon}(S') \cap \mathrm{lt}(G) = \emptyset$.
{Finding the maximal independent sets of indeterminates}
$\mathcal{M}' = \mathcal{M}$
while $U \neq \emptyset$ do
  Select $u$ from $U$
  $U = U \setminus \{u\}$
  if $\mathrm{Mon}(S \cup \{u\}) \cap \mathrm{lt}(G) = \emptyset$ then
    $\mathcal{M}' =$ Algorithm 3$(G, S \cup \{u\}, U, \mathcal{M}')$
  end if
end while
{Testing if $S$ is already contained in some element of $\mathcal{M}'$}
$\mathcal{M}'' = \mathcal{M}'$, $t = 1$
while $\mathcal{M}'' \neq \emptyset$ and $t = 1$ do
  Select $M$ from $\mathcal{M}''$, $\mathcal{M}'' = \mathcal{M}'' \setminus \{M\}$.
  if $S \subseteq M$ then
    $t = 0$
  end if
end while
if $t = 1$ then
  $\mathcal{M}' = \mathcal{M}' \cup \{S\}$
end if
```

The running time of the algorithm is exactly as that of computing the combinatorial dimension for fields except for the computation of short reduced Gröbner basis. The computation of short reduced Gröbner basis depends on the coefficient ring, A. When $A = \Bbbk$ or $\mathbb{Z}$, the time complexity is doubly exponential (computation of a single Gröbner basis) and when $A = \Bbbk[y_1,\ldots,y_m]$, the complexity is still doubly exponential but involves two Gröbner basis computations, first in $\Bbbk[y_1,\ldots,y_m]$ and then in $A[x_1,\ldots,x_n]$.

5. Relation between Krull dimension and combinatorial dimension of $A[x_1,\ldots,x_n]/\mathfrak{a}$

The results we derive in this section will also help us derive a relation between the degree of a Hilbert polynomial and Krull dimension (Section 6.3).

Lemma 5.1. *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal and M be an A-algebra. Then there exists a homomorphism from $A[x_1, \ldots, x_n]$ to $M[x_1, \ldots, x_n]$. Let $\mathfrak{a}^e$ represent the extension of the ideal $\mathfrak{a}$ in $M[x_1, \ldots, x_n]$ under the homomorphism. We have*

$$M \otimes_A A[x_1, \ldots, x_n]/\mathfrak{a} \cong M[x_1, \ldots, x_n]/\mathfrak{a}^e.$$

Proof. Clearly, $M[x_1, \ldots, x_n]/\mathfrak{a}^e$ is an A-module. Consider the following operation: for any $f + \mathfrak{a} \in A[x_1, \ldots, x_n]/\mathfrak{a}$ and $g + \mathfrak{a}^e \in M[x_1, \ldots, x_n]/\mathfrak{a}^e$, let $(f + \mathfrak{a})(g + \mathfrak{a}^e) = fg + \mathfrak{a}^e$. It is well defined because $\mathfrak{a} \subseteq \mathfrak{a}^e$. This implies $M[x_1, \ldots, x_n]/\mathfrak{a}^e$ is an $A[x_1, \ldots, x_n]/\mathfrak{a}$-module as well. We define the following homomorphism,

$$\phi : A^{(A[x_1,\ldots,x_n]/\mathfrak{a}\times M)} \to M[x_1, \ldots, x_n]/\mathfrak{a}^e$$
$$\phi(\sum_{i\in\Lambda}(a_i x^{\alpha_i} + \mathfrak{a}, m_i)) = \sum_{i\in\Lambda}(a_i m_i x^{\alpha_i} + \mathfrak{a}^e).$$

Note that ϕ is A-multilinear. Therefore, there exist the following homomorphisms,

$$\psi : A[x_1, \ldots, x_n]/\mathfrak{a} \otimes_A M \to M[x_1, \ldots, x_n]/\mathfrak{a}^e$$

and

$$\pi : A^{(A[x_1,\ldots,x_n]/\mathfrak{a}\times M)} \to A[x_1, \ldots, x_n]/\mathfrak{a} \otimes_A M$$

such that $\phi = \psi \circ \pi$. Since ϕ is surjective, ψ is surjective too. Consider

$$\psi(\sum_{i\in\Lambda}(a_i x^{\alpha_i} + \mathfrak{a} \otimes_A m_i)) = 0.$$

We have

$$\sum_{i\in\Lambda}(a_i x^{\alpha_i} + \mathfrak{a} \otimes_A m_i) = \sum_{i\in\Lambda}(x^{\alpha_i} + \mathfrak{a} \otimes_A a_i m_i).$$

Now, $\pi(\sum_{i\in\Lambda}(x^{\alpha_i} + \mathfrak{a}, a_i m_i)) = \sum_{i\in\Lambda}(x^{\alpha_i} + \mathfrak{a} \otimes_A a_i m_i)$. This implies $\phi(\sum_{i\in\Lambda}(x^{\alpha_i} + \mathfrak{a}, a_i m_i)) = 0$. Since x^{α_i}s are standard monomials, if the sum is equal to zero then each $a_i m_i = 0$. Therefore, $\sum_{i\in\Lambda}(a_i x^{\alpha_i} + \mathfrak{a} \otimes_A m_i) = 0$ and ψ is injective. We have the following isomorphism,

$$M \otimes_A A[x_1, \ldots, x_n]/\mathfrak{a} \cong M[x_1, \ldots, x_n]/\mathfrak{a}^e. \qquad \square$$

Proposition 5.2. *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that it has a monic short reduced Gröbner basis, $G = \{g_1, \ldots, g_t\}$ w.r.t. some monomial order $\prec$. Let $\mathfrak{p} \subsetneq A$ be a prime ideal and $k(\mathfrak{p})\,(= A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})$ be the residue field of $\mathfrak{p}$. Consider the ring homomorphism,*

$$\nu : A[x_1, \ldots, x_n] \longrightarrow k(\mathfrak{p})[x_1, \ldots, x_n] \tag{2}$$

such that $\nu(x_i) = x_i$ for $x_i \in \{x_1, \ldots, x_n\}$ and for $a \in A$,

$$\nu(a) = \begin{cases} 0 & \text{for } a \in \mathfrak{p} \\ a & \text{for } a \notin \mathfrak{p}. \end{cases}$$

If $\mathfrak{a}^e$ is the extension of $\mathfrak{a}$ in $k(\mathfrak{p})[x_1, \ldots, x_n]$, then $\nu(G) = \{\nu(g_1), \ldots, \nu(g_t)\}$ is a Gröbner basis for $\mathfrak{a}^e$.

Proof. If

$$\langle \mathrm{lt}(\mathfrak{a})\rangle k(\mathfrak{p})[x_1, \ldots, x_n] = \langle \mathrm{lt}(\mathfrak{a}^e)\rangle,$$

then $\nu(G) = \{\nu(g_1), \ldots, \nu(g_t)\}$ is a Gröbner basis of $\mathfrak{a}^e$ in $k(p)[x_1, \ldots, x_n]$. Since G is a monic basis it also follows that $\nu(g)$, $g \in G$ is monic and therefore $\nu(G)$ is a monic Gröbner basis for $\mathfrak{a}^e$. We first show $\langle \mathrm{lt}(\mathfrak{a})\rangle k(\mathfrak{p})[x_1, \ldots, x_n] \subseteq \langle \mathrm{lt}(\mathfrak{a}^e)\rangle$. This is true for any ring homomorphism (Bayer et al., 1991, Proposition 3.4). It is enough to show that each generator of $\langle \mathrm{lt}(\mathfrak{a})\rangle k(\mathfrak{p})[x_1,\dots,x_n]$ belongs to $\langle \mathrm{lt}(\mathfrak{a}^e)\rangle$. The generators of $\langle \mathrm{lt}(\mathfrak{a})\rangle k(\mathfrak{p})[x_1,\dots,x_n]$ are $\nu(\mathrm{lt}(f))$, $f\in\mathfrak{a}$. For each $f\in\mathfrak{a}$, either $\nu(\mathrm{lt}(f))=0$ if $\mathrm{lc}(f)\in\mathfrak{p}$ or $\nu(\mathrm{lt}(f))=\mathrm{lt}(f)=\mathrm{lt}(\nu(f))\in\langle \mathrm{lt}(\mathfrak{a}^e)\rangle$, if $\mathrm{lc}(f)\notin\mathfrak{p}$.

Let $f\in\mathfrak{a}^e$ and $\mathrm{lt}(f)=cx^{\alpha}$. We have

$$f=\sum_{i=1}^{t}\nu(g_i)b_i,\quad b_i\in k(\mathfrak{p})[x_1,\dots,x_n].$$

We claim that $\mathrm{lt}(g_j)\mid x^{\alpha}$ for some $j\in\{1,\dots,t\}$. If not, for each $\mathrm{lt}(g_j)$, $b_j=0$ since G is a monic short reduced Gröbner basis and $\nu(\mathrm{lt}(g_i))=\mathrm{lt}(g_i)=\mathrm{lm}(g_i)$. Let $g_j\in G$ be such that $\mathrm{lm}(g_j)\mid x^{\alpha}$. Therefore, $x^{\alpha}\in\langle\mathrm{lt}(\mathfrak{a})\rangle$ and $cx^{\alpha}\in\langle\mathrm{lt}(\mathfrak{a})\rangle k(\mathfrak{p})[x_1,\dots,x_n]$. We have $\nu(G)$ is a Gröbner basis for $\mathfrak{a}^e$. □

Consider the ring homomorphism,

$$f: A\longrightarrow A[x_1,\dots,x_n]/\mathfrak{a}. \tag{3}$$

We have the corresponding mapping associated with f,

$$f^*:\mathrm{Spec}(A[x_1,\dots,x_n]/\mathfrak{a})\longrightarrow \mathrm{Spec}(A). \tag{4}$$

Consider a prime ideal $\mathfrak{p}$ in A. The subspace $f^{*-1}(\mathfrak{p})$ of $\mathrm{Spec}(A[x_1,\dots,x_n]/\mathfrak{a})$ is naturally homeomorphic to $\mathrm{Spec}(k(\mathfrak{p})\otimes_A A[x_1,\dots,x_n]/\mathfrak{a})$, where $k(\mathfrak{p})$ is the residue field of $\mathfrak{p}$, $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ (Atiyah and Macdonald, 1969, Exercise 3.21). That is, we have a homeomorphism between the set of primes of $A[x_1,\dots,x_n]/\mathfrak{a}$ lying over $\mathfrak{p}$ and $\mathrm{Spec}(k(\mathfrak{p})\otimes_A A[x_1,\dots,x_n]/\mathfrak{a})$. By Lemma 5.1, we have

$$k(\mathfrak{p})\otimes_A A[x_1,\dots,x_n]/\mathfrak{a}\cong k(\mathfrak{p})[x_1,\dots,x_n]/\mathfrak{a}^e. \tag{5}$$

Theorem 5.3. *Let $\mathfrak{a}$ be a proper ideal in $A[x_1,\dots,x_n]$ such that it has a monic Gröbner basis w.r.t. some monomial ordering. Let $\mathfrak{p}$ be a prime ideal in A and let P be a prime ideal in $A[x_1,\dots,x_n]/\mathfrak{a}$ such that P is maximal among the prime ideals lying over $\mathfrak{p}$. Then,*

$$\mathrm{ht}(P)=\mathrm{ht}(\mathfrak{p})+\mathrm{kdim}(k(\mathfrak{p})[x_1,\dots,x_n]/\mathfrak{a}^e),$$

where $k(\mathfrak{p})$ is the residue field of $\mathfrak{p}$ and $\mathfrak{a}^e$ is the extension of the ideal, $\mathfrak{a}$ under the ring homomorphism given by (2).

Proof. Consider the ring homomorphism given in (3),

$$f: A\longrightarrow A[x_1,\dots,x_n]/\mathfrak{a}.$$

Since $\mathfrak{a}$ has a monic Gröbner basis w.r.t. some monomial ordering, $A[x_1,\dots,x_n]/\mathfrak{a}$ is a free A-module. This implies f is a flat homomorphism of Noetherian rings and therefore we have from Matsumura (1980, 13.B Theorem 19),

$$\mathrm{ht}(P)=\mathrm{ht}(\mathfrak{p})+\mathrm{kdim}((A[x_1,\dots,x_n]/\mathfrak{a})_P\otimes k(\mathfrak{p})).$$

To ease the notation, we denote $A[x_1,\dots,x_n]/\mathfrak{a}$ as $\mathcal{A}$. The corresponding prime of $\mathcal{A}\otimes k(\mathfrak{p})=\mathcal{A}_{\mathfrak{p}}/\mathfrak{p}\mathcal{A}_{\mathfrak{p}}$ is $P\mathcal{A}_{\mathfrak{p}}/\mathfrak{p}\mathcal{A}_{\mathfrak{p}}$. Let us denote this prime as P^*. Then by Matsumura (1980, 13.A) we have that the local ring,

$$(\mathcal{A}\otimes k(\mathfrak{p}))_{P^*}=\mathcal{A}_P\otimes k(\mathfrak{p}).$$

Therefore,

$$\mathrm{kdim}(\mathcal{A}_P\otimes k(\mathfrak{p}))=\mathrm{kdim}((A[x_1,\dots,x_n]/\mathfrak{a})_P\otimes k(\mathfrak{p}))=\mathrm{ht}(P^*).$$

Consider $A[x_1,\dots,x_n]/\mathfrak{a}\otimes k(\mathfrak{p})$. By (5), it is isomorphic to $k(\mathfrak{p})[x_1,\dots,x_n]/\mathfrak{a}^e$. All maximal ideals in the affine algebra $k(\mathfrak{p})[x_1,\dots,x_n]/\mathfrak{a}^e$ are of the same height equal to $\mathrm{kdim}(k(\mathfrak{p})[x_1,\dots,x_n]/\mathfrak{a}^e)$. Therefore,

$$\mathrm{kdim}((A[x_1,\dots,x_n]/\mathfrak{a})_P\otimes k(\mathfrak{p}))=\mathrm{kdim}(k(\mathfrak{p})[x_1,\dots,x_n]/\mathfrak{a}^e),$$

and we have

$$\mathrm{ht}(P)=\mathrm{ht}(\mathfrak{p})+\mathrm{kdim}(k(\mathfrak{p})[x_1,\dots,x_n]/\mathfrak{a}^e).\qquad\square$$

5.1. Krull dimension of A-algebras for lexicographic orderings

Proposition 5.4. *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that it has a monic short reduced Gröbner basis w.r.t. lexicographic ordering, $\prec$. Let $\mathfrak{p} \subsetneq A$ be a prime ideal and $k(\mathfrak{p})$ be the residue field of $\mathfrak{p}$ $(= A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})$. Let ν be the ring homomorphism as described in Proposition 5.2 and $\mathfrak{a}^e$ be the extension of $\mathfrak{a}$ in $k(\mathfrak{p})[x_1, \ldots, x_n]$. Then,*

$$\mathrm{cdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e) = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}).$$

Proof. Let G be the monic short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. a lexicographic ordering $\prec$. From Proposition 5.2, we have that $\nu(G)$ is a monic Gröbner basis for $\mathfrak{a}^e$ and $\mathrm{lt}(G) = \mathrm{lt}(\nu(G))$. Therefore, the set of indeterminates, $S \subseteq X$ such that $\mathrm{Mon}(A[S]) \cap \mathrm{lt}(G) = \emptyset$ is the same as the set of indeterminates, $S' \subseteq X$ that satisfy $\mathrm{Mon}(k(\mathfrak{p})[S']) \cap \mathrm{lt}(\nu(G)) = \emptyset$. Then by Corollary 4.12,

$$\mathrm{cdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e) = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$$

and hence the proof. □

Corollary 5.5. *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be a proper ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a lexicographic order $\prec$. Then,*

$$\mathrm{kdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) = \mathrm{kdim}(A) + \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}).$$

Proof. From Proposition 5.4, we have

$$\mathrm{cdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e) = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}).$$

When the coefficient ring is a field, $\mathrm{kdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e) = \mathrm{cdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e)$. This implies that the equation in Proposition 5.3 becomes

$$\mathrm{ht}(P) = \mathrm{ht}(\mathfrak{p}) + \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}).$$

Since $\mathfrak{a}$ is a proper ideal with a monic Gröbner basis, the mapping in (4), $f^* : \mathrm{Spec}(A[x_1, \ldots, x_n]/\mathfrak{a}) \longrightarrow \mathrm{Spec}(A)$, is surjective and we have

$$\mathrm{kdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) = \mathrm{kdim}(A) + \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}). \qquad \square$$

Given a Noetherian integral domain, using Corollary 5.5 we give a Gröbner basis algorithm to compute the Krull dimension of A-algebras, $A[x_1, \ldots, x_n]/\mathfrak{a}$ that have a free A-module representation w.r.t. a lexicographic ordering. This is listed in Algorithm 4. This algorithm calls Algorithm 2, which returns the maximal sets of indeterminates independent modulo $\mathfrak{a}$ and the combinatorial dimension of the corresponding A-algebra.

Algorithm 4 Algorithm for finding the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ for lexicographic orderings.

```
Input $G$, short reduced Gröbner basis of $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ w.r.t. a lexicographic ordering, $\prec$,
$d_A$, Krull dimension of the ring, $A$,
$X = \{x_1, \ldots, x_n\}$
Output $d$, Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$.
if $G$ is not monic then
    Exit
end if
$c = 0$, $S = \emptyset$, $t = 0$, $\mathcal{S} = \emptyset$
{Calls the combinatorial dimension algorithm}
$\mathcal{S}, c =$ Algorithm 2$(G, X)$
$d = c + d_A$
```

5.2. Examples

We illustrate below examples that compute the Krull dimension of residue class rings of polynomial rings over a Noetherian integral domain, A using combinatorial dimension.

Example 5.6. Consider the ideal $\mathfrak{a} = \langle xy, xz \rangle \subseteq A[x, y, z]$ and the lexicographic ordering $z \prec y \prec x$. Consider the A-algebra $\mathcal{A} = A[x, y, z]/\mathfrak{a}$. One way to determine the Krull dimension of $\mathcal{A}$ is given below. We have

$$\text{kdim}(\mathcal{A}) = \sup\{\text{kdim}(\mathcal{A}/\mathfrak{P}) : \mathfrak{P} \text{ minimal prime}\}.$$

Let $\mathfrak{P}$ be a minimal prime of $\mathcal{A}$. Then $\mathfrak{P} = \mathfrak{p}/\langle xy, xz \rangle$ with $\mathfrak{p}$ prime in $A[x, y, z]$ and minimal over $\langle xy, xz \rangle$. The associated isolated primes of $\langle xy, xz \rangle$ are $\langle x \rangle$ and $\langle y, z \rangle$. Then,

$$\begin{aligned}\text{kdim}(\mathcal{A}) &= \sup\{(\text{kdim}(A[x, y, z]/\langle y, z \rangle), \text{kdim}(A[x, y, z]/\langle x \rangle)\} \\ &= \text{kdim}(A) + 2.\end{aligned}$$

We can also compute the Krull dimension using the relation we derived in the previous section. The short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. $\prec$ is $\{xy, xz\}$ and it is monic and therefore $\mathcal{A}$ has a free A-module representation w.r.t. a lexicographic ordering. The $\text{cdim}(\mathcal{A}) = 2$ since $S = \{y, z\}$ is a maximal independent set of indeterminates modulo $\mathfrak{a}$. Therefore we have

$$\text{kdim}(\mathcal{A}) = \text{cdim}(\mathcal{A}) + \text{kdim}(A) = \text{kdim}(A) + 2.$$

Example 5.7. Consider the ideal $\mathfrak{a} = \langle xy + 1 \rangle \subseteq A[x, y]$ and the lexicographic ordering $y \prec x$. One can see that the A-algebra $\mathcal{A} = A[x, y]/\mathfrak{a}$ is isomorphic to the ring of Laurent polynomials with coefficients in A, $A[x^{\pm 1}]$. Therefore, the Krull dimension of $\mathcal{A}$ is equal to $\text{kdim}(A[x^{\pm 1}]) = \text{kdim}(A) + 1$.

We can use the relation we derived since $\mathcal{A}$ has a free A-module representation w.r.t. $\prec$. The $\text{cdim}(\mathcal{A}) = 1$ with $S = \{x\}$ a maximal independent set modulo the ideal. Therefore $\text{kdim}(\mathcal{A}) = \text{kdim}(A) + 1$.

Example 5.8. Let $\mathfrak{a} = \langle x^2y+x+1, y^3+z+1 \rangle \subseteq A[x, y, z]$ be an ideal. To determine the Krull dimension of the A-algebra $\mathcal{A} = A[x, y, z]/\mathfrak{a}$, we first compute the Gröbner basis of $\mathfrak{a}$ w.r.t. the lexicographic ordering $z \prec y \prec x$. It is given by $\{y^3 + z + 1, x^2z + x^2 - xy^2 - y^2, x^2y + x + 1\}$. It is monic and therefore we can apply the relation we derived. We construct the Left Basic Set w.r.t. $\prec$, $S = \{z\}$. Therefore, $\text{cdim}(\mathcal{A}) = |S| = 1$. Therefore, $\text{kdim}(\mathcal{A}) = \text{kdim}(A) + 1$.

Example 5.9. Let $\mathfrak{a} = \langle x^2 + 2x + 1, y^3 + 2z + 1 \rangle \subseteq A[x, y, z]$ be an ideal. The Gröbner basis of $\mathfrak{a}$ w.r.t. the lexicographic ordering $z \prec y \prec x$ is $\{x^2 + 2x + 1, y^3 + 2z + 1\}$. It is monic and therefore we can apply the relation we derived to compute the Krull dimension of the A-algebra, $\mathcal{A} = A[x, y, z]/\mathfrak{a}$. The LBS w.r.t. $\prec$, $S = \{z\}$ and therefore, $\text{cdim}(\mathcal{A}) = |S| = 1$ and $\text{kdim}(\mathcal{A}) = \text{kdim}(A) + 1$.

Example 5.10. Let $\mathfrak{a} = \langle x^2 + zx, y + 6z \rangle \subseteq \mathbb{Z}[x, y, z]$ be an ideal. The Gröbner basis of $\mathfrak{a}$ w.r.t. the lexicographic ordering $z \prec y \prec x$ is $\{x^2 + zx, y + 6z\}$. It is monic and therefore we can apply the relation we derived to compute the Krull dimension of the $\mathbb{Z}$-algebra $\mathbb{Z}[x, y, z]/\mathfrak{a}$. The LBS w.r.t. $\prec$, $S = \{z\}$ and therefore, $\text{cdim}(\mathbb{Z}[x, y, z]/\mathfrak{a}) = |S| = 1$ and $\text{kdim}(\mathbb{Z}[x, y, z]/\mathfrak{a}) = 2$.

6. Hilbert polynomials in $A[x_1, \ldots, x_n]$

6.1. Hilbert function and Hilbert series

Proposition 6.1. *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that it has a monic short reduced Gröbner basis, $G = \{g_1, \ldots, g_t\}$ w.r.t. a degree compatible monomial ordering. We denote $\mathcal{A} = A[x_1, \ldots, x_n]/\mathfrak{a}$. For d a non-negative integer, we define*

$$\mathcal{A}_{\leq d} = \{f + \mathfrak{a} : f \in A[x_1, \ldots, x_n], \deg(f) \leq d\}.$$

Then, $\mathcal{A}_{\leq d}$ is a finitely generated, free A-module.

Proof. Let a basis for $\mathcal{A}$ be given by the set, $\mathcal{B} = \{x^\alpha + \mathfrak{a} : \mathrm{lm}(g_i) \nmid x^\alpha\}$. Consider the following set, $\mathcal{B}^{(d)} = \{x^\alpha + \mathfrak{a} : x^\alpha + \mathfrak{a} \in \mathcal{B}, \deg(x^\alpha) \leq d\}$.

Claim 2. *$\mathcal{B}^{(d)}$ is an A-module basis for $\mathcal{A}_{\leq d}$.*

Clearly, $\mathcal{B}^{(d)}$ is a subset of $\mathcal{A}_{\leq d}$. Consider $f + \mathfrak{a} \in \mathcal{A}_{\leq d}$. Since $\deg(f) \leq d$ and we have a degree compatible ordering, $\mathrm{lt}(f) \leq d$. This implies that $f + \mathfrak{a}$ can be written as $\sum_{x^\alpha + \mathfrak{a} \in \mathcal{B}^{(d)}} a_i (x^\alpha + \mathfrak{a})$, $a_i \in A$. Thus, $\mathcal{B}^{(d)}$ generates $\mathcal{A}_{\leq d}$. $\mathcal{B}^{(d)}$ is linearly independent since it is a subset of the basis, $\mathcal{B}$. We have, therefore, that $\mathcal{A}_{\leq d}$ is free and finitely generated. □

We refer to the size of $\mathcal{B}^{(d)}$ as the free rank of $\mathcal{A}_{\leq d}$ and it is denoted as $\mathrm{FreeRank}_A(\mathcal{A}_{\leq d})$. Note that any two bases for a free module over a commutative ring have the same cardinality.

Consider $\mathcal{A} = A[x_1, \ldots, x_n]/\mathfrak{a}$ such that it has a free A-module representation w.r.t. a degree compatible monomial ordering. We define the Hilbert function, $h_\mathfrak{a} : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ as

$$h_\mathfrak{a}(d) = \mathrm{FreeRank}_A(\mathcal{A}_{\leq d}).$$

The formal power series

$$H_\mathfrak{a}(t) = \sum_{d=0}^{\infty} h_\mathfrak{a}(d) t^d \in \mathbb{Z}[[t]]$$

is called the Hilbert series of $\mathfrak{a}$.

Theorem 6.2. *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible ordering. Then,*

$$H_\mathfrak{a}(t) = H_{\langle \mathrm{lt}(\mathfrak{a}) \rangle}(t).$$

Proof. Let $\mathcal{A} = A[x_1, \ldots, x_n]/\mathfrak{a}$ and $G = \{g_1, \ldots, g_t\}$ be a short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. a degree compatible ordering. Consider the following map for a specific set of coset representatives $C_{J_{x^\alpha}}$, $x^\alpha \in \mathrm{Mon}(A[x_1, \ldots, x_n])$, in A.

$$\begin{aligned} \phi : \mathcal{A} &\longrightarrow A[x_1, \ldots, x_n] \\ g + \mathfrak{a} &\longmapsto \eta_G(g). \end{aligned}$$

The map is well defined (Adams and Loustaunau, 1994, Lemma 4.3.3). For every $d \in \mathbb{Z}_{\geq 0}$, we have the restriction map,

$$\phi_d : \mathcal{A}_{\leq d} \to A[x_1, \ldots, x_n].$$

Let $V_d \subseteq A[x_1, \ldots, x_n]$ be the submodule spanned by all the monomials t with degree $\leq d$ and $t \notin \langle \mathrm{lt}(\mathfrak{a}) \rangle$. Since all $f \in V_d$ are in the normal form w.r.t. G, we get $f = \eta_G(f) = \phi_d(f + \mathfrak{a})$. Therefore, $V_d \subseteq im(\phi_d)$, the image of ϕ_d. Let $f \in im(\phi_d)$. This implies $f = \eta_G(g)$ for some polynomial $g \in A[x_1, \ldots, x_n]$ and $\mathrm{Mon}(f) \notin \langle \mathrm{lt}(\mathfrak{a}) \rangle$. We have that the degree of each monomial in f is less than d since the ordering is degree compatible. Therefore, $f \in V_d$ and $h_\mathfrak{a}(d) = \mathrm{FreeRank}(V_d)$. Note that the definition of V_d depends only on the leading term ideal and therefore two ideals with the same leading term ideal will have the same Hilbert series. □

Algorithm 5 gives a Gröbner basis method to calculate the Hilbert series of an ideal in $A[x_1, \ldots, x_n]$.

Algorithm 5 Computing the Hilbert series of an ideal $\mathfrak{a}$ in $A[x_1,\ldots,x_n]$ when $A[x_1,\ldots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible monomial ordering.

```
Input A degree compatible monomial ordering $\prec$,
$G = \{g_1,\ldots,g_s\}$, a monic short reduced Gröbner basis of $\mathfrak{a}$ based on the ordering, $\prec$.
Output Hilbert series $H_{\mathfrak{a}}(t)$.
Let $m_1,\ldots,m_s$ be the leading monomials of $G$.
if $s = 0$ then
    Return $H_{\mathfrak{a}}(t) = \frac{1}{(1-t)^{n+1}}$.
else
    $J = \langle m_2,\cdots,m_s\rangle$ and
    $J' = \langle \mathrm{lcm}(m_1,m_2),\cdots,\mathrm{lcm}(m_1,m_s)\rangle$.
    Compute $H_J(t)$ and $H_{J'}(t)$ by a recursive call of the algorithm.
    Return
        $H_{\mathfrak{a}}(t) = \frac{1-t^{\deg(m_1)}}{(1-t)^{n+1}} + H_J(t) - H_{J'}(t)$.
end if
```

Proposition 6.3. *Algorithm 5 terminates after finitely many steps and calculates $H_{\mathfrak{a}}(t)$ correctly.*

Proof. With the assumption that $A[x_1,\ldots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible monomial ordering, the proof is identical to that of fields (Kemper, 2011, Theorem 11.9). □

The Hilbert–Serre theorem follows as a natural consequence of the above algorithm.

Theorem 6.4 *(Hilbert–Serre theorem). Let $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$ be an ideal such that $A[x_1,\ldots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible ordering. Then the Hilbert series of the ideal has the form*

$$H_{\mathfrak{a}}(t) = \frac{a_0 + a_1 t + \cdots + a_k t^k}{(1-t)^{n+1}},$$

with $k \in \mathbb{Z}_{\geq 0}$ and $a_i \in \mathbb{Z}$. Moreover, the Hilbert function $h_{\mathfrak{a}}(d)$ is a polynomial for large d. The polynomial

$$p_{\mathfrak{a}} = \sum_{i=0}^{k} a_i C(x+n-i, n) \in \mathbb{Q}[x]$$

called the Hilbert polynomial satisfies $h_{\mathfrak{a}}(d) = p_{\mathfrak{a}}(d)$ for sufficiently large integer d.

Whenever the A-module $A[x_1,\ldots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible monomial ordering all the properties of Hilbert functions for affine $\Bbbk$-algebras hold here as well.

6.2. Relation between Hilbert polynomials and combinatorial dimension

Let $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$ be an ideal such that $A[x_1,\ldots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible monomial ordering. We first show that the degree of the Hilbert polynomial is equal to its combinatorial dimension. A free A-module representation implies monic leading terms and this implies all the properties of Hilbert functions for leading term ideals follow exactly as that of fields. One such property is the equivalence of the combinatorial dimension of $A[x_1,\ldots,x_n]/\langle \mathrm{lt}(\mathfrak{a})\rangle$ and the degree of Hilbert polynomial of $\langle \mathrm{lt}(\mathfrak{a})\rangle$.

Theorem 6.5. *If $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$ is an ideal such that $A[x_1,\ldots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible monomial order, then the degree of the Hilbert polynomial of $\langle \mathrm{lt}(\mathfrak{a})\rangle$ is equal to the combinatorial dimension of $A[x_1,\ldots,x_n]/\langle \mathrm{lt}(\mathfrak{a})\rangle$.*

We will now show that for any arbitrary ideal $\mathfrak{a}$, $\mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a})$ is equal to the degree of the Hilbert polynomial of $\mathfrak{a}$.

Theorem 6.6. *Let $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ be a proper ideal such that $A[x_1,\dots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible ordering $\prec$. Then, $\mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a})$ equals the degree of the Hilbert polynomial of $\mathfrak{a}$.*

Proof. Let d denote the combinatorial dimension of $\mathfrak{a}$. Let the set $\{x_{i_1},\dots,x_{i_d}\}$ be a set of independent indeterminates modulo $\mathfrak{a}$ of maximal cardinality. Let s be a non-negative integer. From Theorem 6.1, we have that $\mathrm{Mon}(A[x_{i_1},\dots,x_{i_d}])_{\leq s}$ is a linearly independent set of $\mathcal{A}_{\leq s}$. Therefore, $C(d+s,s) \leq h_{\mathfrak{a}}(s)$. Since the binomial coefficient is a polynomial function in s of degree d, the $\mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a})$ is at most the degree of the Hilbert polynomial.

Let $\langle \mathrm{lt}(\mathfrak{a})\rangle$ be the leading term ideal of $\mathfrak{a}$ w.r.t. $\prec$. If $S = \{x_{i_1},\dots,x_{i_k}\} \subseteq \{x_1,\dots,x_n\}$ is not independent modulo $\mathfrak{a}$, then there exists a non-zero polynomial $f \in \mathfrak{a} \cap A[x_{i_1},\dots,x_{i_k}]$. We have $\mathrm{lm}(f) \in \langle \mathrm{lt}(\mathfrak{a})\rangle \cap A[x_{i_1},\dots,x_{i_k}]$. This implies S is not independent modulo $\langle \mathrm{lt}(\mathfrak{a})\rangle$. Therefore, the set of independent indeterminates modulo $\langle \mathrm{lt}(\mathfrak{a})\rangle$ is a subset of the set of independent indeterminates modulo $\mathfrak{a}$. Therefore, $\mathrm{cdim}(A[x_1,\dots,x_n]/\langle \mathrm{lt}(\mathfrak{a})\rangle) \leq \mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a})$. By Theorem 6.2 and Theorem 6.5, we have that the degree of the Hilbert polynomial is at most $\mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a})$. □

This corollary directly follows.

Corollary 6.7. *Given a proper ideal $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ such that $A[x_1,\dots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible ordering. If S is a set of maximal cardinality of indeterminates that are independent modulo $\langle \mathrm{lt}(\mathfrak{a})\rangle$, then S is a set of maximal cardinality of indeterminates that are independent modulo $\mathfrak{a}$. Also,*

$$\mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a}) = \mathrm{cdim}(A[x_1,\dots,x_n]/\langle \mathrm{lt}(\mathfrak{a})\rangle).$$

6.3. Krull dimension of A-algebras for degree compatible orderings

Proposition 6.8. *Let $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ be an ideal such that it has a monic short reduced Gröbner basis w.r.t. a degree compatible ordering $\prec$. Let $\mathfrak{p} \subsetneq A$ be a prime ideal and $k(\mathfrak{p})$ be the residue field of $\mathfrak{p}$ $(= A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})$. Let ν be the ring homomorphism as described in Proposition 5.2 and $\mathfrak{a}^e$ be the extension of $\mathfrak{a}$ in $k(\mathfrak{p})[x_1,\dots,x_n]$. Then,*

$$H_{\mathfrak{a}^e}(t) = H_{\mathfrak{a}}(t).$$

Proof. Let G be the monic short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. a lexicographic ordering $\prec$. From Proposition 5.2, we have that $\nu(G)$ is a monic Gröbner basis for $\mathfrak{a}^e$ and $\mathrm{lt}(G) = \mathrm{lt}(\nu(G))$. Therefore, we have $H_{\mathfrak{a}^e}(t) = H_{\langle \mathrm{lt}(\mathfrak{a})\rangle}(t)$. From Theorem 6.2 we have $H_{\mathfrak{a}^e}(t) = H_{\langle \mathrm{lt}(\mathfrak{a})\rangle}(t) = H_{\mathfrak{a}}(t)$. □

In the case of A-algebras with a free A-module representation w.r.t. a lexicographic ordering, we have seen that $\mathrm{cdim}(k(\mathfrak{p})[x_1,\dots,x_n]/\mathfrak{a}^e) = \mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a})$ (Proposition 5.4). This is true in the case of A-algebras with a free A-module representation w.r.t. a degree compatible monomial ordering as well.

Proposition 6.9. *Let $\mathfrak{a} \subseteq A[x_1,\dots,x_n]$ be an ideal such that it has a monic short reduced Gröbner basis w.r.t. a degree compatible ordering, $\prec$. Let $\mathfrak{p} \subsetneq A$ be a prime ideal and $k(\mathfrak{p})$ be the residue field of $\mathfrak{p}$ $(= A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})$. Let ν be the ring homomorphism as described in Proposition 5.2 and $\mathfrak{a}^e$ be the extension of $\mathfrak{a}$ in $k(\mathfrak{p})[x_1,\dots,x_n]$. Then,*

$$\mathrm{cdim}(k(\mathfrak{p})[x_1,\dots,x_n]/\mathfrak{a}^e) = \mathrm{cdim}(A[x_1,\dots,x_n]/\mathfrak{a}).$$

Proof. Let G be the monic short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. $\prec$. As shown previously, $\nu(G)$ is a monic Gröbner basis for $\mathfrak{a}^e$ and $\mathrm{lt}(G) = \mathrm{lt}(\nu(G))$. From Proposition 6.8 we have $\deg(p_{\mathfrak{a}^e}) = \deg(p_{\mathfrak{a}})$. From Theorem 6.6, $\mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) = \deg(p_{\mathfrak{a}})$. Since over fields, $\mathrm{cdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e) = \deg(p_{\mathfrak{a}^e})$, we have

$$\mathrm{cdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e) = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}). \qquad \square$$

Corollary 6.10. *Let $A[x_1, \ldots, x_n]/\mathfrak{a}$ be a finitely generated A-algebra such that it has a free A-module representation w.r.t. a degree compatible ordering $\prec$. Then,*

$$\begin{aligned}\mathrm{kdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) &= \mathrm{kdim}(A) + \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})\\ &= \mathrm{kdim}(A) + \deg(p_{\mathfrak{a}}).\end{aligned}$$

Proof. The proof goes along the same lines as Proposition 5.4. From Proposition 6.9, we have

$$\mathrm{cdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e) = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}).$$

When the coefficient ring is a field, $\mathrm{kdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e) = \mathrm{cdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e)$. This implies that the equation in Proposition 5.3 becomes

$$\mathrm{ht}(P) = \mathrm{ht}(\mathfrak{p}) + \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}).$$

Since $\mathfrak{a}$ is a proper ideal with a monic Gröbner basis, the mapping in (4), $f^* : \mathrm{Spec}(A[x_1, \ldots, x_n]/\mathfrak{a}) \longrightarrow \mathrm{Spec}(A)$, is surjective and we have

$$\mathrm{kdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) = \mathrm{kdim}(A) + \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}).$$

Since by Theorem 6.6, $\deg(p_{\mathfrak{a}}) = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$, we have the result. $\square$

We give below an algorithm (Algorithm 6) to compute the Krull dimension of certain A-algebras, $A[x_1, \ldots, x_n]/\mathfrak{a}$, that have a free A-module representation w.r.t. a degree compatible ordering. The correctness of the algorithm follows from Corollary 6.10.

Algorithm 6 Algorithm for finding the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ for degree compatible orderings.

```
Input $G$, short reduced Gröbner basis of $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ w.r.t. a degree compatible monomial ordering, $\prec$,
$d_A$, Krull dimension of $A$,
Output $d$, Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$.
if $G$ is not monic then
  Exit
end if
{Calls the Hilbert Serre algorithm}
$H_{\mathfrak{a}}(t) =$ Algorithm 5$(G, \prec)$
{$H_{\mathfrak{a}}(t)$ is the form $\frac{a_0+a_1t+\cdots+a_kt^k}{(1-t)^{n+1}}$}
$p_{\mathfrak{a}}(x) = \sum_{i=0}^{k} a_i C(x+n-i, n)$
$k = \deg(p_{\mathfrak{a}})$
$d = k + d_A$
```

6.4. Examples

We give below examples that compute the Krull dimension of residue class rings of polynomial rings over a Noetherian integral domain A using Hilbert polynomials.

Example 6.11. Consider the ideal $\mathfrak{a} = \langle xy, xz \rangle \subseteq A[x, y, z]$ and the deglex ordering with $z \prec y \prec x$. Consider the A-algebra $\mathcal{A} = A[x, y, z]/\mathfrak{a}$. The short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. $\prec$ is $\{xy, xz\}$ and it is monic. Therefore $\mathcal{A}$ has a free A-module representation w.r.t. a degree compatible monomial ordering. By using the recursive algorithm Algorithm 5, we have

$$\begin{aligned} H_{\mathfrak{a}}(t) &= \frac{-t^2+t+1}{(1-t)^3} \\ &= 1+4t+8t^2+13t^3+\cdots \\ p_{\mathfrak{a}}(x) &= x^2+5x+2. \\ \deg(p_{\mathfrak{a}}) &= 2. \end{aligned}$$

Using Corollary 6.10, we have

$$\operatorname{kdim}(\mathcal{A}) = \deg(p_{\mathfrak{a}}) + \operatorname{kdim}(A) = \operatorname{kdim}(A) + 2.$$

Example 6.12. Consider the ideal $\mathfrak{a} = \langle xy+1\rangle \subseteq A[x,y]$ and deglex ordering with $y \prec x$. We determine below the Krull dimension of the A-algebra $\mathcal{A} = A[x,y]/\mathfrak{a}$. We have

$$\begin{aligned} H_{\mathfrak{a}}(t) &= \frac{1-t^2}{(1-t)^3} \\ &= 1+3t+5t^2+7t^3+9t^4+\cdots \\ p_{\mathfrak{a}}(x) &= 2x+1. \\ \deg(p_{\mathfrak{a}}) &= 1. \end{aligned}$$

Therefore, $\operatorname{kdim}(\mathcal{A}) = \operatorname{kdim}(A)+1$.

Example 6.13. Let $\mathfrak{a} = \langle x^2+zx, y+6z\rangle \subseteq \mathbb{Z}[x,y,z]$ be an ideal. The Gröbner basis of $\mathfrak{a}$ w.r.t. the deglex ordering $z \prec y \prec x$ is $\{x^2+zx, y+6z\}$. We have

$$\begin{aligned} H_{\mathfrak{a}}(t) &= \frac{t^3-t^2-t+1}{(1-t)^4} \\ &= 1+3t+5t^2+7t^3+\cdots \\ p_{\mathfrak{a}}(x) &= 2x+1. \\ \deg(p_{\mathfrak{a}}) &= 1. \end{aligned}$$

Therefore, $\operatorname{kdim}(\mathbb{Z}[x,y,z]/\mathfrak{a}) = \operatorname{kdim}(\mathbb{Z})+1 = 2$.

7. Concluding remarks

As we can see from the examples given in this paper, to determine the Krull dimension of $A[x_1,\ldots,x_n]/\mathfrak{a}$, previously, one had to exploit the individual properties of each ideal. In this paper, we derived a relation between combinatorial dimension and Krull dimension that gives us an algorithmic method to compute the Krull dimension of the A-algebra provided it has a free A-module representation w.r.t. either a lexicographic or degree compatible monomial order. A natural question to ask is can we have the similar relation for other monomial orders. For polynomial rings over fields, the relation for all monomial orders is proved using Carrà Ferro (1987, Theorem 3.1). An affirmative answer seems likely for $A[x_1,\ldots,x_n]$ as well but we have yet to have a formal proof.

In Kredel and Weispfenning (1988), the authors conjecture that for a prime ideal $\mathfrak{a} \subseteq \Bbbk[x_1,\ldots,x_n]$ any maximal set of indeterminates strongly independent mod $\mathfrak{a}$ is also maximal independent mod $\mathfrak{a}$ and hence determines the dimension of $\Bbbk[x_1,\ldots,x_n]/\mathfrak{a}$. The conjecture was shown to be true in Kalkbrener and Sturmfels (1995). We conjecture the same for prime ideals in $A[x_1,\ldots,x_n]$. In this paper, for a Noetherian integral domain A we have shown that the maximal strongly independent set of indeterminates constructed from the left basic set w.r.t. a lexicographic ordering is also maximal independent mod $\mathfrak{a}$ and equal to the combinatorial dimension of $A[x_1,\ldots,x_n]/\mathfrak{a}$, when $A[x_1,\ldots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. the ordering. We conjecture that for a prime ideal $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$, any maximal set of indeterminates strongly independent mod $\mathfrak{a}$ is also maximal independent mod $\mathfrak{a}$. If this is true, then the cardinality of such a set determines the combinatorial and Krull dimension of $A[x_1,\ldots,x_n]/\mathfrak{a}$.

Acknowledgements

The authors thank the anonymous reviewers for suggestions and comments that have led to a significant improvement of the manuscript.

References

Adams, W., Loustaunau, P., 1994. An Introduction to Gröbner Bases. American Mathematical Society.

Atiyah, M., Macdonald, I.G., 1969. Introduction to Commutative Algebra. Addison–Wesley Series in Mathematics.

Bayer, D., Galligo, A., Stillman, M., 1991. Gröbner bases and extension of scalars. In: Proceedings Comput. Algebraic Geom. and Commut. Algebra. Cortona, Italy.

Carrà Ferro, G., 1987. Some properties of the lattice points and their application to differential algebra. Commun. Algebra 15 (12), 2625–2632.

Francis, M., Dukkipati, A., 2014. On reduced Gröbner basis and Macaulay–Buchberger basis theorem over Noetherian rings. J. Symb. Comput. 65, 1–14.

Kalkbrener, M., Sturmfels, B., 1995. Initial complexes of prime ideals. Adv. Math. 116 (2), 365–376.

Kemper, G., 2011. A Course in Commutative Algebra. Springer-Verlag.

Kredel, H., Weispfenning, V., 1988. Computing dimension and independent sets for polynomial ideals. J. Symb. Comput. 6 (2–3), 231–247.

Kreuzer, M., Robbiano, L., 2005. Computational Commutative Algebra 2. Springer.

Matsumura, H., 1980. Commutative Algebra, 2nd edition. Benjamin-Cummings Pub. Co.

Mora, F., Möller, H.M., 1983. The computation of the Hilbert function. In: van Hulzen, J.A. (Ed.), Computer Algebra. EUROCAL '83. In: Lecture Notes in Computer Science, vol. 162. Springer.

Pauer, F., 2007. Gröbner bases with coefficients in rings. J. Symb. Comput. 42 (11–12).