Gröbner Basis Algorithms for Polynomial Ideal Theory over Noetherian Commutative Rings

A THESIS

SUBMITTED FOR THE DEGREE OF

Doctor of Philosophy

IN THE

Faculty of Engineering

BY

Maria Francis

Computer Science and Automation
Indian Institute of Science
Bangalore – 560 012 (INDIA)

May, 2017

DEDICATED TO

my family

Acknowledgements

I always wanted to teach mathematics, but I never envisaged myself as a researcher, capable of finding new problems in the area and solving them. It was my research supervisor, Dr Ambedkar Dukkipati's unwavering faith in me throughout the entire course of my doctoral study that led me to believe in my capability to do research in computational algebra. I would like to thank him for not only introducing me to this beautiful and elegant subject but also never failing to give me the encouragement and support needed for my work.

I would like to express my sincere thanks to Indian Institute of Science (IISc) and particularly the Computer Science and Automation (CSA) department at IISc for giving me the opportunity to pursue research in a world class environment. The emphasis that the institute gives on building theoretical concepts is, I believe, the foundation of any good research. The faculty at IISc has been very approachable and I would like to take this opportunity to thank Prof. Dr. Basudeb Datta and Dr Sanjit Chatterjee for all the help and advice they have rendered to me. I am also extremely grateful to the staff at the CSA department for all the administrative support.

The Algorithmic Algebra lab (the lab I was part of) has seen many students come and go and all of them in some way or the other have influenced my life. I would like to particularly thank Gaurav, for being a good friend, hearing me out whenever I was stuck in my work and going out of the way to help me in my times of need. I am grateful for the company of Abhishek, Nithish and Annervaz for they made the environment in the lab relaxed and informal. Ashwin and Debarghya, thank you for being the go-to people in the lab for anything technical. I would also like to thank Sushma for all the help she gave me especially with the proofreading of this thesis.

I made two very close friends at IISc - Shalini and Manogna - and I am extremely grateful to them for their support and friendship. I have to thank Shalini in particular for her patient listening of all my problems and calming me down by always helping me focus on the big picture. I will miss all the wonderful conversations we had about books and food and the restaurants we kept trying out, all welcome and much needed distractions from my studies here.

Acknowledgements

My father taught me two things – do the best that you can right now rather than thinking of what you could have done better in the past and read and learn as much as you can for that is the only way to lead a fruitful life. I have relied on these two lessons several times during my doctoral study. My mother has been my rock all my life, always encouraging me to face every situation in life with equanimity and giving me the confidence to follow my instincts. I feel truly blessed for having my parents' constant encouragement and support in this academic pursuit.

My deepest appreciation goes to my husband, Anoop, who was with me at every step of this journey. He was so involved that I am sure even with no background in algebra he understands every word of my thesis. He believed in me and always helped me keep things in perspective. This helped me immensely to stay positive about my work. He has made innumerable sacrifices during these years for my studies and I thank him for his understanding and kindness.

Abstract

One of the fundamental problems in commutative algebra and algebraic geometry is to understand the nature of the solution space of a system of multivariate polynomial equations over a field $\Bbbk$, such as real or complex numbers. An important algorithmic tool in this study is the notion of Gröbner bases (Buchberger, 1965). Given a system of polynomial equations, $f_1 = 0, \ldots, f_m = 0$, Gröbner basis is a "canonical" generating set of the ideal generated by $f_1, \ldots, f_m$, that can answer, constructively, many questions in computational ideal theory. It generalizes several concepts of univariate polynomials like resultants to the multivariate case, and answers decisively the ideal membership problem. The dimension of the solution set of an ideal $\mathfrak{a}$ called the affine variety, an important concept in algebraic geometry, is equal to the Krull dimension of the corresponding coordinate ring, $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. Gröbner bases were first introduced to compute $\Bbbk$-vector space bases of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ and use that to characterize zero-dimensional solution sets. Since then, Gröbner basis techniques have provided a generic algorithmic framework for computations in control theory, cryptography, formal verification, robotics, etc, that involve multivariate polynomials over fields.

The main aim of this thesis is to study problems related to computational ideal theory over Noetherian commutative rings (e.g: the ring of integers, $\mathbb{Z}$, the polynomial ring over a field, $\Bbbk[y_1, \ldots, y_m]$, etc) using the theory of Gröbner bases. These problems surface in many domains including lattice based cryptography, control systems, system-on-chip design, etc. Although, formal and standard techniques are available for polynomial rings over fields, the presence of zero divisors and non units make developing similar techniques for polynomial rings over rings challenging.

Given a polynomial ring over a Noetherian commutative ring, A and an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$, the first fundamental problem that we study is whether the residue class polynomial ring, $A[x_1, \ldots, x_n]/\mathfrak{a}$ is a free A-module or not. Note that when $A = \Bbbk$, the answer is always 'yes' and the $\Bbbk$-vector space basis of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ plays an important role in computational ideal theory over fields. In our work, we give a Gröbner basis characterization for $A[x_1, \ldots, x_n]/\mathfrak{a}$ to have a free A-module representation w.r.t. a monomial ordering. For such A-algebras, we

give an algorithm to compute its A-module basis. This extends the Macaulay-Buchberger basis theorem to polynomial rings over Noetherian commutative rings. These results help us develop a theory of border bases in $A[x_1, \ldots, x_n]$ when the residue class polynomial ring is finitely generated. The theory of border bases is handled as two separate cases: (i) $A[x_1, \ldots, x_n]/\mathfrak{a}$ is free and (ii) $A[x_1, \ldots, x_n]/\mathfrak{a}$ has torsion submodules.

For the special case of $A = \mathbb{Z}$, we show how short reduced Gröbner bases and the characterization for a free A-module representation help identify the cases when $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is isomorphic to $\mathbb{Z}^N$ for some $N \in \mathbb{N}$. Ideals in such $\mathbb{Z}$-algebras are called ideal lattices. These structures are interesting since this means we can use the algebraic structure, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ as a representation for point lattices and extend all the computationally hard problems in point lattice theory to $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. Univariate ideal lattices are widely used in lattice based cryptography for they are a more compact representation for lattices than matrices. In this thesis, we give a characterization for multivariate ideal lattices and construct collision resistant hash functions based on them using Gröbner basis techniques. For the construction of hash functions, we define a worst case problem, shortest substitution problem w.r.t. an ideal in $\mathbb{Z}[x_1, \ldots, x_n]$, and establish hardness results for this problem.

Finally, we develop an approach to compute the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ using Gröbner bases, when A is a Noetherian integral domain. When A is a field, the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ has several equivalent algorithmic definitions by which it can be computed. But this is not true in the case of arbitrary Noetherian rings. We introduce the notion of combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ and give a Gröbner basis method to compute it for residue class polynomial 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 $A[x_1, \ldots, x_n]/\mathfrak{a}$. 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.

Publications/Preprints Based on this Thesis

1. Francis, M. and A. Dukkipati (2014). On Reduced Gröbner Basis and Macaulay-Buchberger Basis Theorem Over Noetherian Rings. *Journal Of Symbolic Computation*, 65:1-14, arXiv:1304.6889v5.

2. Francis, M. and A. Dukkipati (2017). On Ideal Lattices, Gröbner Bases and Generalized Hash Functions. *Conditionally accepted in Journal of Algebra and its Applications* arXiv:1410.2011.

3. A. Dukkipati, N. Pai and M. Francis (2017). Border Bases for Polynomial Rings over Noetherian Rings. arXiv:1405.0472.

4. Francis, M. and A. Dukkipati (2017). On Computing Krull Dimension of Residue Class Polynomial Rings over Integral Domains using Gröbner Bases. *Journal Of Symbolic Computation*, In Press, Accepted Manuscript, Available Online March 24, 2017, arXiv:1602.04300.

Contents

Chapter 1

Introduction

Learning abstract algebra is like reading sheet music without actually playing the musical instrument as the beauty of the subject is often buried under the formal theory. The study of algorithms in algebra, known as algorithmic algebra or computational algebra, stemmed from the lack of constructive techniques in algebra and the advent of fast yet inexpensive computers. By providing computational tools, algorithmic algebra attempts to give a concrete picture of the abstract concepts in algebra. Here, we will first trace these algorithmic techniques to their origins in multivariate polynomial rings over fields, $\Bbbk[x_1, \ldots, x_n]$, and then to polynomial rings over Noetherian commutative rings, $A[x_1, \ldots, x_n]$.

There has been extensive research on algorithmic techniques for various computational problems in $\Bbbk[x_1, \ldots, x_n]$. These methods span from computational ideal theory to computational algebraic geometry. Certainly, most of it can be attributed to Buchberger's theory of Gröbner bases (Buchberger, 1965). Can one generalize these techniques to multivariate polynomial rings over Noetherian commutative rings? This is an interesting question as these structures include polynomial rings over integers, $\mathbb{Z}[x_1, \ldots, x_n]$, polynomial rings over polynomial rings such as $\Bbbk[y][x_1, \ldots, x_n]$, $\Bbbk[y_1, \ldots, y_m][x_1, \ldots, x_n], \mathbb{Z}[y_1, \ldots, y_m][x_1, \ldots, x_n]$, etc. They have important applications in cryptography, control theory, coding theory, algebraic geometry, etc. For example, in lattice based cryptography, the coefficients of the polynomials are from $\mathbb{Z}$ and in control theory, parametric equations have coefficients from a polynomial ring, $\Bbbk[y_1, \ldots, y_m]$. Formulating techniques similar to those in $\Bbbk[x_1, \ldots, x_n]$ for polynomial rings with coefficients from rings is quite challenging. This thesis looks at developing computational techniques using Gröbner bases for polynomial ideal theory in $A[x_1, \ldots, x_n]$.

Consider a system of polynomial equations in n variables. One is interested in the solution

space of a system of $m \geq 1$ polynomial equations in $n \geq 1$ variables over a field, $\Bbbk$:

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0, \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0, \end{aligned} \tag{1.1}$$

where $f_i \in \Bbbk[x_1, \ldots, x_n]$, $i = 1, \ldots, m$. An n-tuple, $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\Bbbk}$ is called a solution for the above system of polynomial equations if $f_i(\alpha_1, \ldots, \alpha_n) = 0$, for all $i = 1, \ldots, m$. Over a field, $\Bbbk$, the set of all solutions of (1.1) is called an affine variety and is represented as $\mathcal{V}(f_1, \ldots, f_m)$. For ease of explanation, we assume that $\Bbbk$ is algebraically closed in this section. What a computer algebraist means by the nature of the solution space can be encapsulated by the following question.

Question 1.1 *Is the system of polynomial equations consistent, i.e. is $\mathcal{V}(f_1, \ldots, f_m)$ nonempty? If yes, then what is the cardinality of $\mathcal{V}(f_1, \ldots, f_m)$ if it is finite?*

When a system of polynomial equations has a finite number of solutions in an algebraically closed field, we say that it is zero-dimensional since the associated affine variety is of dimension zero. A polynomial system of equations with infinitely many solutions is said to be positive-dimensional. A natural question to ask at this point is, do we have a result analogous to the Fundamental Theorem of Algebra in the multivariate case? Bézout's theorem is the closest we have for an answer. Given two polynomial equations in two variables of degrees d_1 and d_2, the theorem states that it can have at most $d_1 d_2$ solutions. Note that the statement of the result is not completely qualified, we need to consider points at infinity, an algebraically closed field and assume that the polynomials do not have a common component. The result can be extended to higher dimensions as well. It is clear that the number of solutions is exponential in the number of variables which makes solving polynomial equations a hard problem.

In (1.1), if the degree of each of the monomials is 1 we have the well-studied linear system of equations, for which several solution techniques such as Gaussian elimination exist. For a multivariate polynomial system of equations with higher degrees, one of the most widely used tool to study its solution space is Gröbner bases (Buchberger, 1965). The theory of Gröbner bases is a generalization of the ideas of Gaussian elimination and the Euclidean division algorithm. A system of multivariate polynomials can be transformed to a Gröbner basis, a set of polynomials with "special" properties and the same solution space as the initial set of polynomials, since they generate the same ideal.

The ideal generated by the polynomials, $f_1, \ldots, f_m$, is given by

$$\mathfrak{a} = \langle f_1, \ldots f_m \rangle = \Big\{ \sum_{i=1}^{m} h_i f_i : h_i \in \Bbbk[x_1, \ldots, x_n] \Big\}.$$

Note that the system of polynomial equations given by $\{f_1, \ldots, f_m\}$ and the ideal it generates have the same solution space, i.e.

$$\mathcal{V}(\{f_1, \ldots, f_m\}) = \mathcal{V}(\langle f_1, \ldots, f_m \rangle) = \mathcal{V}(\mathfrak{a}).$$

Thus ideals can replace the set of polynomials and is the fundamental object in our study of polynomial equations. The Hilbert basis theorem ensures that all ideals are finitely generated in a polynomial ring over a Noetherian ring, A.

Question 1.2 *How does transforming the set of polynomials to its corresponding Gröbner basis help us in solving the system of polynomial equations?*

Gröbner bases generate a triangular system for the corresponding polynomial system of equations that captures geometric notions like dimension of a variety, the number of solutions for a zero-dimensional variety, etc. It also allows for the Euclidean division algorithm to be directly extended to the multivariate case. In the multivariate case, the Euclidean polynomial division algorithm gives different remainders for a different sequence of generating divisors. But if we use the equivalent Gröbner basis of the generating polynomials, the remainder is unique irrespective of the order of divisors. Thus, the method of Gröbner bases decisively solves the ideal membership problem: given an ideal $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$, is $f \in \mathfrak{a}$. The ideal membership problem is crucial in understanding the solution space of $\mathfrak{a}$ (and equivalently that of the set of generating polynomials of $\mathfrak{a}$) because its geometric analogue is determining if the variety of f, $\mathcal{V}(f)$ is in $\mathcal{V}(\mathfrak{a})$. It gives an idea of the solution set and therefore can be loosely interpreted as the enumeration of the complete set of roots.

To determine the consistency of a system of polynomial equations, we make use of Hilbert's Nullstellensatz to deduce that the system has no solution if and only if the reduced Gröbner basis of the ideal it generates is $\{1\}$. Note that the reduced Gröbner basis is a Gröbner basis with certain restrictions imposed on it to ensure uniqueness of the basis. To determine if a system has finite number of solutions, we need the notion of standard monomials. Standard monomials are monomials that are not elements of the leading term ideal. They form a $\Bbbk$-vector space basis of the residue class polynomial ring, $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ (Macaulay, 1927). Since the leading term ideal is an infinite set the definition of standard monomials does not provide us

with a method to determine them. On the other hand, the triangular system of polynomial equations given by a Gröbner basis gives us an algorithmic method, the Macaulay-Buchberger basis theorem (Buchberger, 1965), to compute the standard monomials. The result states that given a Gröbner basis G, the standard monomials are the set of monomials, x^α such that $\mathrm{lt}(g_i) \nmid x^\alpha$ for each $g_i \in G, i = 1, \ldots, t$, i.e. the leading terms of the Gröbner basis do not divide them. The number of elements of the set of standard monomials is the cardinality of the affine variety. Therefore, the system of equations has a finite number of solutions if and only if for each $i = 1, \ldots, n$, there exists $j = 1, \ldots, t$ such that the leading term of g_j is equal to ${x_i}^\nu$ for some $\nu \in \mathbb{N}$ and $g_j \in G$.

The dimension of an affine variety is defined as the maximal chain of distinct nonzero irreducible subvarieties. For an algebraically closed field, it is equal to the Krull dimension of the affine $\Bbbk$-algebra, $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. Given a positive dimensional system of polynomial equations, there exist Gröbner basis techniques to compute the dimension. One of these techniques is based on the concept of combinatorial dimension (Kredel and Weispfenning, 1988; Kreuzer and Robbiano, 2005), which can be computed using Gröbner basis techniques. The combinatorial dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ is equal to the dimension of the solution space, $\mathcal{V}(\mathfrak{a})$. Another Gröbner basis technique uses the result that the degree of the Hilbert polynomial of $\mathfrak{a}$ is equal to the Krull dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ (Mora and Möller, 1983).

Gröbner bases also solve several classical problems in computational algebra and algebraic geometry such as the computation of intersection of ideals, saturation of ideal, elimination ideals, etc. Thus, Gröbner bases are the backbone for all computations relating to polynomial equations over fields. The "special properties" of Gröbner bases ensure that many techniques from the univariate case can be extended to the multivariate case as long as we compute a Gröbner basis for the ideal. The algorithmic framework that Gröbner bases have built in algebra has fueled research in areas as diverse as robotics (Kalker-Kalkman, 1993), formal verification (Tran and Vardi, 2007), biology (Laubenbacher, 2003) and cryptography (Faugère and Joux, 2003).

After the introduction of Gröbner bases, several approaches were studied to generalize Gröbner basis theory to polynomial rings over Noetherian commutative rings, monoid rings, submodules of $\Bbbk[x_1, \ldots, x_n]^m$ $m \in \mathbb{N}$, etc. Some of the first approaches to extend the theory to polynomial rings over Noetherian commutative rings were given by (Spear, 1977), (Trinks, 1978), (G.Zacharias, 1978), etc. These methods were studied in more detail for the special case of principal ideal rings in (Möller, 1988). Polynomial rings over principal ideal rings and principal ideal domains were further studied in (Norton, 2001) and (Pan, 1989), respectively. Several approaches have been proposed for other specialized cases such as when A is a Euclidean ring

(Kandri-Rody and Kapur, 1988), a finite commutative ring (Byrne and Mora, 2009), a non-commutative ring (Pritchard, 1996) and a free monoid and group ring (Madlener and Reinert, 1993; Ackermann and Kreuzer, 2006). Gröbner basis theory for polynomial rings over commutative regular rings was first studied in (Weispfenning, 1989). Commutative regular rings are in general not Noetherian rings. Note that any direct product of fields is a commutative regular ring. They generalize Boolean rings and therefore techniques in the paper are a composition of techniques over fields and Boolean algebras. Gröbner basis techniques have been extended to submodules of $A[x_1, \ldots, x_n]^m$ $m \in \mathbb{N}$, where A is a Noetherian commutative ring, in (Rutman, 1992) and (Lezama, 2008). Kalkbrener (1998) describes algorithms to compute the heights, radicals and primary decomposition of ideals in $A[x_1, \ldots, x_n]$ by lifting the algorithmic methods from A to $A[x_1, \ldots, x_n]$.

Variations of Gröbner bases like 'dynamical Gröbner bases' have base rings that are not fields such as principal ideal rings (Yengui, 2006) and Dedekind rings with zero divisors (Hiss et al., 2010). They have important applications in error-correcting codes. Another variation called SAGBI bases (Robbiano and Sweedler, 1990; Kapur and Madlener, 1989) were extended to quotient rings over a commutative Noetherian domain in (Stillman and Tsai, 1999). SAGBI bases have also been studied for Cox-Nagata rings in (Sturmfels and Xu, 2010).

Recently, there has been renewed interest in polynomial rings over rings. For instance, certain residue class rings over $\mathbb{Z}[x]$ called ideal lattices (Micciancio, 2002; Lyubashevsky and Micciancio, 2006) have shown to be isomorphic to integer lattices, an important cryptographic primitive (Ajtai, 1996) and certain cyclic lattices in $\mathbb{Z}[x]$ have been used in NTRU cryptographic schemes (Hoffstein et al., 1998). Boolean polynomial rings over a boolean ring have been used to solve Sudoku and other combinatorial puzzles (Sato et al., 2011). Further, polynomial rings over $\mathbb{Z}/2^k$ have been used to prove the correctness of data paths in system-on-chip design (Greuel et al., 2011). The results given in (Byrne and Mora, 2009) for when the coefficient ring is a finite commutative ring are used to solve a key equation that appears in decoding algorithms for alternant codes over commutative finite chain rings.

For a good exposition on Gröbner bases over Noetherian commutative rings one can refer to (Adams and Loustaunau, 1994, Chapter 4). However, the theory is limited to basic definitions and concepts like reduction, division algorithm, etc and the validity of many key results have not been explored (Greuel et al., 2011). For example, the following question regarding the A-module structure of a residue class polynomial ring over a Noetherian ring is open.

Question 1.3 *For a residue class polynomial ring over a Noetherian commutative ring A, $A[x_1, \ldots, x_n]/\mathfrak{a}$, can we use Gröbner bases to compute an A-module basis if it is free?*

What is this thesis about?

The aim of this thesis is to develop an algorithmic framework for computational ideal theory over Noetherian commutative rings using Gröbner bases. Specifically, we address the following problems in this thesis.

1. How can we characterize ideals in $A[x_1, \ldots, x_n]$ that give rise to residue class polynomial rings that are free A-modules?
2. For a residue class polynomial ring, $A[x_1, \ldots, x_n]/\mathfrak{a}$, that is a free A-module, can we determine an A-module basis, i.e. can we extend the Macaulay-Buchberger basis theorem to rings?
3. Can we extend the concept of border bases to $A[x_1, \ldots, x_n]$?
4. For the special case of $A = \mathbb{Z}$, can univariate ideal lattices in $\mathbb{Z}[x]/\mathfrak{a}$ be extended to the multivariate case, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$?
5. Can we propose algorithmic techniques to compute the Krull dimension of the A-algebra, $A[x_1, \ldots, x_n]/\mathfrak{a}$?

1.1 What is a Gröbner Basis?

Gröbner basis principles form the underlying theory of this thesis and in the previous section we had explained broadly how Gröbner basis techniques can be applied to understand the solution space of a system of polynomial equations. We give the definition of Gröbner bases here for the case of polynomial rings over fields, $\Bbbk[x_1, \ldots, x_n]$. We will define these concepts for polynomial rings over Noetherian commutative rings, $A[x_1, \ldots, x_n]$, in Chapter 2. The reader can refer to (O'Shea et al., 2007), (Adams and Loustaunau, 1994) and (Becker et al., 1993), classic textbooks on Gröbner bases for more details and applications. For a quick overview of Gröbner bases, one can also refer to (Sturmfels, 2005). A Gröbner basis for an ideal is always w.r.t. a 'monomial order', a total ordering on the monomials in the polynomial that satisfies certain properties ensuring a unique leading term (lt) for the polynomial. We define it more formally below. The total ordering is necessary because in multivariate polynomials, unlike in the univariate case, total degree cannot give a unique leading term. Consider the polynomial $f = x^2y + xy^2 \in \Bbbk[x, y]$. Both the terms in f are of degree 3 and therefore we need to impose more conditions on the monomials.

Definition 1.4 *A monomial order on $\Bbbk[x_1, \ldots, x_n]$ is a total order, $\prec$ on the set of all monomials which has the following two properties:*

1. *If* $x^\alpha \prec x^\beta$, *then* $x^{\alpha+\gamma} \prec x^{\beta+\gamma}$ *for all* $\alpha, \beta, \gamma \in \mathbb{N}^n$.

2. $1 \prec x^\alpha$ *for all* $\alpha \in \mathbb{N}^n \setminus \{0\}$.

Once we fix the monomial order, the largest monomial of a polynomial, f w.r.t. $\prec$ is called the leading monomial, $\mathrm{lm}(f)$. The coefficient of the leading monomial is called the leading coefficient, $\mathrm{lc}(f)$ and together the term is called the leading term, $\mathrm{lt}(f)$, i.e. $\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lm}(f)$. One of the most common monomial orders is the lexicographic monomial order which orders the monomials by comparing exponents of x_1, and then in the case of a tie, exponents of x_2 and so forth. It is similar to the ordering in a dictionary.

We have described the ideal membership problem and its significance in understanding the solution space of an ideal, $\mathfrak{a}$ in the previous section. An algorithmic solution for the ideal membership problem in $\Bbbk[x]$ is the Euclidean polynomial division algorithm. Since $\Bbbk[x]$ is a Principal Ideal Domain (PID), $\mathfrak{a}$ is generated by a single polynomial, g. To determine if any $f \in \Bbbk[x]$ is in $\mathfrak{a}$ we have to apply the division algorithm on f with g as the divisor. The algorithm returns q and r such that,

$$f = qg + r, \quad \deg(r) \lneq \deg(g).$$

If $r = 0$, then $f \in \mathfrak{a}$. Note that in the above equation we say that "f reduces to r" on reduction with g and write it as ,

$$f \xrightarrow{g}_+ r.$$

The "+" sign indicates that the reduction to r has proceeded through multiple steps and further reduction is not possible. Can we extend the same algorithm to the multivariate case to solve the ideal membership problem for an ideal, $\mathfrak{a}$ in $\Bbbk[x_1, \ldots, x_n]$?

Let $\{f_1, \ldots, f_s\} \subseteq \Bbbk[x_1, \ldots, x_n]$ be the generators of $\mathfrak{a}$. For an $f \in \Bbbk[x_1, \ldots, x_n]$, our aim is to find $h_i \in \Bbbk[x_1, \ldots, x_n]$, $i = 1, \ldots, s$ and $r \in \Bbbk[x_1, \ldots, x_n]$ such that

$$f = h_1 f_1 + \cdots + h_s f_s + r,$$

and no term in r can be divided by the leading terms of $f_1, \ldots, f_s$. We denote it as,

$$f \xrightarrow{\{f_1, \ldots, f_s\}}_+ r.$$

Like in the univariate case, if the remainder, $r = 0$, we can conclude that $f \in \mathfrak{a}$. Thus, $r = 0$ is a sufficient condition for the ideal membership problem. But the following example shows us that it is not a necessary condition.

Example 1.5 *Let $f_1 = xy+1$ and $f_2 = y^2 - x$ and $\mathfrak{a} = \langle f_1, f_2 \rangle$. Consider the graded lex order, $y \prec x$. If $f = xy^2 - x^2$, by the below calculation using multivariate polynomial algorithm, we have $f \notin \mathfrak{a}$.*

$$\begin{array}{rl} h_1: & y \\ h_2: & 0 \\ f_1: xy+1 & \sqrt{xy^2 - x^2} \\ f_2: y^2 - x & \\ & \underline{\quad xy^2 + y} \\ & -x^2 - y \end{array}$$

On the other hand, if we use a different sequence of divisors we have zero as the remainder, as shown below.

$$\begin{array}{rl} h_1: & 0 \\ h_2: & x \\ f_1: xy+1 & \sqrt{xy^2 - x^2} \\ f_2: y^2 - x & \\ & \underline{\quad xy^2 - x^2} \\ & 0 \end{array}$$

The first calculation shows that even if $f \in \mathfrak{a}$, it is still possible to obtain a nonzero remainder on division.

The "special" properties of Gröbner bases ensure that once we transform the divisor set to a Gröbner basis, we can perform the division algorithm in any order of the divisors and the remainder will still be unique. It is one of the characterizations of Gröbner bases. In the above case the Gröbner basis of $\mathfrak{a}$ is given by $G = \{xy + 1, y^2 - x, x^2 + y\}$. One can verify that the remainder for any sequence of divisors is 0.

Now, we define Gröbner bases formally. The leading term ideal of a set, S w.r.t. a monomial order, $\prec$ is the ideal generated by the leading terms of all the polynomials in S and it is denoted as $\langle \mathrm{lt}(S) \rangle$, i.e.

$$\langle \mathrm{lt}_{\prec}(S) \rangle = \langle \{ \mathrm{lt}_{\prec}(f) \mid f \in S \} \rangle.$$

Consequently, the leading term ideal of an ideal, $\mathfrak{a}$ denoted as $\langle \mathrm{lt}(\mathfrak{a}) \rangle$, is the ideal generated by all the leading terms of polynomials in $\mathfrak{a}$.

Definition 1.6 *A finite subset $G = \{g_1, \ldots, g_t\} \subseteq \mathfrak{a}$ ($\mathfrak{a} \neq \{0\}$) is said to be a Gröbner basis of $\mathfrak{a}$ if*

$$\langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle = \langle \mathrm{lt}(\mathfrak{a}) \rangle.$$

A Gröbner basis, G of the set of polynomials $\{f_1, \ldots, f_m\}$ generates the corresponding ideal and therefore,

$$\mathcal{V}(\{f_1, \ldots, f_m\}) = \mathcal{V}(\langle f_1, \ldots, f_m \rangle) = \mathcal{V}(G).$$

It can be shown that every ideal in $\Bbbk[x_1, \ldots, x_n]$ has a Gröbner basis. Gröbner basis is not unique for an ideal : if G is a Gröbner basis for $\mathfrak{a}$, then any finite subset of $\mathfrak{a}$ that contains G is also a Gröbner basis. As stated before 'reduced Gröbner basis' remedies this situation.

Definition 1.7 *A Gröbner basis, $G = \{g_1, \ldots, g_t\}$, is called a reduced Gröbner basis if*

1. *for each $g_i \in G$, $i = 1, \ldots, t$, $\mathrm{lc}(g_i) = 1$,*
2. *for each $g_i \in G$, $i = 1, \ldots, t$, no monomial of g_i lies in $\langle \mathrm{lt}(G \setminus \{g_i\}) \rangle$.*

One can show that a unique reduced Gröbner basis w.r.t. a monomial order always exists for a nonzero polynomial ideal.

1.2 Contributions of the Thesis

Our aim is to develop Gröbner basis algorithms for algebraic problems in $A[x_1, \ldots, x_n]$ and throughout this thesis our focus is on residue class polynomial rings over A, $A[x_1, \ldots, x_n]/\mathfrak{a}$. When $A = \Bbbk$, we have seen how significant the $\Bbbk$-vector space and $\Bbbk$-algebra structures of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ are in the study of polynomial equations over $\Bbbk$. We summarize the important contributions of this thesis below.

1. For an ideal, $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$, we give a Gröbner basis characterization for $A[x_1, \ldots, x_n]/\mathfrak{a}$ to have a free A-module representation w.r.t. a monomial ordering. Note that when $A = \Bbbk$ the residue class polynomial ring is always free. We introduce the concept of 'short reduced Gröbner basis', a reduced Gröbner basis that satisfies certain additional properties, and use that to give a necessary and sufficient condition. The characterization is the most significant result in this thesis and all the other observations we make are built from this result.

   Result 1.8 *(Francis and Dukkipati, 2014, Theorem 3.12) Let G be a short reduced Gröbner basis for $\mathfrak{a}$ w.r.t. some monomial ordering, $\prec$. Then, $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. $\prec$, i.e.*

   $$A[x_1, \ldots, x_n]/\mathfrak{a} \cong A^N, \quad \text{for some } N \in \mathbb{N},$$

   if and only if G is monic.

2. Given an A-module, $A[x_1, \ldots, x_n]/\mathfrak{a}$, that has a free A-module representation, we give an algorithm to compute its A-module basis. This extends the Macaulay Buchberger basis theorem to polynomial rings over Noetherian commutative rings.

   Result 1.9 *(Francis and Dukkipati, 2014, Theorem 4.1) Let $G = \{g_1, \ldots, g_t\}$ be a short reduced Gröbner basis for an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$. Suppose G is monic then an A-module basis for $A[x_1, \ldots, x_n]/\mathfrak{a}$ is given by $S = \{x^\alpha + \mathfrak{a} : \mathrm{lm}(g_i) \nmid x^\alpha, i = 1, \ldots, t\}$.*

3. Border basis is a generating set like Gröbner basis for an ideal in $\mathbb{k}[x_1, \ldots, x_n]$, but it is numerically more stable than Gröbner basis. It is defined only for ideals that give rise to finitely generated residue class polynomial rings over fields. In this thesis, we extend border bases to $A[x_1, \ldots, x_n]$, for the cases when the residue class polynomial ring is a free A-module and when it has torsion submodules. For a free A-module, we have a direct extension but for residue class polynomial rings with torsion we first need to generalize the Macaulay-Buchberger basis theorem to such structures. Then border bases follow as an application of the theorem.

4. For the special case of $A = \mathbb{Z}$, i.e. the coefficient ring is the ring of integers, we show that free and finitely generated residue class polynomial rings over $\mathbb{Z}$ are isomorphic to integer lattices. Therefore, ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ are isomorphic to integer sublattices and are called multivariate ideal lattices. From Result 1.8, we have that if the short reduced Gröbner basis is monic, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is a free $\mathbb{Z}$-module. Thus, in this thesis we not only characterize multivariate ideal lattices, we also describe a Gröbner basis technique to locate them. We formally state the characterization for integers below.

   Result 1.10 *The $\mathbb{Z}$-module, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ has ideal lattices if and only if the short reduced Gröbner basis of $\mathfrak{a}$ is monic.*

5. Using multivariate ideal lattices, we show how one can build collision resistant cryptographic hash functions. To prove collision resistance, we first extend the Smallest Polynomial Problem (SPP) proposed for univariate ideal lattices to the multivariate case. In the univariate case, the hardness of SPP was shown by using a known hard problem called the Shortest Conjugate Problem (SCP). To show the hardness of SPP in the multivariate case we formulate a new problem called the Smallest Substitution Problem ($SSub$) and show that SCP can be polynomially reduced to $SSub$. Once we establish the hardness of SPP we show that if there exists a polynomial time algorithm that can find

a collision in the hash function with nonnegligible probability then SPP can be solved in polynomial time for every multivariate ideal lattice in the ring.

6. For a Noetherian integral domain, A we explore algorithmic techniques 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. either lexicographic or degree compatible monomial orders using Gröbner bases. We first extend the notion of combinatorial dimension (cdim), Hilbert series, Hilbert function and Hilbert polynomial ($p_{\mathfrak{a}}$) to $A[x_1, \ldots, x_n]/\mathfrak{a}$. We then give Gröbner basis algorithms to compute these quantities. In fields, the degree of the Hilbert polynomial, combinatorial dimension and Krull dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ are equal to each other. In the case of integral domains, we derive certain relations between these three quantities for residue class polynomial rings that have a free A-module representation w.r.t. either degree compatible or lexicographic monomial orderings. For A-algebras with a free A-module representation w.r.t. a lexicographic ordering, we have

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

For A-algebras with a free A-module representation w.r.t. a degree compatible monomial ordering, we have

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

The immediate application of these relations is that we have a uniform method, independent of the ideal, to compute the Krull dimension of certain A-algebras. These relations give an algorithmic interpretation for the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$. This is relevant because they are the first steps towards understanding the solution space of a system of polynomial equations over integral domains.

1.3 Organization of the Thesis

This thesis can be regarded as a study of residue class polynomial polynomial rings over Noetherian commutative rings. Given an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$, we study the A-module and A-algebra structure of $A[x_1, \ldots, x_n]/\mathfrak{a}$. We also look at special cases of the coefficient ring, A and for $A = \mathbb{Z}$, we explore the practical applications of the residue class polynomial ring in lattice based cryptography. We describe the chapters in this thesis below.

1. Chapter 2 describes certain preliminaries regarding Gröbner bases theory for polynomial rings over Noetherian commutative rings. We also define combinatorial dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$, Hilbert function, Hilbert series and Hilbert polynomial of an ideal $\mathfrak{a}$ in

$\Bbbk[x_1, \ldots, x_n]$ and also describe Gröbner basis techniques that can be used to compute these quantities. We study ideal lattices in the univariate case and show how collision resistant hash functions can be built from them. We also give some preliminaries regarding border bases in $\Bbbk[x_1, \ldots, x_n]$ and state some key results from the Gröbner bases theory for submodules in $\Bbbk[x_1, \ldots, x_n]^m$.

2. From Chapter 3 onwards, we focus on polynomial rings over Noetherian commutative rings. This chapter describes the characterization of free residue class polynomial rings over Noetherian commutative rings using Gröbner bases. To derive the necessary and sufficient condition, we introduce a special type of Gröbner basis called 'short reduced Gröbner basis'. The characterization is the crux of this thesis as it enables us to extend several properties of fields to rings for a subset of ideals for which the residue class polynomial ring has a free A-module representation w.r.t. a monomial order. As an application of the characterization we show how it can used to extend border bases to $A[x_1, \ldots, x_n]$ for a subset of ideals. We will see in the subsequent chapters how the characterization enables us to locate ideal lattices in $\mathbb{Z}[x_1, \ldots, x_n]$ and compute the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ that have a free A-module representation w.r.t. some monomial order.

3. In Chapter 4, we look at the special case of $A = \mathbb{Z}$, the ring of integers. We extend the concept of univariate ideal lattices to the multivariate case and show that only free residue class polynomial rings over $\mathbb{Z}$ can have ideal lattices. Using short reduced Gröbner basis we also show how to locate multivariate ideal lattices. Since multivariate ideal lattices are compact representations of integer lattices, the natural question to ask is can we have cryptographic primitives built using them. The answer is yes and we show how to construct collision resistant hash functions using multivariate ideal lattices.

4. In Chapter 5, we restrict our coefficient ring to integral domains. We explore the possibility of computing the Krull dimension of A-algebras, $A[x_1, \ldots, x_n]/\mathfrak{a}$, that have a free A-module representation w.r.t. some monomial order using Gröbner bases. For this we introduce the concepts of combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ and the Hilbert polynomial of $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$. We also show how these quantities can be computed using Gröbner bases. We derive certain relations that connect the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$, its combinatorial dimension and the degree of the Hilbert polynomial of $\mathfrak{a}$ for A-algebras that have a free A-module representation w.r.t. either lexicographic or degree compatible monomial orders. These relations are an elegant generalization of the relations we have for fields.

5. We extend border bases to residue class polynomial rings that are finitely generated but may contain torsion submodules in Chapter 6. We first give a generalized version of the Macaulay-Buchberger basis theorem, the weak MB basis theorem, and use that to define border bases for ideals that give rise to residue class polynomial rings that are finitely generated but not necessarily free.

6. We give possible future directions and concluding remarks in Chapter 7. We need to revisit all the concepts we have introduced in this thesis for A-algebras that do not have a free A-module representation w.r.t. any monomial order. It will be interesting to explore how to build other cryptographic primitives like digital signatures, identification schemes using multivariate ideal lattices. We also need to develop software packages that can determine the A-module representation of $A[x_1, \ldots, x_n]/\mathfrak{a}$. Once we implement it, we can use it to locate multivariate ideal lattices. These software packages have to be integrated to one of the computer algebra systems (CAS). These packages will simplify computations for researchers working with either polynomial equations over integers or parametric equations over polynomial rings.

Chapter 2

Preliminaries

Throughout this thesis, $\Bbbk$ denotes a field, $\mathbb{Z}$ the ring of integers and $\mathbb{N}$ the set of non-negative integers. We use A to denote a Noetherian commutative ring. In Chapter 5, A is restricted to Noetherian integral domains. An affine space of dimension n over a field $\Bbbk$ is denoted as $\mathbb{A}^n_{\Bbbk}$. A polynomial ring in indeterminates $x_1, \ldots, x_n$ over A is denoted as $A[x_1, \ldots, x_n]$. We represent a monomial in $x_1, \ldots, x_n$ (or $\theta_1, \ldots, \theta_n$) as x^α (or θ^α), where $\alpha \in \mathbb{N}^n$. The monoid isomorphism between the set of all monomials in indeterminates $x_1, \ldots, x_n$ and $\mathbb{N}^n$ allows us to denote the set of all monomials by $\mathbb{N}^n$. We use $\mathbb{N}^n_M$ and $\mathbb{N}^n_{<M}$ to represent the set of monomials of degree M and monomials of degree less than M, respectively. By 'term' we mean cx^α, where $c \in A$ and $c \neq 0$. We will denote all the terms in $A[x_1, \ldots, x_n]$ by $\mathrm{Ter}(A[x_1, \ldots, x_n])$ and all the monomials in $A[x_1, \ldots, x_n]$ by $\mathrm{Mon}(A[x_1, \ldots, x_n])$. Let $T \subseteq \mathrm{Ter}(A[x_1, \ldots, x_n])$ be a set of terms, possibly infinite. We define the monomial part of T, denoted by $\mathrm{Mon}(T)$, as $\mathrm{Mon}(T) = \{x^\alpha \in \mathbb{N}^n : ax^\alpha \in T, \text{ for some nonzero } a \in A\}$. A polynomial, f in $x_1, \ldots, x_n$ with coefficients from A is given by

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

where $\Lambda_f \subsetneq \mathbb{N}^n$ is a finite set and $a_\alpha \in A$. Λ_f is called the support of the polynomial f, denoted by $\mathrm{supp}(f)$. The set of monomials appearing with nonzero coefficients in f is denoted by $\mathrm{Mon}(f)$. The set of all terms appearing in f is denoted by $\mathrm{Ter}(f)$, i.e. $\mathrm{Ter}(f) = \{a_\alpha x^\alpha \mid \alpha \in \Lambda\}$. If $F \subseteq A[x_1, \ldots, x_n]$ is a set of polynomials then $\mathrm{Mon}(F) = \bigcup_{f \in F} \mathrm{Mon}(f)$. Similarly, $\mathrm{Ter}(F) = \bigcup_{f \in F} \mathrm{Ter}(f)$. We use the notation $\mathfrak{a}$ for polynomial ideals in $A[x_1, \ldots, x_n]$ and I or $\mathcal{I}$ for ideals in the coefficient ring, A. Given a set of terms T and an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$ the set of residue class elements of T modulo $\mathfrak{a}$ is denoted by $T + \mathfrak{a}$. That is $T + \mathfrak{a} = \{ax^\alpha + \mathfrak{a} : ax^\alpha \in T\}$. We represent a module over a ring, A spanned by a set S as $\mathrm{Span}_A(S)$.

The notion of monomial order, $\prec$ given in Definition 1.4 can be directly extended from

$\Bbbk[x_1, \ldots, x_n]$ to $A[x_1, \ldots, x_n]$. With respect to a monomial order, we have the leading monomial ($\text{lm}_\prec$), leading coefficient ($\text{lc}_\prec$), leading term ($\text{lt}_\prec$) and multidegree of a polynomial ($\text{multideg}_\prec$), where $\text{lt}_\prec(f) = \text{lc}_\prec(f)\text{lm}_\prec(f)$ and $\text{multideg}_\prec(f) = \max_\prec\{\alpha \in \Lambda_f\}$ in $A[x_1, \ldots, x_n]$. In certain scenarios, we also consider another concept of degree of a polynomial which we will denote in this thesis 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.

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

A degree compatible monomial ordering, $\prec$ is a monomial ordering on $A[x_1, \ldots, x_n]$ such that two monomials $x^\alpha, x^{\alpha'}$ 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. An example of degree compatible monomial order is the graded lexicographic monomial order which orders by total degree first, then breaks ties using lexicographic order.

Example 2.1 *Let $\prec$ be a graded lex order with $x_1 \prec x_2$ and $f = 3x_2^2 + x_1^2 + 4x_2 \in \mathbb{Z}[x_1, x_2]$ be a polynomial. Then $3x_2^2$ is the leading term of f w.r.t. $\prec$.*

The leading term ideal (or initial ideal) of a set $S \subseteq A[x_1, \ldots, x_n]$, is $\langle \text{lt}_\prec(S)\rangle = \langle\{\text{lt}_\prec(f) \mid f \in S\}\rangle$. The leading term ideal of an ideal, $\mathfrak{a}$ is denoted as $\langle \text{lt}(\mathfrak{a})\rangle$. When there is no confusion regarding which monomial order to consider we omit the monomial order subscript $\prec$ from the notations. Since A is a Noetherian ring, $A[x_1, \ldots, x_n]$ is Noetherian too.

2.1 Gröbner Bases in $\Bbbk[x_1, \ldots, x_n]$

In Section 1.1, we gave the definition of a Gröbner basis for an ideal in $\Bbbk[x_1, \ldots, x_n]$. We now look at how to compute a Gröbner basis and how Gröbner bases can be used as a tool to study polynomial equations in $\Bbbk[x_1, \ldots, x_n]$.

2.1.1 Computation of Gröbner bases - Buchberger's algorithm

Buchberger (1965) gave an algorithm to compute the Gröbner basis of an ideal in $\Bbbk[x_1, \ldots, x_n]$. Consider any two nonzero polynomials, $f, g \in \Bbbk[x_1, \ldots, x_n]$ and let L denote the $\text{lcm}(\text{lm}(f), \text{lm}(g))$. The polynomial,

$$\text{Spoly}(f, g) = \frac{L}{\text{lt}(f)}f - \frac{L}{\text{lt}(g)}g,$$

is called the S-polynomial of f and g. The construction of this polynomial can be understood if we study Example 1.5. The nonuniqueness in the remainder is because some term in f, cx^α, is divisible by the leading terms of two different divisors, f_1, f_2, which in turn implies it is divisible

by the lcm, L, of the divisors. If we reduce f using f_1 we get $h_1 = f - \frac{cx^\alpha}{\mathrm{lt}(f_1)} f_1$ and if we reduce f with f_2, we get $h_2 = f - \frac{cx^\alpha}{\mathrm{lt}(f_2)} f_2$. Therefore, the ambiguity in the division algorithm that leads to different remainders is created by $h_1 - h_2 = \frac{cx^\alpha}{L}\mathrm{Spoly}(f_1, f_2)$. Since S-polynomials take care of the ambiguity in the division algorithm, adding the S-polynomials to the set of generating set of polynomials is a necessary step in computing the Gröbner basis. Buchberger's criterion states that this necessary condition is also sufficient: computing the S-polynomials removes *all* the ambiguities.

Theorem 2.2 *Let $G = \{g_1, \ldots, g_t\}$ be a set of nonzero polynomials in $\Bbbk[x_1, \ldots, x_n]$. Then G is a Gröbner basis for the ideal, $\langle g_1, \ldots, g_t\rangle$ if and only if for all $i \neq j$,*

$$\mathrm{Spoly}(g_i, g_j) \xrightarrow{G}_+ 0.$$

The algorithm to compute the Gröbner basis follows from the the above characterization. The algorithm, though simple to understand, is computationally expensive. It can be fur-

Algorithm 1 Computing the Gröbner basis of an ideal, $\mathfrak{a} = \langle f_1, \ldots, f_s\rangle$ in $\Bbbk[x_1, \ldots, x_n]$

Input $f = \{f_1, \ldots, f_s\} \subseteq \Bbbk[x_1, \ldots, x_n]$ with $f_i \neq 0$ for $i = 1, \ldots, s$
Output $G = \{g_1, \ldots, g_t\}$, a Gröbner basis for the ideal generated by F
$G = F$, $\mathcal{G} = \{\{f_i, f_j\} : f_i \neq f_j,\ f_i, f_j \in G\}$
while $\mathcal{G} \neq \phi$ **do**
  Choose $\{f, g\} \in \mathcal{G}$
  $\mathcal{G} = \mathcal{G} \setminus \{\{f, g\}\}$
  $\mathrm{Spoly}(f, g) \xrightarrow{G}_+ h$, where h is completely reduced w.r.t. G
  if $h \neq 0$ **then**
    $\mathcal{G} = \mathcal{G} \cup \{\{f, h\} :$ for all $f \in G\}$
    $G = G \cup \{h\}$
  end if
end while

ther improved to reduce the computation time by using strategies like removing unnecessary S-polynomial calculations (Giovini et al., 1991), etc. There are also other approaches to compute the Gröbner basis of an ideal. For example, Faugère's F4 and F5 algorithms (Faugère, 1999, 2002) make use of linear algebraic techniques but have the same underlying mathematical principles as the Buchberger's algorithm. Despite that, in general, the time complexity for Gröbner basis computations is doubly exponential in the number of indeterminates. However, they are often computable in practice and most computer algebra systems such as CoCoA[1],

[1] http://cocoa.dima.unige.it/

Magma[1], GAP[2], Maple[3], SageMath[4] and Macaulay2[5] have routines that implement them.

2.1.2 Elementary applications of Gröbner bases

The theory of Gröbner bases has been the backbone of computational ideal theory. Given an ideal $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$, one can consider the following problems (Adams and Loustaunau, 1994):

1. How to determine the coset representatives of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$?
2. How to compute a $\Bbbk$-vector space basis of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$?
3. How does one characterize zero-dimensional ideals using Gröbner bases?
4. How does the structure of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ help us in the study of the affine variety of $\mathfrak{a}$?

One can see from the characterizations of Gröbner bases that the remainder on reduction of an element $f \in \Bbbk[x_1, \ldots, x_n]$ with respect to a Gröbner basis, G, is always unique. The remainder is called the normal form of f and is denoted as $\eta_G(f)$. We have the following result that gives us the coset representatives of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$.

Proposition 2.3 *(Adams and Loustaunau, 1994, Proposition 2.1.4) Let $f, g \in \Bbbk[x_1, \ldots, x_n]$. Then,*

$$f \equiv g \bmod \mathfrak{a} \text{ if and only if } \eta_G(f) = \eta_G(g).$$

Therefore, the set $\{\eta_G(f) : f \in \Bbbk[x_1, \ldots, x_n]\}$ is a set of coset representatives for $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$.

A $\Bbbk$-vector space basis of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ is given by the Macaulay basis theorem.

Theorem 2.4 (Macaulay Basis Theorem (Macaulay, 1927)) *Let $\mathfrak{a}$ be an ideal in $\Bbbk[x_1, \ldots, x_n]$. The residue classes of the terms in $\Bbbk[x_1, \ldots, x_n]/\langle \mathrm{lt}(\mathfrak{a})\rangle$ form a $\Bbbk$-vector space basis of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. That is, the $\Bbbk$-vector space basis of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ is $S = \{x^\alpha + \mathfrak{a} : x^\alpha \notin \langle \mathrm{lt}(\mathfrak{a})\rangle\}$.*

The above result does not provide an algorithmic method to compute a $\Bbbk$-vector space basis of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. Gröbner bases were introduced by Buchberger (1965) to give an algorithmic technique for computing it.

[1] http://magma.maths.usyd.edu.au/magma/
[2] http://www.gap-system.org/
[3] http://www.maplesoft.com/
[4] http://www.sagemath.org/
[5] http://www.math.uiuc.edu/Macaulay2/

Theorem 2.5 (Macaulay-Buchberger Basis Theorem) *Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for an ideal $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$. A basis for the $\Bbbk$-vector space $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ is given by $S = \{x^\alpha + \mathfrak{a} : \mathrm{lm}(g_i) \nmid x^\alpha, i = 1, \ldots, t\}$.*

The following is an important result in computational ideal theory.

Theorem 2.6 *(Adams and Loustaunau, 1994, Theorem 2.2.7) Let $\Bbbk$ be a field and $\overline{\Bbbk}$, an algebraic closure of $\Bbbk$. Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for an ideal $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$. The following statements are equivalent.*

1. *The variety of an ideal, $\mathcal{V}_{\overline{\Bbbk}}(\mathfrak{a})$, is finite.*
2. *For each $i = 1, \ldots, n$, there exists $j = 1, \ldots, t$ such that $\mathrm{lm}(g_j) = x_i^\nu$ for some $\nu \in \mathbb{N}$.*
3. *The dimension of the $\Bbbk$-vector space $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ is finite.*

We will discuss the dimension of an affine variety in Section 2.4 and show that one of the characterizations for an affine variety to have dimension zero is that the variety is a finite set. Therefore an ideal, $\mathfrak{a}$, that satisfies one of the equivalent conditions above is called a zero-dimensional ideal. The second statement in the above theorem gives us a convenient "triangular" form for the Gröbner basis of $\mathfrak{a}$ and we can determine the points in the variety easily using this form. A direct consequence of the second statement is that we can order the elements in G such that the first n elements of G will have leading terms in just one variable. If we use lexicographic ordering we can also have an ordering such that that the first element in G will be a polynomial only in x_1, the second element, a polynomial only in x_1, x_2 and so on. Thus the problem of solving the system of multivariate polynomial equations reduces to the problem of solving a polynomial equation in one variable.

Corollary 2.7 *(Adams and Loustaunau, 1994, Corollary 2.2.11) Let $\mathfrak{a}$ be a zero-dimensional ideal and G the reduced Gröbner basis of $\mathfrak{a}$ w.r.t. a lexicographic monomial order, $\prec$ with $x_1 \prec x_2 \prec \cdots \prec x_n$. Then we can order $g_1, \ldots, g_t$ such that g_1 contains only the variables x_1, g_2 contains the variables x_1 and x_2 and $\mathrm{lm}(g_2)$ is a power of x_2, g_3 contains only the variables x_1, x_2 and x_3 and $\mathrm{lm}(g_3)$ is a power of x_3 and so forth until g_n.*

The above result illustrates how Gröbner bases generalize Gaussian elimination for linear systems by generating a "triangular" system for the nonlinear polynomial system. As for positive dimensional ideals, the dimension of the affine variety is given by the Krull dimension of the affine $\Bbbk$-algebra, $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. We will see in the succeeding sections, how Gröbner basis techniques can be used to compute the Krull dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$.

2.2 Gröbner bases in $\Bbbk[x_1, \ldots, x_n]^m$

The standard basis for $\Bbbk[x_1, \ldots, x_n]^m$ is the set containing the following vectors:

$$\overrightarrow{e_1} = (1, 0, \ldots, 0), \overrightarrow{e_2} = (0, 1, \ldots, 0), \ldots, \overrightarrow{e_m} = (0, 0, \ldots, 1).$$

A monomial in $\Bbbk[x_1, \ldots, x_n]^m$ is of the form $x^\alpha \overrightarrow{e_i}$, $1 \leq i \leq m$, where x^α is a monomial in $\Bbbk[x_1, \ldots, x_n]$. We denote the monomial $x^\alpha \overrightarrow{e}$ as $\overrightarrow{X}$.

Definition 2.8 *Let $\overrightarrow{X} = x^\alpha \overrightarrow{e_i}$ and $\overrightarrow{Y} = x^\beta \overrightarrow{e_j}$ be two monomials in $\Bbbk[x_1, \ldots, x_n]^m$. We say that $\overrightarrow{X}$ divides $\overrightarrow{Y}$ provided $i = j$ and x^α divides x^β.*

Terms are defined as a vector of the type $c\overrightarrow{X}$, where $c \in \Bbbk \setminus \{0\}$ and $\overrightarrow{X}$ is a monomial in $\Bbbk[x_1, \ldots, x_n]^m$. A monomial order, $\prec$ is assumed on the monomials in $\Bbbk[x_1, \ldots, x_n]^m$ (Adams and Loustaunau, 1994, Definition 3.5.1). It is a total order that is analogous to the monomial order in $\Bbbk[x_1, \ldots, x_n]$. Examples for monomial order include TOP (Term Over Position)and POT (Position Over Term) (Adams and Loustaunau, 1994, Definition 3.5.2 and 3.5.3). Now we proceed to define Gröbner bases for submodules in $\Bbbk[x_1, \ldots, x_n]^m$.

Definition 2.9 *A set of nonzero vectors $G = \{\overrightarrow{g_1}, \ldots, \overrightarrow{g_t}\}$ contained in the submodule M is called a Gröbner basis for M if and only if for all $\overrightarrow{f} \in M$, there exists $i = 1, \ldots, t$ such that $\mathrm{lm}(\overrightarrow{g_i})$ divides $\mathrm{lm}(\overrightarrow{f})$.*

The concept of S-polynomials and the Buchberger algorithm to compute Gröbner bases in $\Bbbk[x_1, \ldots, x_n]$ can be directly extended to $\Bbbk[x_1, \ldots, x_n]^m$.

2.3 Border Bases in $\Bbbk[x_1, \ldots, x_n]$

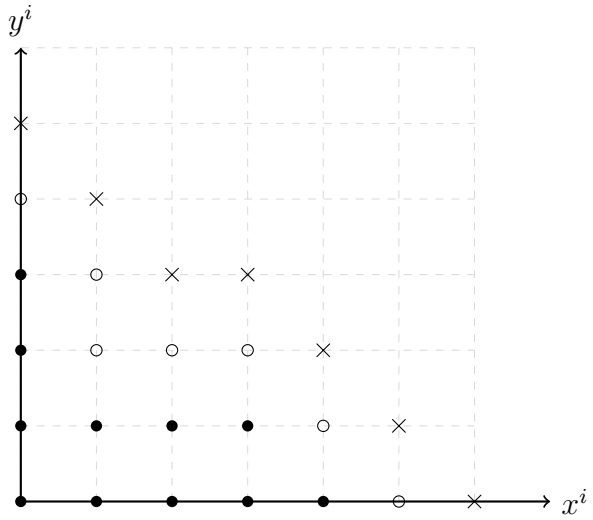
Border bases, an alternative to Gröbner bases, described in (Kehrein et al., 2005; Kehrein and Kreuzer, 2005) are known to be numerically more stable than Gröbner bases for small perturbations of the coefficients (Stetter, 2004). For a good exposition the reader can refer to (Kreuzer and Robbiano, 2005, Section 6.4). There has been considerable interest in the theory of border bases, from characterization (Kehrein and Kreuzer, 2005) to methods of computation (Kehrein and Kreuzer, 2006) to computational hardness (Ananth and Dukkipati, 2012). Here we briefly recall a few definitions related to border bases.

Definition 2.10 *A finite set of monomials $\mathcal{O} \subseteq \mathbb{N}^n$ is called an order ideal if it is closed under forming divisors i.e., for $x^\alpha \in \mathbb{N}^n$ if $x^\beta \in \mathcal{O}$ and $x^\alpha | x^\beta$ then $x^\alpha \in \mathcal{O}$.*

Definition 2.11 *Let $\mathcal{O} \subseteq \mathbb{N}^n$ be an order ideal. The border of $\mathcal{O}$ is the set $\partial\mathcal{O} = (x_1\mathcal{O} \cup \ldots \cup x_n\mathcal{O}) \setminus \mathcal{O}$. The first border closure of $\mathcal{O}$ is defined as the set $\mathcal{O} \cup \partial\mathcal{O}$ and it is denoted by $\overline{\partial\mathcal{O}}$.*

Note that $\overline{\partial\mathcal{O}}$ is also an order ideal. By convention, for $\mathcal{O} = \emptyset$ we set $\partial\mathcal{O} = \{1\}$.

Example 2.12 *(Kehrein et al., 2005, Example 4.2.3) Consider the order ideal $\mathcal{O}$ given by $\{1, x, y, x^2, y^2, xy, x^3, y^3, x^2y, x^4, x^3y\} \subseteq \mathbb{N}^2$. We illustrate below the order ideal (represented in the figure by filled circles) and its first two borders (shown in the figure using circles and cross marks).*



Definition 2.13 *Let $\mathcal{O} = \{x^{\alpha_1}, \ldots, x^{\alpha_s}\} \subseteq \mathbb{N}^n$ be an order ideal, and let $\partial\mathcal{O} = \{x^{\beta_1}, \ldots, x^{\beta_t}\}$ be its border. A set of polynomials $B = \{b_1, \ldots, b_t\} \subseteq \Bbbk[x_1, \ldots, x_n]$ is called an $\mathcal{O}$-border prebasis if the polynomials have the form*

$$b_j = x^{\beta_j} - \sum_{i=1}^{s} c_{ij} x^{\alpha_i} \quad ,$$

where $c_{ij} \in \Bbbk$ for $1 \leq i \leq s$ and $1 \leq j \leq t$.

Definition 2.14 *Let $\mathcal{O} = \{x^{\alpha_1}, \ldots, x^{\alpha_s}\} \subseteq \mathbb{N}^n$ be an order ideal and $B = \{b_1, \ldots, b_t\}$ be an $\mathcal{O}$-border prebasis consisting of polynomials in $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$. We say that the set B is an $\mathcal{O}$-border basis of $\mathfrak{a}$ if the residue classes of $x^{\alpha_1}, \ldots, x^{\alpha_s}$ form a $\Bbbk$-vector space basis of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$.*

2.4 Dimension of Ideals in $\mathbb{k}[x_1, \ldots, x_n]$

We have seen how Gröbner bases can be used to characterize a system of polynomial equations that has an affine variety of finite cardinality. The Krull dimension or simply dimension of an affine variety generalizes the notion of cardinality to polynomial systems with infinite number of solutions. Given an algebraically closed field, $\mathbb{k}$, the dimension of an affine variety is defined as the the maximal length, d, of chains of distinct nonempty subvarieties of $\mathcal{V} \subseteq \mathbb{A}^n_{\mathbb{k}}$, $\mathcal{V}_0 \subsetneq \mathcal{V}_1 \subsetneq \ldots \subsetneq \mathcal{V}_d$. Intuitively, one can see that it generalizes the notion of dimension of a vector space. It is equal to the Krull dimension of the affine $\mathbb{k}$-algebra, $\mathbb{k}[x_1, \ldots, x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is the ideal corresponding to the polynomial system and $\mathbb{k}$ is algebraically closed. In order to determine techniques to compute the dimension of an affine variety we study the affine $\mathbb{k}$-algebra. In the literature, the Krull dimension of $\mathbb{k}[x_1, \ldots, x_n]/\mathfrak{a}$ is sometimes referred to as the dimension of the ideal, $\mathfrak{a}$ (Becker et al., 1993). In this thesis, we use both the terminologies interchangeably. We review here different Gröbner basis approaches to compute the dimension of an ideal. We look at formal definitions below.

Definition 2.15 (Affine Variety) *A subset $V \subseteq \mathbb{A}^n_{\mathbb{k}}$ is called an affine variety if V is the set of solutions of a system of polynomial equations in $\mathbb{k}[x_1, \ldots, x_n]$. That is, there exist $f_1, \ldots, f_s \in \mathbb{k}[x_1, \ldots, x_n]$ such that $V = \{(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{k}} : f_i(a_1, \ldots, a_n) = 0, i = 1, \cdots, s\}$*

Definition 2.16 (Vanishing Ideal) *Let $V \subseteq \mathbb{A}^n_{\mathbb{k}}$ be a set of points. The vanishing ideal of V is defined as*

$$\mathcal{I}(V) = \{f \in \mathbb{k}[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V\}.$$

We recall the definition of radical ideals below.

Definition 2.17 *Given an ideal $I \subseteq A$ in a ring A, the radical ideal of I is*

$$\sqrt{I} = \{f \in A : \text{ there exists a positive integer } k \text{ such that } f^k \in I\}.$$

An ideal is called a radical ideal if $\sqrt{I} = I$.

Clearly, the vanishing ideal is a radical ideal.

Hilbert's Nullstellensatz gives the relation between the vanishing ideal of an affine variety of an ideal and the ideal itself.

Theorem 2.18 (Strong Hilbert's Nullstellensatz) *Let $\mathbb{k}$ be an algebraically closed field and $\mathfrak{a} \subseteq \mathbb{k}[x_1, \ldots, x_n]$ be an ideal. Then $\mathcal{I}(\mathcal{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*

Lemma 2.19 *Let $\Bbbk$ be a field and $V \subseteq \mathbb{A}^n_\Bbbk$ an affine variety. Then $\mathcal{V}(\mathcal{I}(V)) = V$.*

Definition 2.20 *Let $V \subseteq \mathbb{A}^n_\Bbbk$ be an affine variety. Let $\mathcal{I}(V) \subseteq \Bbbk[x_1, \ldots, x_n]$ be the vanishing ideal of V. Then the coordinate ring of V is the residue class polynomial ring,*

$$\Bbbk[V] = \Bbbk[x_1, \ldots, x_n]/\mathcal{I}(V).$$

The below result is key in understanding the relationship between the Krull dimensions of the coordinate ring and the affine variety. This result gives the correspondence between radical ideals in the coordinate ring and the subvarieties of an affine variety.

Theorem 2.21 *(Kemper, 2011, Theorem 1.23) Let V be an affine variety over an algebraically closed field, $\Bbbk$. Then there is an inclusion-reversing bijection between the set of subvarieties $W \subseteq V$ and the set of radical ideals $J \subseteq \Bbbk[V]$. The bijection is given by mapping a subvariety $W \subseteq V$ to $\mathcal{I}(W)/\mathcal{I}(V) \subseteq \Bbbk[V]$, and mapping an ideal $J \subseteq \Bbbk[V]$ to*

$$\mathcal{V}_V(J) = \{x \in V : f(x) = 0 \text{ for all } f \in J\}.$$

Let W be a subvariety of V and $J \subseteq \Bbbk[V]$ be the vanishing ideal corresponding to W, then $\Bbbk[W] \cong \Bbbk[V]/J$, with an isomorphism given by

$$\begin{aligned} \Bbbk[V]/J &\to \Bbbk[W], \\ f + J &\mapsto f|_W, \end{aligned}$$

where $f|_W$ is the restriction of f on W.

A characterization for irreducible algebraic subsets of $\mathbb{A}^n_\Bbbk$ is given below.

Theorem 2.22 *Let $\Bbbk$ be a field and $V \subseteq \mathbb{A}^n_\Bbbk$ be a set of points, equipped with the Zariski topology. Then V is irreducible if and only if the corresponding vanishing ideal, $\mathcal{I}(V)$ is a prime ideal.*

Definition 2.23 *Let M denote a collection of sets. A chain is a subset of M that is ordered by inclusion, $\subseteq$. The length of a chain, $\mathcal{C}$ denoted as $\text{length}(\mathcal{C})$ is equal to $|\mathcal{C}| - 1$. By convention, if $M = \phi$, then length of $\mathcal{C}$ is -1.*

Definition 2.24 *Let A be a ring. The spectrum of A, $\text{Spec}(A)$, is the set of all prime ideals in A, i.e.*

$$\text{Spec}(A) = \{P \subseteq A : P \text{ is a prime ideal}\}.$$

Definition 2.25 (Krull Dimension) *(Kemper, 2011, Definition 5.1)*

1. *Let V be a topological space and M, the set of all closed, irreducible subsets of V. Then the dimension of V (also called the Krull dimension) is defined as*

$$\text{kdim}(V) = \sup\{\text{length}(\mathcal{C}) : \mathcal{C} \text{ is a chain in } M\}.$$

2. *Let A be a ring. Then the dimension of A (also called the Krull dimension) is defined as*

$$\text{kdim}(A) = \text{kdim}(\text{Spec}(A)).$$

Remark 2.26 *The dimension of a ring, A, given by* $\text{kdim}(\text{Spec}(A))$*, is equal to* $\text{length}(\text{Spec}(A))$ *since the closed, irreducible subsets of* $\text{Spec}(A)$ *correspond to the prime ideals of A. Therefore, one can also define the Krull dimension of a ring as the maximal length of a chain of prime ideals of A.*

Proposition 2.27 *Let $\Bbbk$ be a field. We have that the dimension of a $V \subseteq \mathbb{A}^n_\Bbbk$ is the dimension of V with the Zariski topology. So if $\Bbbk$ is algebraically closed and V is an affine variety, then*

$$\text{kdim}(V) = \text{kdim}(\Bbbk[V]).$$

Proof: From Theorem 2.22 and Theorem 2.21 we have that the closed, irreducible subsets of V correspond to prime ideals in the coordinate ring, $\Bbbk[V]$, and hence the proposition follows.□

Remark 2.28

1. *Note that when we equate the dimension of the coordinate ring and the dimension of the affine variety in Proposition 2.27 we assume that the underlying field is algebraically closed. The result does not hold otherwise. Consider the case of an ideal $\mathfrak{a} = \langle x^2+y^2\rangle \subseteq \mathbb{R}[x,y]$. The Krull dimension of the affine $\mathbb{R}$-algebra is 1 but the dimension of the solution set, $\mathcal{V} = \{(0,0)\} \subseteq \mathbb{R}^2$ is 0.*

2. *Every field has Krull dimension 0.*

3. *The ring of integers, $\mathbb{Z}$ has Krull dimension 1, with all the maximal chains of prime ideals of the form $\{0\} \subsetneq \langle p\rangle$, with p a prime number. Every principal ideal domain that is not a field has Krull dimension 1.*

4. *A polynomial ring, $\Bbbk[x_1,\ldots,x_n]$ over a field, $\Bbbk$, has dimension n.*

5. *The dimension of an affine $\Bbbk$-algebra, $\Bbbk[x_1,\ldots,x_n]/\mathfrak{a}$, is always finite.*

Using the definition of Krull dimension one can easily prove the following characterization for zero-dimensional sets.

Proposition 2.29 *Let $V \subseteq \mathbb{A}^n_{\Bbbk}$ be a nonempty subset. Then* $\operatorname{kdim}(V) = 0$ *if and only if V is finite.*

Definition 2.25 is not an algorithmic definition for Krull dimension and it is difficult to compute the dimension of an affine variety from it. Therefore, several equivalent definitions have been proposed for the Krull dimension of an affine algebra (equal to the dimension of the corresponding affine variety for an algebraically closed field) and we look at three of these definitions in this section. These definitions not only give us computational methods but also provide an algorithmic interpretation for Krull dimension. For a detailed description of these equivalent definitions and how these three different notions of dimension fit in the dimension theory of affine varieties, the reader can refer to (Kreuzer and Robbiano, 2005, Section 5.6, 5.7).

2.4.1 Transcendence degree of an affine $\Bbbk$-algebra

Definition 2.30 *Let $\mathcal{A}$ be a $\Bbbk$-algebra and $d \in \mathbb{N}$.*

1. *A subset of $\mathcal{A}$, $\{a_1, \ldots, a_d\}$, of size d is said to be algebraically independent over $\Bbbk$ if for all nonzero polynomials $f \in \Bbbk[y_1, \ldots, y_d]$ we have $f(a_1, \ldots, a_d) \neq 0$.*

2. *Let $K/\Bbbk$ be a field extension. A set of d elements $r_1, \ldots, r_d \in K$ is called a (finite) transcendence basis of $K/\Bbbk$ if $\{r_1, \ldots, r_d\}$ is algebraically independent over $\Bbbk$ and there exists no element $r_{d+1} \in K \setminus \{r_1, \ldots, r_d\}$ such that $\{r_1, \ldots, r_{d+1}\}$ is algebraically independent over $\Bbbk$.*

Note that if a field extension $K/\Bbbk$ has a finite transcendence basis then all transcendence bases of $K/\Bbbk$ have the same number of elements.

Definition 2.31 *Let $K/\Bbbk$ be a field extension for which there exists a finite transcendence basis, $\{r_1, \ldots, r_d\}$. Then* $\operatorname{trdeg}_{\Bbbk}(K) = d$ *is called the transcendence degree of $K/\Bbbk$. If there is no finite basis,* $\operatorname{trdeg}_{\Bbbk}(K) = \infty$.

The result below gives the relation between algebraic independence and the dimension of an affine $\Bbbk$-algebra.

Proposition 2.32 *Let $\mathfrak{a}$ be a proper ideal in $\Bbbk[x_1, \ldots, x_n]$.*

1. *The maximal number of algebraically independent elements in* $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ *over* $\Bbbk$ *is equal to the Krull dimension of* $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$.

2. *If* $\mathfrak{a}$ *is a prime ideal, let* $\mathrm{Quot}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$ *be the field of fractions of* $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. *Then the transcendence degree of* $\mathrm{Quot}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$ *over* $\Bbbk$ *is equal to the Krull dimension of* $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. *For an arbitrary proper ideal* $\mathfrak{a}$, *the maximal dimension of an isolated prime ideal associated with* $\mathfrak{a}$ *gives the Krull dimension of* $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$.

The above proposition can be proved in many ways. Kemper (2011) proves it directly by showing that a maximal set of algebraically independent elements in $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ over $\Bbbk$ gives rise to a maximal chain of prime ideals in $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. Whereas, Kreuzer and Robbiano (2005) first prove that the cardinality of a maximal set of algebraically independent elements is equal to the degree of the Hilbert polynomial of $\mathfrak{a}$ and then show that the latter is equal to the Krull dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. We will discuss the relation between the degree of the Hilbert polynomial and dimension of an affine $\Bbbk$-algebra in Section 5.3.

Using the notion of algebraically independent elements of a $\Bbbk$-algebra we can characterize zero-dimensional ideals. The following result gives a characterization for zero-dimensional ideals in $\Bbbk[x_1, \ldots, x_n]$, that they have a finite $\Bbbk$-vector space basis for $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$.

Theorem 2.33 *Let* $\mathcal{A} \neq \{0\}$ *be an affine* $\Bbbk$*-algebra. Then the following statements are equivalent:*

1. $\mathrm{kdim}(\mathcal{A}) = 0$.

2. $\mathcal{A}$ *is algebraic over* $\Bbbk$.

3. *The dimension of the corresponding* $\Bbbk$*-vector space is finite.*

For an algebraically closed field, Theorem 2.29 is equivalent to the above result. This is the reason why in Chapter 1 we refer to ideals with a finite set of solutions as zero-dimensional ideals. Since the above theorem and Theorem 2.29 are equivalent to Conditions (1) and (3) of Theorem 2.6 for algebraically closed fields, we have a Gröbner basis characterization for zero-dimensional affine varieties and affine $\Bbbk$-algebras.

2.4.2 Combinatorial dimension of an affine $\Bbbk$-algebra

The concepts of maximal independent sets of variables modulo an ideal and the combinatorial dimension of the associated residue class polynomial ring give a simple yet powerful approach to computing the dimension of affine varieties. Kredel and Weispfenning (1988) first introduced these concepts and proposed a Gröbner basis algorithm to generate the maximal independent

sets of variables modulo an ideal. Combinatorial dimension is the largest number of elements among the maximal sets of variables independent modulo the ideal. These concepts have geometric interpretations for they can be used to determine independent sets and the dimensions of isolated prime ideals associated with $\mathfrak{a}$. But the most important application of combinatorial dimension is that it gives a fast and simple algorithm to compute the Krull dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. In fact, the algorithm is faster than the Hilbert polynomial method that we describe in Section 2.4.3, for Gröbner bases computed from a lexicographic monomial order.

Definition 2.34 (Combinatorial Dimension) *Let $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ 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 $\mathfrak{a} \cap \Bbbk[X] = \{0\}$. 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 $\Bbbk[x_1, \ldots, n]/\mathfrak{a}$, denoted as* $\operatorname{cdim}(\Bbbk[x_1, \ldots, n]/\mathfrak{a})$.

For an independent set Y modulo $\mathfrak{a}$, the canonical $\Bbbk$-algebra homomorphism $\Bbbk[Y] \to \Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ has to be injective.

Theorem 2.35 *Let $\mathfrak{a}$ be a proper ideal in $\Bbbk[x_1, \ldots, x_n]$. Then,*

$$\operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}) = \operatorname{kdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}).$$

Kredel and Weispfenning (1988) proves this result by showing that the $\operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$ is equal to the maximal number of algebraic independent elements in $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ over $\Bbbk$ which in turn is equal to the Krull dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ (Theorem 2.32). It can also be proved by using Hilbert polynomials (Kreuzer and Robbiano, 2005).

The reason to study combinatorial dimension of an affine $\Bbbk$-algebra instead of Krull dimension is because the former can be computed using Gröbner basis methods. Before we give the algorithm, we state some results that will help us validate the steps of the algorithm. The Krull dimension of an ideal $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$, is the maximal Krull dimension of an isolated prime ideal associated with $\mathfrak{a}$. The same is true for combinatorial dimension as well.

Lemma 2.36 *Let $\mathfrak{a}$ be an ideal in $\Bbbk[x_1, \ldots, x_n]$. Then* $\operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$ *is the maximum of* $\operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{p})$*, where $\mathfrak{p}$ is an isolated prime ideal associated with $\mathfrak{a}$.*

Proposition 2.37 *Let $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ be a prime ideal. Then, all maximal set of indeterminates independent modulo $\mathfrak{a}$ have the same cardinality.*

It turns out that to apply the theory of Gröbner bases to compute the independent set of variables modulo an ideal we need to modify the concept of independence modulo $\mathfrak{a}$ to include monomial order.

Definition 2.38 *Let $S \subseteq X$ be a set of indeterminates and $\prec$ be a monomial order in $\Bbbk[x_1, \ldots, x_n]$. Then, $\Bbbk[S/(X \setminus S)]$ denotes the following set,*

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

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

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

Example 2.39 *Let $\mathfrak{a} = \langle y - x \rangle$ be an ideal in $\Bbbk[x, y]$ and consider a monomial order $x \prec y$. Then $S = \{y\}$ is independent but not strongly independent modulo $\mathfrak{a}$.*

We now seek to determine the conditions by which we can conclude that a maximal set of indeterminates that is strongly independent modulo $\mathfrak{a}$ is also maximal independent modulo $\mathfrak{a}$. We define a special type of maximal strongly independent set, the Left Basic Set of an ideal, $\mathfrak{a}$.

Definition 2.40 (Left Basic Set (LBS)) *Let $\prec$ be a monomial order in $\Bbbk[x_1, \ldots, x_n]$ and $\mathfrak{a}$ be an ideal in $\Bbbk[x_1, \ldots, x_n]$. Given the set of indeterminates, X, we define $S_k \subseteq X, 0 \leq k \leq n$ inductively as,*

$$S_0 = \phi$$

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

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

S_n is maximal strongly independent modulo $\mathfrak{a}$ with respect to $\prec$. For lexicographic ordering, we have the following result for prime ideals.

Corollary 2.41 *Let $\mathfrak{a}$ be a prime ideal in $\Bbbk[x_1, \ldots, x_n]$, $\prec$ be a lexicographic ordering and S be the left basic set of $\mathfrak{a}$ w.r.t. $\prec$. Then S is maximal independent modulo $\mathfrak{a}$ and so $|S| = \mathrm{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$.*

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

Theorem 2.42 *Let $\mathfrak{a}$ be a proper ideal in $\Bbbk[x_1, \ldots, x_n]$ and $\prec$ be a lexicographic monomial order. Let*

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

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

We now show how Gröbner bases can be used to build a left basic set.

Theorem 2.43 *Let $\prec$ be a monomial ordering in $\Bbbk[x_1, \ldots, x_n]$ and $S \subseteq X$ be a set of indeterminates. Let G be a Gröbner basis of an ideal, $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ w.r.t. $\prec$. Then S is strongly independent modulo $\mathfrak{a}$ w.r.t. $\prec$ if and only if $\Bbbk[S] \cap \operatorname{lt}(G) = \phi$.*

Corollary 2.44 *Let $\prec$ be a monomial order in $\Bbbk[x_1, \ldots, x_n]$ and G be a Gröbner basis of an ideal $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ w.r.t. $\prec$. Algorithm 2 determines the left basic set of $\mathfrak{a}$ w.r.t. $\prec$.*

Algorithm 2 Finding the Left Basic Set of an ideal $\mathfrak{a}$ in $\Bbbk[x_1, \ldots, x_n]$

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

The below theorem illustrates how we can compute the combinatorial dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ for lexicographic monomial orders. This simple Gröbner basis algorithm gives us a powerful and fast technique to compute the Krull dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$.

Theorem 2.45 *Let $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal and G be its Gröbner basis w.r.t. a lexicographic monomial ordering, $\prec$. Let $S \subseteq X$ be a set of indeterminates such that*

$$\operatorname{Mon}(\Bbbk[S]) \cap \operatorname{lt}(G) = \phi,$$

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 $|S| = \operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$.

2.4.3 Hilbert polynomials and Krull dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$

From Theorem 2.33 we have that a positive dimensional $\Bbbk$-algebra is always an infinite dimensional $\Bbbk$-vector space. We can divide this infinite dimensional vector space into pieces of finite dimensional vector spaces, ordered by total degrees of a polynomial. The idea behind Hilbert series is to study the structure of the residue class polynomial ring by looking at these finite dimensional pieces. The relevance of Hilbert series is due to its links to the Krull dimension of the affine $\Bbbk$-algebra. Hilbert series can be computed by a Gröbner basis algorithm, thus giving us a new and fast algorithm to compute the Krull dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$.

Proposition 2.46 *Let $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal and $\mathcal{A} = \Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ be the corresponding affine $\Bbbk$-algebra. For d, a nonnegative integer, define*

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

Then, $\mathcal{A}_{\leq d}$ is a finite dimensional $\Bbbk$-vector space.

The Hilbert function, $h_{\mathfrak{a}} : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$, is defined as

$$h_{\mathfrak{a}}(d) = \dim_{\Bbbk}(\mathcal{A}_{\leq d}).$$

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 2.47 *(Hilbert series of a principal ideal) If $\mathfrak{a} = \langle f \rangle \subseteq \Bbbk[x_1, \ldots, x_n]$ is a principal ideal, then*

$$H_{\mathfrak{a}}(t) = \frac{1 - t^{\deg(f)}}{(1-t)^{n+1}} \quad \text{if } f \neq 0 \text{ and}$$
$$H_{\mathfrak{a}}(t) = \frac{1}{(1-t)^{n+1}} \quad \text{if } f = 0.$$

To give a Gröbner basis algorithm to compute the Hilbert series of an ideal one needs to first determine the relation between the Hilbert series of an ideal and the Hilbert series of its leading term ideal.

Theorem 2.48 *Let* $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ *be an ideal and* $\prec$ *be a degree compatible monomial ordering. Then,*

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

The algorithm listed below gives a Gröbner basis method to calculate the Hilbert series of an ideal in $\Bbbk[x_1, \ldots, x_n]$.

Algorithm 3 Computing the Hilbert series of an ideal, $\mathfrak{a}$ in $\Bbbk[x_1, \ldots, x_n]$.

Input A degree compatible monomial ordering $\prec$,
$G = \{g_1, \ldots, g_s\}$, a 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
$J = \langle m_2, \ldots, m_s \rangle$ and
$J' = \langle \operatorname{lcm}(m_1, m_2), \ldots, \operatorname{lcm}(m_1, m_s) \rangle$.
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

For the proof of correctness and termination of the algorithm, one can refer to (Kemper, 2011, Theorem 11.9). The Hilbert-Serre theorem follows as a natural consequence of the above algorithm.

Corollary 2.49 (Hilbert-Serre theorem) *(Kemper, 2011, Corollary 11.10) Let $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal. 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,

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

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

We now give the key result of this section, the relation between Hilbert polynomials and the Krull dimension of the residue class polynomial ring over $\Bbbk$.

Theorem 2.50 *Let $\mathcal{A} = \Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ be an affine $\Bbbk$-algebra and $p_{\mathfrak{a}}$ be the Hilbert polynomial of $\mathfrak{a}$. Then,*

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

The above result can be proved using Noether normalization lemma and the notion of algebraically independent elements of $\mathcal{A}$ over $\Bbbk$ (Kemper, 2011). On the other hand, one can also

prove the result by determining a maximal chain of prime ideals in $\mathcal{A}$ (Kreuzer and Robbiano, 2005).

2.4.4 Hilbert polynomials and combinatorial dimension

Let $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal. We prove the equivalence of the combinatorial dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ and the degree of Hilbert polynomial of $\mathfrak{a}$ using the concept of 'translate' (O'Shea et al., 2007, Section 2, Chapter 9). Since the ideal, $\mathfrak{a}$ and the leading term ideal, $\langle \mathrm{lt}(\mathfrak{a}) \rangle$, have the same Hilbert function, it is enough to study Hilbert functions for monomial ideals. In a study of monomial ideals in general, it does not make sense to specify the monomial ordering and therefore it is never stated. But the monomial ideals that we consider here are leading term ideals and they are constructed assuming a degree compatible ordering.

Definition 2.51 *For each monomial ideal $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$, let*

$$\mathcal{C}(\mathfrak{a}) = \{u \in \mathrm{Mon}(\Bbbk[x_1, \ldots, x_n]) : u \notin \mathfrak{a}\}$$

be the set of standard monomials of $\mathfrak{a}$, i.e. the set of monomials not in $\mathfrak{a}$.

For any two sets $S_1, S_2 \subseteq \mathrm{Mon}(\Bbbk[x_1, \ldots, x_n])$, define the product as $S_1 S_2 = \{u \cdot v : u \in S_1, v \in S_2\}$.

Definition 2.52 *For every integer $r = 1, \ldots, n$, every set of indeterminates $\{x_{i_1}, \ldots, x_{i_r}\} \subseteq \{x_1, \ldots, x_n\}$, and every $u \in \mathrm{Mon}(\Bbbk[x_1, \ldots, x_n])$, the set of monomials*

$$\{u\} \cdot \mathrm{Mon}(\Bbbk[x_{i_1}, \ldots, x_{i_r}])$$

is called a translate of dimension r. Also, by convention, every singleton set $\{u\} \subseteq \mathrm{Mon}(\Bbbk[x_1, \ldots, x_n])$ is called a translate of dimension 0.

We give below the key results that connect the degree of the Hilbert polynomial with the combinatorial dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. Proofs for all these results can be found in (Winkler, 2010).

Theorem 2.53 *If $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ is a monomial ideal, then $\mathcal{C}(\mathfrak{a})$ can be written as a finite disjoint union of translates.*

Lemma 2.54 *Let $u \in \mathrm{Mon}(\Bbbk[x_1, \ldots, x_n])$ and $t = \deg(u)$.*

(i) The number of monomials of degree $\leq s$ in the translate $\{u\} \cdot \mathrm{Mon}(\Bbbk[x_1, \ldots, x_m])$ is equal to the binomial coefficient, $C(m + s - t, s - t)$, provided $s \geq t$.

(ii) For $s \geq t$, the number of monomials is a polynomial function of s of degree m and the coefficient of s^m is $1/m!$.

Theorem 2.55 *If $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ is a proper monomial ideal, then for all s sufficiently large, the number of monomials not in $\mathfrak{a}$ of degree $\leq s$ is a polynomial of degree d in s. This degree, d is equal to the combinatorial dimension of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. Also, the coefficient of s^d in the polynomial is positive.*

The polynomial in the above theorem is the Hilbert polynomial and so far we have shown that given a monomial ideal, the degree of the Hilbert polynomial is the same as the combinatorial dimension. We have also seen that with respect to a degree compatible ordering, the Hilbert functions of both the ideal and the leading term ideal are the same. The below result states that for any arbitrary ideal, $\mathfrak{a}$, $\operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$ is equal to the degree of the Hilbert polynomial of $\mathfrak{a}$.

Theorem 2.56 *Let $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal, $\prec$ be a degree compatible ordering and $\mathcal{A}$ be the residue class polynomial ring, $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. Then, $\operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$ equals the degree of the Hilbert polynomial of $\mathfrak{a}$.*

Proof: Let d be the combinatorial dimension of $\mathfrak{a}$. Let the set $\{x_{i_1}, \ldots, x_{i_d}\}$ be a set of independent indeterminates modulo $\mathfrak{a}$ of maximal cardinality. Let s be a nonnegative integer. Then, the residue classes of $\operatorname{Mon}(A[x_{i_1}, \ldots, x_{i_d}])_{\leq s}$ is a linearly independent subset of $\mathcal{A}_{\leq s}$. By Lemma 2.54, $C(d+s, s) \leq h_{\mathfrak{a}}(s)$. Since the binomial coefficient is a polynomial function in s of degree d, the $\operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$ is at most the degree of the Hilbert polynomial.

Let $\langle \operatorname{lt}(\mathfrak{a}) \rangle$ be the leading term ideal of $\mathfrak{a}$ with respect to $\prec$. If $X = \{x_{i_1}, \ldots, x_{i_k}\} \subseteq \{x_1, \ldots, x_n\}$ is not independent modulo $\mathfrak{a}$, then there exists a nonzero polynomial, $f \in \mathfrak{a} \cap \Bbbk[x_{i_1}, \ldots, x_{i_k}]$. We have, $\operatorname{lm}(f) \in \langle \operatorname{lt}(\mathfrak{a}) \rangle \cap A[x_{i_1}, \ldots, x_{i_k}]$. This implies X is not independent modulo $\langle \operatorname{lt}(\mathfrak{a}) \rangle$. Therefore, the set of independent indeterminates modulo $\langle \operatorname{lt}(\mathfrak{a}) \rangle$ is a subset of the set of independent indeterminates modulo $\mathfrak{a}$. Therefore, $\operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\langle \operatorname{lt}(\mathfrak{a}) \rangle) \leq \operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$. By Theorem 2.48 and Theorem 2.55, we have that the degree of the Hilbert polynomial is at most $\operatorname{cdim}(\Bbbk[x_1, \ldots, x_n]/\mathfrak{a})$. □

2.5 Gröbner Bases for Polynomial Rings over Rings

In this section we give a brief description on how to generalize the theory of Gröbner bases to polynomial rings over a Noetherian commutative ring, A. This generalization is not straightforward as one needs to take into account nonunits and zero divisors in rings. Indeed, many results do not hold in $A[x_1, \ldots, x_n]$ and basic definitions need to be modified to accommodate

the ideals of coefficients in A. Even though several approaches have been proposed to extend the theory of Gröbner bases to polynomial rings over rings, only a small set of properties have been studied in depth. We describe below the existing Gröbner basis theory developed for $A[x_1, \ldots, x_n]$. For a more detailed description, the reader can refer to (Adams and Loustaunau, 1994, Chapter 4).

2.5.1 Basic definitions

The notion of "divisibility" of leading terms is inherently present in all the concepts that make use of Gröbner bases in polynomial computations. In the case of fields, divisibility does not differentiate between dividing with leading terms or leading monomials. This is not true in the case of $A[x_1, \ldots, x_n]$.

Consider the reduction of a polynomial f with a nonzero polynomial g in $\Bbbk[x_1, \ldots, x_n]$. We say that $f \xrightarrow{g} h$ if and only if $\mathrm{lm}(g)$ divides a term in f. By convention, reduction in rings is confined only to the leading terms of f, i.e. we reduce f to h by g if the leading term of f is divisible by the leading term of g, not if any term is divisible by $\mathrm{lt}(g)$. This makes reduction simpler and with this definition most Gröbner basis concepts can be extended from fields to rings without any changes except for the concept of reduced Gröbner basis. For reduction in fields it is enough to check if the leading term of f is divisible by the leading monomial of g even though the actual reduction happens with the leading term of g. Clearly, in rings this is not a sufficient condition : $\mathrm{lc}(g)$ may not divide $\mathrm{lc}(f)$ even if $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$. One of the obvious workarounds for this problem is to include a very restrictive condition that $\mathrm{lt}(g)$ should divide $\mathrm{lt}(f)$ to the definition of reduction. Many implementations of Gröbner bases over integers, including that of `Macaulay 2` and `Sage`, define reduction in this way. However, such a definition is very restrictive and a reasonable theory can be built with it only if we assume that the ring of coefficients is a PID. Instead, we expand the definition to allow for a linear combination of leading terms of the divisor polynomials, whose leading monomials divide the leading monomial of f, to reduce f.

Definition 2.57 *Let f, h and $\{f_1, \ldots, f_s\}$, be a set of nonzero polynomials in $A[x_1, \ldots, x_n]$. We say that f reduces to h w.r.t. $\{f_1, \ldots, f_s\}$, denoted as*

$$f \xrightarrow{\{f_1, \ldots, f_s\}} h,$$

if and only if

$$h = f - (c_1 x^{\alpha_1} f_1 + \cdots + c_s x^{\alpha_s} f_s),$$

where $c_1, \ldots, c_s \in A$ *and for* $c_i \neq 0$, $\mathrm{lm}(f) = x^{\alpha_i}\mathrm{lm}(f_i)$, $i = 1, \ldots, s$ *and*

$$\mathrm{lt}(f) = c_1 x^{\alpha_1}\mathrm{lt}(f_1) + \cdots + c_s x^{\alpha_s}\mathrm{lt}(f_s).$$

The above definition ensures that $\mathrm{lm}(h) \prec \mathrm{lm}(f)$.

In this thesis, we assume some conditions about the Noetherian ring, A which are essential to the algorithms we propose. The main idea behind these assumptions is that in the ring, A, a system of linear equations over A is *solvable* (Adams and Loustaunau, 1994).

Definition 2.58 *We say that a system of linear equations is solvable in* A *if the following conditions are satisfied.*

1. *Given* $a, a_1, \ldots, a_l \in A$, *there is an algorithm to determine whether* $a \in \langle a_1, \ldots, a_l\rangle$ *and if it is, the algorithm can compute* $b_1, \ldots, b_l \in A$ *such that* $a = a_1 b_1 + \cdots + a_l b_l$.

2. *Given* $a_1, \ldots, a_l \in A$, *there is an algorithm that computes a set of generators for the* A*-module,*
$$\mathrm{Syz}(a_1, \ldots, a_l) = \{(b_1, \ldots, b_l) \in A^l : a_1 b_1 + \cdots + a_l b_l = 0\}.$$

The ring of integers, $\mathbb{Z}$, the polynomial rings over fields, $\Bbbk[y_1, \ldots, y_m]$, $\mathbb{Z}[\sqrt{-5}]$ are examples of rings that satisfy these conditions.

In the above definition, the set, $\mathrm{Syz}(a_1, \ldots, a_l)$ is called a syzygy module. A formal definition of syzygy module is given below.

Definition 2.59 *Let* A *be a Noetherian ring and* $\mathcal{I} = \langle a_1, \ldots, a_s\rangle$, *an ideal in* A. *Consider the* A*-module homomorphism,* ϕ,

$$\begin{aligned} \phi : A^s &\to \mathcal{I} \\ (b_1, \ldots, b_s) &\mapsto \sum_{i=1}^{s} b_i a_i. \end{aligned}$$

The kernel of the homomorphism is called the syzygy module of the $1 \times s$ *matrix* $\begin{bmatrix} a_1 \cdots a_s \end{bmatrix}$ *and satisfies,*

$$b_1 a_1 + \cdots + b_s a_s = 0.$$

If $\mathfrak{a} = \langle f_1, \ldots, f_s\rangle \subseteq A[x_1, \ldots, x_n]$ then $\mathrm{Syz}(f_1, \ldots, f_s)$ is a $A[x_1, \ldots, x_n]$-submodule of $A[x_1, \ldots, x_n]^s$. $\mathrm{Syz}(f_1, \ldots, f_s)$ can be viewed as the set of all solutions of the following linear equation with polynomial coefficients, f_i, $i = 1, \ldots, s$

$$f_1\chi_1 + \cdots + f_s\chi_s = 0.$$

With the modified definition of reduction (Definition 2.57), we can now state the multivariate division algorithm over A.

Theorem 2.60 *(Adams and Loustaunau, 1994, Theorem 4.1.10) Let $f, f_1, \ldots, f_s \in A[x_1, \ldots, x_n]$ with $f_1, \ldots, f_s \neq 0$ and the set $F = \{f_1, \ldots, f_s\}$. Then there is an $r \in A[x_1, \ldots, x_n]$, minimal with respect to F, such that $f \xrightarrow{F}_+ r$. Moreover, there are $h_1, \ldots, h_s \in A[x_1, \ldots, x_n]$ such that*

$$f = h_1 f_1 + \cdots + h_s f_s + r$$

with

$$\mathrm{lm}(f) = \max((\max_{1 \leq i \leq s} \mathrm{lm}(h_i)\mathrm{lm}(f_i)), \mathrm{lm}(r)).$$

If linear equations are solvable in A, then $h_1, \ldots, h_s, r$ are computable.

We are now equipped to give the definition of Gröbner bases for an ideal in $A[x_1, \ldots, x_n]$ and its equivalent characterizations.

Definition 2.61 *Let $\mathfrak{a}$ be an ideal in $A[x_1, \ldots, x_n]$ and $G = \{g_1, \ldots, g_t\}$ be a set of nonzero polynomials in $\mathfrak{a}$. G is called a Gröbner basis of an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$ if and only if*

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

Theorem 2.62 *(Adams and Loustaunau, 1994, Theorem 4.1.12) Let $\mathfrak{a}$ be an ideal in $A[x_1, \ldots, x_n]$ and let $G = \{g_1, \ldots, g_t\}$ be a set of nonzero polynomials in $\mathfrak{a}$. Then the following are equivalent.*

1. *G is a Gröbner basis.*
2. *For any polynomial $f \in A[x_1, \ldots, x_n]$ we have*

$$f \in \mathfrak{a} \text{ if and only if } f \xrightarrow{G}_+ 0.$$

3. *For $f \in \mathfrak{a}$, $f = h_1 g_1 + \cdots + h_t g_t$ for some polynomials $h_1, \ldots, h_t \in A[x_1, \ldots, x_n]$ such that $\mathrm{lm}(f) = \max_{1 \leq i \leq t}(\mathrm{lm}(h_i)\mathrm{lm}(g_i))$.*

The Gröbner basis of an ideal in $A[x_1, \ldots, x_n]$ generates the ideal. If G is a Gröbner basis and $f \in \langle G \rangle$ and $f \xrightarrow{G}_+ r$, where r is minimal, then $r = 0$. However, even if the the set of divisors in the multivariate division algorithm is a Gröbner basis the remainder is not necessarily unique unless the polynomial, f, is in the ideal. This is one of the key differences of Gröbner bases over rings from fields.

Example 2.63 *Consider the ideal, $\langle 2x^2, 3y^2 + x^2\rangle$ in $\mathbb{Z}[x, y]$. The generators form a Gröbner basis, G, for the ideal with respect to deglex ordering with $x \prec y$. Let $f = 6x^2y^2 - x^4$. If we reduce f with G we get two different remainders for two different sequence of divisors, which is given below.*

$$\begin{array}{rl} h_1: & 3y^2 \\ h_2: & 0 \\ f_1: 2x^2 & \\ f_2: 3y^2 + x^2 & \sqrt{6x^2y^2 - x^4} \\ & \underline{\quad 6x^2y^2 \quad} \\ & -x^4 \end{array}$$

$$\begin{array}{rl} h_1: & 0 \\ h_2: & 2x^2 \\ f_1: 2x^2 & \\ f_2: 3y^2 + x^2 & \sqrt{6x^2y^2 - x^4} \\ & \underline{\quad 6x^2y^2 + 2x^4 \quad} \\ & -3x^4 \end{array}$$

2.5.2 Computation of Gröbner bases

We state below the Buchberger criterion for rings. The criterion is the same for rings and fields, but in the case of rings, the syzygy modules are submodules of $(A[x_1, \ldots, x_n])^s$.

Theorem 2.64 *(Adams and Loustaunau, 1994, Theorem 4.2.3) Let $G = \{g_1, \ldots, g_t\}$ be a set of nonzero polynomials and $\mathcal{B}$ a homogeneous generating set for $\mathrm{Syz}(\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t))$. Then G is a Gröbner basis for the ideal $\langle g_1, \ldots, g_t\rangle$ if and only if for all $(h_1, \ldots, h_t) \in \mathcal{B}$ we have*

$$h_1g_1 + \cdots + h_tg_t \xrightarrow{G}_+ 0.$$

For the case when $A = \Bbbk$ the above statement of the theorem for $\Bbbk[x_1, \ldots, x_n]$ is different from the statement given in Theorem 2.2. But they are equivalent because each element of $\mathcal{B}$ gives rise to an S-polynomial (Adams and Loustaunau, 1994, Proposition 3.2.3, Corollary 3.2.6). In fields, the S-polynomials give us the homogeneous generating set of the syzygy module. Below, we describe the construction of $\mathcal{B}$ for rings.

Definition 2.65 *For any subset $J \subseteq \{1, \ldots, s\}$, let $x^{\alpha_J} = \mathrm{lcm}(x^{\alpha_j} : j \in J)$. We say that J is saturated with respect to $x^{\alpha_1}, \ldots, x^{\alpha_s}$, provided that for all $j = 1, \ldots, s$, if $x^{\alpha_j} \mid x^{\alpha_J}$, then $j \in J$.*

The below theorem gives a construction for a homogeneous generating set for $\mathrm{Syz}(c_1 x^{\alpha_1}, \ldots, c_s x^{\alpha_s})$.

Theorem 2.66 *(Adams and Loustaunau, 1994, Theorem 4.2.6) For each set $J \subseteq \{1, \ldots, s\}$, which is saturated with respect to $x^{\alpha_1}, \ldots, x^{\alpha_s}$, let $\mathcal{B}_J = \{b_{1J}, \ldots, b_{\nu_J J}\}$ be a generating set for the A-module of syzygies $\mathrm{Syz}(c_j : j \in J)$. (Each $b_{\nu J}$ is in the A-module $A^{|J|}$). For each such $b_{\nu J}$, denote its j th coordinate by ${b_{\nu J}}^{(j)}$. Set*

$$s_{\nu J} = \sum_{j \in J} {b_{\nu J}}^{(j)} \frac{x^{\alpha_J}}{x^{\alpha_j}} e_j,$$

where $s_{\nu J}$ is an element in $(A[x_1, \ldots, x_n])^s$. Then the set of vectors $s_{\nu J}$, for J ranging over all such saturated subsets of $\{1, \ldots, s\}$ and $1 \leq \nu \leq \nu_J$, forms a homogeneous generating set for the syzygy module $\mathrm{Syz}(c_1 x^{\alpha_1}, \ldots, c_s x^{\alpha_s})$.

The set of vectors $\{s_{\nu J}\}$ plays the same role over rings as S-polynomials do over fields. We give below a basic description of the algorithm for computing a Gröbner basis in $A[x_1, \ldots, x_n]$.

Algorithm 4 Computing the Gröbner basis of an ideal, $\mathfrak{a} = \langle f_1, \ldots, f_s \rangle$ in $A[x_1, \ldots, x_n]$

Input $f = \{f_1, \ldots, f_s\} \subseteq A[x_1, \ldots, x_n]$ with $f_i \neq 0$ for $i = 1, \ldots, s$
Output $G = \{g_1, \ldots, g_t\}$, a Gröbner basis for the ideal generated by F
$G = \phi$, $G' = F$
while $G \neq G'$ **do**
  $G = G'$. We refer to the elements of G as $g_1, \ldots, g_t$.
  Compute $\mathcal{B}$, a homogeneous generating set for $\mathrm{Syz}(\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t))$
  for each $h = (h_1, \ldots, h_t) \in \mathcal{B}$ **do**
    Reduce $h_1 g_1 + \cdots + h_t g_t \xrightarrow{G'}_+ r$, r minimal w.r.t. G'
  end for
  if $r \neq 0$ **then**
    $G' = G' \cup \{r\}$
  end if
end while

Evidently, computing the homogeneous generating set, $\mathcal{B}$ using Theorem 2.66 is computationally the most expensive step in the algorithm. But Möller (1988) gives an efficient technique to avoid calculating duplicate syzygies. The idea is to use the already computed syzygies to compute the new syzygies.

2.5.3 Coset representatives of $A[x_1, \ldots, x_n]/\mathfrak{a}$

In this section, we give a brief outline of how to describe the coset representatives of $A[x_1, \ldots, x_n]/\mathfrak{a}$ given a set of coset representatives of coefficient ideals in A. Previously, we have seen that the reduction of a polynomial with a Gröbner basis in rings gives us a unique remainder only when the polynomial is in the ideal. This is the reason why computing the coset representatives of $A[x_1, \ldots, x_n]/\mathfrak{a}$ w.r.t. a Gröbner basis of $\mathfrak{a}$ is not straightforward.

First, we state some definitions. We say that the ring A has 'effective coset representatives' if for any ideal I in A, we can determine a complete set C of coset representatives of A/I and we have a procedure to find, for all $a \in A$, an element $c \in C$ such that $a \equiv c \mod I$. Such rings include $\mathbb{Z}$ and finite rings of the form, $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$. Consider a Gröbner basis $G = \{g_1, \ldots, g_t\}$ for an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$. With respect to the set $\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)\}$, consider the saturated subsets of $\{1, \ldots, t\}$ (Definition 2.65). Then for each saturated subset $J \subseteq \{1, \ldots, t\}$, let I_J denote the ideal of A generated by $\{\mathrm{lc}(g_i) : i \in J\}$ (if $J = \phi$ then $I_J = \{0\}$). Let C_J denote a complete set of coset representatives for A/I_J and let $J_{x^\alpha} = \{i : \mathrm{lm}(g_i) \mid x^\alpha\}$ for each monomial, x^α.

Definition 2.67 *We assume the notations from above. Given a polynomial $r \in A[x_1, \ldots, x_n]$, we say it is totally reduced if for every cx^α that is a term in r, $c \in C_{J_{x^\alpha}}$. Given two polynomials, $f, r \in A[x_1, \ldots, x_n]$, r is said to be a normal form for f if $f \equiv r \pmod{\mathfrak{a}}$ and r is totally reduced.*

The normal form depends not only on G but also on the choices of the sets of coset representatives C_J for the set of saturated subsets J. The following theorem gives us the complete set of coset representatives for $A[x_1, \ldots, x_n]/\mathfrak{a}$.

Theorem 2.68 *(Adams and Loustaunau, 1994, Theorem 4.3.3) Let G be a Gröbner basis for the nonzero ideal $\mathfrak{a}$ of $A[x_1, \ldots, x_n]$. Assume that for each saturated subset $J \subseteq \{1, \ldots, t\}$, we have chosen a complete set of coset representatives C_J for the ideal I_J. Then every $f \in A[x_1, \ldots, x_n]$ has a unique normal form.*

Let us look at an example.

Example 2.69 *Consider the ideal $\mathfrak{a}$ in $\mathbb{Z}[x, y]$ with $\{f_1, f_2, f_3, f_4, f_5\}$ as its Gröbner basis, where $f_1 = 4xy + x$, $f_2 = 3x^2 + y$, $f_3 = 5x$, $f_4 = 4y^2 + y$, $f_5 = 5y$. For any monomial, $x^\alpha \notin \{1, x, y\}$, $I_{J_{x^\alpha}} = \mathbb{Z}$ and therefore $C_{J_{x^\alpha}} = \{0\}$. For 1, we have $I_{J_1} = \{0\}$ and $C_{J_1} = \mathbb{Z}$. For x, we have $I_{J_x} = \langle 5 \rangle$ and $C_{J_x} = \mathbb{Z}_5$. For y, we have $I_{J_y} = \langle 5 \rangle$ and $C_{J_y} = \mathbb{Z}_5$. Therefore the complete set of coset representatives of $\mathbb{Z}[x, y]/\langle f_1, f_2, f_3, f_4, f_5 \rangle = \{a + bx + cy \mid a \in \mathbb{Z}, b \in \mathbb{Z}_5, c \in \mathbb{Z}_5\}$.*

2.5.4 Reduced Gröbner bases over rings

One can arrive at a definition of reduced Gröbner bases over rings analogous to that of fields, as defined in (Arnold, 2003), but it may not exist in all cases. A new definition of reduced Gröbner basis over rings is given by Pauer (2007), and it ensures the existence of a reduced Gröbner basis for any ideal in a polynomial ring over the ring, A. Henceforth, in this thesis, "reduced Gröbner basis" refers to Pauer's definition of reduced Gröbner basis unless otherwise stated. Before we proceed further we give a brief account of this concept.

We introduce the following notations and definitions. For any ideal I in A, we select a finite system, $\mathrm{Gen}(I)$ of generators of I, and a mapping η_I from A to A such that $\eta_I(0) = 0$, η_I is constant for each coset of I and for any $z \in A$ we have $\eta_I(z) \in z + I$.

Example 2.70 *Let $A = \mathbb{Z}$. Let I be an ideal generated by $a_1, \ldots, a_m$ and $a = \gcd(a_1, \ldots, a_m)$. Let $z \in \mathbb{Z}$. Then we can choose $\mathrm{Gen}(I) = \{a\}$ and $\eta_I(z) = z \bmod a$.*

Let $\mathfrak{a}$ be an ideal in $A[x_1, \ldots, x_n]$ and $\alpha \in \mathbb{N}^n$. Let G be a Gröbner basis for $\mathfrak{a}$ and let $\mathrm{lm}(G)$ denote the set of leading monomials in G. We represent the leading coefficient ideal of all polynomials in $\mathfrak{a}$ of degree α as $\langle \mathrm{lc}(\alpha, \mathfrak{a})\rangle$, i.e. $\langle \mathrm{lc}(\alpha, \mathfrak{a})\rangle = \langle \mathrm{lc}(f) : f \in \mathfrak{a}, \deg(f) = \alpha\rangle$. Similarly, the leading coefficient ideal of all polynomials in $\mathfrak{a}$ such that the leading monomial of the polynomials divide x^α is denoted as $\langle \mathrm{lc}(< \alpha, \mathfrak{a})\rangle$. We have $\langle \mathrm{lc}(< \alpha, \mathfrak{a})\rangle = \langle \mathrm{lc}(f) : f \in \mathfrak{a}, \alpha \in \deg(f) + \mathbb{N}^n, \alpha \neq \deg(f)\rangle$. We use $\mathrm{Gen}(\alpha, \mathfrak{a})$ to represent the set of all nonzero $\eta_{\langle \mathrm{lc}(<\alpha,\mathfrak{a})\rangle}(a)$, where a belongs to the set of all generators of $\langle \mathrm{lc}(\alpha, \mathfrak{a})\rangle$. We give below the definition of $\mathrm{Gen}(\alpha, \mathfrak{a})$.

Definition 2.71 *We assume notations as above. For each $x^\alpha \in \mathrm{lm}(G)$ we define,*

$$\mathrm{Gen}(\alpha, \mathfrak{a}) = \{\eta_{\langle \mathrm{lc}(<\alpha,\mathfrak{a})\rangle}(a) : a \in \mathrm{Gen}(\langle \mathrm{lc}(\alpha, \mathfrak{a})\rangle)\} \setminus \{0\}.$$

As defined above, $\eta_{\langle \mathrm{lc}(<\alpha,\mathfrak{a})\rangle}(a)$ is an element in the coset, $a + \langle \mathrm{lc}(< \alpha, \mathfrak{a})\rangle$.

We proceed now to Pauer's definition of reduced Gröbner basis over rings.

Definition 2.72 *(Pauer, 2007, Definition 17) A Gröbner basis G of $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ is a reduced Gröbner basis w.r.t. a monomial order $\prec$ iff*

(i) for all $\alpha \in \mathbb{N}^n$ such that $x^\alpha \in \mathrm{lm}(G)$, the map

$$\begin{aligned} \{g \in G : \deg(g) = \alpha\} &\longrightarrow \mathrm{Gen}(\alpha, \mathfrak{a}) \\ g &\longmapsto \mathrm{lc}(g) \end{aligned}$$

is bijective and

(ii) for all $g = \sum_{\beta \in \mathbb{N}^n} c_{\beta,g} x^\beta \in G$ *and all* $\alpha \in \mathbb{N}^n$ *with* $\alpha \neq \deg(g)$ *and* $c_{\alpha,g} \neq 0$ *we have* $c_{\alpha,g} = \eta_{\langle \mathrm{lc}(\alpha,\mathfrak{a})\rangle}(c_{\alpha,g})$.

Theorem 2.73 *(Pauer, 2007) There exists a reduced Gröbner basis for every ideal* $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$.

It can be seen that different choices of the generators for the leading coefficient ideal of each leading monomial in G, $\mathrm{Gen}(\langle \mathrm{lc}(\alpha, \mathfrak{a})\rangle)$, lead to a different $\mathrm{Gen}(\alpha, \mathfrak{a})$, which in turn lead to a different reduced Gröbner basis. Once we fix $\mathrm{Gen}(\alpha, \mathfrak{a})$ for all $x^\alpha \in \mathrm{lm}(G)$, the reduced Gröbner basis G is unique.

Theorem 2.74 *(Pauer, 2007) The reduced Gröbner basis* G *for an ideal* $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ *is unique upto* $\mathrm{Gen}(\alpha, \mathfrak{a})$ *for all* $x^\alpha \in \mathrm{lm}(G)$.

2.6 Univariate Ideal Lattices & Lattice Based Cryptography

Lattice based cryptography is one of the most sought-after areas in mathematical cryptography today. This is due to several reasons. It comes with strong worst-case/average-case security guarantees. Implementing cryptographic functions in lattice cryptography requires only simple arithmetic operations, but at the same time, it is extremely versatile, leading to several applications including the seminal cryptosystem of fully homomorphic encryption (Gentry, 2009). The fact that some lattice-based cryptosystems appear to be resistant to attacks by quantum computers is another reason for its appeal.

Ideal lattices, an important tool in lattice based cryptography, are ideals with point lattice structure as well (Lyubashevsky and Micciancio, 2006). Univariate ideal lattices, ideal lattices in $\mathbb{Z}[x]$, are well studied as they provide a compact and efficient representation for integer lattices and all the computationally hard problems in point lattice theory can be extended to them. They have been used to build provably secure signature and identification schemes (Lyubashevsky and Micciancio, 2008; Lyubashevsky, 2008) and collision resistant hash functions (Lyubashevsky and Micciancio, 2006).

2.6.1 Integer lattices

Let $\mathbb{R}^m$ be the m-dimensional Euclidean space.

Definition 2.75 *A lattice in* $\mathbb{R}^m$ *is the set*

$$\mathcal{L}(b_1, \ldots, b_n) = \{\sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z}\}$$

of all integral combinations of n *linearly independent vectors* $b_1, \ldots, b_n$ *in* $\mathbb{R}^m (m \geq n)$.

The integers n and m are called the rank and dimension of the lattice, respectively. The sequence of vectors $b_1, \ldots, b_n$ is called a lattice basis. When $n = m$, we say that $\mathcal{L}$ is full rank or full dimensional. An example of n-dimensional lattice is the set $\mathbb{Z}^n$ of all vectors with integral coordinates. In sequel, whenever we mention lattices we mean integer lattices, lattices where the basis vectors have integer coordinates. Integer lattices are additive subgroups of $\mathbb{Z}^N$, $N \in \mathbb{N}$. For a good exposition on lattices, one can refer to (Micciancio and Goldwasser, 2002).

The following parameters are associated with a lattice and describe the lattice's properties. The lattice computational problems are based on these parameters.

1. The determinant of a lattice given by a basis B of size n, denoted by $\det(\mathcal{L}(B))$, is the n-dimensional volume of the fundamental parallelepiped $\mathcal{P}(B)$ spanned by the basis vectors. The determinant is a lattice invariant, i.e. it does not depend on the basis with which we computed the determinant. If the lattice is full rank then the determinant of the lattice is the absolute value of the determinant of the basis matrix, i.e. $\det(\mathcal{L}(B)) = \det(B)$. For integer matrices, the determinant is an integer. In general, we have

   $$\det(\mathcal{L}(B)) = \sqrt{\det(B^T B)}.$$

   In this case, it is not necessarily an integer.

2. The successive minima of a lattice, $\lambda_1, \ldots, \lambda_n$ is defined as follows. Given a m-dimensional open ball of radius r centered at 0, $\mathcal{B}_m(0, r) = \{x \in \mathbb{R}^m : \|x\| \lneq r\}$, the ith minimum, λ_i, is the radius of the smallest open ball $\mathcal{B}_m(0, r)$, containing i linearly independent lattice vectors.

   $$\lambda_i(\mathcal{L}) = \inf\{r : \dim(\text{span}(\mathcal{L} \cap \mathcal{B}_m(0, r))) \geq i\}.$$

3. The minimum distance is the length of the shortest nonzero lattice vector and is the same as the minimum distance between any two distinct lattice points. It is the special case of the successive minima with $i = 1$.

   $$\lambda_1(\mathcal{L}) = \min_{x \neq y \in \mathcal{L}} \|x - y\| = \min_{x \in \mathcal{L} \setminus \{0\}} \|x\|$$

4. The covering radius of a lattice, $\rho(\mathcal{L})$, is the smallest real number such that the closed spheres of radius ρ centered around all lattice points cover the entire space, i.e. any point in span(B) is within distance ρ from the lattice.

The following observations can be easily proved.

Remark 2.76 *For any lattice $\mathcal{L}$ and target point t (in the span of the lattice) there is at most one lattice point within distance (strictly less than) $\lambda(\mathcal{L})/2$ from t.*

Remark 2.77 *For any lattice $\mathcal{L}$ and target point t (in the span of the lattice) there is at least one lattice point within distance $\rho(\mathcal{L})$ from t.*

Remark 2.78 *For any n-dimensional lattice, the successive minima $\lambda_1, \ldots, \lambda_n$ and the covering radius are related by the chain of inequalities*

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq 2\rho \leq \sqrt{n}\lambda_n.$$

An important result in lattices that gives a relation between the successive minima and the determinant of the lattice is the famous Minkowski inequality.

Theorem 2.79 (Minkowski Inequality) *For any lattice $\mathcal{L}$,*

$$\lambda(\mathcal{L}) \leq \Big(\prod_{i=1}^{n} \lambda_i(\mathcal{L})\Big)^{1/n} \leq \sqrt{\gamma_n}\det(\mathcal{L})^{1/n},$$

where $\gamma_n \leq n$ is a function of the dimension and does not depend on the specific lattice.

2.6.2 Computational problems for lattice based cryptography

Among the four fundamental parameters of the lattice, only the determinant of the lattice can be computed efficiently. Determining the minimum distance, successive minima and covering radius of a lattice efficiently are well-known hard problems. The algorithms that compute them approximately and run in polynomial time give rise to approximation factors that are exponential in the dimension of the lattice. The famous LLL-algorithm (Lenstra et al., 1982) runs in polynomial time but gives an approximation factor of $2^{(n-1)/2}$ for the shortest vector problem (SVP). The most recent algorithm to solve SVP (Ajtai et al., 2001) also achieves only an exponential approximation factor of $2^{O(n \ln \ln n/\ln n)}$. In fact, the cryptographic functions based on lattices are built under the assumption that there exists no efficient algorithm that can achieve polynomial approximation factors at most $\gamma(n) = n^{O(1)}$, at least in the worst case.

A problem is said to be hard in complexity theory if it is hard in the worst case instance. But in cryptography it is hard only if it is hard in the average case. This ensures that when we consider a key at random, no polynomial time algorithm can break the scheme with non-negligible probability. The possibility of having cryptographic applications based on lattice problems was brought to light by Ajtai (1996). The paper shows how to build cryptographic functions that are on an average as hard to break as the worst case instances of certain lattice problems. It is important that the average case hardness of the cryptographic function is based on the worst case instance of the lattice problem since many lattice approximation algorithms perform much better on an average than their worst case bounds.

We give below certain lattice problems, the hardness of solving these problems form the crux of lattice based cryptography. The approximation versions of these problems return solutions that are within some specified factor, γ, from the exact solution.

Definition 2.80 (Shortest Vector Problem (SVP)) *Given a lattice $\mathcal{L}$, find a nonzero lattice vector x such that $\|x\| \leq \|y\|$ for any other $y \in \mathcal{L}$.*

Definition 2.81 (Approximate SVP) *Given a lattice $\mathcal{L}$, find a nonzero lattice vector x such that $\|x\| \leq \gamma\|y\|$, $\gamma \in \mathbb{C}$ for any other $y \in \mathcal{L}$.*

We will mention from now onwards either the exact or the approximate version of the computational problem depending on the context. Note that the only difference is the factor of approximation, γ.

Definition 2.82 (Closest Vector Problem (CVP)) *Given a lattice $\mathcal{L}$, a target point t and a distance bound d, the closest vector problem (CVP) asks for a lattice point $v \in \mathcal{L}$ at distance $\|t - v\| \leq d$ from the target, provided such a lattice point exists. In the exact version of CVP, the distance bound is $d = \min_{v \in \mathcal{L}} \|t - v\|$ between the target and the lattice. In the approximate problem CVP_γ one sets $d = \gamma \cdot \min_{v \in \mathcal{L}} \|t - v\|$. Two special versions of the CVP are:*

1. *the bounded distance decoding problem (BDD) where $d \lneq \lambda/2$, and*
2. *the absolute distance decoding problem (ADD) where $d \geq \rho$.*

In the first case when $d \lneq \lambda/2$, if a solution exists it will be unique (See Remark 2.76). In the second case when $d \geq \rho$, a solution is always guaranteed but it is not generally unique (See Remark 2.77).

Definition 2.83 (Shortest Independent Vector Problem ($SIVP_c$)) *Given an n-dimensional lattice, $\mathcal{L}$, find n linearly independent lattice vectors, $b_1, \ldots, b_n \in \mathcal{L}$ such that $\max_i \|b_i\| \leq c\lambda_n(\mathcal{L})$. The case $c = 1$ corresponds to the exact solving of the problem.*

Note that the n linearly independent lattice vectors are not necessarily a basis for the given lattice. There are lattices such that all its bases must necessarily contain vectors that are longer than λ_n. In most applications it is enough to have a set of short linearly independent vectors and therefore this distinction is not a major concern.

A lattice based cryptosystem can be intuitively described as follows. The public key is a lattice basis B containing long vectors and the secret key S is the set of short lattice vectors.

- Encryption. A message m is encoded as an integer vector x. The function takes x and a small perturbation vector r and outputs $t = Bx + r$. The vector r should be short enough so that we can recover Bx from t using the secret basis, S. The vector x is chosen in such a way that Bx looks like a random lattice point.

- Decryption. It is based on CVP approximation algorithms. Given t, one can easily compute $S^{-1}t$. Round each coordinate to the closest integer and multiply the result by S. Since the vector r is chosen to be short enough, the recovered vector is x itself.

2.6.3 Univariate ideal lattices

When Ajtai (1996) introduced the concept of building cryptographic functions that were hard in the average case based on the worst case assumptions of lattice problems, it was considered a breakthrough. But Ajtai's discovery and subsequent work were interesting only from a theoretical point of view because of the inefficiency of the cryptographic functions built from lattices. The problem was in describing lattices as $n \times n$ matrices and that resulted in a computation time that was at least quadratic in n. Micciancio (2002) introduced efficiently computable one-way functions for a certain class of lattices called cyclic lattices (See Definition 2.85, Lemma 2.86). The algebraic representation of cyclic lattices is more compact and therefore the computation time is almost linear in n. But one-way functions are of limited use since they can only be used to prove the existence of cryptographic primitives like digital signatures and private key encryption. Lyubashevsky and Micciancio (2006) introduced the concept of ideal lattices (in one variable) and described how to create collision resistant hash functions with them, a much more useful cryptographic primitive.

An ideal lattice is an integer lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ that is also an ideal in $\mathbb{Z}[x]/\langle f \rangle$ for some monic polynomial $f \in \mathbb{Z}[x]$. We now formally define ideal lattices in one variable.

Definition 2.84 *Given a monic polynomial $f \in \mathbb{Z}[x]$, an ideal lattice is an integer lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ such that it is isomorphic, as a $\mathbb{Z}$-module, to an ideal $\mathfrak{A}$ in $\mathbb{Z}[x]/\langle f \rangle$.*

The following $\mathbb{Z}$-module homomorphism between $\mathbb{Z}[x]/\langle f\rangle$ and $\mathbb{Z}^N$, where f is a monic polynomial of degree N, further elucidates the definition of ideal lattices.

$$\begin{aligned}\phi : \mathbb{Z}[x]/\langle f\rangle &\longrightarrow \mathbb{Z}^N \\ \sum_{i=0}^{N-1} a_i x^i + \langle f\rangle &\longmapsto (a_0, \cdots, a_{N-1}).\end{aligned}$$

Clearly, ϕ is an isomorphism that implies all $\mathbb{Z}$-modules (including ideals) in $\mathbb{Z}[x]/\langle f\rangle$ are isomorphic to sublattices (subgroups) of $\mathbb{Z}^N$. Therefore, all ideals in $\mathbb{Z}[x]/\langle f\rangle$ are ideal lattices.

A special class of ideal lattices is cyclic lattices.

Definition 2.85 *A set $\mathcal{L}$ in $\mathbb{Z}^N$ is a cyclic lattice*

(i) for all $v, w \in \mathcal{L}$, $v + w$ is also in $\mathcal{L}$,

(ii) for all $v \in \mathcal{L}$, $-v$ is also in $\mathcal{L}$, and

(iii) for all $v \in \mathcal{L}$, a cyclic shift of v is also in $\mathcal{L}$.

One can easily verify the following fact.

Lemma 2.86 *A set $\mathcal{L}$ in $\mathbb{Z}^N$ is a cyclic lattice if $\phi^{-1}(\mathcal{L})$ is an ideal in $\mathbb{Z}[x]/\langle x^N - 1\rangle$.*

2.6.3.1 Computational problems for ideal lattices

For any ideal $\mathfrak{A} \subseteq \mathbb{Z}[x]/\langle f\rangle$ we use ${\lambda_i}^p(\mathfrak{A})$ to indicate ${\lambda_i}^p(\mathcal{L}(\mathfrak{A}))$. The following norms can be defined on $\mathbb{Z}[x]$: the infinity norm, $\|g\|_\infty$ that takes the maximum coefficient of all the terms in the polynomial, and the norm with respect to an ideal $\langle f\rangle \subseteq \mathbb{Z}[x]$, $\|g\|_f$, that takes the maximum coefficient of all the terms in the polynomial reduced modulo the ideal, $\langle f\rangle$.

Given a monic polynomial, f and the corresponding residue class polynomial ring, $\mathbb{Z}[x]/\langle f\rangle$, the following properties are essential for the security proofs of the hash function: (i) f should be irreducible which ensures that every ideal in $\mathbb{Z}[x]/\langle f\rangle$ is a full rank lattice, and (ii) the norm of any polynomial g with respect to the ideal $\langle f\rangle$, $\|g\|_f$, should not be much larger than $\|g\|_\infty$. The second property is formally captured with a parameter called the expansion factor.

Definition 2.87 *Let $f \in \mathbb{Z}[x]$. The expansion factor, $\mathcal{E}$ of f is defined as*

$$\mathcal{E}(f, k) = \max_{g \in \mathbb{Z}[x], \deg(g) \leq k \deg(f) - 1} \frac{\|g\|_f}{\|g\|_\infty},$$

where $k \in \mathbb{N}$.

We give the bounds for the expansion factor of certain polynomials in $\mathbb{Z}[x]$. The proofs have been skipped for brevity.

Theorem 2.88 *1.* $\mathcal{E}(x^n-1,k) \leq k$, *2.* $\mathcal{E}(x^{n-1}+x^{n-2}+\cdots+1,k) \leq 2k$, *3.* $\mathcal{E}(x^n+1,k) \leq k$, *where* $k \in \mathbb{N}$.

Definition 2.89 *The approximate Shortest Polynomial Problem (*$SPP_\gamma(\mathfrak{A})$*) is defined as follows: given an ideal* $\mathfrak{A} \subseteq \mathbb{Z}[x]/\langle f \rangle$*, where* f *is a monic polynomial, determine a* $g \in \mathfrak{A}$ *such that* $g \neq 0$ *and* $\|g\|_f \leq \gamma {\lambda_1}^{\infty}(\mathfrak{A})$.

We will use the notation $f-SPP$ for SPP restricted to ideals of the ring, $\mathbb{Z}[x]/\langle f \rangle$. The $f-SPP$ problem for any monic, irreducible f is the worst case problem studied in (Lyubashevsky and Micciancio, 2006), upon which the security of the hash functions is based. Well-known hard problems can be reduced to SPP, thus showing its hardness. Let $\mathcal{L}(f)$ denote the set of all lattices associated with $\mathbb{Z}[x]/\langle f \rangle$, where f is a monic polynomial. Then one can find a direct reduction from $\mathcal{L}(f)-SVP_\gamma$ to $\mathcal{L}(f)-SPP_\gamma$ (and also the other way around). Another hardness result gives a reduction from $\langle x^n-1\rangle - SPP_{2\gamma}$ to $\langle x^{n-1}+x^{n-2}+\cdots+1\rangle - SPP_\gamma$. This is useful because then we can establish the security of hash functions using the hardness of the shortest vector problem for cyclic lattices of prime dimension, a complexity assumption used in (Micciancio, 2002) to build one-way functions. Another problem that is reduced to SPP is the problem of finding complex numbers with small conjugates in ideals of subrings of a number field called the Smallest Conjugate Problem (SCP).

2.6.3.2 Hash functions using ideal lattices

Hash functions are keyed functions that take long strings as inputs and output short digests that have the following property : it is computationally hard to find two distinct inputs $x \neq y$ such that $f(x) = f(y)$ where f is the hash function. In (Lyubashevsky and Micciancio, 2006), a hash function is designed for ideal lattices in the ring, $R = \mathbb{Z}_p[x]/\langle f \rangle$ where $f \in \mathbb{Z}_p[x]$ is a monic, irreducible polynomial of degree n and p is an integer of order approximately n^2. Let $D = \{g \in R : \|g\|_f \leq d\}$ be a strategically chosen subset of R. The hash function family is given by $\mathcal{H}(R,D,m)$, where $m \in \mathbb{N}$. Let the expansion factor, $\mathcal{E}(f,3) \leq \eta$, for some $\eta \in \mathbb{R}$. Select m random elements $a_1,\ldots,a_m$ to form an ordered m-tuple, $(a_1,\ldots,a_m)$ from R. Then the hash function $\mathfrak{h}$ maps the elements of D^m to R as follows: if $b = (b_1,\ldots,b_m) \in D^m$, then $\mathfrak{h}(b) = \sum_{i=1}^m a_i \cdot b_i$. We have $|D^m| = (2d+1)^{nm}$ and $R = p^n$, and therefore if $m \gtrsim \frac{\log p}{\log 2d}$ then $\mathfrak{h} \in \mathcal{H}$ will have collisions. The paper shows that if there is a polynomial time algorithm that can find with nonnegligible probability a collision then SPP can be solved in polynomial time for every lattice in the the ring, R.

Theorem 2.90 *Let $\mathcal{H}(R, D, m)$ be the associated hash function family as mentioned above with $R = \mathbb{Z}_p[x]/\langle f \rangle$, $m \geq \frac{\log p}{\log 2d}$ and $p \geq 8\eta dmn^{1.5}\sqrt{\log n}$. Then, for $\gamma = 8\eta^2 dmn\log^2 n$, there is a polynomial time reduction from $f - SPP_\gamma(\mathfrak{A})$, for any ideal, $\mathfrak{A} \subseteq R$, to $Collision_{\mathcal{H}}(\mathfrak{h})$ where $\mathfrak{h}$ is chosen uniformly at random from $\mathcal{H}$.*

Let $\mathcal{C}$ be an oracle such that when given a uniformly random $\mathfrak{h} \in \mathcal{H}$, $\mathcal{C}(\mathfrak{h})$ returns a solution to $Collision_{\mathcal{H}}(\mathfrak{h})$ with nonnegligible probability in polynomial time. The paper then proceeds to give an algorithm to solve $f - IncSPP_\gamma$ when given access to the oracle, $\mathcal{C}$, where $IncSPP$ is an incremental version of the SPP problem. It can be shown that $f - SPP_\gamma \leq f - IncSPP_\gamma$ and therefore we have a reduction from $f - SPP(\mathfrak{A})$ for any ideal $\mathfrak{A}$ to $Collision_{\mathcal{H}}(\mathfrak{h})$ for any random $\mathfrak{h}$.

Chapter 3

Reduced Gröbner Bases and Macaulay-Buchberger Basis Theorem over Noetherian Rings

We have seen in the earlier chapters how the residue class polynomial ring over a field, $\Bbbk$, with its vector space and algebra structure, plays an important role in developing computational tools for algebraic problems in $\Bbbk[x_1, \ldots, x_n]$. In this chapter, we study the A-module structure of residue class polynomial rings over a Noetherian commutative ring, A. The first question that arises is whether the residue class polynomial is a free A-module or not. When $A = \Bbbk$, the corresponding residue class polynomial ring is always free but for a general Noetherian commutative ring it may not be so. Here, we give a Gröbner basis characterization for the residue class polynomial ring have a free A-module representation. The characterization allows us to extend the Gröbner basis method of computing a $\Bbbk$-vector space basis of residue class polynomial rings over a field $\Bbbk$ (Macaulay-Buchberger basis theorem) to rings, i.e. $A[x_1, \ldots, x_n]/\mathfrak{a}$, where $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ is an ideal. We give some insights into the characterization for two special cases, when $A = \mathbb{Z}$ and $A = \Bbbk[\theta_1, \ldots, \theta_m]$. We also look at extending this characterization to submodules of $A[x_1, \ldots, x_n]^m$, $m \in \mathbb{N}$. The characterization we give is the foundation of this thesis and all the other results we give rely on the free A-module structure of $A[x_1, \ldots, x_n]/\mathfrak{a}$. The results given in this chapter are also described in (Francis and Dukkipati, 2014).

In Section 3.1, we give a necessary and sufficient condition for the quotient ring, $A[x_1, \ldots, x_n]/\mathfrak{a}$ to have a free A-module representation w.r.t. a monomial order. In Section 3.2, we give the Macaulay-Buchberger basis theorem for $A[x_1, \ldots, x_n]/\mathfrak{a}$ that have a free A-module representation and also give an algorithm to compute an A-module basis. We study two special cases

of the coefficient ring, A in Section 3.3. We generalize the theory of Gröbner bases described above for polynomial rings over A to submodules in $A[x_1,\ldots,x_n]^m$, $m \in \mathbb{N}$ in Section 3.4. In Section 3.5, we extend border bases to $A[x_1,\ldots,x_n]$ directly, the characterization enables us to do so.

3.1 Characterization of $A[x_1,\ldots,x_n]/\mathfrak{a}$

Consider an ideal $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$. Let $G = \{g_i : i = 1,\ldots,t\}$ be a Gröbner basis for $\mathfrak{a}$ w.r.t. a monomial order, $\prec$. We recall a few definitions from Section 2.5. We have that, $J_{x^\alpha} = \{i : \mathrm{lm}(g_i) \mid x^\alpha, g_i \in G\}$ 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. Consider $A/I_{J_{x^\alpha}}$. We assume that the coefficient ring A has effective coset representatives. Let $C_{J_{x^\alpha}}$ represent a set of coset representatives of the equivalence classes in $A/I_{J_{x^\alpha}}$. Let $f \in A[x_1,\ldots,x_n]$. On reducing f with G we get $f = \sum_{i=1}^{m} a_i x^{\alpha_i} \bmod \langle G\rangle$, where $a_i \in A$. If $A[x_1,\ldots,x_n]/\langle G\rangle$ is a finitely generated A-module of size m, then corresponding to coset representatives, $C_{J_{x^{\alpha_1}}},\ldots,C_{J_{x^{\alpha_m}}}$, there exists an A-module homomorphism,

$$\begin{aligned} \phi : A[x_1,\ldots,x_n]/\langle G\rangle &\longrightarrow A/I_{J_{x^{\alpha_1}}} \times \cdots \times A/I_{J_{x^{\alpha_m}}} \\ \sum_{i=1}^{m} a_i x^{\alpha_i} + \langle G\rangle &\longmapsto (c_1 + I_{J_{x^{\alpha_1}}},\cdots,c_m + I_{J_{x^{\alpha_m}}}), \end{aligned} \tag{3.1}$$

where $c_i = a_i \bmod I_{J_{x^{\alpha_i}}}$ and $c_i \in C_{J_{x^{\alpha_i}}}$. Note that ϕ depends on the choice of coset representatives, $C_{J_{x^{\alpha_1}}},\ldots,C_{J_{x^{\alpha_m}}}$ and the monomial order, $\prec$.

Given a Gröbner basis G and the set of coset representatives C_J for the saturated subsets J, every $f \in A[x_1,\ldots,x_n]$ has a unique normal form (Theorem 2.68). This shows that the map, ϕ, is well-defined. The mapping ϕ is surjective by construction. Consider $f+\mathfrak{a}, g+\mathfrak{a}$ where $f,g \in A[x_1,\ldots,x_n]$. On reducing f,g with G, we get $f = \sum_{i=1}^{m} a_i x^{\alpha_i} \bmod \langle G\rangle$ and $g = \sum_{i=1}^{m} b_i x^{\alpha_i} \bmod \langle G\rangle$, where $a_i, b_i \in A$. Let $\phi(f) = (c_1 + I_{J_{x^{\alpha_1}}},\ldots,c_m + I_{J_{x^{\alpha_m}}})$ and $\phi(g) = (d_1 + I_{J_{x^{\alpha_1}}},\ldots,d_m + I_{J_{x^{\alpha_m}}})$, where $c_i = a_i \bmod I_{J_{x^{\alpha_i}}}$, $d_i = b_i \bmod I_{J_{x^{\alpha_i}}}$ and $c_i, d_i \in C_{J_{x^{\alpha_i}}}$. Let $c_i = d_i \bmod I_{J_{x^{\alpha_i}}}$ for all $i = 1,\ldots,m$. Then $c_i = d_i$ since the set of coset representatives, $C_{J_{x^{\alpha_i}}}$ is fixed. This implies, $f - g$ is an element of $\mathfrak{a}$ and $f+\mathfrak{a} = g+\mathfrak{a}$. Hence, ϕ is injective and an A-module isomorphism.

We refer to $A/I_{J_{x^{\alpha_1}}} \times \cdots \times A/I_{J_{x^{\alpha_m}}}$ as the A-module representation of $A[x_1,\ldots,x_n]/\mathfrak{a}$ 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 $i = 1,\ldots,m$. This implies $A[x_1,\ldots,x_n]/\mathfrak{a} \cong A^m$, i.e. $A[x_1,\ldots,x_n]/\mathfrak{a}$ has an A-module basis and it is free. We say that $A[x_1,\ldots,x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G (or w.r.t. $\prec$). Note that every

basis of a finitely generated free A-module is finite. If the A-module is infinitely generated, we say that it has a free A-module representation w.r.t. G (or w.r.t. $\prec$) if $I_{J_{x^\alpha}} = \{0\}$ for all $x^\alpha \notin \langle \mathrm{lm}(\mathfrak{a})\rangle$ and $I_{J_{x^\alpha}} = \{1\}$ for all $x^\alpha \in \langle \mathrm{lm}(\mathfrak{a})\rangle$.

We give below the definition of standard monomials in $A[x_1, \ldots, x_n]$, w.r.t. an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$.

Definition 3.1 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal. We call a monomial x^α in $A[x_1, \ldots, x_n]$, a standard monomial w.r.t. $\mathfrak{a}$ if none of the leading terms of the ideal divide the monomial, i.e. $x^\alpha \notin \langle \mathrm{lt}(\mathfrak{a})\rangle$.*

We present below the sufficient condition for $A[x_1, \ldots, x_n]/\mathfrak{a}$ to have a free A-module representation w.r.t. G.

Theorem 3.2 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be a nonzero ideal. Let G be a Gröbner basis for $\mathfrak{a}$ w.r.t. a monomial ordering, $\prec$. If G is monic then $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G.*

Proof: Let $G = \{g_i : i = 1, \ldots, t\}$ be a monic Gröbner basis of the ideal. For a monomial x^α, $J_{x^\alpha} = \{i : g_i \in G, \mathrm{lm}(g_i) \mid x^\alpha\}$. For a monomial x^α such that $\mathrm{lm}(g_i) \nmid x^\alpha$, for all $g_i \in G$, we have $J_{x^\alpha} = \phi$. Therefore, the leading coefficient ideal corresponding to those x^αs, $I_{J_{x^\alpha}}$ is $\{0\}$ and the set of coset representatives $C_{J_{x^\alpha}}$ for $A/I_{J_{x^\alpha}}$ is the entire ring, A. For a monomial x^α such that for some g_i, $\mathrm{lm}(g_i) \mid x^\alpha$, we have $J_{x^\alpha} \neq \phi$. Since all the $g_i \in G$ are monic, $I_{J_{x^\alpha}} = \{1\}$, and therefore the set of coset representatives consist of only 0. The only monomials that are part of the generating set therefore are monomials x^α such that $\mathrm{lm}(g_i) \nmid x^\alpha$, for all $g_i \in G$. Let $S = \{x^\alpha + \mathfrak{a} : \mathrm{lm}(g_i) \nmid x^\alpha, \forall g_i \in G\}$. Let S' be any subset of S. Consider,

$$\sum_{x^{\alpha_j}+\mathfrak{a} \in S'} b_j(x^{\alpha_j} + \mathfrak{a}) = 0, \quad b_j \in A, \quad b_j \neq 0.$$

This implies,

$$\sum_{x^{\alpha_j}+\mathfrak{a} \in S'} b_j x^{\alpha_j} + \mathfrak{a} = 0.$$

Therefore we have,

$$\sum_{x^{\alpha_j}+\mathfrak{a} \in S'} b_j x^{\alpha_j} \in \mathfrak{a}.$$

But that means $\mathrm{lt}(g_i) \mid x^{\alpha_j}$ for some j and for some $g_i \in G$, which is a contradiction. Therefore, S is a basis for $A[x_1, \ldots, x_n]/\langle G\rangle$. Thus the A-module, $A[x_1, \ldots, x_n]/\mathfrak{a}$ is free and has a free A-module representation w.r.t. G. □

Note that in the above theorem $A[x_1, \ldots, x_n]/\mathfrak{a}$ need not be finitely generated. If $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and the Gröbner basis of $\mathfrak{a}$ is monic, then there exists a $N \in \mathbb{N}$ such that $A[x_1, \ldots, x_n]/\mathfrak{a} \cong A^N$.

For the necessary condition we introduce the concept of short reduced Gröbner basis.

Definition 3.3 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal. A reduced Gröbner basis G of $\mathfrak{a}$ is called a short reduced Gröbner basis if for each $x^\alpha \in \mathrm{lm}(G)$, the length of the generating set for its leading coefficient ideal, $\mathrm{Gen}(\alpha, \mathfrak{a})$ is minimal.*

Note that the reduced Gröbner basis mentioned in the above definition is Pauer's reduced Gröbner basis (Pauer, 2007), the structure of which is described in Section 2.5.4.

Example 3.4 *Consider the ideal $\mathfrak{a}$ for which $G = \{3x^2, 5x^2, y\}$ is a Gröbner basis. Let us calculate a short reduced Gröbner basis. For the leading monomial x^2, $\mathrm{Gen}((2,0), \mathfrak{a}) = \{\gcd(3,5)\} = \{1\}$ is the generating set of minimal length. For the leading monomial y, $\mathrm{Gen}((0,1), \mathfrak{a}) = \{1\}$ is the generating set of minimal length. The short reduced Gröbner basis for the ideal is therefore $G = \{x^2, y\}$.*
Now for the same ideal $\mathfrak{a}$, let us assume that $\mathrm{Gen}(\langle \mathrm{lc}(\alpha, \mathfrak{a})\rangle)$ is taken as the same set of generators given in the basis and not their gcd. *Therefore, for the leading monomial x^2, $\mathrm{Gen}((2,0), \mathfrak{a}) = \{3, 5\}$ and for the leading monomial y, $\mathrm{Gen}((0,1), \mathfrak{a}) = \{1\}$. For each degree $\alpha \in \{(2,0), (0,1)\}$, if we look at the map between $\{g \in G : \deg(g) = \alpha\}$ and $\mathrm{Gen}(\alpha, \mathfrak{a})$ given by each element g mapping to its leading coefficient, it is a bijective map. Therefore $G = \{3x^2, 5x^2, y\}$ is a reduced Gröbner basis w.r.t. this definition of $\mathrm{Gen}(\langle \mathrm{lc}(\alpha, \mathfrak{a})\rangle)$. Thus, $\mathrm{Gen}(\alpha, \mathfrak{a})$ is a factor that determines the reduced Gröbner basis.*

We prove a lemma below that leads us to the necessary condition.

Lemma 3.5 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be a nonzero ideal and 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: Let $G = \{g_i : i = 1, \ldots, t\}$ be a short reduced Gröbner basis of the ideal, $\mathfrak{a}$. Let the leading coefficient ideals associated with G, $I_{J_{x^\alpha}}$ be either trivial or $\langle 1\rangle$. Suppose G is not monic. Choose $g \in G$ such that g is not monic and for all $g_j \in G$ such that $\mathrm{lm}(g) \neq \mathrm{lm}(g_j)$, we have $\mathrm{lm}(g_j) \nmid \mathrm{lm}(g)$. This is assured since if $g_j \in G$ and $\mathrm{lm}(g_j) \mid \mathrm{lm}(g)$ then either $\mathrm{lc}(g_j) = 1$ or $\mathrm{lc}(g_j) \neq 1$. If $\mathrm{lc}(g_j) = 1$ then g can be removed from the reduced basis, this contradicts the uniqueness of the reduced Gröbner basis. If g_j is not monic then we can choose g_j as g. Let $\mathrm{lm}(g) = r$. By assumption, $I_{J_r} = \langle 1\rangle$ or $\{0\}$. Since $J_r \neq \phi$, we have $I_{J_r} \neq \{0\}$. This

implies, $\langle \mathrm{lc}(g_i) : g_i \in G, g_i \mid r\rangle = \langle 1\rangle$. By choice of g the ideal consists of only the leading coefficients of generators g_i such that $\mathrm{lm}(g_i) = r$. Thus, we have the leading coefficient ideal of generators with the same degree as g, $\langle \mathrm{lc}(\deg(g), \mathfrak{a})\rangle = \langle 1\rangle$. The generating set of minimal length for $\langle \mathrm{lc}(\deg(g), \mathfrak{a})\rangle$, $\mathrm{Gen}(\langle \mathrm{lc}(\deg(g), \mathfrak{a})\rangle) = \{1\}$. This implies $\mathrm{Gen}(\deg(g), \mathfrak{a}) = \{1\}$, since any other set of elements from A that generate $\langle 1\rangle$ is of size strictly greater than 1 and its length is not minimal. To construct the short reduced Gröbner basis we assumed that $\mathrm{Gen}(\alpha, \mathfrak{a})$ is a generating set of minimal length. Therefore, $\mathrm{Gen}(\deg(g), \mathfrak{a}) = \{1\}$ and g is a monic polynomial, which contradicts the fact that the basis G is not monic.

To prove the other direction, suppose G is monic. For a monomial x^α, we have $J_{x^\alpha} = \{i : g_i \in G, \mathrm{lm}(g_i) \mid x^\alpha\}$. For a monomial x^α such that $\mathrm{lm}(g_i) \nmid x^\alpha$, for all $g_i \in G$, we have $J_{x^\alpha} = \phi$. This implies that the leading coefficient ideal, $I_{J_{x^\alpha}} = \{0\}$. For a monomial x^α such that $\mathrm{lm}(g_i) \mid x^\alpha$ for some $i = 1, \ldots, t$, we have $J_{x^\alpha} \neq \phi$ and $I_{J_{x^\alpha}} = \langle \mathrm{lc}(g_i) : i \in J_{x^\alpha}\rangle$. Since G is monic this implies, $I_{J_{x^\alpha}} = \langle 1\rangle$. □

We are now ready to give the necessary condition of the characterization for a finitely generated residue class polynomial ring.

Theorem 3.6 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be a nonzero ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is a finitely generated A-module and G be a short reduced Gröbner basis for $\mathfrak{a}$. If $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G, then G is monic.*

Proof: Let $G = \{g_i : i = 1, \ldots, t\}$ be a short reduced Gröbner basis of the ideal, $\mathfrak{a}$. Since $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G, there are only two possibilities for the leading coefficient ideals associated with G, $I_{J_{x^\alpha}} = \{0\}$ or $I_{J_{x^\alpha}} = \langle 1\rangle$. From Lemma 3.5, G is a monic basis. □

We state the characterization result as follows.

Proposition 3.7 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be a nonzero ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated. Let G be a short reduced Gröbner basis for $\mathfrak{a}$ w.r.t. some monomial ordering $\prec$. Then, $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G,*

$$A[x_1, \ldots, x_n]/\mathfrak{a} \cong A^N, \quad \text{for some } N \in \mathbb{N}$$

if and only if G is monic.

The necessity for $\mathrm{Gen}(\alpha, \mathfrak{a})$ to be of minimal length can be illustrated by the following example.

Example 3.8 *Consider Example 3.4. We have $\mathfrak{a} \subseteq \mathbb{Z}[x, y]$ given by its Gröbner basis, $G = \{3x^2, 5x^2, y\}$. The Gröbner basis $G = \{3x^2, 5x^2, y\}$ is a reduced Gröbner basis for the ideal*

when we select the generators for the leading coefficient ideal for each leading monomial in G, $\mathrm{Gen}(\langle \mathrm{lc}(\alpha, \mathfrak{a})\rangle)$ *as the same set given in the example. It is not a monic basis. But one can see that* $\mathbb{Z}[x, y]/\langle G\rangle$ *is free. A short reduced Gröbner basis for the same ideal* $\mathfrak{a}$*, determined by considering the* gcd *of the generators of the leading coefficient ideal of each monomial in G, is* $\{x^2, y\}$*. The generating set* $\mathrm{Gen}(\alpha, \mathfrak{a})$ *is of minimal length when the* gcd *of the generators is considered. The short reduced Gröbner basis is monic and leads us to the correct conclusion that* $\mathbb{Z}[x, y]/\langle G\rangle$ *is free.*

We give the necessary condition for a residue class polynomial ring that is not finitely generated as an A-module.

Theorem 3.9 *Let* $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ *be a nonzero ideal and* G *be a short reduced Gröbner basis of* $\mathfrak{a}$*. If* $A[x_1, \ldots, x_n]/\mathfrak{a}$ *has a free* A*-module representation w.r.t.* G*, then* G *is monic.*

Proof: By definition, if $A[x_1, \ldots, x_n]/\mathfrak{a}$ 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 3.5, G is monic. □

Thus we have the characterization result for both finite and infinitely generated residue class polynomial rings.

Theorem 3.10 *Let* $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ *be a nonzero ideal and* G *be a short reduced Gröbner basis of* $\mathfrak{a}$*.* $A[x_1, \ldots, x_n]/\mathfrak{a}$ *has a free* A*-module representation w.r.t.* G *if and only if* G *is monic.*

3.2 Macaulay-Buchberger Basis Theorem Over Rings

The Macaulay basis theorem can be extended directly from fields to rings, i.e. $S = \{x^\alpha + \mathfrak{a} : x^\alpha$ is a standard monomial, i.e. $x^\alpha \notin \langle \mathrm{lt}(\mathfrak{a})\rangle\}$ is an A-module basis for $A[x_1, \ldots, x_n]/\mathfrak{a}$ if $A[x_1, \ldots, x_n]/\mathfrak{a}$ is free. We extend below the Macaulay-Buchberger basis theorem over rings.

Theorem 3.11 (Macaulay-Buchberger Basis Theorem Over Rings) *Let* $G = \{g_1, \ldots, g_t\}$ *be a short reduced Gröbner basis for an ideal* $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$*. Suppose* G *is monic then an* A*-module basis for* $A[x_1, \ldots, x_n]/\mathfrak{a}$ *is given by* $S = \{x^\alpha + \mathfrak{a} : \mathrm{lm}(g_i) \nmid x^\alpha, i = 1, \ldots, t\}$*.*

Proof: From the characterization result we have that $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G if and only if the short reduced Gröbner basis for $\mathfrak{a}$ is monic. The proof is along the same lines as Theorem 3.2. □

In the above theorem the necessity for G to be a short reduced Gröbner basis can be explained as follows. Unlike in the case of fields, for any Gröbner basis G in $A[x_1, \ldots, x_n]$ and any $x^\alpha \in \mathbb{N}^n$, $x^\alpha \in \langle \mathrm{lt}(\mathfrak{a}) \rangle$ does not imply $\mathrm{lt}(g_i) \mid x^\alpha$, for some $g_i \in G$. If G is the short reduced Gröbner basis and $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G then each $g_i \in G$ is monic. We then have $x^\alpha \in \langle \mathrm{lt}(\mathfrak{a}) \rangle$ if and only if $\mathrm{lt}(g_i) \mid x^\alpha$, for some $g_i \in G$.

This is explained in the following example.

Example 3.12 *Consider an ideal $\mathfrak{a} \subseteq \mathbb{Z}[x, y]$ generated by the Gröbner basis, $G = \{3x^2, 5x^2, y\}$. It can be seen that $3x^2$ cannot be reduced further by $\{5x^2, y\}$. Similarly, $5x^2$ is minimal w.r.t. the set $\{3x^2, y\}$ and y is minimal w.r.t. $\{3x^2, 5x^2\}$. Therefore G is a minimal Gröbner basis. Consider the monomial x^2. It is in the ideal, $\langle \mathrm{lt}(\mathfrak{a}) \rangle$ since $x^2 = (2)(5)x^2 - (3)(3)x^2$. But none of the leading terms divide x^2, $5x^2 \nmid x^2$, $3x^2 \nmid x^2$ and $y \nmid x^2$. Now consider a short reduced Gröbner basis of the ideal, $\{x^2, y\}$. A $\mathbb{Z}$-module basis of $\mathbb{Z}[x, y]/\mathfrak{a}$ is the set of residue classes of $\{x^\alpha : x^2 \nmid x^\alpha, y \nmid x^\alpha\} = \{1 + \mathfrak{a}, x + \mathfrak{a}\}$.*

In the zero-dimensional case, Gröbner basis generalizes the notion of Gaussian elimination by generating a maximum possible triangular system of polynomial equations over a field (Theorem 2.6). We can extend this result to the case of polynomials over rings too, as shown below.

Theorem 3.13 *Let $\mathfrak{a}$ be an ideal in $A[x_1, \ldots, x_n]$ and $G = \{g_1, \ldots, g_t\}$ be a monic short reduced Gröbner basis for $\mathfrak{a}$ w.r.t. a monomial order, $\prec$. We have from the characterization that $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. G. The following statements are equivalent.*

(i) For each $i = 1, \ldots, n$, there exists $j = 1, \ldots, t$ such that $\mathrm{lm}(g_j) = x_i^\nu$ for some $\nu \in \mathbb{N}$.

(ii) The rank of the free A-module, $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finite.

Proof: (i)$\Longrightarrow$ (ii). The short reduced Gröbner basis of the ideal $\mathfrak{a}$ is monic implies that the A-module $A[x_1, \ldots, x_n]/\mathfrak{a}$ is free and the basis is the set of cosets of monomials such that none of the leading monomials of the Gröbner basis divide the monomial. Since for every $i = 1, \ldots, n$, there exists $j = 1, \ldots, t$ such that $\mathrm{lm}(g_j) = x_i^\nu$ for some $\nu \in \mathbb{N}$, there are only finitely many power products which are reduced w.r.t. G and hence the dimension of the free A-module is finite.

(ii)$\Longrightarrow$ (i). We have that the rank of the free A-module $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finite. Assume for some $i = 1, \ldots, n$ there is no $j = 1, \ldots, t$ such that $\mathrm{lm}(g_j) = x_i^\nu$ for some $\nu \in \mathbb{N}$. Then the

powers of x_i, $1, x_i, x_i^2, \ldots$ are linearly independent and therefore contradicts the finite rank of the A-module, $A[x_1, \ldots, x_n]/\mathfrak{a}$. □

Our characterization (Proposition 3.7) and the Macaulay-Buchberger basis theorem (Theorem 3.11) give rise to an algorithm to compute an A-module basis of a free residue class ring, $A[x_1, \ldots, x_n]/\mathfrak{a}$, when it is finitely generated. The correctness of the algorithm directly follows from the characterization of a free $A[x_1, \ldots, x_n]/\mathfrak{a}$ and the Macaulay-Buchberger basis theorem. The termination of the algorithm is ensured since we have a finitely generated and free A-module, $A[x_1, \ldots, x_n]/\mathfrak{a}$, which implies it has a finite basis.

Algorithm 5 Finding the A-module basis of finitely generated residue class polynomial rings over rings

Input $A[x_1, \ldots, x_n]/\mathfrak{a}$,
$G = \{g_1, \ldots, g_t\}$, a short reduced Gröbner basis of $\mathfrak{a}$,
$S \subseteq A[x_1, \ldots, x_n]/\mathfrak{a}$,
$M \subseteq \mathbb{N}^n$.
Output $S = A$-module basis of $A[x_1, \ldots, x_n]/\mathfrak{a}$.
$S = \phi$, $M = \phi$
if G is not monic **then**
  Exit.
else
  while $\mathbb{N}^n \setminus M \neq \phi$ **do**
    for each monomial $x^\alpha \in \mathbb{N}^n \setminus M$
    if $\mathrm{lm}(g_i) \mid x^\alpha$ for some $i = 1, \ldots, t$ **then**
      $M = M \cup \{x^\beta \in \mathbb{N}^n : x^\alpha \mid x^\beta\}$.
    else
      $S = S \cup \{x^\alpha + \mathfrak{a}\}$,
      $M = M \cup \{x^\alpha\}$.
    end if
  end while
end if

3.3 Special cases, $A = \mathbb{Z}$ and $A = \Bbbk[\theta_1, \ldots, \theta_m]$

Now we look at two special cases $A = \mathbb{Z}$ and $A = \Bbbk[\theta_1, \ldots, \theta_m]$. In the case of $A = \mathbb{Z}$ we make use of the fact that the ring is a PID in the proof and in the case of $A = \Bbbk[\theta_1, \ldots, \theta_m]$ we rely on the existence of a unique strong reduced Gröbner basis for any ideal in $\Bbbk[\theta_1, \ldots, \theta_m]$

(Nabeshima, 2009).

3.3.1 Special case : $A = \mathbb{Z}$

For general rings, we arrived at the conclusion that if a finitely generated A-module, $A[x_1, \ldots, x_n]/\mathfrak{a}$, has a free A-module representation w.r.t. a monomial order, $\prec$ then its short reduced Gröbner basis G w.r.t. $\prec$ is monic, by finding a contradiction to the minimality of the length of the generating set. But here we argue that if the reduced Gröbner basis is not monic then there exists some g such that $\langle \mathrm{lc}(\mathrm{deg}(g), \mathfrak{a})\rangle = \langle c\rangle$, where $c \in \mathbb{Z}$ and $c \neq 1$. But this means that the set of coset representatives for the monomial $\mathrm{lm}(g)$, $C_{J_{\mathrm{lm}(g)}}$ can never be zero. This is a contradiction to our assumption that $\mathbb{Z}[x_1 \ldots, x_n]/\mathfrak{a} \cong \mathbb{Z}^N$ w.r.t. G.

An example which illustrates the characterization is the case when the ideal in $\mathbb{Z}[x_1, \ldots, x_n]$ is a lattice ideal. A lattice ideal, $\mathfrak{a}_\mathcal{L}$ in $\Bbbk[x_1, \ldots, x_n]$ is defined as the binomial ideal generated by $\{x^{v^+} - x^{v^-}\}$ where v^+ and v^- are nonnegative with disjoint support and $v^+ - v^- \in \mathcal{L}$, where $\mathcal{L}$ is a lattice. Lattice ideals in polynomial rings over $\mathbb{Z}$ can be defined in the same way. In this case, the binomial ideal is generated over the polynomial ring, $\mathbb{Z}[x_1, \ldots, x_n]$. The generators of the ideal are binomials with the terms having opposite sign and the coefficients of both the terms equal to absolute value 1. When we compute the Gröbner basis of the ideal, at every stage of the computation – S-polynomial calculation and reduction – we add generators that are binomials with terms having opposite sign and coefficients of absolute value 1. Therefore the Gröbner basis is monic which implies that the short reduced Gröbner basis of the ideal is also monic. From the characterization we have that the quotient ring $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}_\mathcal{L}$ is free. We will now formally state the result.

Theorem 3.14 *Let $\mathcal{L}$ be a lattice and $\mathfrak{a}_\mathcal{L}$, the associated lattice ideal. Then, the quotient ring $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}_\mathcal{L}$ is a free $\mathbb{Z}$-module.*

Another application of the characterization is that we can identify ideals in $\mathbb{Z}[x_1, \ldots, x_n]$ for which all the ideals in the corresponding residue class polynomial rings are integer lattices, i.e. all ideals are ideal lattices. We formally state that below. We will discuss this in detail in Chapter 4.

Theorem 3.15 *Let $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ be an ideal. All ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ are integer lattices if and only if the short reduced Gröbner basis of $\mathfrak{a}$ for some monomial order, $\prec$, is monic.*

3.3.2 Special case : $A = \Bbbk[\theta_1, \ldots, \theta_m]$

We now consider the next special case where the coefficient ring is itself a polynomial ring over the field $\Bbbk$, $\Bbbk[\theta_1, \ldots, \theta_m]$. We consider here the definition of strong reduced Gröbner basis

defined in (Nabeshima, 2009) and give an alternate characterization for this definition as well. The strong reduced Gröbner basis defined in (Nabeshima, 2009) is specific to polynomial rings over polynomial rings.

For ease of notation, we denote the indeterminates $\theta_1, \ldots, \theta_m$ as Θ and $x_1, \ldots, x_n$ as X. In the polynomial ring $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]$, we define leading monomial, leading coefficient and leading term w.r.t. the monomial ordering on X indeterminates and we denote them as lm_X, lc_X and lt_X.

Definition 3.16 (Strong Reduced Gröbner Basis (Nabeshima, 2009)) *Let $\prec_{X,\Theta} := (\prec_1, \prec_2)$ be a block ordering, $\mathfrak{a}$ an ideal in $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]$ and G a subset of $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]$. For $e \in \mathrm{lm}_X(G)$, let $G_e = \{f \in G \mid \mathrm{lm}_X(f) = e\}$. Then a strong reduced Gröbner basis G for $\mathfrak{a}$ w.r.t. to $\prec_1$ and $\prec_2$ is a Gröbner basis for $\mathfrak{a}$ in $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]$ such that for all $p \in G$,*

(i) no term in p lies in $\langle \mathrm{lt}(G \backslash \{p\}) \rangle$ in $\Bbbk[\theta_1, \ldots, \theta_m, x_1, \ldots, x_n]$ w.r.t. $\prec_{X,\Theta}$,

(ii) no term in p lies in $\langle \mathrm{lt}_X(G \backslash \{p\}) \rangle$ in $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]$ w.r.t. $\prec_1$,

(iii) for $e \in \mathrm{lm}_X(G)$, $\mathrm{lc}_X(G_e)$ is the reduced Gröbner basis for an ideal generated by itself w.r.t. $\prec_2$ in the quotient ring $\Bbbk[\theta_1, \ldots, \theta_m]/\mathfrak{J}_e$ where $\mathfrak{J}_e$ is an ideal generated by $\mathfrak{L} = \{\mathrm{lc}_X(g) \mid g \in G \backslash G_e$ such that $\mathrm{lm}(g) \mid e\}$.

We give below the necessary and sufficient condition for a finitely generated $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]/\mathfrak{a}$ to be a free $\Bbbk[\theta_1, \ldots, \theta_m]$-module, in terms of strong reduced Gröbner basis.

Theorem 3.17 *Let $\mathfrak{a} \subseteq \Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]$ be a nonzero ideal such that $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated. Let $\prec_{X,\Theta} := (\prec_1, \prec_2)$ be a block ordering and G be the strong reduced Gröbner basis for $\mathfrak{a}$ w.r.t. $\prec_1$ and $\prec_2$. Then, $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]/\mathfrak{a}$ has a free $\Bbbk[\theta_1, \ldots, \theta_m]$-module representation w.r.t. G if and only if G is monic.*

Proof: The proof for if $G = \{g_i : i = 1, \ldots, t\}$ is a monic Gröbner basis of the ideal, $\mathfrak{a}$ w.r.t. $\prec_1$ and $\prec_2$ then $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]/\mathfrak{a}$ has a free $\Bbbk[\theta_1, \ldots, \theta_m]$-module representation w.r.t. G is same as Theorem 3.2, with $A = \Bbbk[\theta_1, \ldots, \theta_m]$. The set, $S = \{x^\alpha + \mathfrak{a} : \mathrm{lm}(g_i) \nmid x^\alpha, \forall g_i \in G\}$ forms the A-module basis. Note that in the proof, $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]/\mathfrak{a}$ need not be finitely generated. If $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated, then there exists a $N \in \mathbb{N}$ such that $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]/\mathfrak{a} \cong \Bbbk[\theta_1, \ldots, \theta_m]^N$.

Conversely, let $\mathfrak{a} \subseteq \Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]$ be an ideal such that $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]/\mathfrak{a}$ is a finitely generated $\Bbbk[\theta_1, \ldots, \theta_m]$-module and let G be the strong reduced Gröbner basis for $\mathfrak{a}$.

Assume $\Bbbk[\theta_1,\ldots,\theta_m][x_1,\ldots,x_n]/\mathfrak{a}$ has a free $\Bbbk[\theta_1,\ldots,\theta_m]$-module representation w.r.t. G, we have to prove that G is monic. In Definition 3.16 of strong reduced Gröbner basis, consider the third condition. We have, for any monomial x^α in the strong reduced Gröbner basis, $\mathrm{lc}_X(G_{x^\alpha})$ is the reduced Gröbner basis in the ring $\Bbbk[\theta_1,\ldots,\theta_m]/\mathfrak{J}_{x^\alpha}$. Suppose the strong reduced Gröbner basis G is not monic. Then, there exists a $g \in G$ such that g is not monic w.r.t. $\prec_1$ and $\mathrm{lm}(g_j) \nmid \mathrm{lm}(g)$, for all $g_j \in G$, such that $\mathrm{lm}(g_j) \neq \mathrm{lm}(g)$. Let $\mathrm{lm}_X(g) = r$. Since g is not monic, $\langle \mathrm{lc}_X(G_r)\rangle \neq 1$ in $\Bbbk[\theta_1,\ldots,\theta_m]/\mathfrak{J}_r$. But $\Bbbk[\theta_1,\ldots,\theta_m][x_1,\ldots,x_n]/\langle G\rangle \cong \Bbbk[\theta_1,\ldots,\theta_m]^N$, $N \in \mathbb{N}$, implies that $I_{J_r} = \langle 1\rangle$. This means $\langle \mathrm{lc}_X(g_i) : g_i \in G, \mathrm{lm}(g_i) \mid r\rangle = \langle 1\rangle$. But $\langle \mathrm{lc}_X(g_i) : g_i \in G, \mathrm{lm}(g_i) \mid r\rangle = \langle \mathrm{lc}_X(G_r)\rangle + \mathfrak{J}_r$. We have $\langle \mathrm{lc}_X(G_r)\rangle + \mathfrak{J}_r = \langle 1\rangle$. This means $\langle \mathrm{lc}_X(G_r)\rangle = \langle 1\rangle$ in $\Bbbk[\theta_1,\ldots,\theta_m]/\mathfrak{J}_r$ which contradicts the fact that G is not monic. Therefore G is a monic basis. □

Example 3.18 *Consider the ring $\Bbbk[a][x]$. We have a Gröbner basis $G = \{f_1, f_2\}$ where $f_1 = a^2x - a$, $f_2 = (a^3-1)x - a^2 + 1$. The set of all leading monomials in G is $\{x\}$. We have $G_x = \{f_1, f_2\}$ and $\mathrm{lc}_{\{x\}}(G_x) = \{a^2, a^3-1\}$. Since there are no other monomials other than x we have $\mathfrak{L} = \phi$, which implies $\Bbbk[a]/\mathfrak{J}_x = \Bbbk[a]$. So now as per the third condition in the definition we have that $\mathrm{lc}_{\{x\}}(G_x)$ should be a reduced Gröbner basis in $\Bbbk[a]$. The reduced Gröbner basis of $\{a^2, a^3-1\} = \{1\}$. Therefore, we compute a new polynomial g such that $\langle g\rangle = \langle G\rangle$, $\langle \mathrm{lm}_{\{x\}}(g)\rangle = \langle \mathrm{lm}_{\{x\}}(G)\rangle$ and $\mathrm{lc}_{\{x\}}(g) = \{1\}$. This $g = af_1 - f_2 = x - 1$. Thus $\{g\}$ is the strong reduced Gröbner basis and it is monic. This implies $\Bbbk[a][x]/\langle G\rangle$ is a free $\Bbbk[a]$–module.*

Now, we proceed to study how strong reduced Gröbner bases are related to short reduced Gröbner bases. Let $\prec_{X,\Theta} := (\prec_1, \prec_2)$ be a block ordering and $\mathfrak{a}$ an ideal in $\Bbbk[\theta_1,\ldots,\theta_m][x_1,\ldots,x_n]$. For each $x^\alpha \in \mathfrak{a}$, we can construct a generating set of minimal length for $\mathrm{Gen}(\alpha, \mathfrak{a})$ by taking the reduced Gröbner basis w.r.t. $\prec_2$ as the set of generators for any ideal I in $\Bbbk[\theta_1,\ldots,\theta_m]$ and for any polynomial $h \in \Bbbk[\theta_1,\ldots,\theta_m]$, by considering the mapping $\eta_I(h)$ as the normal form of h w.r.t. I and $\prec_2$. The corresponding Pauer's reduced Gröbner basis is the short reduced Gröbner basis. One can see from the below result that short reduced Gröbner basis is also the strong reduced Gröbner basis.

Proposition 3.19 *Let $\prec_{X,\Theta} := (\prec_1, \prec_2)$ be a block ordering and $\mathfrak{a} \subseteq \Bbbk[\theta_1,\ldots,\theta_m][x_1,\ldots,x_n]$ be an ideal. Let G be the short reduced Gröbner basis of $\mathfrak{a}$ constructed by taking the reduced Gröbner basis w.r.t. $\prec_2$ as the set of generators for any ideal I in $\Bbbk[\theta_1,\ldots,\theta_m]$ and for any polynomial $h \in \Bbbk[\theta_1,\ldots,\theta_m]$, by considering the mapping $\eta_I(h)$ as the normal form of h w.r.t. I and $\prec_2$. Then G is the strong reduced Gröbner basis.*

Proof: We have to prove that the short reduced Gröbner basis of $\mathfrak{a}$, $G = \{g_i : i = 1,\ldots,t\}$ satisfies that the three conditions mentioned in Definition 3.16.

(i) Suppose a term in $p \in G$ lies in $\langle \mathrm{lt}(G\backslash\{p\})\rangle$ in $\Bbbk[\theta_1,\ldots,\theta_m,x_1,\ldots,x_n]$ w.r.t. $\prec_{X,\Theta}$. Let that term be $a\theta^\beta x^\alpha$, where $a \in \Bbbk$, θ^β is a monomial in $\theta_1,\ldots,\theta_m$, $\beta \in \mathbb{Z}^m_{\geq 0}$ and $\alpha \in \mathbb{N}^n$. The coefficient of the term, $a\theta^\beta x^\alpha$ in $\Bbbk[\theta_1,\ldots,\theta_m][x_1,\ldots,x_n]$ is $a\theta^\beta$. We have, $\theta^\beta \in \langle \mathrm{lc}_X(\mathrm{lt}(G\backslash\{p\}))\rangle$. Since $\langle \mathrm{lc}_X(\mathrm{lt}(G\backslash\{p\}))\rangle$ is a monomial ideal, θ^β is divisible by $\mathrm{lc}_X(\mathrm{lt}(g_i))$ for some $g_i \in G\backslash\{p\}$. Since we have a block ordering with ordering of $\{x_1,\ldots,x_n\}$ variables taking precedence over the $\{\theta_1,\ldots,\theta_m\}$ variables, it can be seen that $\mathrm{lc}_X(\mathrm{lt}(g_i))$ is the leading monomial of the polynomial $\mathrm{lc}_X(g_i)$ in $\Bbbk[\theta_1,\ldots,\theta_m]$. Let us first look at the case when $a\theta^\beta$ is a term in the leading coefficient, $\mathrm{lc}_X(p)$. We have that $\mathrm{lc}_X(p)$ is an element of the reduced Gröbner basis of the ideal $\langle \mathrm{lc}_X(\deg(\mathrm{lc}_X(p)),\mathfrak{a})\rangle$ and therefore no term in $\mathrm{lc}_X(p)$ (including $a\theta^\beta$) can be reduced by the leading monomials of the polynomials in the reduced Gröbner basis other than itself. We therefore have a contradiction. Now we consider the case when $a\theta^\beta$ is not a term in the leading coefficient. Then we have from the definition of reduced Gröbner basis that θ^β is the normal form w.r.t. the ideal $\langle \mathrm{lc}(\deg(\theta^\beta),\mathfrak{a})\rangle$ and $\prec_2$. But since $\theta^\beta \in \langle \mathrm{lc}_X(\mathrm{lt}(G\backslash\{p\}))\rangle$, we have that the normal form is zero which is a contradiction.

(ii) Suppose a term in $p \in G$ lies in $\langle \mathrm{lt}_X(G\backslash\{p\})\rangle$ in $\Bbbk[\theta_1,\ldots,\theta_m][x_1,\ldots,x_n]$ w.r.t. $\prec_1$. Let $h(\theta) \in \Bbbk[\theta_1,\ldots,\theta_m]$ be the coefficient of that term in $\Bbbk[\theta_1,\ldots,\theta_m][x_1,\ldots,x_n]$. We have, $h(\theta) \in \langle \mathrm{lc}_X(\mathrm{lt}_X(G\backslash\{p\}))\rangle$. Let us first look at the case when $h(\theta)$ is the leading coefficient of p, $\mathrm{lc}_X(p)$. We have that $\mathrm{lc}_X(p)$ is an element of the reduced Gröbner basis of the ideal $\langle \mathrm{lc}_X(\deg(\mathrm{lc}_X(p)),\mathfrak{a})\rangle$ and therefore cannot be reduced by the leading monomials of the polynomials in the reduced Gröbner basis other than itself. We therefore have a contradiction. Now we consider the case when $h(\theta)$ is not the leading coefficient. Then we have from the definition of reduced Gröbner basis that $h(\theta)$ is the normal form w.r.t. the ideal $\langle \mathrm{lc}(\deg(h(\theta)),\mathfrak{a})\rangle$ and $\prec_2$. Since $h(\theta) \in \langle \mathrm{lc}_X(\mathrm{lt}(G\backslash\{p\}))\rangle$, we have that the normal form is zero which is a contradiction.

(iii) In short reduced Gröbner basis, for each $e \in \mathrm{lm}_X(G)$ we choose the reduced Gröbner basis for the ideal, $\langle \mathrm{lc}_X(g_i) : g_i \in G, \mathrm{lm}(g_i) \mid e\rangle$ in $\Bbbk[\theta_1,\ldots,\theta_m]$ as its generators. We have $\mathrm{lc}_X(G_e) = \{\mathrm{lc}_X(g_i) : g_i \in G, \mathrm{lm}_X(g_i) = e\}$. Since $\mathrm{lc}_X(G_e)$ is a subset of $\mathrm{Gen}(\langle \mathrm{lc}_X(g_i) : g_i \in G, \mathrm{lm}(g_i) \mid e\rangle)$, it is the reduced Gröbner basis of the ideal generated by itself in $\Bbbk[\theta_1,\ldots,\theta_m]$. In the short reduced Gröbner basis G over $\Bbbk[\theta_1,\ldots,\theta_m][x_1,\ldots,x_n]$, the coefficient of each term of a basis element is the normal form w.r.t. the ideal formed by the leading coefficients of all $g_i \in G$ such that $\mathrm{lm}(g_i)$ divides the term. Therefore, $\mathrm{lc}_X(G_e)$ is the reduced Gröbner basis of the ideal generated by itself in $\Bbbk[\theta_1,\ldots,\theta_m]/\mathfrak{J}_e$ where $\mathfrak{J}_e$ is an ideal generated by $\mathfrak{L} = \{\mathrm{lc}_X(g) \mid g \in G\backslash G_e \text{ such that } \mathrm{lm}(g) \mid e\}$.

Thus the short Gröbner basis G satisfies the three conditions of Definition 3.16, hence it is the strong reduced Gröbner basis. □

Proposition 3.20 *Let $\prec_{X,\Theta} := (\prec_1, \prec_2)$ be a block ordering and $\mathfrak{a} \subseteq \Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]$ be an ideal. Let G be the strong reduced Gröbner basis for $\mathfrak{a}$ w.r.t. $\prec_{X,\Theta}$. Then G is the short reduced Gröbner basis for $\mathfrak{a}$.*

Proof: For every ideal $\mathfrak{a}$ in $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]$ there exists a short reduced Gröbner basis. We have shown in the above proposition that the short reduced Gröbner basis is a strong reduced Gröbner basis. We have that strong reduced Gröbner basis for an ideal $\mathfrak{a}$ in $\Bbbk[\theta_1, \ldots, \theta_m][x_1, \ldots, x_n]$ is unique (Nabeshima, 2009). This implies that the strong reduced Gröbner basis G is the short reduced Gröbner basis. □

We would like to mention here that Nabeshima's strong reduced Gröbner basis should not be confused with the concept of strong Gröbner basis defined for ideals in polynomial rings over PIDs (Adams and Loustaunau, 1994). To avoid confusion, we mention the former as strong reduced Gröbner basis and the latter as strong Gröbner basis. We give below the definition of strong Gröbner basis.

Definition 3.21 *Let $G = \{g_1, \ldots, g_t\} \subseteq A[x_1, \ldots, x_n]$ be a set of nonzero polynomials. G is said to be a strong Gröbner basis for the ideal $\mathfrak{a}$ it generates, if for each $f \in \mathfrak{a}$, there exists a $g_i \in G$ such that $\mathrm{lt}(g_i) \mid \mathrm{lt}(f)$.*

The definition does not require A to be a PID but it can be easily shown that strong Gröbner bases exist only if A is a PID. In a PID, strong Gröbner bases coincide with the short reduced Gröbner bases. We give below an example to illustrate the difference between strong Gröbner basis and short reduced Gröbner basis.

Example 3.22 *Consider the polynomial ring, $\Bbbk[a_1, a_2][x]$. Let $G = \{a_1^2 x, a_2^2 x\}$ be the set of generators of an ideal in $\Bbbk[a_1, a_2][x]$. G is the short reduced Gröbner basis for the ideal since $\{a_1^2, a_2^2\}$ is the reduced Gröbner basis of the ideal it generates in $\Bbbk[a_1, a_2]$. Consider $f = (a_1^3 + a_2^3)x$. We have, $\mathrm{lt}(G) = \{a_1^2 x, a_2^2 x\}$ and $\mathrm{lt}(f) = (a_1^3 + a_2^3)x$. There exists no $g \in G$ such that $\mathrm{lt}(g) \mid \mathrm{lt}(f)$. But, $\mathrm{lt}(f) \in \langle \mathrm{lt}(G) \rangle$. Therefore, G is not a strong Gröbner basis.*

3.4 Gröbner Basis Algorithms for Modules over Noetherian Rings

We generalize the theory of Gröbner bases described above for ideals in polynomial rings over A to submodules in $A[x_1, \ldots, x_n]^m$, $m \in \mathbb{N}$. We extend Pauer's reduced Gröbner bases to submodules in $A[x_1, \ldots, x_n]^m$ and using that define short reduced Gröbner bases for submodules. This

structure is extremely useful in identifying submodules, M of $A[x_1, \ldots, x_n]^m$ that give rise to A-modules, $A[x_1, \ldots, x_n]^m/M$ that have a free A-module representation w.r.t. some monomial order, $\prec$. The generalization is an interesting mix of techniques from the theory of Gröbner bases over rings and the techniques for submodules in $\Bbbk[x_1, \ldots, x_n]^m$.

The concepts of monomial, term order and divisibility of monomials can be carried forward from $\Bbbk[x_1, \ldots, x_n]^m$. Terms are of special significance in $A[x_1, \ldots, x_n]$. It is defined as a vector of the type $c\overrightarrow{X}$ where $c \in A \setminus \{0\}$ and $\overrightarrow{X}$ is a monomial in $A[x_1, \ldots, x_n]^m$. The divisibility for terms needs to be addressed separately. Given $\overrightarrow{X} = cx^\alpha \overrightarrow{e_i}$ and $\overrightarrow{Y} = dx^\beta \overrightarrow{e_j}$, terms in $A[x_1, \ldots, x_n]^m$, we say that $\overrightarrow{X}$ divides $\overrightarrow{Y}$ if $i = j$ and cx^α divides dx^β.

Definition 3.23 *Given $\overrightarrow{f}, \overrightarrow{h} \in A[x_1, \ldots, x_n]^m$ and a set of nonzero vectors $F = \{\overrightarrow{f_1}, \ldots \overrightarrow{f_s}\}$ in $A[x_1, \ldots, x_n]^m$ we say that $\overrightarrow{f}$ reduces to $\overrightarrow{h}$ modulo F in one step denoted by*

$$\overrightarrow{f} \xrightarrow{F} \overrightarrow{h}$$

if and only if

$$\overrightarrow{h} = \overrightarrow{f} - (c_1 x^{\alpha_1} \overrightarrow{f_1} + \cdots + c_s x^{\alpha_s} \overrightarrow{f_s})$$

where $c_1, \ldots, c_s \in A$, $x^{\alpha_1}, \ldots, x^{\alpha_s}$ are monomials in $A[x_1, \ldots, x_n]$, $\mathrm{lm}(\overrightarrow{f}) = x^{\alpha_i}\mathrm{lm}(\overrightarrow{f_i})$ for all $i = 1, \ldots, s$ such that $c_i \neq 0$, and $\mathrm{lt}(\overrightarrow{f}) = c_1 x^{\alpha_1}\mathrm{lt}(\overrightarrow{f_1}) + \cdots + c_s x^{\alpha_s}\mathrm{lt}(\overrightarrow{f_s})$.

The main difference in the definition of reduction from the case of fields is that here when we consider the sum that eliminates the leading term of the vector we have to consider the coefficients of the monomial vectors as well. If we compare it with the theory of Gröbner bases over rings, the difference is that the elements that eliminate the leading term vector in $A[x_1, \ldots, x_n]^m$ come from the ring, $A[x_1, \ldots, x_n]$. We can easily extend the concept of reduction to multiple steps. Analogous to the concept of completely reduced in the case of ideals and modules over fields here we have the concept of minimal. The difference is that here we do not need all the term vectors to be reduced, only the leading term vector.

We give below the division algorithm for polynomial modules with coefficients from Noetherian rings.

Theorem 3.24 *Let $F = \{\overrightarrow{f_1}, \ldots, \overrightarrow{f_s}\}$ with $\overrightarrow{f_i} \neq \overrightarrow{0}, i = 1, \ldots, s$ be vectors in $A[x_1, \ldots, x_n]^m$. Then there is an $\overrightarrow{r} \in A[x_1, \ldots, x_n]^m$, minimal w.r.t. F such that*

$$\overrightarrow{f} \xrightarrow{F}_+ \overrightarrow{r}.$$

Moreover there are $h_1, \ldots, h_s \in A[x_1, \ldots, x_n]$ *such that*

$$\overrightarrow{f} = h_1\overrightarrow{f_1} + \cdots + h_s\overrightarrow{f_s} + \overrightarrow{r},$$

with $\mathrm{lm}(\overrightarrow{f}) = \max(\max_{1\le i\le s}(\mathrm{lm}(h_i)\mathrm{lm}(\overrightarrow{f_i})), \mathrm{lm}(\overrightarrow{r}))$.

We now define Gröbner basis for modules over rings.

Theorem 3.25 *The following statements are equivalent for a submodule* $M \subseteq A[x_1, \ldots, x_n]^m$ *and* $G = \{\overrightarrow{g_1}, \ldots, \overrightarrow{g_t}\} \subseteq M$ *with* $\overrightarrow{g_i} \neq \overrightarrow{0}, 1 \le i \le t$*:*

(i) $\mathrm{Span}_{A[x_1,\ldots,x_n]}(\mathrm{Lt}(G)) = \mathrm{Span}_{A[x_1,\ldots,x_n]}(\mathrm{Lt}(M))$.

(ii) For any vector $\overrightarrow{f} \in A[x_1, \ldots, x_n]^m$ *we have*

$$\overrightarrow{f} \in M \Longleftrightarrow \overrightarrow{f} \xrightarrow{G}_{+} \overrightarrow{0}.$$

(iii) For all $\overrightarrow{f} \in M$ *there exist* $h_1, \ldots, h_t \in A[x_1, \ldots, x_n]$ *such that*

$$\overrightarrow{f} = h_1\overrightarrow{g_1} + \cdots + h_s\overrightarrow{g_t}$$

and $\mathrm{lm}(\overrightarrow{f}) = \max_{1\le i\le t}(\mathrm{lm}(h_i)\mathrm{lm}(\overrightarrow{g_i}))$.

Definition 3.26 *A set of nonzero vectors contained in a submodule* $M \subseteq A[x_1, \ldots, x_n]^m$ *is called a Gröbner basis for* M *provided* G *satisfies any one of the three equivalent conditions of the theorem above.*

The concepts of S-polynomials and Buchberger algorithm to compute Gröbner basis in $A[x_1, \ldots, x_n]$ can be directly extended to $A[x_1, \ldots, x_n]^m$.

3.4.1 Short reduced Gröbner bases in $A[x_1, \ldots, x_n]^m$

Below, we extend Pauer's reduced Gröbner basis in $A[x_1, \ldots, x_n]$ to $A[x_1, \ldots, x_n]^m$. We introduce the following notations and definitions. For any ideal I in A, we select a finite system, $\mathrm{Gen}(I)$ of generators of I, and a mapping η_I from A to A as described in Section 2.5.4. Let M be a submodule in $A[x_1, \ldots, x_n]^m$ and $\alpha \in \mathbb{N}^n$. Let G be a Gröbner basis for M and let $\mathrm{lm}(G)$ denote the set of leading monomials in G. We represent the leading coefficient ideal of all polynomial vectors in M such that its leading monomial is of the form $\overrightarrow{X_i}$ as $\langle \mathrm{lc}(\overrightarrow{X_i}, M)\rangle$, $i = 1, \ldots, m$ i.e. $\langle \mathrm{lc}(\overrightarrow{X_i}, M)\rangle = \langle \mathrm{lc}(\overrightarrow{f}) : \overrightarrow{f} \in M, \mathrm{lm}(\overrightarrow{f}) = \overrightarrow{X_i}\rangle$. Similarly, the leading coefficient

ideal of all polynomials in M such that the leading monomial of the polynomials divide $\overrightarrow{X_i}$ is denoted as $\langle \mathrm{lc}(< \overrightarrow{X_i}, M)\rangle$. For each $\overrightarrow{X_i} \in \mathrm{lm}(G)$ we have,

$$\mathrm{Gen}(\overrightarrow{X_i}, M) = \{\eta_{\langle \mathrm{lc}(<\overrightarrow{X_i},M)\rangle}(a) : a \in \mathrm{Gen}(\langle \mathrm{lc}(\overrightarrow{X_i}, M)\rangle)\} \setminus \{0\}.$$

We proceed now to extend Pauer's definition of reduced Gröbner basis to submodules in $A[x_1, \ldots, x_n]^m$.

Definition 3.27 *A Gröbner basis G of $M \subseteq A[x_1, \ldots, x_n]^m$ is a reduced Gröbner basis w.r.t. a monomial order $\prec$ iff*

(i) for all $\overrightarrow{X_i} \in \mathbb{N}^n \overrightarrow{e_i}$, $i = 1, \ldots, m$ such that $\overrightarrow{X_i} \in \mathrm{lm}(G)$, the map

$$\begin{aligned} \{\overrightarrow{g} \in G : \mathrm{lm}(\overrightarrow{g}) = \overrightarrow{X_i}\} &\longrightarrow \mathrm{Gen}(\overrightarrow{X_i}, M) \\ \overrightarrow{g} &\longmapsto \mathrm{lc}(\overrightarrow{g}) \end{aligned}$$

is bijective and

(ii) for all $\overrightarrow{g} := \sum_{j=1}^{r} c_{j,\overrightarrow{g}} \overrightarrow{X_j} \in G$, $r \in \mathbb{N}$ and all $i = 1, \ldots, m$ such that $\overrightarrow{X_i} \neq \mathrm{lm}(\overrightarrow{g})$ and $c_{i,\overrightarrow{g}} \neq 0$ we have $c_{i,\overrightarrow{g}} = \eta_{\langle \mathrm{lc}(\overrightarrow{X_i},M)\rangle}(c_{i,\overrightarrow{g}})$.

Theorem 3.28 *There exists a reduced Gröbner basis for every submodule $M \subseteq A[x_1, \ldots, x_n]^m$.*

Proof: The proof follows from Proposition 19 in (Pauer, 2007). □

Just like in rings, different choices of the generators for $\mathrm{Gen}(\langle \mathrm{lc}(\overrightarrow{X}, M)\rangle)$, lead to different $\mathrm{Gen}(\overrightarrow{X}, M)$, which in turn lead to different reduced Gröbner bases. But the following result ensures that we can have uniqueness once we fix $\mathrm{Gen}(\overrightarrow{X}, M)$.

Proposition 3.29 *The reduced Gröbner basis G for a submodule $M \subseteq A[x_1, \ldots, x_n]^m$ is unique upto $\mathrm{Gen}(\overrightarrow{X}, M)$ for all $\overrightarrow{X} \in \mathrm{lm}(G)$.*

Definition 3.30 *Let $M \subseteq A[x_1, \ldots, x_n]^m$ be a submodule. A reduced Gröbner basis G of M is called a short reduced Gröbner basis if for each $\overrightarrow{X} \in \mathrm{lm}(G)$, the length of the generating set for its leading coefficient ideal, $\mathrm{Gen}(\overrightarrow{X}, M)$ is minimal.*

We will see in the next section that short reduced Gröbner basis helps us characterize submodules M that give rise to free A-modules, $A[x_1, \ldots, x_n]^m/M$.

3.4.2 Characterization of $A[x_1, \ldots, x_n]^m/M$

In this section we look at one of the main applications of Gröbner bases over modules - providing a characterization for a finitely generated $A[x_1, \ldots, x_n]^m/M$ to have a free A-module representation and determining its A-module basis. For the characterization we need the concept of short reduced Gröbner basis described in Definition 3.30. Consider a submodule $M \subseteq A[x_1, \ldots, x_n]^m$. Let $G = \{\overrightarrow{g_i} : i = 1, \ldots, t\}$ be a Gröbner basis for M w.r.t a monomial order, $\prec$. We have, $J_{\overrightarrow{X}} = \{i : \mathrm{lm}(\overrightarrow{g_i}) \mid \overrightarrow{X}, \overrightarrow{g_i} \in G\}$, $I_{J_{\overrightarrow{X}}} = \langle\{\mathrm{lc}(\overrightarrow{g_i}) : i \in J_{\overrightarrow{X}}\}\rangle$ and $C_{J_{\overrightarrow{X}}}$ represents a set of coset representatives of the equivalence classes in $A/I_{J_{\overrightarrow{X}}}$. We refer to $I_{J_{\overrightarrow{X}}}$ as the leading coefficient ideal w.r.t. G. If $A[x_1, \ldots, x_n]^m/M$ is a finitely generated A-module of size s, then corresponding to coset representatives, $C_{J_{\overrightarrow{X_1}}}, \ldots, C_{J_{\overrightarrow{X_s}}}$, there exists an A-module isomorphism,

$$\begin{aligned} \phi : A[x_1, \ldots, x_n]^m/M &\longrightarrow A/I_{J_{\overrightarrow{X_1}}} \times \cdots \times A/I_{J_{\overrightarrow{X_s}}} \\ \sum_{i=1}^{m} a_i \overrightarrow{X_i} + M &\longmapsto (c_1 + I_{J_{\overrightarrow{X_1}}}, \cdots, c_s + I_{J_{\overrightarrow{X_s}}}), \end{aligned} \tag{3.2}$$

where $c_i = a_i \bmod I_{J_{\overrightarrow{X_i}}}$ and $c_i \in C_{J_{\overrightarrow{X_i}}}$. We refer to $A/I_{J_{\overrightarrow{X_1}}} \times \cdots \times A/I_{J_{\overrightarrow{X_s}}}$ as the A-module representation of $A[x_1, \ldots, x_n]^m/M$ w.r.t. G (or $\prec$). We present below two results that give a necessary and sufficient condition for a finitely generated $A[x_1, \ldots, x_n]^m/M$ to have a free A-module representation w.r.t. a Gröbner basis (or a monomial order).

Theorem 3.31 *Let $M \subseteq A[x_1, \ldots, x_n]^m$ be a nonzero submodule. Let G be a Gröbner basis for M w.r.t. a monomial ordering, $\prec$. If G is monic then $A[x_1, \ldots, x_n]^m/M$ has a free A-module representation w.r.t. G.*

Proof: The proof is along the lines of the proof of Theorem 3.2. □

Note that in the above theorem $A[x_1, \ldots, x_n]^m/M$ need not be finitely generated. If $A[x_1, \ldots, x_n]^m/M$ is finitely generated and the Gröbner basis of M is monic, then there exists a $N \in \mathbb{N}$ such that $A[x_1, \ldots, x_n]^m/M \cong A^N$.

For the necessary condition we need the concept of short reduced Gröbner basis.

Lemma 3.32 *Let $M \subseteq A[x_1, \ldots, x_n]^m$ be a nonzero submodule such that $A[x_1, \ldots, x_n]^m/M$ is a finitely generated A-module and let G be a short reduced Gröbner basis for M. 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 the proof of Lemma 3.5. □

We are now ready to give the necessary condition of the characterization.

Theorem 3.33 *Let $M \subseteq A[x_1, \ldots, x_n]^m$ be a nonzero submodule such that $A[x_1, \ldots, x_n]^m/M$ is a finitely generated A-module and let G be a short reduced Gröbner basis for M w.r.t. $\prec$. If $A[x_1, \ldots, x_n]^m/M$ has a free A-module representation w.r.t. $\prec$, then G is monic.*

Proof: The proof follows the proof of Theorem 3.6. □

We state the characterization result as follows.

Proposition 3.34 *Let $M \subseteq A[x_1, \ldots, x_n]^m$ be a nonzero submodule such that $A[x_1, \ldots, x_n]^m/M$ is finitely generated. Let G be a short reduced Gröbner basis for M w.r.t. some monomial ordering, $\prec$. Then, $A[x_1, \ldots, x_n]^m/M$ has a free A-module representation w.r.t. G,*

$$A[x_1, \ldots, x_n]^m/M \cong A^N, \quad \text{for some } N \in \mathbb{N}$$

if and only if G is monic.

3.4.3 Macaulay-Buchberger basis theorem for modules over rings

Section 3.2 illustrates how the Macaulay-Buchberger basis theorem can be extended to rings. We extend both the Macaulay basis theorem and Macaulay-Buchberger basis theorem to submodules over rings.

Theorem 3.35 (Macaulay Basis Theorem for Modules over Rings) *$S = \{\overrightarrow{X} + M : \overrightarrow{X} \notin \langle \mathrm{lt}(M) \rangle_{A[x_1,\ldots,x_n]}\}$ is an A-module basis for $A[x_1, \ldots, x_n]^m/M$ if $A[x_1, \ldots, x_n]^m/M$ is free.*

Note that for every $\overrightarrow{X} + M \in S$, $\overrightarrow{X}$ is called a standard monomial w.r.t. $M \subseteq A[x_1, \ldots, x_n]^m$.

Theorem 3.36 (Macaulay-Buchberger Basis Theorem for Modules over Rings) *Let $G = \{\overrightarrow{g_1}, \ldots, \overrightarrow{g_t}\}$ be a short reduced Gröbner basis for a submodule $M \subseteq A[x_1, \ldots, x_n]^m$. Suppose G is monic then an A-module basis for $A[x_1, \ldots, x_n]^m/M$ is given by $S = \{\overrightarrow{X} + M : \mathrm{lm}(\overrightarrow{g_i}) \nmid \overrightarrow{X}, i = 1, \ldots, t\}$.*

3.5 An Application of the Free A-module Representation - Border Bases

The Gröbner basis characterization of $A[x_1, \ldots, x_n]/\mathfrak{a}$ with a free A-module representation given in Proposition 3.7 allows us to study residue class polynomial rings over Noetherian commutative rings as two different classes: $A[x_1, \ldots, x_n]/\mathfrak{a}$ with a free A-module representation w.r.t. some monomial order and $A[x_1, \ldots, x_n]/\mathfrak{a}$ with no free A-module representation w.r.t. any monomial order. This thesis focuses mainly on residue class polynomial rings over A with a

free A-module representation. Many properties of these structures are similar to the properties of residue class polynomial rings over fields. This implies that many of the techniques that we use in fields can be directly applied to these structures allowing us to extend several concepts and algorithmic techniques from fields to rings atleast for a certain subclass of ideals in $A[x_1, \ldots, x_n]$. In this section, we look at how to extend the concept of border bases to ideals in $A[x_1, \ldots, x_n]$, given $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and has a free A-module representation.

Border bases have proven to be a numerically more stable tool to describe zero-dimensional ideals in $\Bbbk[x_1, \ldots, x_n]$ than Gröbner bases (Kehrein and Kreuzer, 2005; Stetter, 2004). For a brief description of border bases in $\Bbbk[x_1, \ldots, x_n]$, the reader can refer to Section 2.3. In this section, based on the characterization given in Proposition 3.7, we extend border bases to polynomial rings over A.

We first define the order ideal and the border of an order ideal in the same way as in $\Bbbk[x_1, \ldots, x_n]$.

Definition 3.37 *A finite set $\mathcal{O} \subseteq \mathbb{N}^n$ is called an order ideal if $x^\alpha \in \mathcal{O}$ and $x^\beta \mid x^\alpha$ where $x^\beta \in \mathbb{N}^n$ implies $x^\beta \in \mathcal{O}$.*

Definition 3.38 *Let $\mathcal{O} \subseteq \mathbb{N}^n$ be an order ideal, then the border of $\mathcal{O}$ is defined as*

$$\partial\mathcal{O} = (x_1\mathcal{O} \cup x_2\mathcal{O} \cup \cdots \cup x_n\mathcal{O}) \setminus \mathcal{O}.$$

We now define $\mathcal{O}$- border prebasis. The only difference we have here is that the coefficients come from a Noetherian commutative ring, A.

Definition 3.39 *Let $\mathcal{O} \subseteq \mathbb{N}^n$, $\mathcal{O} = \{x^{\alpha_1}, \ldots, x^{\alpha_s}\}$ be an order ideal and $\partial\mathcal{O} = \{x^{\beta_1}, \ldots, x^{\beta_t}\}$ be the border of $\mathcal{O}$. Then a finite set of polynomials $\mathcal{B} = \{b_1, \ldots, b_t\} \subseteq A[x_1, \ldots, x_n]$ is said to be a $\mathcal{O}$- border prebasis if $\{b_1, \ldots, b_t\}$ are of the form,*

$$b_i = x^{\beta_i} - \sum_{j=1}^{s} c_{ij}x^{\alpha_j}, c_{ij} \in A.$$

Given an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ if $\mathcal{B} \subseteq \mathfrak{a}$ then $\mathcal{B}$ is said to be an $\mathcal{O}$-border prebasis of $\mathfrak{a}$.

Once we have an $\mathcal{O}$-border prebasis with coefficients from the ring the definition of border basis directly follows.

Definition 3.40 *Let $\mathcal{O} \subseteq \mathbb{N}^n$, $\mathcal{O} = \{x^{\alpha_1}, \ldots, x^{\alpha_s}\}$ be an order ideal and $\mathcal{B} = \{b_1, \ldots, b_t\} \subseteq A[x_1, \ldots, x_n]$ be an $\mathcal{O}$-border prebasis. Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$*

is finitely generated and has a free A-module representation w.r.t. some monomial order, $\prec$. Then $\mathcal{B}$ is said to be an $\mathcal{O}$-border basis if $\mathcal{B} \subseteq \mathfrak{a}$ and $\mathcal{O} = \{x^\alpha : \mathrm{lm}(g) \nmid x^\alpha, \forall g \in G$, where G is a monic short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. $\prec\}$.

We give below certain results associated with border basis in $\Bbbk[x_1, \ldots, x_n]$ that are valid in $A[x_1, \ldots, x_n]$ as well. The proofs of these theorems are exactly in the same lines as in $\Bbbk[x_1, \ldots, x_n]$ and hence we skip them here. Note that in fields, border basis is defined only for zero-dimensional ideals. In rings, $\mathcal{O}$-border basis exists if and only if $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and has a free A-module representation w.r.t. some monomial order, $\prec$, i.e. if the short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. $\prec$ is monic.

We have the following theorem that illustrates how border bases generalize the notion of Gröbner bases.

Theorem 3.41 *Let $\mathcal{O} = \{x^{\alpha_1}, \ldots, x^{\alpha_s}\}$ be an order ideal and $\mathcal{B} \subseteq A[x_1, \ldots, x_n]$ be an $\mathcal{O}$-border basis of an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$. Then $\mathcal{B}$ generates $\mathfrak{a}$.*

The uniqueness of the $\mathcal{O}$-border basis can be extended easily to rings.

Theorem 3.42 *Let $\mathcal{O} = \{x^{\alpha_1}, \ldots, x^{\alpha_s}\}$ be an order ideal and let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and has a free A-module representation w.r.t. $\prec$. Assume that $\mathcal{O} = \{x^\alpha : \mathrm{lm}(g) \nmid x^\alpha, \forall g \in G$, where G is a monic short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. $\prec\}$. Then there exists an unique $\mathcal{O}$-border basis, $\mathcal{B}$ of A.*

The below theorem illustrates the uniqueness of the remainder when we reduce it with an $\mathcal{O}$-border basis.

Theorem 3.43 *Let $\mathcal{B} = \{b_1, \ldots, b_t\} \subseteq A[x_1, \ldots, x_n]$ be an $\mathcal{O}$-border basis of an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$. Let $f \in A[x_1, \ldots, x_n]$, then remainder of f when we reduce it with $\mathcal{B}$ is unique.*

Example 3.44 *Let $\mathcal{O} = \{1, x\}$ be an order ideal in $\mathbb{Z}[x, y]$. The border of $\mathcal{O}$, $\partial\mathcal{O} = \{x^2, y, xy\}$. Then $\mathcal{B} = \{x^2 - 1, y - 1, xy - x\}$ is an $\mathcal{O}$ - border prebasis. Consider the ideal $\mathfrak{a}$ generated by $\{x^2 - 1, y - 1, xy - x\}$. Clearly, $\mathcal{B} \subseteq \mathfrak{a}$. Consider, $\mathbb{Z}[x, y]/\mathfrak{a}$. First, we have to determine if it has a free $\mathbb{Z}$-module representation and we use our characterization result for that. Then, we need to determine if the order ideal $\mathcal{O}$ is a $\mathbb{Z}$-module basis of the quotient ring. Consider the generator set $\mathcal{B} = \{x^2 - 1, y - 1, xy - x\}$. A Gröbner basis of this ideal is $\{x^2 - 1, y - 1\}$ for the monomial order, $x \prec y$. Since it is monic, $\mathbb{Z}[x, y]/\mathfrak{a}$ is free. The order ideal $\mathcal{O} = \{1, x\}$ forms a $\mathbb{Z}$-module basis of $\mathbb{Z}[x, y]/\mathfrak{a}$. This means $\mathcal{B} = \{x^2 - 1, y - 1, xy - x\}$ is an $\mathcal{O}$-border basis of the ideal, $\mathfrak{a}$.*

Chapter 4

Multivariate Ideal Lattices and its Applications in Lattice Based Cryptography

We have already seen how the Gröbner basis characterization of $A[x_1, \ldots, x_n]/\mathfrak{a}$ with a free A-module representation (Proposition 3.7) and short reduced Gröbner bases (Definition 3.3) can be used to locate ideal lattices in $\mathbb{Z}[x_1, \ldots, x_n]$ (Theorem 3.15). We discuss them in more detail in this chapter. In the second half of this chapter, we establish the existence of hash functions based on multivariate ideal lattices and prove that they are collision resistant. This class of generalized hash functions includes hash functions based on univariate ideal lattices that were previously studied in cryptography. We propose certain worst case problems, based on which, we establish the security of these hash functions. We show the hardness of these problems for some special cases.

4.1 Multivariate Ideal Lattices

Ideals in the residue class ring, $\mathbb{Z}[x]/\langle f \rangle$, for any monic polynomial $f \in \mathbb{Z}[x]$, are integer lattices as well and hence are known as ideal lattices. This is because $\mathbb{Z}[x]/\langle f \rangle$ is isomorphic to $\mathbb{Z}^N$ (as a $\mathbb{Z}$-module) if and only if f is monic. The presence of both ideal and lattice properties make ideal lattices a powerful tool in lattice based cryptography. The reason for the popularity of ideal lattices in lattice cryptography is that they provide a compact representation for integer lattices. In fact, ideal lattices have been used to build several cryptographic primitives that include digital signatures (Lyubashevsky and Micciancio, 2008), hash functions (Lyubashevsky and Micciancio, 2006) and identification schemes (Lyubashevsky, 2008). Recall that in Sec-

tions 2.6.1, 2.6.2 we discuss basic concepts in lattice based cryptography and in Section 2.6.3 we describ univariate ideal lattices. We also give a brief overview of collision resistant hash functions that are built using univariate ideal lattices in Section 2.6.3.2.

Here, we study how one can extend ideal lattices to the multivariate polynomial ring, $\mathbb{Z}[x_1, \ldots, x_n]$. We show that in the study of multivariate ideal lattices, the theory of Gröbner bases plays an important role. Given an ideal $\mathfrak{a}$ in $\mathbb{Z}[x_1, \ldots, x_n]$, we study the cases for which ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ are also lattices. First, we define cyclic lattices in the multivariate case. We show that ideal lattices exist if and only if the corresponding residue class polynomial rings over $\mathbb{Z}$ have a free $\mathbb{Z}$-module representation, for which we give a characterization based on short reduced Gröbner bases. For the construction of many cryptographic primitives, full rank lattices are essential and we derive the condition for a multivariate ideal lattice to be full rank. We also give an example of a class of binomial ideals in $\mathbb{Z}[x_1, \ldots, x_n]$, that gives rise to full rank integer lattices.

4.1.1 Multivariate cyclic lattices

Cyclic lattices in one variable are ideals in $\mathbb{Z}[x]/\langle x^N - 1\rangle$, for some $N \in \mathbb{N}$. Univariate ideal lattices are a generalization of univariate cyclic lattices. Here, we define multivariate cyclic shifts, a generalization of univariate cyclic shifts and show that the multivariate cyclic shifts of an element in an ideal in $\mathbb{Z}[x_1, \ldots, x_n]/\langle {x_1}^{r_1} - 1, \cdots, {x_n}^{r_n} - 1\rangle$ is also in the ideal. Therefore, all ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\langle {x_1}^{r_1} - 1, \cdots, {x_n}^{r_n} - 1\rangle$ are multivariate cyclic lattices.

Consider $\mathbb{Z}[x_1, \ldots, x_n]/\langle {x_1}^{r_1} - 1, \cdots, {x_n}^{r_n} - 1\rangle$, for some $r_1, \ldots, r_n \in \mathbb{N}$. Let $\mathfrak{a} = \langle {x_1}^{r_1} - 1, \cdots, {x_n}^{r_n} - 1\rangle$ and $r_1 \times r_2 \times \cdots \times r_n = N$. Then, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is a free $\mathbb{Z}$-module, isomorphic to $\mathbb{Z}^N$ with $\mathcal{B} = \{{x_1}^{\alpha_1} \ldots {x_n}^{\alpha_n} + \mathfrak{a} : \alpha_k = 0, \ldots, r_k - 1, k = 1, \ldots, n\}$ as a $\mathbb{Z}$-module basis. Given an element of the residue class polynomial ring,

$$\sum_{j=1}^{N} a_{(\alpha_{1j}, \ldots, \alpha_{nj})} {x_1}^{\alpha_{1j}} \ldots {x_n}^{\alpha_{nj}} + \mathfrak{a},$$

where $\alpha_{kj} = 0, \ldots, r_k - 1$ and $a_{(\alpha_{1j}, \ldots, \alpha_{nj})} \in \mathbb{Z}$. This can be represented using a tensor, $\mathcal{A} \in \mathbb{Z}^{r_1 \times \cdots \times r_n}$ defined as $\mathcal{A}_{i_1, \ldots, i_n} = a_{(i_1 - 1, \ldots, i_n - 1)}$, where $A_{i_1, \ldots, i_n}$ denotes $(i_1, \ldots, i_n)$-th element in the tensor $\mathcal{A}$. Now consider $\mathbb{Z}^N$ and suppose $r_1, \ldots, r_n \in \mathbb{N}$ such that $r_1 \times r_2 \times \cdots \times r_n = N$. Given a lattice $\mathcal{L} \subseteq \mathbb{Z}^N$, where $\mathbb{Z}^N = \mathbb{Z}^{r_1 \times \cdots \times r_n}$, it is easy to see that a one-to-one correspondence exists between a vector in $\mathcal{L}$ and a tensor in $\mathbb{Z}^{r_1 \times \cdots \times r_n}$.

Let $\mathcal{A}$ be a tensor in $\mathbb{Z}^{r_1 \times \cdots \times r_n}$. We define a $(n-1)^{\text{th}}$ order tensor for each $i = 1, \ldots, n$ and

denote it as $A_i(j)$, where $A_i(j) \in \mathbb{Z}^{r_1 \times r_2 \times \cdots \times r_{i-1} \times r_{i+1} \times \cdots \times r_n}$, $j = 0, \ldots, r_i - 1$. We have,

$$A_i(j)_{(k_1,\ldots,k_{i-1},k_{i+1},\ldots,k_n)} = \mathcal{A}_{(k_1,\ldots,k_{i-1},j,k_{i+1},\ldots,k_n)}, \;\; j = 0, \ldots, r_i - 1.$$

We construct the following ordered set of $(n-1)^{\text{th}}$ order tensors for each $i = 1, \ldots, n$,

$$\mathcal{A}_i = (A_i(0), A_i(1), \cdots, A_i(r_i - 1)).$$

Using this set, we introduce a notion of multivariate cyclic shifts.

Definition 4.1 *Let $\mathcal{L} \subseteq \mathbb{Z}^N = \mathbb{Z}^{r_1 \times \cdots \times r_n}$ be a lattice and $\mathcal{A} \in \mathbb{Z}^{r_1 \times \cdots \times r_n}$, a tensor in $\mathcal{L}$. The i^{th}-multivariate cyclic shift of $\mathcal{A}$, $\sigma_i(\mathcal{A})$ is a cyclic shift of elements in the ordered set, $\mathcal{A}_i$.*

Observe that multiplying an element in $\mathbb{Z}[x_1, \ldots, x_n]/\langle {x_1}^{r_1} - 1, \cdots, {x_n}^{r_n} - 1\rangle$ with x_i results in a cyclic shift in the ordered set, $\mathcal{A}_i$, $i = 1, \ldots, n$. This is also equivalent to a cyclic permutation in the n^{th} order tensor along the i^{th} direction.
We now formerly define multivariate cyclic lattices.

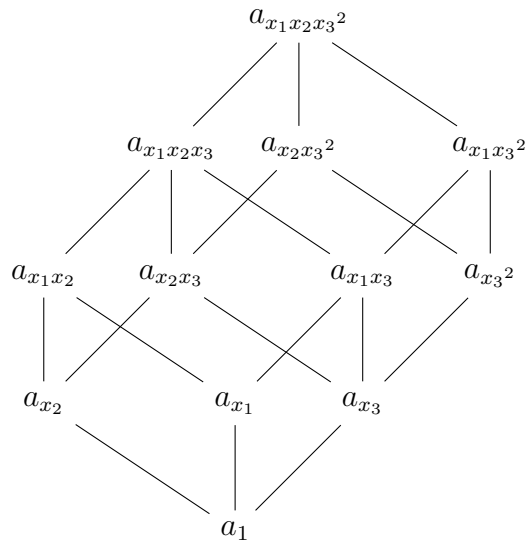
Definition 4.2 *A lattice $\mathcal{L}$ in $\mathbb{Z}^N = \mathbb{Z}^{r_1 \times \cdots \times r_n}$ is a multivariate cyclic lattice if for all $v \in \mathcal{L}$, a i^{th}-multivariate cyclic shift of v is also in $\mathcal{L}$ for all $i = 1, \ldots, n$.*

Example 4.3 *Consider the case when $n = 3$ and we have $r_1 = 2$, $r_2 = 2$ and $r_3 = 3$. The residue class ring associated to it is $\mathbb{Z}[x_1, x_2, x_3]/\langle {x_1}^2 - 1, {x_2}^2 - 1, {x_3}^3 - 1\rangle$. It is isomorphic to the space of 3^{rd} order tensors, $\mathbb{Z}^{2\times 2\times 3}(\cong \mathbb{Z}^{12})$. The following set of monomials form the set of coset representatives for a $\mathbb{Z}$-module basis,*

$$\{1, x_1, x_2, x_3, {x_3}^2, x_1x_2, x_1x_3, x_1{x_3}^2, x_2x_3, x_2{x_3}^2, x_1x_2x_3, x_1x_2{x_3}^2\}.$$

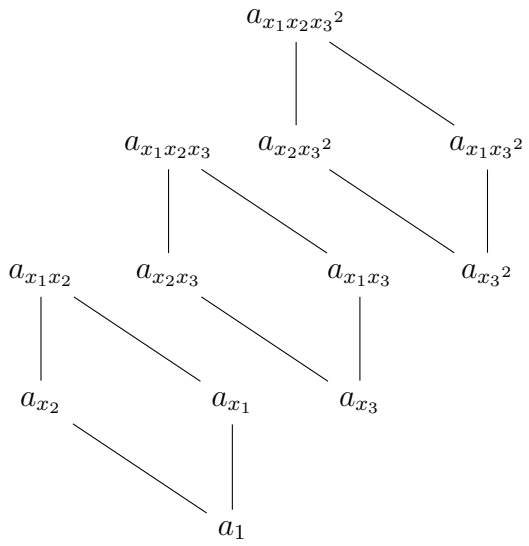
Any element in the residue class ring can be represented as a 3^{rd} order tensor, $\mathcal{A} \in \mathbb{Z}^{2\times 2\times 3}$. Let a_{x^α} be the coefficient of the basis element, x^α. We can represent $\mathcal{A}$ as follows,

$\mathcal{A} =$



.

The following tensors represent $A_3(0)$, $A_3(1)$ *and* $A_3(2)$ *respectively.*



.

$A_3(0)$, $A_3(1)$ *and* $A_3(2)$ *represent* 2^{nd} *order tensors corresponding to* $x_3 = 0$, $x_3 = 1$ *and* $x_3 = 2$ *respectively. Similarly,* $A_2(0)$ *and* $A_2(1)$ *represent* 2^{nd} *order tensors corresponding to* $x_2 = 0$ *and* $x_2 = 1$ *and* $A_1(0)$ *and* $A_1(1)$ *represent* 2^{nd} *order tensors corresponding to* $x_1 = 0$ *and* $x_1 = 1$. *Multiplying with* x_3 *here results in a cyclic rotation of* $A_3(0)$, $A_3(1)$ *and* $A_3(2)$.

Multiplying with a monomial ${x_1}^{\alpha_1} \cdots {x_n}^{\alpha_n}$ in the general case results in a composition of α_i shifts in $\mathcal{A}_i$ for each $i = 1, \ldots, n$. The commutativity of multiplication is taken care of as the shifts act on an independent set of subtensors and this makes the order of the composition of cyclic shifts irrelevant. That is, the order in which we perform the cyclic shifts between $\mathcal{A}_i$ and $\mathcal{A}_j$ does not matter for $i, j = 1, \ldots, n$.

Proposition 4.4 *Every ideal in*

$$\mathbb{Z}[x_1, \ldots, x_n]/\langle {x_1}^{r_1} - 1, {x_2}^{r_2} - 1, \cdots, {x_n}^{r_n} - 1\rangle$$

is a multivariate cyclic lattice.

4.1.2 Multivariate ideal lattices and short reduced Gröbner bases

Now we give the formal definition of multivariate ideal lattices.

Definition 4.5 *Given an ideal $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$, a multivariate ideal lattice is an integer lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ that is isomorphic, as a $\mathbb{Z}$-module, to an ideal $\mathfrak{A}$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$.*

In sequel, by ideal lattices we mean multivariate ideal lattices.

The $\mathbb{Z}$-module structure of $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is crucial in locating ideal lattices in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. In this section, we study the case when the residue class polynomial ring over $\mathbb{Z}$ has a free $\mathbb{Z}$-module representation w.r.t. a monomial order, i.e. $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a} \cong \mathbb{Z}^m$, for some $m \in \mathbb{N}$. In that case, corresponding to every ideal, $\mathfrak{A}$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, there exists a subgroup in $\mathbb{Z}^m$. Hence the ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ are indeed ideal lattices. One can use short reduced Gröbner bases (Definition 3.3) to find the different $\mathbb{Z}$-module representations of $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. Section 3.1 gives a detailed description of how to determine these representations for residue class polynomial rings over a Noetherian commutative ring, A. When $A = \mathbb{Z}$, in the definition of short reduced Gröbner basis the generator of the leading coefficient ideal is taken as the gcd of all generators. The short reduced Gröbner basis is unique for a particular monomial order and hence once we fix a monomial order, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ has a unique $\mathbb{Z}$-module representation. From Proposition 3.7 we have, the following result for the case when $A = \mathbb{Z}$.

Corollary 4.6 *If the short reduced Gröbner basis of an ideal, $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ w.r.t. some monomial ordering is monic, then every ideal in the $\mathbb{Z}$-module, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is an ideal lattice.*

We illustrate the above result by an example.

Example 4.7 *Let $\mathfrak{a} = \langle 3x^2, 5x^2, y\rangle$ be an ideal in $\mathbb{Z}[x, y]$. The short reduced Gröbner basis for the ideal w.r.t. lexicographic order $y \prec x$ is $G = \{x^2, y\}$. Since G is monic, $\mathbb{Z}[x, y]/\mathfrak{a}$ has a free representation and hence the $\mathbb{Z}$-module is free and isomorphic to $\mathbb{Z}^2$. All ideals in $\mathbb{Z}[x, y]/\mathfrak{a}$ are ideal lattices. For example, the ideal generated by $6x + \langle x^2, y\rangle$ is isomorphic to the lattice, $\mathcal{L}([(0, 6)])$. Note that here $\mathcal{L}([(0, 6)])$ denotes the subgroup generated by $(0, 6)$ in $\mathbb{Z}^2$.*

Below we show that if $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is not a free $\mathbb{Z}$-module then it does not contain any ideal lattices.

Proposition 4.8 *If a finitely generated $\mathbb{Z}$-module, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is not free then no ideal in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is an integer lattice.*

Proof: We have the following structure theorem over a principal ideal domain (PID),

$$\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a} \cong \mathbb{Z}^l \oplus \mathbb{Z}/\langle w_1 \rangle \oplus \cdots \oplus \mathbb{Z}/\langle w_k \rangle.$$

Clearly, if there is a nonzero torsion part in the above direct sum decomposition then $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ will not have a free $\mathbb{Z}$-module representation w.r.t. any Gröbner basis. Also, we assume w.l.o.g. that the free part is nonzero. Let G be the Gröbner basis of the ideal, $\mathfrak{a}$ w.r.t. to some monomial ordering. Consider the isomorphism in (3.1) w.r.t. G. Assume there exists an ideal, $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ such that it is an integer lattice. Let $x^{\alpha_r} + \mathfrak{a} \in \mathfrak{A}$ be an element such that the leading coefficient ideal of x^{α_r} in $\mathbb{Z}$, $I_{J_{x^{\alpha_r}}}$ is equal to $\{0\}$. This implies that the set of coset representatives, $C_{J_{x^{\alpha_r}}} = \mathbb{Z}$, and therefore the monomial corresponds to the free part in (3.1). Consider the ideal generated by $x^{\alpha_r} + \mathfrak{a}$. Since the $\mathbb{Z}$-module is not free we have $I_{J_{x^{\alpha_j}}} \neq \{0\}$ and $C_{J_{x^{\alpha_j}}} \neq \mathbb{Z}$ for some monomial x^{α_j} in the isomorphism. Let $c \in C_{J_{x^{\alpha_j}}}$. Since $c_i x^{\alpha_i} + \mathfrak{a} \in \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, $c x^{\alpha_j} x^{\alpha_r} + \mathfrak{a} \in \langle x^{\alpha_r} + \mathfrak{a} \rangle$. This implies, the ideal generated by a free element contains torsion elements. Thus the $\mathbb{Z}$-module, $\mathfrak{A}$ has torsion elements and is not isomorphic to an integer lattice, which is a contradiction. □

Corollary 4.9 *Every ideal, $\mathfrak{a}$ in $\mathbb{Z}[x_1, \ldots, x_n]$ is an ideal lattice if and only if $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is a free and finitely generated $\mathbb{Z}$-module.*

4.1.3 Full rank lattices in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$

We recall that in the definition of ideal lattices in $\mathbb{Z}[x]$ the choice of the polynomial f in $\mathbb{Z}[x]/\langle f \rangle$ is restricted to monic polynomials. But in the construction of many cryptographic primitives like collision resistant hash functions f is assumed to be an irreducible polynomial. This condition ensures that the ideal lattice is full rank and hence prevents easy collision attacks (Lyubashevsky and Micciancio, 2006). In the multivariate case, we derive a necessary and sufficient condition for full rank ideal lattices.

Proposition 4.10 *Let $\{g_1, \ldots, g_t\}$ be a monic short reduced Gröbner basis of an ideal $\mathfrak{a}$ in $\mathbb{Z}[x_1, \ldots, x_n]$ such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a} \cong \mathbb{Z}^N$ for some $N \in \mathbb{N}$. All ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ are full rank lattices if and only if $\mathfrak{a}$ is a prime ideal.*

Proof: Let $\mathfrak{a} = \langle g_1, \ldots, g_t \rangle$ be a prime ideal. Consider an ideal $\mathfrak{A} = \langle f_1 + \mathfrak{a}, \ldots, f_s + \mathfrak{a} \rangle$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, where $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$. Since $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a} \cong \mathbb{Z}^N$ we have a finite

basis, $\mathcal{B} = \{b_1 + \mathfrak{a}, \ldots, b_N + \mathfrak{a}\}$. We have to prove that there are N linearly independent vectors in $\mathfrak{A}$. Consider $f_1 b_1, \ldots, f_1 b_N$. Let $c_1 f_1 b_1 + \cdots + c_N f_1 b_N \in \langle g_1, \ldots, g_t \rangle$. This implies $f_1(c_1 b_1 + \cdots + c_N b_N) \in \langle g_1, \ldots, g_t \rangle$. Since $\langle g_1, \ldots, g_t \rangle$ is a prime ideal, either $f_1 \in \langle g_1, \ldots, g_t \rangle$ or $(c_1 b_1 + \cdots + c_N b_N) \in \langle g_1, \ldots, g_t \rangle$. But both cases cannot happen. Therefore $c_i = 0$ for all $i = 1, \ldots, N$. This implies that $f_1 b_1 + \mathfrak{a}, \ldots, f_1 b_N + \mathfrak{a}$ are linearly independent and the ideal lattice is full rank.

Conversely, assume that $\mathfrak{a}$ is not a prime ideal. Then there exists $l, h \in \mathbb{Z}[x_1, \ldots, x_n]$ such that $lh \in \langle g_1, \ldots, g_t \rangle$ but $l \notin \langle g_1, \ldots, g_t \rangle$ and $h \notin \langle g_1, \ldots, g_t \rangle$. This implies, $l = \sum_{i=1}^{N} c_i b_i$ and $h = \sum_{i=1}^{N} d_i b_i$, where $b_i + \mathfrak{a} \in \mathcal{B}$, the basis for $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ and $c_i, d_i \in \mathbb{Z}$. Consider the ideal lattice $\langle l + \mathfrak{a} \rangle$. We have $lh \in \langle g_1, \ldots, g_t \rangle$ and this implies $l \sum_{i=1}^{N} d_i b_i \in \langle g_1, \ldots, g_t \rangle$. But $l \notin \langle g_1, \ldots, g_t \rangle$ and $\sum_{i=1}^{N} d_i b_i \notin \langle g_1, \ldots, g_t \rangle$. The set $\{lb_1 + \mathfrak{a}, \ldots, lb_N + \mathfrak{a}\}$ contains linearly dependent vectors and the rank of the ideal lattice $\langle l + \mathfrak{a} \rangle$ is $\lneq N$. Therefore, if the ideal $\mathfrak{a}$ is not a prime ideal then there exist lattices in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ that are not full rank. □

Determining if an ideal is prime or not is important for many practical applications. An algorithm for primality testing in polynomial rings, over any commutative Noetherian ring, A can be found in (Gianni et al., 1988).

We now give an example of a class of binomial ideals that is prime and gives rise to free residue class polynomial rings. Given an integer lattice, $\mathcal{L}$, a lattice ideal, $\mathfrak{a}_\mathcal{L}$ in $\mathbb{k}[x_1, \ldots, x_n]$ is defined as the binomial ideal generated by $\{x^{v^+} - x^{v^-}\}$ where v^+ and v^- are nonnegative with disjoint support and $v^+ - v^- \in \mathcal{L}$ (Katsabekis et al., 2010). Lattice ideals in polynomial rings over $\mathbb{Z}$ can be defined in the same way. In this case, the binomial ideal is generated over the polynomial ring, $\mathbb{Z}[x_1, \ldots, x_n]$. The generators of the ideal are binomials with the terms having opposite sign and the coefficients of both the terms equal to absolute value 1. One can show that the short reduced Gröbner basis of the lattice ideal is monic (Section 3.3.1). In this case, by Proposition 3.7, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}_\mathcal{L}$ is free. Hence, we have the following fact.

Theorem 4.11 *Every ideal in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}_\mathcal{L}$, where $\mathfrak{a}_\mathcal{L}$ is a lattice ideal, is an ideal lattice.*

The saturation of an integer lattice, $\mathcal{L} \subseteq \mathbb{Z}^m$ is a lattice, defined as

$$Sat(\mathcal{L}) = \{\alpha \in \mathbb{Z}^m \mid d\alpha \in \mathcal{L} \text{ for some } d \in \mathbb{Z}, d \neq 0\}.$$

We say that an integer lattice $\mathcal{L}$ is saturated if $\mathcal{L} = Sat(\mathcal{L})$. It can be easily shown that the lattice ideal $\mathfrak{a}_\mathcal{L}$ is prime if and only if $\mathcal{L}$ is saturated. Note that in the commutative algebra literature prime lattice ideals are also called toric ideals (Bigatti et al., 1999). Thus, toric ideals in $\mathbb{Z}[x_1, \ldots, x_n]$ give rise to full rank integer lattices.

4.2 Hard Problems for Multivariate Ideal Lattices

We now look at how to build cryptographic hash functions based on multivariate ideal lattices. Firstly, we define some hard computational problems that are specific to multivariate ideal lattices and using these hardness results prove the collision resistance of the hash functions.

4.2.1 Expansion Factor

Given $f \in \mathbb{Z}[x_1, \ldots, x_n]$, the following norms can be defined on $\mathbb{Z}[x_1, \ldots, x_n]$: the infinity norm, $\|f\|_\infty$ that takes the maximum coefficient of all the terms in the polynomial and the norm w.r.t. an ideal $\mathfrak{a}$ and a monomial order $\prec$, $\|f\|_{\mathfrak{a},\prec}$ that takes the maximum coefficient of all the terms in the polynomial reduced modulo $\mathfrak{a}$ w.r.t. $\prec$.

Given a finitely generated residue class polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ with a free $\mathbb{Z}$-module representation w.r.t a monomial order $\prec$, the ideal $\mathfrak{a}$ should satisfy the following properties that are essential for the security proofs of the hash function: (i) the ideal $\mathfrak{a}$ should be a prime ideal, which ensures that every ideal in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is a full rank lattice, and (ii) the norm of any polynomial f w.r.t. the ideal $\mathfrak{a}$ and monomial order $\prec$, $\|f\|_{\mathfrak{a},\prec}$ should not be much larger than $\|f\|_\infty$. The second property is formally captured with a parameter called the expansion factor that we define for the multivariate case below.

For a given finite set of generators, $\text{maxdeg}_{x_i}(\mathfrak{a})$ denotes the maximum degree of a variable x_i among the generators of the ideal $\mathfrak{a}$. We represent the maximum degree of a variable x_i in a polynomial g as $\text{maxdeg}_{x_i}(g)$.

Definition 4.12 *Let $\mathfrak{a} = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$. The expansion factor $\mathcal{E}$ of $\mathfrak{a}$ is defined as*

$$\mathcal{E}(\mathfrak{a}, \prec, (k_1, \ldots, k_n)) = \max_{\substack{\text{maxdeg}_{x_i}(g) \leq k_i(\text{maxdeg}_{x_i}(\mathfrak{a})) \\ \forall i = 1, \ldots, n \\ g \in \mathbb{Z}[x_1, \ldots, x_n]}} \frac{\|g\|_{\mathfrak{a},\prec}}{\|g\|_\infty},$$

where $k_i \in \mathbb{N}$, $i = 1, 2, \ldots, n$.

We give a result that bounds the expansion factor of ideals for which the residue class polynomial ring is finitely generated and has a free $\mathbb{Z}$-module representation.

Theorem 4.13 *Let $G = \{g_1, \ldots, g_s\}$ be a short reduced Gröbner basis of an ideal $\mathfrak{a}$ w.r.t. a monomial order $\prec$ such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$ (i.e. G is monic). Then for any $f \in \mathbb{Z}[x_1, \ldots, x_n]$, $\|f\|_{\mathfrak{a},\prec} \leq \|f\|_\infty (2 \cdot (\|g\|_\infty)_{\max})^k$, where $(\|g\|_\infty)_{\max}$ denotes the maximum norm among the generators of the ideal and k is of the order $O((\deg(f))^n (\max_{1 \leq i \leq s} \deg(g_i))^n)$.*

Proof: First we reduce f with the generators $\{g_1, \ldots, g_s\}$. Let g_j be the generator such that $\text{lm}(f) = x^\alpha \text{lm}(g_j)$ for some x^α. Then, $f_1 = f - \text{lc}(f)x^\alpha g_j$. Since G is monic, during the reduction process one needs to consider only one generator of the ideal at a time. We have,

$$\begin{aligned}\|f_1\|_\infty \leq \|f\|_\infty + \|f\|_\infty \|g_j\|_\infty &\leq 2\|f\|_\infty \|g_j\|_\infty \\ &\leq 2\|f\|_\infty (\|g\|_\infty)_{\max}.\end{aligned}$$

Next we can reduce f_1 by any of the generators in the Gröbner basis to get f_2 and continue this process. This process will terminate after k steps, where k is of the order $O((\deg(f))^n (\max_i \deg(g_i))^n)$ (Thieu, 2013). The exact number of iterations cannot be determined unless we know the exact structure of the ideal and the polynomial. Hence,

$$\|f\|_{\mathfrak{a},\prec} \leq \|f\|_\infty (2 \cdot (\|g\|_\infty)_{\max})^k.$$

Unlike in the univariate case, here we cannot bound the expansion factor tightly because both the structure of the ideal and the polynomial being reduced have a role to play in the number of iterations in the reduction. In the univariate case an intuition can be given on how to select an ideal with a "small" expansion factor (Lyubashevsky and Micciancio, 2006). It would be an interesting problem to come up with similar observations in the multivariate case.

4.2.2 Worst Case Problems

For any ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ we use ${\lambda_i}^p(\mathfrak{A})$ to indicate ${\lambda_i}^p(\mathcal{L}(\mathfrak{A}))$, where λ_i represents the i-th successive minima w.r.t. the ℓ_p norm.

Definition 4.14 *The approximate Shortest Polynomial Problem ($SPP_\gamma(\mathfrak{A})$) is defined as follows: given an ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, where $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$, determine a $g \in \mathfrak{A}$ such that $g \neq 0$ and $\|g\|_{\mathfrak{a},\prec} \leq \gamma {\lambda_1}^\infty(\mathfrak{A})$, where λ_1 represents the minimum distance.*

We use the notation $\mathcal{L}(\mathfrak{a})$ to denote the set of all lattices associated with $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ and use $\mathfrak{a} - SPP$ when we consider SPP for ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is as described above. In Section 4.3, we show how well known hard problems can be reduced to $\mathfrak{a} - SPP_\gamma$.

We give below a lemma that relates ${\lambda_1}^\infty$ with ${\lambda_N}^\infty$ for an ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is a prime ideal and $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is free and finitely generated of dimension N. It shows that ${\lambda_N}^\infty$ cannot be much bigger than ${\lambda_1}^\infty$ if the ideal is prime.

Lemma 4.15 *For every ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is a prime ideal and $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated of size N and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$, we have*

$$\lambda_N{}^{\infty}(\mathfrak{A}) \leq \mathcal{E}(\mathfrak{a}, \prec, (2, \ldots, 2))\lambda_1{}^{\infty}(\mathfrak{A}).$$

Proof: Let g be a polynomial in $\mathfrak{A}$ reduced w.r.t. $\mathfrak{a}$ such that $\|g\|_{\infty} = \lambda_1{}^{\infty}(\mathfrak{A})$. Let $\mathcal{B} = \{b_1, \ldots, b_N\}$ be the basis for $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. Then $\{gb_1, \ldots, gb_N\}$ is a linearly independent set because $\mathfrak{a}$ is a prime ideal. Also, $\text{maxdeg}_{x_i}(gb_i) \leq 2 \cdot \text{maxdeg}_{x_i}(\mathfrak{a})$. For $i = 1, \ldots, N$,

$$\begin{aligned} \|gb_i\|_{\mathfrak{a},\prec} \leq \mathcal{E}(\mathfrak{a}, \prec, (2, \ldots, 2))\|gb_i\|_{\infty} &\leq \mathcal{E}(\mathfrak{a}, \prec, (2, \ldots, 2))\|g\|_{\infty}, \\ &= \mathcal{E}(\mathfrak{a}, \prec, (2, \ldots, 2))\lambda_1{}^{\infty}(\mathfrak{A}). \end{aligned}$$

□

Now, we define an incremental version of SPP.

Definition 4.16 *The approximate Incremental Shortest Polynomial Problem ($IncSPP_{\gamma}(\mathfrak{A}, g)$) is defined as follows: Given an ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ and $g \in \mathfrak{A}$ such that $\|g\|_{\mathfrak{a},\prec} \lneq \gamma\lambda_1{}^{\infty}(\mathfrak{A})$, determine an $h \in \mathfrak{A}$ such that $\|h\|_{\mathfrak{a},\prec} \neq 0$ and $\|h\|_{\mathfrak{a},\prec} \leq \|g\|_{\mathfrak{a},\prec}/2$.*

The following result directly follows.

Lemma 4.17 *There is a polynomial time reduction from $\mathfrak{a} - SPP_{\gamma}$ to $\mathfrak{a} - IncSPP_{\gamma}$.*

4.3 Hardness Results

Let $\mathfrak{a}$ and $\mathfrak{a}'$ be ideals in $\mathbb{Z}[x_1, \ldots, x_n]$ defined as $\mathfrak{a} = \langle {x_1}^{r_1} - 1, {x_2}^{r_2} - 1, \ldots, {x_n}^{r_n} - 1\rangle, r_i \in \mathbb{N}, i = 1, 2, \ldots, n$, and $\mathfrak{a}' = \langle {x_1}^{r_1 - 1} + {x_1}^{r_1 - 2} + \cdots + 1, \ldots, {x_n}^{r_n - 1} + {x_n}^{r_n - 2} + \cdots + 1\rangle$. We prove that solving SPP_{γ} in an ideal in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is equivalent to finding the approximate shortest polynomial in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}'$. Note that if each r_i is a prime number then $\mathfrak{a}'$ is a prime ideal and we have full rank lattices. It also means that each of the generators is irreducible. If one can solve the approximate shortest polynomial problem in the ideal lattices of $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}'$, then one can also solve the approximate shortest polynomial problem in multivariate cyclic lattices (where each r_i is prime), that we conjecture is a hard problem.

Lemma 4.18 *Let $\mathfrak{A}$ be an ideal in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ such that the residue class polynomial ring is finitely generated of size N and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$. Given the generators for $\mathfrak{A}$, there is a polynomial time algorithm to find the basis for the lattice of $\mathfrak{A}$, $\mathcal{L}(\mathfrak{A})$.*

Proof: Let $\mathfrak{A} = \{g_1 + \mathfrak{a}, \ldots, g_m + \mathfrak{a}\}$. Let the residue classes of $\mathcal{B} = \{b_1, \ldots, b_N\}$ be a basis for $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. Consider the set $G = \{g_1 b_1 + \mathfrak{a}, \ldots, g_1 b_N + \mathfrak{a}, \ldots, g_m b_1 + \mathfrak{a}, \ldots, g_m b_N + \mathfrak{a}\}$. All the elements of $\mathfrak{A}$ can be written as an integer combination of elements in G and therefore $\mathfrak{A}$ is a $\mathbb{Z}$-module. Using Hermite normal form one can determine the basis of the $\mathbb{Z}$-module as an additive group in polynomial time. □

Lemma 4.19 *Let $\mathfrak{a}$ and $\mathfrak{a}'$ be ideals as defined as above. Given a multivariate cyclic lattice $\mathfrak{A}$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ of dimension N, there is a polynomial time reduction from the problem of approximating the shortest vector in $\mathfrak{A}$ within a factor of 2γ to approximating the shortest vector in an ideal in the ring, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}'$ within a factor of γ.*

Proof: Let f be a polynomial of smallest infinity norm such that $f + \mathfrak{a} \in \mathfrak{A}$ and $f + \mathfrak{a}$ is reduced modulo $\mathfrak{a}$ w.r.t. some monomial order, $\prec$. If $f \notin \mathfrak{a}'$, $\|f\|_{\mathfrak{a}', \prec} \leq 2\|f\|_\infty$, since its residue class is reduced w.r.t. $\mathfrak{a}'$. There exists a nonzero polynomial in $\mathfrak{A}$ whose infinity norm is at most $2\|f\|_\infty$. Thus the algorithm for approximating the shortest polynomial in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}'$ to within a factor of γ will find a nonzero polynomial of infinity norm at most $2\gamma\|f\|_\infty$. Every nonzero polynomial in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}'$ is nonzero in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. If $f \in \mathfrak{a}'$, we have $f \in \mathfrak{a}' \cap \mathfrak{A}$. Since f is reduced w.r.t. $\mathfrak{a}$, f is a sum of integer multiples of the generators of $\mathfrak{a}'$. We can find a basis for the one dimensional lattice $\mathfrak{a}' \cap \mathfrak{A}$ and the generator will be the shortest polynomial. □

Conjecture 4.20 *Approximation problems like SVP_γ are computationally hard in multivariate cyclic lattices with prime powers.*

The conjecture is based on the assumption that the SVP_γ problem is hard for univariate cyclic lattices of prime powers (Micciancio, 2002). Given,

$$\mathbb{Z}[x_1, \ldots, x_n]/\langle {x_1}^{r_1} - 1, {x_2}^{r_2} - 1, \cdots, {x_n}^{r_n} - 1\rangle, \;\; r_i \in \mathbb{N},$$

where each r_i is prime, the multivariate cyclic lattice in n indeterminates is equivalent to n independent univariate cyclic lattices of prime powers. This is because the multivariate cyclic shifts in the n^{th} order tensor $\mathcal{A}_i$ for each $i = 1, \ldots, n$ are independent of each other (see Section 4.1.1). This implies, the assumption that the SVP_γ problem is hard for univariate cyclic lattices of prime powers can be applied for each $i = 1, 2, \ldots, n$ individually. Therefore, if the approximation problems are hard for univariate cyclic lattices with prime powers then they are computationally hard for multivariate cyclic lattices with prime powers as well.

We now give the hardness results for multivariate ideal lattices based on results from function fields of algebraic varieties. A function field of an affine variety $\mathcal{V}$ is the quotient field of the

coordinate ring $\Bbbk[x_1,\ldots,x_n]/\mathcal{I}(\mathcal{V})$, often described as the field of rational functions on $\mathcal{V}$. Note that in the univariate case, the SPP problem can be reduced to the problem of finding small conjugates in ideals of subrings of a number field which is a hard problem (Lyubashevsky and Micciancio, 2006).

To prove the hardness of SPP we define the following problem. Let $\mathfrak{a}$ be an ideal in $\mathbb{Z}[x_1,\ldots,x_n]$ such that $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is free and finitely generated. Consider the variety of $\mathfrak{a}$ in $\mathbb{C}^n$, $\mathcal{V}_{\mathbb{C}}(\mathfrak{a})$. Then for every $(a_1,\ldots,a_n)\in\mathcal{V}_{\mathbb{C}}(\mathfrak{a})$ the following mapping

$$\begin{aligned}\psi : \mathbb{Z}[a_1,\ldots,a_n] &\longrightarrow \mathbb{Z}[x_1,\ldots,x_n]/\sqrt{\mathfrak{a}}\\ \sum_{i=1}^{l}\alpha_i {a_1}^{i_1}\ldots {a_n}^{i_n} &\longmapsto \sum_{i=1}^{l}\alpha_i {x_1}^{i_1}\ldots {x_n}^{i_n}+\sqrt{\mathfrak{a}},\end{aligned} \tag{4.1}$$

where $l\in\mathbb{N}$ and $\sqrt{\mathfrak{a}}$ is the radical of the ideal, is an isomorphism. When $\mathbb{Z}[x_1,\ldots,x_n]/\sqrt{\mathfrak{a}}$ is free and finitely generated, $\mathcal{V}_{\mathbb{C}}(\mathfrak{a})$ is a finite set. For ease of notation we will omit the subscript $\mathbb{C}$ and denote the variety as $\mathcal{V}(\mathfrak{a})$.

For $(a_1,\ldots,a_n)\in\mathcal{V}(\mathfrak{a})$ and $\alpha=\sum_{i=1}^{l}\alpha_i {a_1}^{i_1}\cdots {a_n}^{i_n}$, a polynomial in $\mathbb{Z}[a_1,\ldots,a_n]$, we define $\text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha)$ as $\max\limits_{1\le i\le l}(|\ \alpha_i\ |)$. Let ψ_j be the isomorphism defined as in (4.1) for each element of the affine variety, $\mathcal{V}(\mathfrak{a})$. Given an ideal I in $\mathbb{Z}[a_1,\ldots,a_n]$, $(a_1,\ldots,a_n)\in\mathcal{V}(\mathfrak{a})$, for an element $\alpha=\sum_{i=1}^{l}\alpha_i {a_1}^{i_1}\ldots {a_n}^{i_n}$ in I, we define

$$\text{maxsub}(\alpha)=\max_{1\le j\le N}\{\sum_{i=1}^{l}\alpha_i {a_1}^{(j)^{i_1}}\ldots {a_n}^{(j)^{i_n}} : ({a_1}^{(j)},\ldots,{a_n}^{(j)})\in\mathcal{V}(\mathfrak{a})\}.$$

Definition 4.21 *(Approximate Smallest Substitution Problem (SSub)) Let $\mathfrak{a}\subseteq\mathbb{Z}[x_1,\ldots,x_n]$ be an ideal such that $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is free and finitely generated. Let the finite variety, $\mathcal{V}(\mathfrak{a})$ be of cardinality N. Given an ideal I in $\mathbb{Z}[a_1,\ldots,a_n]$, $(a_1,\ldots,a_n)\in\mathcal{V}(\mathfrak{a})$, the approximate smallest substitution problem, $SSub_\gamma(I)$ is defined as follows: find an element $\alpha\in I$ such that* $\text{maxsub}(\alpha)\le\gamma\text{maxsub}(\alpha')$, *for all $\alpha'\in I$.*

It is important to note that formulation of the smallest substitution problem in the multivariate case is quite different from the univariate case. In the univariate case, the problem that is mapped to SPP is the smallest conjugate problem (SCP). For any α in the ideal I, first a function called maxConj analogous to the maxsub is defined. The function returns the maximum of the zeroes of the minimum polynomial of α over $\mathbb{Q}$. SCP poses the problem of finding an $\alpha\in I$ such that it has the least maxConj among all the elements in I. This relates to

the problem of isomorphism of number fields for which no polynomial time algorithm is determined (Cohen, 2013, Polynomial Reduction Algorithm). The hardness of SCP is discussed in (Lyubashevsky and Micciancio, 2006). We argue that the smallest substitution problem, $SSub$, relates to the problem of isomorphism of function fields, the multivariate extension of number fields and a hard problem (Pukhlikov, 1998). We show below that SCP is a special instance of the $SSub$ problem. That is, SCP is polynomially reducible to $SSub$.

Theorem 4.22 *Given an monic irreducible polynomial $f \in \mathbb{Z}[x]$ of degree N, let $\mathfrak{a} = \langle f \rangle$ be an ideal in $\mathbb{Z}[x]$. There is a polynomial time reduction from $\mathfrak{a} - SCP$ to $\mathfrak{a} - SSub$.*

Proof: Let $\mathcal{V}$ be the variety associated with $\mathfrak{a}$ of cardinality N. For $a \in \mathcal{V}$, we have the isomorphism, ψ given by (4.1), $\mathbb{Z}[a] \cong \mathbb{Z}[x]/\mathfrak{a}$. An algorithm for $\mathfrak{a} - SSub_\gamma$ returns an $\alpha \in \mathbb{Z}[a]$, $a \in \mathcal{V}(\mathfrak{a})$ such that $\text{maxsub}(\alpha) \leq \gamma \text{maxsub}(\alpha')$, for all $\alpha' \in \mathbb{Z}[a]$. Let $\alpha = \alpha_0 + \alpha_1 a + \cdots + \alpha_{N-1} a^{N-1}$ and

$$\text{maxsub}(\alpha) = \max_{1 \leq j \leq N} \{ \sum_{i=0}^{N-1} \alpha_i {a^{(j)}}^i : a^{(j)} \in \mathcal{V}(\mathfrak{a}) \}.$$

Since the set, $\{\sum_{i=0}^{N-1} \alpha_i {a^{(j)}}^i\}$ is the set of zeroes of the minimal polynomial of α over $\mathbb{Q}$, we have $\text{maxsub}(\alpha) = \text{maxConj}(\alpha)$. Therefore, α is the solution for $\mathfrak{a} - SCP_\gamma$ as well. □

We proceed to find a relation between the maximum coefficient of an element α in the ideal $\mathfrak{A}$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, and the value of maximum substitution of α under the isomorphism described by (4.1). This will help us to prove that SPP is polynomially reducible to $SSub$ as the problem of finding an element with the smallest norm in an ideal, $\mathfrak{A}$ in $\mathbb{Z}[x_1, \ldots, x_n]/\sqrt{\mathfrak{a}}$ is equivalent to the problem of finding an element α in the ideal $\psi^{-1}(\mathfrak{A})$ in $\mathbb{Z}[a_1, \ldots, a_n]$ with the smallest $\text{maxCoeff}_{(a_1, \ldots, a_n)}(\alpha)$.

The following result is easy to see.

Lemma 4.23 *Let $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ be an ideal such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and has a free $\mathbb{Z}$-module representation w.r.t. a monomial order, $\prec$. Let the finite set of zeroes, $\mathcal{V}(\mathfrak{a})$ be of cardinality N. Let $\mathcal{B}$ be the canonical basis of the free residue class ring constructed using Theorem 3.11. Let $\alpha \in \mathbb{Z}[a_1, \ldots, a_n]$, $(a_1, \ldots, a_n) \in \mathcal{V}(\mathfrak{a})$. Let ψ be the isomorphism given by (4.1) and corresponding to each element in $\mathcal{V}$ we have ψ_i, $1 \leq i \leq N$. Let $t = \max_{x^\beta \in \mathcal{B}}(\text{maxsub}(\psi^{-1}(x^\beta)))$. Then,*

$$\text{maxsub}(\alpha) \leq Nt \, \text{maxCoeff}_{({a_1}^{(i)}, \ldots, {a_n}^{(i)})}(\alpha),$$

where $({a_1}^{(i)}, \ldots, {a_n}^{(i)})$ corresponds to ψ_i, $i = 1, \ldots, N$.

The above result allows us to upper bound the maximum substitution w.r.t. a factor (polynomial in N) of the maximum coefficient. To prove that SPP can be polynomially reduced to $SSub$ and vice-versa, we need to give an upper bound for the maximum coefficient w.r.t. the maximum substitution value. We first give a result that upper bounds the maximum coefficient value to a factor (that is not a polynomial in N) of the maximum substitution value. Then for the specific case of

$$\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \ldots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1 \rangle,$$

we give an upper bound to a factor of N.

Lemma 4.24 *Let G be a short reduced Gröbner basis of an ideal $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and has a free $\mathbb{Z}$-module representation w.r.t. G. Let the finite set of zeroes, $\mathcal{V}(\mathfrak{a})$ be of cardinality N and $\mathcal{B}$ be the canonical basis of the free residue class ring. Let $\alpha \in \mathbb{Z}[a_1, \ldots, a_n], (a_1, \ldots, a_n) \in \mathcal{V}(\mathfrak{a})$. We have* $\mathrm{maxsub}(\alpha) \in \mathbb{C}$. *We denote the* $\max_{x^\beta \in \mathcal{B}}(\mathrm{maxsub}(\psi^{-1}(x^\beta)))$ *by t. Let ψ_i be the N distinct isomorphisms in (4.1) for each element in $\mathcal{V}$. For $i = 1, \ldots, n$, let*

$$r_i = \max\{\nu : \nu \in \mathbb{N}, \mathrm{lt}(g) = {x_i}^\nu, g \in G\}.$$

Suppose the following conditions are satisfied.

(1) There exists an integer tuple $(m_1, \ldots, m_n)$, $m_i \in \mathbb{N}$, $m_i \geq r_i$ such that for all $1 \leq k \leq N$ and for $(j_1, \ldots, j_n)$ such that $j_i \leq m_i - 1$ we have,

(a) $1 \leq \left| {a_1}^{(k)j_1} \ldots {a_n}^{(k)j_n} \right| \leq t$ *and*

(b) for every $({a_1}^{(k)}, \ldots, {a_n}^{(k)}) \in \mathcal{V}(\mathfrak{a})$,

$$\sum_{k=1}^{N} ({a_1}^{(k)})^{m_1} \ldots ({a_n}^{(k)})^{m_n} \geq N$$

(2) There exists a constant c such that for all $(j_1, \ldots, j_n)$, where $j_i \neq 0 \bmod m_i$ and for $k = 1, \ldots, N$, we have,

$$\left| \sum_{k=1}^{N} ({a_1}^{(k)})^{j_1} \ldots ({a_n}^{(k)})^{j_n} \right| \leq c \leq 1.$$

Then for all $\alpha \in \mathbb{Q}$, we have

$$\text{maxCoeff}_{({a_1}^{(1)},\ldots,{a_n}^{(1)})}(\alpha) \leq \Big(\frac{Nt}{N(1-c)+c}\Big)\text{maxsub}(\alpha).$$

Proof: The existence of $r_i, i = 1, 2, \ldots, n$ is assured by Theorem 3.13. For each $(j_1, \ldots, j_n)$ such that $0 \leq j_i \leq r_i - 1$, we have the following set of N inequalities, $1 \leq k \leq N$

$$\Big|\psi_k(\alpha){a_1}^{(k)^{m_1-r_1+j_1}} \cdots {a_n}^{(k)^{m_n-r_n+j_n}}\Big| \leq \text{maxsub}(\alpha)t.$$

This is because by definition $|\psi_k(\alpha)| \leq \text{maxsub}(\alpha)$ and by (1.a),

$$|{a_1}^{(k)^{m_1-r_1+j_1}} \ldots {a_n}^{(k)^{m_n-r_n+j_n}}| \leq t.$$

We look at the the system of inequalities for a specific $(j_1, \ldots, j_n)$. Let $\alpha = \sum_{i=1}^{N} \alpha_{(i_1,\ldots,i_n)} {a_1}^{i_1} \cdots {a_n}^{i_n}$. We have,

$$\psi_j(\alpha) = \sum_{i=1}^{m} \alpha_{(i_1,\ldots,i_n)} {a_1}^{(j)^{i_1}} \ldots {a_n}^{(j)^{i_n}},$$

where $({a_1}^{(j)}, \ldots, {a_n}^{(j)}) \in \mathcal{V}(\mathfrak{a})$. For $k = 1, \ldots, N$ we have,

$$\begin{aligned}
&\Big|\psi_k(\alpha)({a_1}^{(k)^{m_1-r_1+j_1}} \ldots {a_n}^{(k)^{m_n-r_n+j_n}})\Big| \\
&= \Big|\alpha_{(0,0,\ldots,0)}{a_1}^{(k)^{m_1-r_1+j_1}} \cdots {a_n}^{(k)^{m_n-r_n+j_n}} + \cdots \\
&\quad + \alpha_{(r_1-j_1,\ldots,r_n-j_n)}{a_1}^{(k)^{m_1}} \ldots {a_n}^{(k)^{m_n}} + \cdots + \alpha_{(r_1-1,\ldots,r_n-1)}{a_1}^{(k)^{m_1+j_1-1}} \ldots {a_n}^{(k)^{m_n+j_n-1}}\Big| \\
&\leq \text{maxsub}(\alpha)t.
\end{aligned}$$

Let $A = \sum_{i=1}^{N} \alpha_{(i_1,\ldots,i_n)}$ and $S_{(j_1,\ldots,j_n)} = \sum_{i=1}^{N} {a_1}^{(i)^{m_1-r_1+j_1}} \cdots {a_n}^{(i)^{m_n-r_n+j_n}}$. Then,

$$\begin{aligned}
&N|\alpha_{r_1-j_1,\ldots,r_n-j_n}| - c(A - |\alpha_{r_1-j_1,\ldots,r_n-j_n}|) \\
&= N|\alpha_{r_1-j_1,\ldots,r_n-j_n}| - c(|\alpha_{(0,\ldots,0)}| + \cdots + |\alpha_{(r_1-j_1-1,\ldots,r_n-j_n-1)}| \\
&\quad + |\alpha_{(r_1-j_1+1,\ldots,r_n-j_n+1)}| + \cdots + |\alpha_{(r_1-1,\ldots,r_n-1)}|) \\
&\leq |\alpha_{(r_1-j_1,\ldots,r_n-j_n)}S_{(r_1,\ldots,r_n)}| - (|\alpha_{(0,\ldots,0)}S_{(j_1,\ldots,j_n)}| + \cdots + |\alpha_{(r_1-j_1-1,\ldots,r_n-j_n-1)}S_{(r_1-1,\ldots,r_n-1)}| + \\
&\quad |\alpha_{(r_1-j_1+1,\ldots,r_n-j_n+1)}S_{(r_1+1,\ldots,r_n+1)}| + \cdots + |\alpha_{(r_1-1+j_1,\ldots,r_n-1+j_n)}|) \\
&\leq |\psi_1(\alpha){a_1}^{(1)^{m_1-r_1+j_1}} \cdots {a_n}^{(1)^{m_n-r_n+j_n}}| + \cdots + |\psi_N(\alpha){a_1}^{(N)^{m_1-r_1+j_1}} \cdots {a_n}^{(N)^{m_n-r_n+j_n}}| \\
&\leq Nt\,\text{maxsub}(\alpha).
\end{aligned}$$

This implies,

$$(N+c)|\alpha_{r_1-j_1,\ldots,r_n-j_n}| - cA \leq Nt\,\text{maxsub}(\alpha)$$
$$|\alpha_{r_1-j_1,\ldots,r_n-j_n}| \leq \frac{Nt\,\text{maxsub}(\alpha)+cA}{N+c}.$$

Let $B = \frac{Nt\,\text{maxsub}(\alpha)+cA}{N+s}$. Since $A = \sum_{i=1}^{N} \alpha_{(i_1,\ldots,i_n)}$ we get $A \leq NB$. We have,

$$(N+c-nc)B \leq Nt\,\text{maxsub}(\alpha).$$

We have $|\alpha_{r_1-j_1,\ldots,r_n-j_n}| \leq B$, which implies,

$$\text{maxCoeff}_{(a_1{}^{(1)},\ldots,a_n{}^{(1)})}(\alpha) \leq \frac{Nt}{N(1-c)+c}\text{maxsub}(\alpha).$$

□

The above lemma gives the bound that is similar to the univariate case. We now study the above lemma for the specific case of

$$\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \ldots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1\rangle.$$

In this case, maxCoeff is bound by a factor of N.

Proposition 4.25 *Let*

$$\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \ldots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1\rangle$$

be an ideal in $\mathbb{Z}[x_1,\ldots,x_n]$. *Then,*

$$\mathcal{V}(\mathfrak{a}) = \{(a_1,\ldots,a_n) \in {\mathbb{A}_{\mathbb{C}}}^n : a_i \text{ is a zero of } {x_i}^{r_i-1} + {x_i}^{r_i-2} + \cdots + 1, i = 1,\ldots,n\}.$$

Proposition 4.26 *Let*

$$\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \ldots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1\rangle$$

be an ideal in $\mathbb{Z}[x_1,\ldots,x_n]$, $\mathcal{V}$ *be the finite set of zeroes of cardinality* N *and* $({a_1}^{(1)},\ldots,{a_n}^{(1)})$ *be one of the zeroes. Let* $\alpha \in \mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$. *Then,*

$$\text{maxCoeff}_{(a_1{}^{(1)},\ldots,a_n{}^{(1)})}(\alpha) \leq N\,\text{maxsub}(\alpha)$$

and

$$\text{maxsub}(\alpha) \leq N \, \text{maxCoeff}_{({a_1}^{(1)},\ldots,{a_n}^{(1)})}(\alpha).$$

Proof: By (4.1), $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is isomorphic to $\mathbb{Z}[a_1,\ldots,a_n]$, where $(a_1,\ldots,a_n) \in \mathcal{V}(\mathfrak{a})$. We have from Lemma 4.23 that

$$\text{maxsub}(\alpha) \leq Nt \, \text{maxCoeff}_{({a_1}^{(1)},\ldots,{a_n}^{(1)})}(\alpha).$$

The zeroes of this ideal are the zeroes of each individual generator (Proposition 4.25). Each individual generating polynomial is a cyclotomic polynomial and therefore all the zeroes of the generators are of norm 1 and so we have $t = 1$ and the following inequality,

$$\text{maxsub}(\alpha) \leq N \, \text{maxCoeff}_{({a_1}^{(1)},\ldots,{a_n}^{(1)})}(\alpha).$$

Now to prove that $\text{maxCoeff}_{({a_1}^{(1)},\ldots,{a_n}^{(1)})}(\alpha) \leq N \, \text{maxsub}(\alpha)$. If the conditions in Lemma 4.24 are satisfied we have that

$$\text{maxCoeff}_{({a_1}^{(1)},\ldots,{a_n}^{(1)})}(\alpha) \leq \frac{Nt}{N(1-c)+c}\text{maxsub}(\alpha).$$

Now we show that the conditions in Lemma 4.24 are indeed satisfied. We have $t = 1$ and $m_i = r_i$. We need to determine if

$$\Big|\sum_{i=1}^{N} {a_1}^{(i)^{m_1}} \ldots {a_n}^{(i)^{m_n}}\Big| \geq N,$$

and if we can find a c such that

$$\Big|\sum_{i=1}^{N} {a_1}^{(i)^{j_1}} \ldots {a_n}^{(i)^{j_n}}\Big| \leq c \leq 1.$$

We have that ${a_i}^{(j)}$ is the zero of ${x_i}^{r_i-1} + {x_i}^{r_i-2} + \cdots + 1$. This implies

$${a_i}^{(j)^{m_i}} = ({a_i}^{(j)}(r_i-1) + {a_i}^{(j)}(r_i-2) + \cdots + 1)({a_i}^{(j)} - 1) + 1 = 1.$$

So, $\Big|\sum_{i=1}^{N} {a_1}^{(i)^{m_1}} \ldots {a_n}^{(i)^{m_n}}\Big| = N$. Since each generator, $g_i = {x_i}^{r_i-1} + {x_i}^{r_i-2} + \cdots + 1$, is a cyclotomic polynomial it has a zero, say ${a_i}^{(1)}$, such that all the remaining zeroes, ${a_i}^{(j)}$ is some

power of this root, i.e. ${a_i}^{(1)^j} = {a_i}^{(j)}$. We also have, ${a_i}^{(j)^{r_i}} = 1$, $j = 1, \ldots, n$. Therefore,

$$ {a_i}^{(j)^k} = {a_i}^{(j)^{k \bmod r_i}}, k \in \mathbb{N}. $$

We will now find a c such that the second condition in Lemma 4.24 is satisfied. For all $(j_1, \ldots, j_n)$, where $j_i \neq 0 \bmod m_i$ for some $i = 1, \ldots, n$, we have,

$$ \Big| \sum_{i=1}^{m} ({a_1}^{(i)})^{j_1} \ldots ({a_n}^{(i)})^{j_n} \Big| = \Big| \sum_{i=1}^{m} ({a_1}^{(i)})^{j_1 \bmod m_1} \ldots ({a_n}^{(i)})^{j_n \bmod m_n} \Big|. $$

We replace the zeroes with powers of ${a_i}^{(1)}$ for $i = 1, \ldots, n$. Therefore we have,

$$ \Big| \sum_{i=1}^{m} ({a_1}^{(i)})^{j_1} \ldots ({a_n}^{(i)})^{j_n} \Big| = \Big| \sum_{i=1}^{m} ({a_1}^{(1)})^{i\, j_1 \bmod m_1} \ldots ({a_n}^{(1)})^{i\, j_n \bmod m_n} \Big| $$
$$ = \Big| \sum_{i=1}^{m} (a_1^{(j_1 \bmod m_1)})^i \ldots (a_n^{(j_n \bmod m_n)})^i \Big| = |-1| = 1. $$

We can take $c = 1$ and apply in the inequality from Lemma 4.24 to get,

$$ \text{maxCoeff}_{({a_1}^{(1)}, \ldots, {a_n}^{(1)})}(\alpha) \leq N \, \text{maxsub}(\alpha). $$

□

The result below connects SPP with $SSub$ by a factor that is polynomial in the cardinality of $\mathcal{V}(\mathfrak{a})$.

Theorem 4.27 *Let*

$$ \mathfrak{a} = \langle {x_1}^{r_1 - 1} + {x_1}^{r_1 - 2} + \cdots + 1, \ldots, {x_n}^{r_n - 1} + {x_n}^{r_n - 2} + \cdots + 1 \rangle $$

be an ideal in $\mathbb{Z}[x_1, \ldots, x_n]$. The residue class polynomial ring, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is free and finitely generated. Let $\mathcal{V}(\mathfrak{a})$ be of cardinality N. Let ψ represent the isomorphism as described in (4.1). Then,

$$ \mathfrak{a} - SPP_{\gamma N^2}(\mathfrak{A}) \leq \mathfrak{a} - SSub_{\gamma}(\psi^{-1}(\mathfrak{A})) \text{ and} \tag{4.2} $$
$$ \mathfrak{a} - SSub_{\gamma N^2}(\psi^{-1}(\mathfrak{A})) \leq \mathfrak{a} - SPP_{\gamma}(\mathfrak{A}). \tag{4.3} $$

Proof: Let $\psi^{-1}(\mathfrak{A}) \subseteq \mathbb{Z}[a_1, \ldots, a_n]$, $(a_1, \ldots, a_n) \in \mathcal{V}(\mathfrak{a})$, be an ideal given by its generators $\mathcal{F} = \{f_1, \ldots, f_k\}$. Then each element in $\mathcal{F}$ can be written in terms of the elements $\{a_1, \ldots, a_n\}$

such that $(a_1, \ldots, a_n) \in \mathcal{V}$. The oracle for $\mathfrak{a} - SPP_\gamma(\mathfrak{A}))$ finds us an element $h \in \mathfrak{A}$ such that its norm is less than $\gamma {\lambda_1}^\infty(\mathfrak{A})$. Let $\alpha = \psi^{-1}(h)$. We have,

$$\text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha) \leq \gamma \cdot \text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha^{'}),$$

for all $\alpha^{'} \in \psi^{-1}(\mathfrak{A})$. Applying Proposition 4.26 twice we get,

$$\begin{aligned}\text{maxsub}(\alpha) &\leq N \cdot \text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha),\\ &\leq N\gamma \cdot \text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha^{'}), \text{for all } \alpha^{'} \in \psi^{-1}(\mathfrak{A}),\\ &\leq N^2\gamma \cdot \text{maxsub}(\alpha^{'}), \text{ for all } \alpha^{'} \in \psi^{-1}(\mathfrak{A}).\end{aligned}$$

Thus we have a $\gamma \cdot N^2$ approximation for $\mathfrak{a} - SSub$. Hence (4.3) holds.

Next, we show (4.2) holds. The oracle for $\mathfrak{a} - SSub_\gamma(\psi^{-1}(\mathfrak{A}))$ finds an element $\alpha \in \psi^{-1}(\mathfrak{A})$ such that $\text{maxsub}(\alpha) \leq \gamma \cdot \text{maxsub}(\alpha^{'})$, for all $\alpha^{'} \in \psi^{-1}(\mathfrak{A})$. Again we apply Proposition 4.26 twice.

$$\begin{aligned}\text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha) &\leq N \cdot \text{maxsub}(\alpha),\\ &\leq N\gamma \cdot \text{maxsub}(\alpha^{'}), \text{ for all } \alpha^{'} \in \psi^{-1}(\mathfrak{A}),\\ &\leq N^2\gamma \cdot \text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha^{'}),\end{aligned}$$

for all $\alpha^{'} \in \psi^{-1}(\mathfrak{A})$. We have a $\gamma \cdot N^2$ approximation for $\mathfrak{a} - SPP$. □

4.4 Collision Resistant Generalized Hash Functions

We can construct hash function families described in Section 2.6.3.2 based on multivariate ideal lattices. Consider a prime ideal, $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ such that the residue class polynomial ring, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is free and finitely generated and is of size $N \in \mathbb{N}$. The hash function family $\mathcal{H}(R, D, m)$ is given by $R = \mathbb{Z}_p[x_1, \ldots, x_n]/\mathfrak{a}$, where $p \in \mathbb{N}$ is approximately of the order N^2 and D is a strategically chosen subset of R and $m \in \mathbb{N}$. Let the expansion factor, $\mathcal{E}(\mathfrak{a}, \prec, (3, 3, \ldots, 3)) \leq \eta$, for some $\eta \in \mathbb{R}$. Let $D = \{g \in R : \|g\|_{\mathfrak{a},\prec} \leq d\}$ for some positive integer d. Then $\mathcal{H}$ maps elements from D^m to R. We have $|D^m| = (2d+1)^{Nm}$ and $|R| = p^N$. If $m \gtrsim \frac{\log p}{\log 2d}$, then $\mathcal{H}$ will have collisions. We show that finding a collision for a hash function randomly chosen from $\mathcal{H}$ is as hard as solving $\mathfrak{a} - SPP_\gamma$ for a particular ideal in $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. As we mentioned before, even though the hardness results of univariate and multivariate ideal lattices are based on different problems, other properties like collision resistance of hash functions are exactly analogous. The reader can refer to (Lyubashevsky and Micciancio, 2006) for detailed

constructions.

Theorem 4.28 *Consider an ideal* $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ *such that the residue class polynomial ring,* $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ *is finitely generated of size* $N \in \mathbb{N}$ *and has a free* $\mathbb{Z}$*-module representation w.r.t.* $\prec$*. Let* $\mathcal{H}(R, D, m)$ *be the associated hash function family as mentioned above with* $R = \mathbb{Z}_p[x_1, \ldots, x_n]/\mathfrak{a}$*,* $m \gtrsim \frac{\log p}{\log 2d}$ *and* $p \geq 8\eta dmN^{1.5}\sqrt{\log N}$*. Then, for* $\gamma = 8\eta^2 dmN \log^2 N$*, there is a polynomial time reduction from* $\mathfrak{a} - SPP_\gamma(\mathfrak{A})$ *to* $Collision_{\mathcal{H}}(\mathfrak{h})$*, where* $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ *is an ideal and* $\mathfrak{h}$ *is a hash function chosen uniformly at random from* $\mathcal{H}$*.*

$Collision_{\mathcal{H}}(\mathfrak{h})$ is the problem of finding a collision given a hash function, $\mathfrak{h}$. The idea is that if one can solve in polynomial time the problem $Collision_{\mathcal{H}}(\mathfrak{h})$ for a randomly chosen $\mathfrak{h}$ then we can solve the $\mathfrak{a} - IncSPP_\gamma$ problem for any ideal $\mathfrak{A}$ and $\gamma = 8\eta^2 dmN \log^2 N$. This implies we have a polynomial reduction from $\mathfrak{a} - SPP_\gamma$ to $Collision_{\mathcal{H}}(\mathfrak{h})$.

We consider an oracle $\mathcal{C}$, which when given an $\mathfrak{h}$ returns a collision with nonnegligible probability and in polynomial time. We are given an ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ and an element of the ideal g such that $\|g\|_\infty \gtrsim 8\eta^2 dmN \log^2 N {\lambda_1}^\infty(\mathfrak{A})$. We have to find a nonzero $h \in \mathfrak{A}$ such that $\|h\|_{\mathfrak{a},\prec} \leq \|g\|_{\mathfrak{a},\prec}/2$.

Given vectors $c, x \in \mathbb{R}^N$ and any $l \gtrsim 0$, $\rho_{l,c}(x) = e^{-\pi\|(x-c)/l\|^2}$ represents a Gaussian function that has its center at c and is scaled by l. The total measure is $\int_{x \in \mathbb{R}^N} \rho_{l,c}(x)dx = l^N$ and therefore $\rho_{l,c}/l^N$ is a probability density function. Micciancio and Regev (2004) introduced certain techniques to approximate the distribution efficiently, effectively allowing us to sample from the distribution, $\rho_{l,c}/l^N$ exactly. In this paper, the results are used in the same way as in (Lyubashevsky and Micciancio, 2006) as the results are for integer lattices in general and not specifically for ideal lattices in one variable.

Let $s = \frac{\|g\|_\infty}{8\eta\sqrt{N}dm \log N}$. Therefore, $\|g\|_\infty = 8\eta dms\sqrt{N} \log N$. Also (Micciancio and Regev, 2004, Lemma 4.1) implies that if we sample $y \in \mathbb{R}^N$ from the distribution ρ_s/s^N, then

$$\triangle(y + \mathfrak{A}, U(\mathbb{R}^N/\mathfrak{A})) \leq (\log N)^{-2 \log N}/2,$$

i.e. $y + \mathfrak{A}$ is a uniformly random coset. We list a procedure in Algorithm 6, by which using the access to the oracle one can determine an h such that it is a solution to the $IncSPP_\gamma$ problem. Now, it is enough to show that Algorithm 6 runs in polynomial time, the inputs to the oracle are uniformly random, and h satisfies all the desired properties.

Lemma 4.29 *Algorithm 6 runs in polynomial time.*

Proof: In Step (4), we need to generate a random coset of $\mathfrak{A}/\langle g \rangle$. Since $\mathfrak{a}$ is a prime ideal, the ideals $\mathfrak{A}$ and $\langle g \rangle$ are $\mathbb{Z}$-modules of dimension n. There is a polynomial time algorithm to

Algorithm 6 Finding the solution of the $IncSPP_\gamma$ problem given access to the *Collision* oracle

1: **Input** Finitely generated $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ with a free $\mathbb{Z}$-module representation w.r.t. $\prec$, $\mathfrak{A} \subseteq \mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ an ideal, and $g \in \mathfrak{A}$ such that $\|g\|_\infty = 8\eta dms\sqrt{N}\log N$.
2: **Output** $h \in \mathfrak{A}$ such that $\|h\| \neq 0$ $\|h\|_{\mathfrak{a},\prec} \leq \|g\|_{\mathfrak{a},\prec}/2$.
3: **for** $i = 1$ to m **do**
4: Generate a random coset of $\mathfrak{A}/\langle g\rangle$ and let v_i be a polynomial in that coset.
5: Generate $y_i \in \mathbb{R}^N$ such that y_i has distribution ρ_s/s^n and consider y_i as a polynomial in $\mathbb{R}[x_1,\ldots,x_n]$.
6: Let $w_i \in \mathbb{R}[x_1,\ldots,x_n]$ be the unique polynomial such that $p(v_i+y_i) \equiv gw_i$ in $\mathbb{R}^N/\langle pg\rangle$. Note that the coefficients of w_i lie in $[0,p)$.
7: Let $a_i = [w_i] \bmod p$.
8: **end for**
9: Give $(a_1,\ldots,a_m)$ as input to the oracle C and using its output determine polynomials $z_1,\ldots,z_m$ such that $\|z\|_{\mathfrak{a},\prec} \leq 2d$ and $\sum_{i=1}^m z_i a_i \equiv 0$ in the ring $\mathbb{Z}_p[x_1,\ldots,x_n]/\mathfrak{a}$. (Details of the construction of z_i can be found in Lemma 4.29).
10: Output $h = \left(\sum_{i=1}^m \left(\frac{g(w_i-[w_i]}{p} - y_i\right)z_i\right) \bmod \mathfrak{a}$.

generate a random element from $\mathfrak{A}/\langle g\rangle$ (Micciancio, 2002, Proposition 8.2). Step (5) and Step (6) will be justified in the following lemma. Step (7) just rounds off the coefficients and takes modulo p and therefore can be done in polynomial time. In Step (9), we feed $(a_1,\ldots,a_m)$ to the *Collision* oracle and it returns $(\alpha_1,\ldots,\alpha_m),(\beta_1,\ldots,\beta_m)$ such that $\|\alpha_i\|_{\mathfrak{a},\prec}, \|\beta_i\|_{\mathfrak{a},\prec} \leq d$ and $\sum_{i=1}^m a_i\alpha_i \equiv \sum_{i=1}^m a_i\beta_i$ in $\mathbb{Z}_p[x_1,\ldots,x_n]/\mathfrak{a}$. Therefore, if we set $z_i = \alpha_i - \beta_i$, it satisfies the properties of Step (9). □

Lemma 4.30 *Consider the polynomials a_i as elements in ${\mathbb{Z}_p}^N$. Then,*

$$\triangle((a_1,\ldots,a_m), U({\mathbb{Z}_p}^{N\times m})) \leq m(\log N)^{-2\log N}/2.$$

Proof: We have chosen v_i from a uniformly random coset of $\mathfrak{A}/\langle g\rangle$. If y_i is in a uniformly random coset of $\mathbb{R}^N/\langle g\rangle$, then $p(v_i+y_i)$ is a uniformly random coset of $\mathbb{R}^N/\langle pg\rangle$. A basis for $\mathbb{R}^N/\langle pg\rangle$ is $\{pgb_1,\ldots,pgb_N\}$ where $\{b_1,\ldots,b_N\}$ is the basis of $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$. Every element in $\mathbb{R}^N/\langle pg\rangle$ can be represented as $\alpha_0 pgb_1 + \cdots + \alpha_N pgb_N$ where $\alpha_i \in [0,1)$. Therefore Step (6) is justified with $w_i = \alpha_0 pb_1 + \cdots + \alpha_N pb_N$. Since we have assumed $p(v_i+y_i)$ is a uniformly random coset of $\mathbb{R}^N/\langle pg\rangle$, the coefficients of w_i are uniform over $[0,p)$ and the input to the oracle in Step (9) is correct. The only thing remaining is to check if the assumption that y_i is in a uniformly random coset of $\mathbb{R}^N/\langle g\rangle$ is correct. It is not exactly uniformly random but very close to it. We have $\triangle(\rho_s/s^n + \mathfrak{A}, U(\mathbb{R}^N/\mathfrak{A})) \leq (\log N)^{-2\log N}/2$. Since a_i is a function

of y_i, we have $\triangle(a_i, U({\mathbb{Z}_p}^N)) \leq (\log N)^{-2\log N}/2$. Since all the a_is are independent we have $\triangle((a_1, \ldots, a_m), U({\mathbb{Z}_p}^{N\times m})) \leq m(\log N)^{-2\log N}/2$. □

The following three lemmas ensure that the output of the algorithm, h satisfies the desired properties of the $IncSPP_\gamma$ problem, i.e. h is nonzero, $h \in \mathfrak{A}$ and $\|h\|_{\mathfrak{a},\prec} \leq \frac{\|g\|_\infty}{2}$.

Lemma 4.31 $h \in \mathfrak{A}$.

Proof: The proof proceeds exactly in the same lines as the univariate case. See (Lyubashevsky and Micciancio, 2006, Lemma 5.4). □

Lemma 4.32 *With probability negligibly different from* 1, $\|h\|_{\mathfrak{a},\prec} \leq \frac{\|g\|_\infty}{2}$.

Proof: See proof of (Lyubashevsky and Micciancio, 2006, Lemma 5.5). □

Lemma 4.33 $Pr[h \neq 0|(a_1, \ldots, a_m)(z_1, \ldots, z_m)] = \Omega(1)$.

Proof: See proof of (Lyubashevsky and Micciancio, 2006, Lemma 5.6). □

Polynomial computations in the univariate case are well studied and efficient methods using FFT have been proposed. A major challenge in designing practical implementations using multivariate ideal lattices is to come up with similar efficient methods for multivariate polynomial computations. We also need to study the security issues of multivariate ideal lattices. Another interesting direction is to see if other cryptographic primitives like digital signatures, identification schemes can be built from multivariate ideal lattices.

Chapter 5

Krull Dimension of Residue Class Polynomial Rings over Integral Domains

One of the fundamental problems in computational ideal theory is determining the dimension of an ideal, i.e. the Krull dimension of the $\Bbbk$-algebra, $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. The dimension of an affine variety associated with an ideal, $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ is the Krull dimension of the affine $\Bbbk$-algebra, $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$, for an algebraically closed field $\Bbbk$. We discuss this in detail in Section 2.4. Since the definition of Krull dimension does not lead to an algorithmic method to compute it, various alternate equivalent definitions have been proposed (See Section 2.4.1, 2.4.2, 2.4.3). The Krull dimension of an affine $\Bbbk$-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 $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$) (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 $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ (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 thesis studies the question of whether one can give Gröbner basis methods to compute the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$, where A is a Noetherian integral domain, given that it has a free A-module representation w.r.t. some monomial order. Note that in this chapter, the coefficient ring A is restricted to integral domains.

For any Noetherian commutative ring, Theorem 3.10 gives a necessary and sufficient condition for a residue class polynomial ring to have a free module representation w.r.t. a monomial

order. It need not necessarily be a finitely generated 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 in Section 5.1. 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 Section 5.1.2. In affine $\Bbbk$-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 in Section 5.2. In Section 5.2.2, we illustrate with examples how this relation gives an algorithmic method to determine the Krull dimension of such A-algebras. We also show that the concepts of Hilbert function, 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 in Section 5.3. We also give a Gröbner basis algorithm to compute these quantities. We then show in Section 5.3.2 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 polynomial ring in Section 5.3.3. 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 $A[x_1, \ldots, x_n]/\mathfrak{a}$ 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.

For a free A-module M, the minimum cardinality of a basis of M is called its free rank and is denoted by $\text{FreeRank}_A(M)$.

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

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

Definition 5.1 *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* $\text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$.

5.1.1 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 5.2 *Let* A *be a Noetherian integral domain and* $\mathfrak{a}$ *be an ideal in* $A[x_1, \ldots, x_n]$*. Then* $\text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$ *is the maximum of* $\text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{p})$*, where* $\mathfrak{p}$ *is an isolated prime ideal associated with* $\mathfrak{a}$*.*

Proof: We will denote $\text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$ 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, $\text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{p}') \geq d$. □

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

Proposition 5.3 *Given a Noetherian integral domain* A*, let* $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ *be a prime ideal. Then, all maximal set 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 $\text{Quot}(A[x_1, \ldots, x_n]/\mathfrak{a})$ 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 $\text{Quot}(A[x_1, \ldots, x_n]/\mathfrak{a})$ 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 $\text{Quot}(A[\overline{S}])(\overline{a})$ and $\overline{a}$ is algebraic over $\text{Quot}(A[\overline{S}])(\overline{b_2})$. Therefore, $\overline{b_1}$ is algebraic over $\text{Quot}(A[\overline{S}])(\overline{b_2})$, which is a contradiction to the independence of $S \cup \{b_1, b_2\}$ modulo $\mathfrak{a}$. □

5.1.2 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 $\mathbb{k}[x_1, \ldots, x_n]$, to polynomial rings over A.

Definition 5.4 *Let $S \subseteq X$ be a set of indeterminates and $\prec$ a monomial order in $A[x_1, \ldots, x_n]$. Then, $A[S/(X \setminus S)]$ denotes the following set,*

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

We say that S is strongly independent modulo $\mathfrak{a}$ if $A[S/(X \setminus S)] \cap \mathfrak{a} = \{0\}$.

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

Lemma 5.5 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be a proper ideal and $\prec$ be a monomial order in $A[x_1, \ldots, x_n]$. 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 $A[x_1, \ldots, x_n]$ 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, $f \in A[x_1, \ldots, x_n]$ be a polynomial and $\prec$ be a monomial order in $A[x_1, \ldots, x_n]$. 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, $t^S \prec \mathrm{lt}(f)^S$.

Theorem 5.6 *Let $S \subseteq X$, $\mathfrak{a}$ be a prime ideal in $A[x_1, \ldots, x_n]$ and $\prec$ be a monomial order such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ 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 $|S| = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$.*

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 $t \in \mathrm{Mon}(A[x_1, \ldots, x_n])$ such that for every $x \in X \setminus S$, the degree of x in t is $\lneq d_x$.

Claim 5.7 *For every $t \in \mathrm{Mon}[x_1, \ldots, x_n] \setminus T$, there exists $0 \neq p, p_1, \ldots, p_m \in A[S]$, $t_1, \ldots, t_m \in T$ 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 $t \in \mathrm{Mon}(A[x_1, \ldots, x_n]) \setminus T$ 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

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

We have $x^{d-d_x} u f_x \in \mathfrak{a}$ 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 5.7 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 5.7, $\mathrm{Quot}(A)[x_1, \ldots, x_n]/\mathfrak{a}$ 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 5.8 (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,*

$$S_0 = \phi$$

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

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 5.6 we have the following result for prime ideals.

Corollary 5.9 *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 $|S| = \operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$.*

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 $t \in \operatorname{Mon}(f_x)$, the degree of t in x is less than or equal to the degree of the leading term of f_x in x. Therefore, $\operatorname{lt}(f_x)^S \geq t^S$ for all terms in f_x. Therefore, S is inessential for f_x and we can apply Theorem 5.6 and $|S| = \operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$. □

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

Theorem 5.10 *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*

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

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

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

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

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

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

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

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

Theorem 5.11 *Let $\prec$ be a monomial ordering in $A[x_1, \ldots, x_n]$ and $S \subseteq X$ be a set of indeterminates. Let G be a Gröbner basis of an ideal, $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ w.r.t. $\prec$. Then S is strongly independent modulo $\mathfrak{a}$ w.r.t. $\prec$ if and only if $A[S] \cap \text{lt}(G) = \phi$.*

Proof: If for some $g \in G$, $\text{lt}(g) \in A[S]$, 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 atleast one $g \in G$ such that $\text{lm}(g) \mid \text{lm}(f)$. Since $\text{lt}(f) \in A[S]$, $\text{lm}(g) \in A[S]$. □

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 5.12 *Let $\prec$ be a monomial order in $A[x_1, \ldots, x_n]$ and G be a Gröbner basis w.r.t. to $\prec$ for an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$. Algorithm 7 determines the left basic set of $\mathfrak{a}$ w.r.t. $\prec$.*

Algorithm 7 Finding the Left Basic Set of an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$

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

Corollary 5.13 *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. 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*

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

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 $|S| = \text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$.

Proof: This result is a direct consequence of Theorem 5.11 and Theorem 5.10. □

The above result gives us an algorithmic technique to determine the combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$. 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, $A[x_1, \ldots, x_n]/\mathfrak{a}$, that have a free A-module representation w.r.t. a lexicographic ordering. The correctness of the algorithm follows from Corollary 5.13. It consists of two routines, Algorithm 8 and Algorithm 9, the latter of which is recursive. Algorithm 9 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 8 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
$c = 0$, $S = \phi$, $U = X$, $\mathcal{M} = \phi$
{Calls the recursive algorithm}
$\mathcal{M}$ = Algorithm 9$(G, S, U, \mathcal{M})$
$\mathcal{S} = \mathcal{M}$
while $\mathcal{M} \neq \phi$ **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 9 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 $\mathrm{Mon}(S) \cap \mathrm{lt}(G) = \phi$,
U, a subset of the indeterminates set X,
$\mathcal{M}$, a set of already computed maximal sets $S^{'}$ with $\mathrm{Mon}(S^{'}) \cap \mathrm{lt}(G) = \phi$.
Output $\mathcal{M}^{'}$, the updated set of maximal set of indeterminates $S^{'}$ with $\mathrm{Mon}(S^{'}) \cap \mathrm{lt}(G) = \phi$.
{Finding the maximal independent sets of indeterminates}
$\mathcal{M}^{'} = \mathcal{M}$
while $U \neq \phi$ **do**
  Select u from U
  $U = U \setminus \{u\}$
  if $\mathrm{Mon}(S \cup \{u\}) \cap \mathrm{lt}(G) = \phi$ **then**
    $\mathcal{M}^{'}$ = Algorithm 9$(G, S \cup \{u\}, U, \mathcal{M}^{'})$
  end if
end while
{ Testing if S is already contained in some element of $\mathcal{M}^{'}$}
$\mathcal{M}^{''} = \mathcal{M}^{'}$, $t = 1$
while $\mathcal{M}^{''} \neq \phi$ 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 $A[x_1, \ldots, x_n]$.

5.2 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 5.3.3).

Lemma 5.14 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal and M be an A-algebra. Then there exists a canonical injection 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. Then 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,

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

□

Proposition 5.15 *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,*

$$\nu : A[x_1,\ldots,x_n] \longrightarrow k(\mathfrak{p})[x_1,\ldots,x_n] \tag{5.1}$$

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

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

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 $\mathrm{lt}(\mathfrak{a})k(\mathfrak{p})[x_1,\ldots,x_n]\subseteq\mathrm{lt}(\mathfrak{a}^e)$. This is true for any ring homomorphism (Bayer et al., 1991, Proposition 3.4). It is enough to show that each generator of $\mathrm{lt}(\mathfrak{a})k(\mathfrak{p})[x_1,\ldots,x_n]$ belongs to $\mathrm{lt}(\mathfrak{a}^e)$. The generators of $\mathrm{lt}(\mathfrak{a})k(\mathfrak{p})[x_1,\ldots,x_n]$ 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 $\nu(\mathrm{lt}(f))=\mathrm{lt}(f)=\mathrm{lt}(\nu(f))\in\mathrm{lt}(\mathfrak{a}^e)$, if $\mathrm{lc}(f)\notin\mathfrak{p}$.

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

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

We claim that $\mathrm{lt}(g_j)\mid x^\alpha$ for some $j\in\{1,\ldots,t\}$. 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, $x^\alpha\in\mathrm{lt}(\mathfrak{a})$ and $cx^\alpha\in\mathrm{lt}(\mathfrak{a})k(\mathfrak{p})[x_1,\ldots,x_n]$. We have, $\nu(G)$ is a Gröbner basis for $\mathfrak{a}^e$. □

Consider the ring homomorphism,

$$f : A \longrightarrow A[x_1, \ldots, x_n]/\mathfrak{a}. \tag{5.2}$$

We have the corresponding mapping associated with f,

$$f^* : \mathrm{Spec}(A[x_1, \ldots, x_n]/\mathfrak{a}) \longrightarrow \mathrm{Spec}(A). \tag{5.3}$$

Consider a prime ideal $\mathfrak{p}$ in A. The subspace $f^{*-1}(\mathfrak{p})$ of $\mathrm{Spec}(A[x_1, \ldots, x_n]/\mathfrak{a})$ is naturally homeomorphic to $\mathrm{Spec}(k(\mathfrak{p}) \otimes_A A[x_1, \ldots, x_n]/\mathfrak{a})$, 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 $A[x_1, \ldots, x_n]/\mathfrak{a}$ lying over $\mathfrak{p}$ and $\mathrm{Spec}(k(\mathfrak{p}) \otimes_A A[x_1, \ldots, x_n]/\mathfrak{a})$. By Lemma 5.14, we have

$$k(\mathfrak{p}) \otimes_A A[x_1, \ldots, x_n]/\mathfrak{a} \cong k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e. \tag{5.4}$$

Theorem 5.16 *Let $\mathfrak{a}$ be a proper ideal in $A[x_1, \ldots, x_n]$ 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 $A[x_1, \ldots, x_n]/\mathfrak{a}$ such that P is maximal among the prime ideals lying over $\mathfrak{p}$. Then,*

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

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 (5.1).

Proof: Consider the ring homomorphism given in (5.2),

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

Since $\mathfrak{a}$ has a monic Gröbner basis w.r.t. some monomial ordering, $A[x_1, \ldots, x_n]/\mathfrak{a}$ 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),

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

To ease the notation, we denote $A[x_1, \ldots, x_n]/\mathfrak{a}$ 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,

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

Consider $A[x_1, \ldots, x_n]/\mathfrak{a} \otimes k(\mathfrak{p})$. By (5.4), it is isomorphic to $k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e$. All maximal ideals in the affine algebra, $k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e$ are of the same height equal to $\text{kdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e)$. Therefore,

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

and we have,

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

□

5.2.1 Krull dimension of A-algebras for lexicographic orderings

Proposition 5.17 *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 5.15 and $\mathfrak{a}^e$ be the extension of $\mathfrak{a}$ in $k(\mathfrak{p})[x_1, \ldots, x_n]$. Then,*

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

Proof: Let G be the monic short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. a lexicographic ordering $\prec$. From Proposition 5.15, we have that $\nu(G)$ is a monic Gröbner basis for $\mathfrak{a}^e$ and $\text{lt}(G) = \text{lt}(\nu(G))$. Therefore, the set of indeterminates, $S \subseteq X$ such that $\text{Mon}(A[S]) \cap \text{lt}(G) = \phi$ is the same as the set of indeterminates, $S' \subseteq X$ that satisfy $\text{Mon}(k(\mathfrak{p})[S']) \cap \text{lt}(\nu(G)) = \phi$. Then by Corollary 5.13,

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

and hence the proof. □

Corollary 5.18 *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,*

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

Proof: From Proposition 5.17, we have

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

When the coefficient ring is a field, $\text{kdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e) = \text{cdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e)$. This implies that the equation in Proposition 5.16 becomes,

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

Since $\mathfrak{a}$ is a proper ideal with a monic Gröbner basis, the mapping in (5.3),
$f^* : \text{Spec}(A[x_1, \ldots, x_n]/\mathfrak{a}) \longrightarrow \text{Spec}(A)$, is surjective and we have,

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

□

Given a Noetherian integral domain, using Corollary 5.18 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 10. This algorithm calls Algorithm 8, which returns the maximal sets of indeterminates independent modulo $\mathfrak{a}$ and the combinatorial dimension of the corresponding A-algebra.

Algorithm 10 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
$c = 0$, $S = \phi$, $t = 0$, $\mathcal{S} = \phi$
{Calls the combinatorial dimension algorithm}
$\mathcal{S}, c =$ Algorithm 8(G, X)
$d = c + d_A$

5.2.2 Examples

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

Example 5.19 *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* $\langle xy, xz\rangle$. *Then either* $\mathfrak{p}$ *is minimal over* $\langle x\rangle$ *or minimal over* $\langle y, z\rangle$. *Also, every minimal prime over* $\langle x\rangle$ *and* $\langle y, z\rangle$ *gives rise to a minimal prime of* $\mathcal{A}$. *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 5.20 *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* $\mathcal{A} = \text{kdim}(A[x^{\pm 1}]) = \text{kdim}(A) + 1$.

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 5.21 *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 5.22 *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,* $\mathrm{cdim}(\mathcal{A}) = |S| = 1$ *and* $\mathrm{kdim}(\mathcal{A}) = \mathrm{kdim}(A) + 1$*.*

Example 5.23 *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,* $\mathrm{cdim}(\mathbb{Z}[x, y, z]/\mathfrak{a}) = |S| = 1$ *and* $\mathrm{kdim}(\mathbb{Z}[x, y, z]/\mathfrak{a}) = 2$*.*

5.3 Hilbert Polynomials in $A[x_1, \ldots, x_n]$

5.3.1 Hilbert function and Hilbert series

Proposition 5.24 *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 nonnegative 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 5.25 $\mathcal{B}^{(d)}$ *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 5.26 *If $\mathfrak{a} = \langle f \rangle \subseteq A[x_1, \ldots, x_n], f \neq 0$ is a principal ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is free, then*

$$H_{\mathfrak{a}}(t) = \frac{1 - t^{\deg(f)}}{(1-t)^{n+1}} \quad \text{if } f \neq 0$$
$$H_{\mathfrak{a}}(t) = \frac{1}{(1-t)^{n+1}} \quad \text{if } f = 0.$$

Proof: The proof is along similar lines as over fields (Kemper, 2011, Proposition 11.4). □

Theorem 5.27 *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,*

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

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.

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

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 $t \notin \mathrm{lt}(\mathfrak{a})$. 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 $\mathrm{Mon}(f) \notin \mathrm{lt}(\mathfrak{a})$. 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. □

The following results will help us give a Gröbner basis algorithm to determine the Hilbert series of an ideal. The proofs are straightforward and therefore we omit the details.

Proposition 5.28 *The ideal, $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ is homogeneous if and only if the short reduced Gröbner basis of $\mathfrak{a}$ is homogeneous.*

Proposition 5.29 *Let I and J be two monomial ideals such that $A[x_1, \ldots, x_n]/I$ and $A[x_1, \ldots, x_n]/J$ have a free A-module representation w.r.t. a monomial order. Then $A[x_1, \ldots, x_n]/I \cap J$ and $A[x_1, \ldots, x_n]/I + J$ also have a free A-module representation w.r.t. the same monomial order.*

Proposition 5.30 *Let I, J be monomial ideals such that $A[x_1, \ldots, x_n]/I$ and $A[x_1, \ldots, x_n]/J$ have a free A-module representation w.r.t a monomial order. Then, $H_{I+J}(t) + H_{I\cap J}(t) = H_I(t) + H_J(t)$.*

Proof: Let $I = \langle g_1, \ldots, g_t \rangle$ and $J = \langle g_{t+1}, \ldots, g_{m+t} \rangle$ be the monic short reduced Gröbner bases with respect to which $A[x_1, \ldots, x_n]/I$ and $A[x_1, \ldots, x_n]/J$ have free A-module representations. For any ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$, we denote $\mathfrak{a}_{\leq d}$ as the set of all elements of the ideal with degree $\leq d$. Any element, $f \in (I + J)_{\leq d}$ can be written as $f = \sum_{i=1}^{m+t} h_i g_i$, where $h_i \in A[x_1, \ldots, x_n]$. Since $\deg(f) \leq d$ and each g_i is a monomial, the equation is valid even when we remove parts of h_i that are of degree $\gtrsim (d - \deg(g_i))$. Therefore, the following map is surjective.

$$\begin{aligned} I_{\leq d} &\to (I + J)_{\leq d}/J_{\leq d}, \\ f &\mapsto f + J_{\leq d}. \end{aligned}$$

The kernel of the map is $(I \cap J)_{\leq d}$. We therefore have,

$$I_{\leq d}/(I \cap J)_{\leq d} \cong (I + J)_{\leq d}/J_{\leq d}.$$

Since the short reduced Gröbner bases of $I, J, I + J, I \cap J$ are monic, the A-modules in the above congruence are free and therefore the following equation holds.

$$\begin{aligned} &\text{FreeRank}_A(I_{\leq d}) - \text{FreeRank}_A(I \cap J)_{\leq d} \\ &= \text{FreeRank}_A(I + J)_{\leq d} - \text{FreeRank}_A J_{\leq d}. \end{aligned}$$

Equivalently,

$$\begin{aligned}
&(\text{FreeRank}_A A[x_1,\ldots,x_n]_{\leq d} - \text{FreeRank}_A(I_{\leq d})) \\
&+ (\text{FreeRank}_A A[x_1,\ldots,x_n]_{\leq d} - \text{FreeRank}_A(J_{\leq d})) = \\
&(\text{FreeRank}_A A[x_1,\ldots,x_n]_{\leq d} - \text{FreeRank}_A(I \cap J)_{\leq d}) + \\
&(\text{FreeRank}_A A[x_1,\ldots,x_n]_{\leq d} - \text{FreeRank}_A(I + J)_{\leq d}).
\end{aligned}$$

We then have the desired result. □

Algorithm 11 gives a Gröbner basis method to calculate the Hilbert Series of an ideal in $A[x_1,\ldots,x_n]$.

Algorithm 11 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
$J' = \langle \text{lcm}(m_1,m_2),\cdots,\text{lcm}(m_1,m_s)\rangle$.
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 5.31 *Algorithm 11 terminates after finitely many steps and calculates $H_{\mathfrak{a}}(t)$ correctly.*

Proof: With each recursive call the value of s decreases and this ensures termination. We have $\mathfrak{a}' = \langle m_1,\cdots,m_s\rangle = \text{lt}(\mathfrak{a})$. By Theorem 5.27, since we have a free A-module representation w.r.t. a degree compatible monomial ordering, the Hilbert series of $\mathfrak{a}'$ and $\mathfrak{a}$ are equal. Therefore, the proof will be complete if we show that the algorithm computes the Hilbert series of $\mathfrak{a}'$ correctly. We use induction. For $s = 0$, by Theorem 5.26 we have that the Hilbert series is computed correctly. For $s \gneq 0$, the algorithm is correct since the ideals, J and J' are monic monomial ideals. It can be easily seen that $J' = J \cap \langle m_1\rangle$ (Kemper, 2011, Theorem 11.9). We

have, $\mathfrak{a}' = J + \langle m_1 \rangle$. Therefore by Proposition 5.30,

$$\begin{aligned} H_{\mathfrak{a}'}(t) &= H_{\langle m_1 \rangle}(t) + H_J(t) - H_{J'}(t), \\ &= \frac{1 - t^{\deg(m_1)}}{(1-t)^{n+1}} + H_J(t) - H_{J'}(t). \end{aligned}$$

This proves the correctness of the algorithm. □

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

Theorem 5.32 (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,

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

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.

5.3.2 Relation between Hilbert polynomials and combinatorial dimension

We first show that given a free A-module, $A[x_1, \ldots, n]/\mathfrak{a}$ with a free A-module representation w.r.t. a degree compatible ordering, the degree of the Hilbert polynomial is equal to its combinatorial dimension. This equality will aid us in giving a relation between Krull dimension and degree of a Hilbert polynomial for degree compatible monomial orderings.

Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible monomial ordering. Since a free A-module representation implies monic leading terms and Theorem 5.27 ensures that $\mathfrak{a}$ and $\mathrm{lt}(\mathfrak{a})$ have the same Hilbert function, it is enough to study Hilbert functions for monomial ideals. In a study of monomial ideals in general, it does not make sense to specify a degree compatible monomial ordering. So in this

section for a monomial ideal, $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]/\mathfrak{a}$, we will only specify that $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t some monomial order, $\prec$. Note that when we look at the monomial ideal as a leading term ideal of an arbitrary ideal, $\mathfrak{I}$ then $A[x_1, \ldots, x_n]/\mathfrak{I}$ needs to have a free A-module representation w.r.t. a degree compatible ordering and the monomial ideal under consideration will be $\mathrm{lt}(\mathfrak{a})(= \mathrm{lm}(\mathfrak{a}))$.

We prove the equivalence of the combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ and the degree of Hilbert polynomial of $\mathfrak{a}$ using the concept of translate (O'Shea et al., 2007, Section 2, Chapter 9).

Definition 5.33 *For each monomial ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$, let*

$$\mathcal{C}(\mathfrak{a}) = \{u \in \mathrm{Mon}(A[x_1, \ldots, x_n]) : u \notin \mathfrak{a}\}$$

be the set of standard monomials of $\mathfrak{a}$.

For any two sets $S_1, S_2 \subseteq \mathrm{Mon}(A[x_1, \ldots, x_n])$ define the product as $S_1 S_2 = \{u \cdot v : u \in S_1, v \in S_2\}$.

Definition 5.34 *For every integer $r \in \{1, \ldots, n\}$, every set of indeterminates $\{x_{i_1}, \ldots, x_{i_r}\} \subseteq \{x_1, \ldots, x_n\}$, and every $u \in \mathrm{Mon}(A[x_1, \ldots, x_n])$, we refer to the set of monomials,*

$$\{u\} \cdot \mathrm{Mon}(A[x_{i_1}, \ldots, x_{i_r}])$$

as a translate of dimension r. Also, by convention every singleton set $\{u\} \subseteq \mathrm{Mon}(A[x_1, \ldots, x_n])$ is called a translate of dimension 0.

Theorem 5.35 *If $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ is a monomial 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, then $\mathcal{C}(\mathfrak{a})$ can be written as a finite disjoint union of translates.*

Proof: The proof goes along the same lines as (Winkler, 2010, Theorem 5.3). □

Lemma 5.36 *Let $u \in \mathrm{Mon}(A[x_1, \ldots, x_n])$ and $t = \deg(u)$.*

(i) The number of monomials of degree $\leq s$ in the translate $\{u\} \cdot \mathrm{Mon}(A[x_1, \ldots, x_m])$ is equal to the binomial coefficient, $C(m + s - t, s - t)$, provided $s \geq t$.

(ii) For $s \geq t$, the number of monomials is a polynomial function of s of degree m and the coefficient of s^m is $1/m!$.

Proof: The proof goes along the same lines as (Winkler, 2010, Theorem 5.5). □

Theorem 5.37 *If $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ is a proper monomial ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. some monomial order, then for all s sufficiently large, the number of monomials not in $\mathfrak{a}$ of degree $\leq s$ is a polynomial of degree d in s. This degree, d is equal to the combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$. Also, the coefficient of s^d in the polynomial is positive.*

Proof: By Theorem 5.35, we can write $\mathcal{C}(\mathfrak{a}) = \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_r$. For $j \in \{1, \ldots, r\}$ and a non-negative integer s we denote the number of monomials in $\mathcal{C}_j$ of degree $\leq s$ by $c_j(s)$ and the number of monomials in $\mathcal{C}(\mathfrak{a})$ of degree $\leq s$ by $c(s)$. Because we have a disjoint union,

$$c(s) = c_1(s) + \cdots + c_r(s).$$

From Lemma 5.36, we have for every $j \in \{1, \ldots, r\}$ there exists a non-negative integer t_j and a univariate polynomial $p_j(x) = a_{m_j}x^{m_j} + \cdots + a_0 \in \mathbb{Q}[x]$, such that

(i) $c_j(s) = p_j(s)$ for every $s \geq t_j$,

(ii) m_j is the dimension of the translate $\mathcal{C}_j$ and $a_{m_j} = 1/m_j!$.

Let $t^* = \max(t_1, \ldots, t_r)$ and m^* be the maximal dimension of the translates $\mathcal{C}_1, \ldots, \mathcal{C}_r$. Clearly, for $s \geq t^*$, the function c is given by a polynomial of degree m^* and the coefficient of s^{m^*} in this polynomial is positive.

Now we need to show that $m^* = \operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$. Let $\{x_{i_1}, \ldots, x_{i_k}\}$ be a set of independent indeterminates modulo $\mathfrak{a}$. Obviously, $\operatorname{Mon}(A[x_{i_1}, \ldots, x_{i_k}]) \subseteq \mathcal{C}(\mathfrak{a})$. Hence, by Lemma 5.36, $k \leq m^*$. Since $\operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$ is the maximal cardinality of any set of independent indeterminates, $\operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) \leq m^*$. Consider the translate $\{u\} \cdot \operatorname{Mon}(A[x_{i_1}, \ldots, x_{i_k}]) \subseteq \mathcal{C}(\mathfrak{a})$. Since $\mathfrak{a}$ is an ideal, we obtain $\operatorname{Mon}(A[x_{i_1}, \ldots, x_{i_k}]) \subseteq \mathcal{C}(\mathfrak{a})$ which implies that $\{x_{i_1}, \ldots, x_{i_k}\}$ is a set of independent indeterminates modulo $\mathfrak{a}$. Therefore, $\operatorname{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) \geq m^*$. □

It can be easily seen from the definition of Hilbert functions and translates that the function, $c(s)$ in the above theorem is the same as the Hilbert function. The degree of the Hilbert polynomial is therefore m^*. So far, we have shown that given a monomial ideal, $\mathfrak{a}$ such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. some monomial ordering, the degree of the Hilbert polynomial of $\mathfrak{a}$ is the same as the combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$. We have also seen in Theorem 5.27 that if $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. a degree compatible ordering, then the Hilbert functions of both the ideal and the leading

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

Theorem 5.38 *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 degree compatible ordering, $\prec$. Then, $\text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$ equals the degree of the Hilbert polynomial of $\mathfrak{a}$.*

Proof: Let d denote the combinatorial dimension of $\mathfrak{a}$. Let the set $\{x_{i_1}, \ldots, x_{i_d}\}$ be a set of independent indeterminates modulo $\mathfrak{a}$ of maximal cardinality. Let s be a non-negative integer. From Theorem 5.24, we have that $\text{Mon}(A[x_{i_1}, \ldots, x_{i_d}])_{\leq s}$ is a linearly independent set of $\mathcal{A}_{\leq s}$. By Lemma 5.36, $C(d+s, s) \leq h_{\mathfrak{a}}(s)$. Since the binomial coefficient is a polynomial function in s of degree d, the $\text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$ is at most the degree of the Hilbert polynomial.

Let $\text{lt}(\mathfrak{a})$ be the leading term ideal of $\mathfrak{a}$ w.r.t. $\prec$. If $S = \{x_{i_1}, \ldots, x_{i_k}\} \subseteq \{x_1, \ldots, x_n\}$ is not independent modulo $\mathfrak{a}$, then there exists a non-zero polynomial, $f \in \mathfrak{a} \cap A[x_{i_1}, \ldots, x_{i_k}]$. We have, $\text{lm}(f) \in \text{lt}(\mathfrak{a}) \cap A[x_{i_1}, \ldots, x_{i_k}]$. This implies S is not independent modulo $\text{lt}(\mathfrak{a})$. Therefore, the set of independent indeterminates modulo $\text{lt}(\mathfrak{a})$ is a subset of the set of independent indeterminates modulo $\mathfrak{a}$. Therefore, $\text{cdim}(A[x_1, \ldots, x_n]/\text{lt}(\mathfrak{a})) \leq \text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$. By Theorem 5.27 and Theorem 5.37, we have that the degree of the Hilbert polynomial is at most $\text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$. □

This corollary directly follows.

Corollary 5.39 *Given a proper ideal, $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ 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 $\text{lt}(\mathfrak{a})$, then S is a set of maximal cardinality of indeterminates that are independent modulo $\mathfrak{a}$. Also,*

$$\text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) = \text{cdim}(A[x_1, \ldots, x_n]/\text{lt}(\mathfrak{a})).$$

Since the combinatorial dimension of the ideal and its leading term ideal are the same, we explore its connections with Gröbner basis.

Theorem 5.40 *Let $\prec$ be a degree compatible monomial ordering in $A[x_1, \ldots, x_n]$ such that given a proper ideal $\mathfrak{a}$, $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. $\prec$. Let G be a monic short reduced Gröbner basis of $\mathfrak{a}$ w.r.t. $\prec$. Let $S \subseteq X$ be a set of indeterminates such that it is the largest subset of X that satisfies $A[S] \cap \text{lt}(G) = \phi$. Then, S is maximal independent modulo $\mathfrak{a}$ and $\text{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) = |S|$.*

Proof: We first show that S is independent modulo $\text{lt}(\mathfrak{a})$. If not, then there exists a $f \in A[S] \cap \text{lt}(\mathfrak{a})$. Since G is a monic Gröbner basis and $\mathfrak{a}$ a proper ideal, there exists $g \in G$ such

that $\mathrm{lt}(g)(=\mathrm{lm}(g)) \mid f$. Therefore, $A[S] \cap \mathrm{lt}(G) \neq \phi$, a contradiction. To prove maximality, consider $S \cup \{x\}$ to be maximal independent modulo $\mathrm{lt}(\mathfrak{a})$. By our hypothesis, there exists $f \in A[S \cup \{x\}] \cap \mathrm{lt}(G)$ and therefore $f \in A[S \cup \{x\}] \cap \mathrm{lt}(\mathfrak{a})$, a contradiction and hence S is maximal. Also, $|S| = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathrm{lt}(\mathfrak{a}))$. By Corollary 5.39, S is maximal independent modulo $\mathfrak{a}$ and $\mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a}) = |S|$. □

5.3.3 Krull dimension of A-algebras for degree compatible orderings

In the case of A-algebras with a free A-module representation w.r.t. a lexicographic ordering, we have seen that $\mathrm{cdim}(k(\mathfrak{p})[x_1, \ldots, x_n]/\mathfrak{a}^e) = \mathrm{cdim}(A[x_1, \ldots, x_n]/\mathfrak{a})$ (Proposition 5.17). 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 5.41 *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. 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 5.15 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. $\prec$. From Proposition 5.15, 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 $\mathrm{Mon}(A[S]) \cap \mathrm{lt}(G) = \phi$ is the same as the set of indeterminates, $S' \subseteq X$ that satisfy $\mathrm{Mon}(k(\mathfrak{p})[S']) \cap \mathrm{lt}(\nu(G)) = \phi$. Then by Theorem 5.40,

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

and hence the proof. □

Corollary 5.42 *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 5.17. From Proposition 5.41, 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, $\text{kdim}(k(\mathfrak{p})[x_1,\ldots,x_n]/\mathfrak{a}^e) = \text{cdim}(k(\mathfrak{p})[x_1,\ldots,x_n]/\mathfrak{a}^e)$. This implies that the equation in Proposition 5.16 becomes,

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

Since $\mathfrak{a}$ is a proper ideal with a monic Gröbner basis, the mapping in (5.3), $f^* : \text{Spec}(A[x_1,\ldots,x_n]/\mathfrak{a}) \longrightarrow \text{Spec}(A)$, is surjective and we have,

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

Since by Theorem 5.38, $\deg(p_\mathfrak{a}) = \text{cdim}(A[x_1,\ldots,x_n]/\mathfrak{a})$, we have the result. □

We give below an algorithm (Algorithm 12) 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 5.42.

Algorithm 12 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 11$(G,\prec)$
{ $H_\mathfrak{a}(t)$ is of the form $\frac{a_0+a_1t+\cdots+a_kt^k}{(1-t)^{n+1}}$}
$p_\mathfrak{a}(x) = \sum_{i=0}^{k} a_i C(x+n-i,n)$
$k = \deg(p_\mathfrak{a})$
$d = k + d_A$

5.3.4 Examples

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

Example 5.43 *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 11, 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 5.42, we have,

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

Example 5.44 *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 5.45 *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, $\operatorname{kdim}(\mathbb{Z}[x,y,z]/\mathfrak{a}) = \operatorname{kdim}(\mathbb{Z})+1 = 2$.

As we can see from the examples given in this chapter, 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. The

relation between combinatorial dimension and Krull dimension 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.

Chapter 6

Macaulay-Buchberger Basis Theorem for Residue Class Polynomial Rings with Torsion and Border Bases over Rings

We generalize the Macaulay-Buchberger basis theorem to the case where the residue class polynomial ring over a Noetherian commutative ring is not necessarily a free module. The Macaulay-Buchberger basis theorem was extended to polynomial rings over rings, when the residue class polynomial ring has a free A-module representation in Theorem 3.11. Here, we relax the condition of free A-module representation of the residue class ring. As an application of this generalization we develop a theory of border bases for ideals where the corresponding residue class rings are finitely generated and have torsion. We present a border division algorithm and prove the termination of the algorithm for a special class of border bases. We show the existence of such border bases and present some characterizations in this regard. We also show that certain reduced Gröbner bases (Section 2.5.4) are contained in this class of border bases.

The reader can refer to Section 2.3 for a brief overview of border bases in $\Bbbk[x_1, \ldots, x_n]$. For a detailed description one can refer to (Kehrein et al., 2005; Kehrein and Kreuzer, 2005). For more recent work on general quotient algebras the reader can refer to (Mourrain, 1999; Mourrain and Trébuchet, 2005, 2008, 2012). All these references look at border bases for polynomial rings over fields. The ideas and efficient algorithms proposed by both of these groups (Prof. Dr. Bernard Mourrain's and Prof. Dr. Martin Kreuzer's) cannot be extended to polynomial rings over rings in an obvious manner. In fact, we were not able to come up with a method to extend

the theory of border bases as proposed by these groups to polynomial rings over Noetherian commutative rings. This is the reason why we look at it from the viewpoint of residue class polynomial rings that have a free A-module representation and those that do not. It is also a continuation of our work of Gröbner bases over rings.

The theory of border bases for residue class polynomial rings over Noetherian commutative rings that are finitely generated and have a free A-module representation w.r.t. some monomial order is described in Section 3.5. In the free case, the Gröbner basis characterization of residue class polynomial rings with a free A-module representation allows us to extend border bases directly from polynomial rings over fields to rings.

We give the generalized Macaulay-Buchberger basis theorem in Section 6.1 and in Section 6.2, we consider the special case of finitely generated residue class polynomial rings. In Section 6.3, we define order ideal, border of an ideal, border closure and border prebases. We also present the border prebasis division algorithm. In Section 6.4, we define a special class of border prebases called acyclic border prebases and show that the border prebasis division algorithm terminates for this class of border bases. In Section 6.5, we define acyclic border bases and give certain characterizations. Finally, a detailed example is worked out in Section 6.6.

6.1 Macaulay-Buchberger Basis Theorem for Residue Class Rings with Torsion

Given an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$ we study the generators of the residue class ring, $A[x_1, \ldots, x_n]/\mathfrak{a}$, when it does not have a free A-module representation. That is, the leading coefficients of polynomials in the short reduced Gröbner basis need not be monic. Through out this section we assume a monomial order, $\prec$.

First, we state the following lemma.

Lemma 6.1 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal and $\langle \mathrm{lt}(\mathfrak{a}) \rangle$ be the leading term ideal. Let $T = \{ax^\alpha \in \mathrm{Ter}(A[x_1, \ldots, x_n]) : ax^\alpha \notin \langle \mathrm{lt}(\mathfrak{a}) \rangle\}$. Then $T + \mathfrak{a}$ generates $A[x_1, \ldots, x_n]/\mathfrak{a}$ as an A-module.*

Proof: Let $\mathrm{Span}_A(T+\mathfrak{a})$ denote the A-module generated by $T+\mathfrak{a}$. Assume that $\mathrm{Span}_A(T+\mathfrak{a}) \subsetneq A[x_1, \ldots, x_n]/\mathfrak{a}$. Then the set $N = \{f \in A[x_1, \ldots, x_n] : f + \mathfrak{a} \notin \mathrm{Span}_A(T + \mathfrak{a})\}$ is nonempty and contains nonzero elements. Then there exists a $f_0 \in N$ such that $\mathrm{lm}(f_0)$ is minimal in the set $\{\mathrm{lm}(f) : f \in N\}$ by the well ordering property of monomial order. If $\mathrm{lt}(f_0) \in T$, then $(f_0 - \mathrm{lt}(f_0)) + \mathfrak{a} \notin \mathrm{Span}_A(T + \mathfrak{a})$. This implies that the polynomial $f_0 - \mathrm{lt}(f_0)$ of smaller leading term than f_0 is an element of N, which is a contradiction. If $\mathrm{lt}(f_0) \in \langle \mathrm{lt}(\mathfrak{a}) \rangle$ then there exists

an element $f' \in \mathfrak{a}$ such that $\mathrm{lt}(f') = \mathrm{lt}(f_0)$. Consider $f_0 - f'$. It lies in N and has a smaller leading term than f_0, a contradiction. □

Remark 6.2 *The proof of the above lemma goes exactly as in the case of fields. But it is worth noting the following. In the case of fields, i.e.* $A = \mathbb{k}$, $\mathrm{lt}(f) \in \langle \mathrm{lt}(\mathfrak{a}) \rangle$ *for some* $f \in \mathbb{k}[x_1, \ldots, x_n]$ *implies that there exists* $f_1 \in \mathfrak{a}$ *such that* $\mathrm{lt}(f_1) \mid \mathrm{lt}(f)$. *On the other hand, in the case of rings,* $\mathrm{lt}(f) \in \langle \mathrm{lt}(\mathfrak{a}) \rangle$ *for some* $f \in A[x_1, \ldots, x_n]$ *implies there exists* $f_1, \ldots, f_s \in \mathfrak{a}$ *such that* $\mathrm{lm}(f_i) \mid \mathrm{lm}(f)$ *and* $\mathrm{lc}(f) \in \langle \mathrm{lc}(f_i) : i = 1, \ldots, s \rangle$. *This is because in rings,* $\langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(\mathfrak{a}) \rangle$ *and for any* $f \in \mathfrak{a}$, $\mathrm{lt}(f) = \sum \mathrm{lt}(h_i)\mathrm{lt}(g_i)$, *where the sum is over all* i *satisfying* $\mathrm{lm}(f) = \mathrm{lm}(h_i)\mathrm{lm}(g_i)$. *Also in fields, there exists only one* $f_0 \in N$ *such that* $\mathrm{lm}(f_0)$ *is minimal in the set* $\{\mathrm{lm}(f) : f \in N\}$. *Whereas in rings, there could be more than one choice for* f_0 *such that* $\mathrm{lm}(f_0)$ *is minimal. But each of these polynomials will have a different leading coefficient.*

Example 6.3 *Let* $G = \{3x, x^2, y\}$ *be the Gröbner basis of an ideal* $\mathfrak{a}$ *in* $\mathbb{Z}[x, y]$. *The leading term ideal,* $\langle \mathrm{lt}(\mathfrak{a}) \rangle = \langle G \rangle$. *Let the set of terms,* $T \subseteq \mathrm{Ter}(\mathbb{Z}[x, y])$ *be defined as in Lemma 6.1. The set* $T + \mathfrak{a} = \{1 + \mathfrak{a}, 1x + \mathfrak{a}, 2x + \mathfrak{a}\}$ *generates* $\mathbb{Z}[x, y]/\mathfrak{a}$ *as a* $\mathbb{Z}$*-module.*

In the case of fields the standard monomials form a vector space basis for the residue class polynomial ring. Here we introduce a similar notion.

Definition 6.4 (Weak Standard Monomials) *Given an ideal,* $\mathfrak{a}$ *in* $A[x_1, \ldots, x_n]$, $\mathrm{Mon}\{ax^\alpha : ax^\alpha \notin \langle \mathrm{lt}(\mathfrak{a}) \rangle\}$ *is called the set of weak standard monomials of* $\mathfrak{a}$.

Example 6.5 *In Example 6.3,* $\mathrm{Mon}(T) = \{1, x\}$ *is the set of weak standard monomials of* $\mathfrak{a} = \langle 3x, x^2, y \rangle$.

Therefore, Lemma 6.1 can also be stated as follows.

Lemma 6.6 *The residue classes of the weak standard monomials of an ideal,* $\mathfrak{a}$ *generate* $A[x_1, \ldots, x_n]/\mathfrak{a}$ *as an* A*-module.*

Here we introduce a structure on monomials called coefficient ideal mapping that will help us generalize the Buchberger result and extend border bases to polynomial rings over rings.

Definition 6.7 (Coefficient Ideal Mapping) *Let* $\mathrm{Id}(A)$ *be the set of all ideals in the ring,* A. *A mapping* $\mathfrak{I} : \mathbb{N}^n \longrightarrow \mathrm{Id}(A)$ *is said to be a coefficient ideal mapping if* $x^\beta \mid x^\alpha$ *implies* $\mathfrak{I}(x^\beta) \subseteq \mathfrak{I}(x^\alpha)$, *for all* $x^\alpha, x^\beta \in \mathbb{N}^n$. *From now on, we denote* $\mathfrak{I}(x^\alpha)$ *by* $\mathfrak{I}_{x^\alpha}$.

Clearly, the Gröbner basis of an ideal fixes a coefficient ideal mapping. Consider the leading coefficient ideal, $I_{J_{x^\alpha}}$ that we constructed in Section 3.1 w.r.t. G. Since J_{x^α} is a saturated set, the mapping $x^\alpha \mapsto I_{J_{x^\alpha}}$ is a coefficient ideal mapping and is denoted by $\mathcal{I}^{(G)}$.

Definition 6.8 *A coefficient ideal mapping $\mathcal{I} : \mathbb{N}^n \to \mathrm{Id}(A)$ is said to be proper if it maps only finitely many monomials to the proper ideals in A.*

Example 6.9 *Consider the mapping $\mathcal{I} : \mathbb{N}^2 \longrightarrow \mathrm{Id}(\mathbb{Z})$. Let $\mathcal{I}(1) = \{0\}, \mathcal{I}(x_1) = \langle 3\rangle$ and every other monomial be mapped to $\langle 1\rangle$. We see that for any $x^\alpha \in \mathbb{N}^2$ such that $x_1 \mid x^\alpha$, $\langle 3\rangle \subseteq \mathcal{I}(x^\alpha)$. Therefore, $\mathcal{I}$ is a proper coefficient ideal mapping.*

Using the coefficient ideal mapping we define a generating set for $A[x_1, \ldots, x_n]/\mathfrak{a}$ that also satisfies a weaker form of the linear independence property.

Definition 6.10 (Weak basis) *Let $\mathfrak{a}$ be an ideal in $A[x_1, \ldots, x_n]$. Let $\mathcal{B}$ be a set of monomials, possibly infinite, and let $\mathcal{I}$ be a coefficient ideal mapping such that $x^\alpha \notin \mathcal{B}$ if and only if $\mathcal{I}_{x^\alpha} = \langle 1\rangle$. We say that the set of residue classes of $\mathcal{B}$ forms a weak basis for $A[x_1, \ldots, x_n]/\mathfrak{a}$ w.r.t. $\mathcal{I}$ if it satisfies the following properties.*

(i) $\mathcal{B} + \mathfrak{a}$ *generates* $A[x_1, \ldots, x_n]/\mathfrak{a}$ *as an* A*-module.*

(ii) If $\sum_{i=1}^{k} a_i x^{\alpha_i} + \mathfrak{a} = 0$*, where* $k \in \mathbb{N}$*,* $x^{\alpha_i} \in \mathcal{B}$ *and* $a_i \neq 0$ *for all* $i = 1, \ldots, k$*, then for some* $j = 1, \ldots, k$*,* $a_j \in \mathcal{I}_{x^{\alpha_j}}$*.*

(iii) If there exists a coefficient ideal mapping $\mathcal{I}'$ such that $\mathcal{I}'_{x^\alpha} \subseteq \mathcal{I}_{x^\alpha}$ for some $x^\alpha \in \mathbb{N}^n$ and $\mathcal{B}' = \{x^\alpha : \mathcal{I}'_{x^\alpha} \neq \langle 1\rangle\}$ satisfies (i) and (ii) w.r.t. $\mathcal{I}'$, then $\mathcal{I}' = \mathcal{I}$.

Remark 6.11 *The linear independence property requires that if $\sum_{i=1}^{k} a_i x^{\alpha_i} + \mathfrak{a} = 0$ then for all $i \in \{1, \ldots, k\}$, $a_i \in \mathcal{I}_{x^{\alpha_i}}$. Therefore, the second condition in Definition 6.10 is a weaker form of the linear independence property. In fact, in the case of fields and residue class polynomial rings with a free A-module representation, the second condition automatically implies the linear independence property.*

Remark 6.12 *The third condition in Definition 6.10 can be interpreted as a minimality condition on the basis. For example, consider the ideal $\mathfrak{a} = \langle 4x_1, {x_1}^2, x_2\rangle \subseteq \mathbb{Z}[x_1, x_2]$. Let $\mathcal{I}$ and $\mathcal{I}'$ be two coefficient ideal mappings such that $\mathcal{I}_1 = 0, \mathcal{I}_{x_1} = \langle 2\rangle$ and for all the other $x^\alpha \in \mathbb{N}^2$, $\mathcal{I}_{x^\alpha} = \langle 1\rangle$ and $\mathcal{I}'_1 = 0, \mathcal{I}'_{x_1} = \langle 4\rangle$ and for all the other $x^\alpha \in \mathbb{N}^2$, $\mathcal{I}'_{x^\alpha} = \langle 1\rangle$. Both $\mathcal{I}$ and $\mathcal{I}'$ satisfy the first two conditions of the weak basis. However, since $\mathcal{I}'_{x_1} (= \langle 4\rangle) \subsetneq \mathcal{I}_{x_1} (= \langle 2\rangle)$, it is with respect to the second coefficient ideal mapping, $\mathcal{I}'$ that we define the weak basis of $\mathbb{Z}[x_1, x_2]/\langle 4x_1, {x_1}^2, x_2\rangle$.*

We now give below a generalization of Macaulay-Buchberger theorem for residue class polynomial rings over rings.

Theorem 6.13 (Generalized MB-basis theorem) *Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis of an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$ and $\mathcal{I}^{(G)}$ the coefficient ideal mapping fixed by G. We have the following properties.*

(i) The set $\mathcal{B} = \{x^\alpha \in \mathbb{N}^n : {\mathcal{I}^{(G)}}_{x^\alpha} \neq \langle 1 \rangle\}$ forms a set of weak standard monomials of $\mathfrak{a}$ w.r.t. G.

(ii) The set of residue classes of $\mathcal{B}$ forms a set of weak basis (Definition 6.10) for the A-module, $A[x_1, \ldots, x_n]/\mathfrak{a}$.

Proof: (i) Let $\mathcal{B}' = \{x^\alpha \in \mathbb{N}^n : ax^\alpha \notin \langle \mathrm{lt}(\mathfrak{a}) \rangle \text{ for some } a \in A\}$ be the set of weak standard monomials of $\mathfrak{a}$. We have to prove that $\mathrm{Span}_A(\mathcal{B}+\mathfrak{a}) = \mathrm{Span}_A(\mathcal{B}'+\mathfrak{a})$. Let $f+\mathfrak{a} = \sum_{i=1}^k a_i x^{\alpha_i} + \mathfrak{a}$, $a_i \in A$, $k \in \mathbb{N}$ and ${\mathcal{I}^{(G)}}_{x^{\alpha_i}} \neq \langle 1 \rangle$. For each $x^{\alpha_i} \in \mathrm{Mon}(\sum_{i=1}^k a_i x^{\alpha_i})$, we have the following two cases.

(a) ${\mathcal{I}^{(G)}}_{x^{\alpha_i}} = \{0\}$. This implies there is no $g_j \in G$ such that $\mathrm{lm}(g_j) \mid x^{\alpha_i}$. This means $a_i x^{\alpha_i} \notin \langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(\mathfrak{a}) \rangle$.

(b) ${\mathcal{I}^{(G)}}_{x^{\alpha_i}} \neq \{0\}$. This implies, there is atleast one $g_j \in G$ such that $\mathrm{lm}(g_j) \mid x^{\alpha_i}$. But we have ${\mathcal{I}^{(G)}}_{x^{\alpha_i}} \neq \langle 1 \rangle$ and therefore there exists some $b \in A$ such that $b \notin {\mathcal{I}^{(G)}}_{x^{\alpha_i}}$. This means $bx^{\alpha_i} \notin \langle \mathrm{lt}(\mathfrak{a}) \rangle$.

In both the cases we have, $x^{\alpha_i} + \mathfrak{a} \in \mathcal{B}' + \mathfrak{a}$. Therefore, $\mathrm{Span}_A(\mathcal{B} + \mathfrak{a}) \subseteq \mathrm{Span}_A(\mathcal{B}' + \mathfrak{a})$.

To prove the opposite inclusion, let $f + \mathfrak{a} \in \mathrm{Span}_A(\mathcal{B}' + \mathfrak{a})$. Let $f + \mathfrak{a} = \sum_{i=1}^k a_i x^{\alpha_i} + \mathfrak{a}$, where $a_i x^{\alpha_i} \notin \langle \mathrm{lt}(\mathfrak{a}) \rangle$ for all $i = 1, \ldots, k$. Since $a_i x^{\alpha_i} \notin \langle \mathrm{lt}(\mathfrak{a}) \rangle$, we have for each x^{α_i}, either $x^{\alpha_i} \notin \langle \mathrm{lm}(\mathfrak{a}) \rangle$ or $x^{\alpha_i} \in \langle \mathrm{lm}(\mathfrak{a}) \rangle$ but $a_i x^{\alpha_i} \notin \langle \mathrm{lt}(\mathfrak{a}) \rangle$. We deal with the two cases separately.

(a) $x^{\alpha_i} \notin \langle \mathrm{lm}(\mathfrak{a}) \rangle$. This means $x^{\alpha_i} \notin \langle \mathrm{lm}(G) \rangle$ and ${\mathcal{I}^{(G)}}_{x^{\alpha_i}} = \{0\}$. Therefore ${\mathcal{I}^{(G)}}_{x^{\alpha_i}} \neq \langle 1 \rangle$.

(b) $x^{\alpha_i} \in \langle \mathrm{lm}(\mathfrak{a}) \rangle$ and $a_i x^{\alpha_i} \notin \langle \mathrm{lt}(\mathfrak{a}) \rangle$. This implies, $a_i x^{\alpha_i} \notin \langle \mathrm{lt}(G) \rangle$. Therefore, we have $a_i \notin {\mathcal{I}^{(G)}}_{x^{\alpha_i}}$ and ${\mathcal{I}^{(G)}}_{x^{\alpha_i}} \neq \langle 1 \rangle$.

Therefore, $\mathrm{Span}_A(\mathcal{B}' + \mathfrak{a}) \subseteq \mathrm{Span}_A(\mathcal{B} + \mathfrak{a})$.

(ii) From Lemma 6.6, we have that $\mathcal{B}'+\mathfrak{a}$ generates $A[x_1, \ldots, x_n]/\mathfrak{a}$ as an A-module and from (i) we have that $\mathrm{Span}_A(\mathcal{B}+\mathfrak{a}) = \mathrm{Span}_A(\mathcal{B}'+\mathfrak{a})$. Therefore $\mathcal{B}+\mathfrak{a}$ generates $A[x_1, \ldots, x_n]/\mathfrak{a}$ as an A-module. Let $\sum_{i=1}^s a_i x^{\alpha_i} + \mathfrak{a} = 0$, where $s \in \mathbb{N}$ and $a_i x^{\alpha_i} + \mathfrak{a} \in \mathrm{Span}_A(\mathcal{B}+\mathfrak{a})$. This implies that $\sum_{i=1}^s a_i x^{\alpha_i} \in \mathfrak{a}$ and $\mathrm{lt}(\sum_{i=1}^s a_i x^{\alpha_i}) \in \langle \mathrm{lt}(\mathfrak{a}) \rangle$. Assume that for each a_i, $i = 1, \ldots, s$, $a_i \notin {\mathcal{I}^{(G)}}_{x^{\alpha_i}}$.

This implies for each $a_i x^{\alpha_i}$, there exist no $g_1, \ldots, g_m \in G, m \in \mathbb{N}$, $m \leq t$ such that $\mathrm{lm}(g_j) \mid x^{\alpha_i}$ for all $j = 1, \ldots, m$ and $a_i \in \langle \mathrm{lc}(g_i) : i \in \{1, \ldots, m\} \rangle$. That is $a_i x^{\alpha_i} \notin \langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(\mathfrak{a}) \rangle$ for all $i \in \{1, \ldots, s\}$. We have a contradiction. Hence, $\sum_{i=1}^{s} a_i x^{\alpha_i} + \mathfrak{a} = 0$ implies for some i, $a_i \in \mathcal{I}^{(G)}{}_{x^{\alpha_i}}$.

Consider a coefficient ideal mapping, $\mathcal{I}'$ such that for any $x^\alpha \in \mathrm{Mon}(A[x_1, \ldots, x_n])$, either $\mathcal{I}'_{x^\alpha} \subsetneq \mathcal{I}^{(G)}_{x^\alpha}$ or $\mathcal{I}'_{x^\alpha} = \mathcal{I}^{(G)}_{x^\alpha}$. Assume $\mathcal{B}' = \{x^\alpha : \mathcal{I}'_{x^\alpha} \neq \langle 1 \rangle\}$ satisfies (i) and (ii) w.r.t. $\mathcal{I}'$. Consider the ideal, $\mathfrak{A} = \langle c_\alpha x^\alpha : c_\alpha \in \mathcal{I}'_{x^\alpha} \rangle$. The ideal, $\mathfrak{A} \subsetneq \langle \mathrm{lt}(\mathfrak{a}) \rangle$ since $\mathcal{I}'_{x^\alpha} \subsetneq \mathcal{I}^{(G)}_{x^\alpha}$ for some x^α. Consider $c_\beta x^\beta \in \langle \mathrm{lt}(\mathfrak{a}) \rangle \setminus \mathfrak{A}$. Let us denote the normal form of $c_\beta x^\beta$ w.r.t. G as h. Then each non zero term in h is of the form $d_\gamma x^\gamma$ such that $d_\gamma \in A/\mathcal{I}^{(G)}_{x^\gamma}$ and $x^\gamma \in \mathcal{B}$. Since $d_\gamma \notin \mathcal{I}^{(G)}_{x^\gamma}$, it is not an element of $\mathcal{I}'_{x^\gamma}$. Also, $c_\beta \notin \mathcal{I}'_{x^\beta}$. Therefore, $\mathcal{B}'$ fails to satisfy Condition (ii) of the definition of weak basis for $c_\beta x^\beta - h$ and therefore we have a contradiction. Thus the set $\mathcal{B} + \mathfrak{a}$ forms a weak basis for the A - module $A[x_1, \ldots, x_n]/\mathfrak{a}$. □

Example 6.14 *Let $\mathfrak{a} = \langle 3x, 4y + 2x, y^2 \rangle$ be an ideal in $\mathbb{Z}[x, y]$. Then $G = \{3x, 4y + 2x, y^2\}$ is a short reduced Gröbner basis w.r.t. lex order with $x \prec y$. Since G is not monic, $\mathbb{Z}[x, y]/\mathfrak{a}$ has a nontrivial torsion submodule. It is also not finitely generated as a $\mathbb{Z}$-module. The leading coefficient ideals calculated w.r.t. G are as follows : $I_1 = \{0\}$, $I_{x^m} = \langle 3 \rangle, m \in \mathbb{N}$, $I_y = \langle 4 \rangle$, $I_{xy} = \langle 3, 4 \rangle = \langle 1 \rangle$ and for all the other monomials, the ideal is equal to $\langle 1 \rangle$. Consider the coefficient ideal mapping fixed by G, $\mathcal{I}^{(G)}{}_{x^\alpha y^\beta} = I_{x^\alpha y^\beta}, \alpha, \beta \in \mathbb{N}$. The set $\mathcal{B} = \{x^\alpha y^\beta : \mathcal{I}^{(G)}{}_{x^\alpha y^\beta} \neq \langle 1 \rangle\}$ is an infinite set given by $\mathcal{B} = \{1, y, x^m, m \in \mathbb{N}\}$ and $\mathcal{B} + \mathfrak{a}$ forms a weak basis of $\mathbb{Z}[x, y]/\mathfrak{a}$.*

Remark 6.15 *Let us consider two special cases.*

Case (i) *$A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation w.r.t. some monomial order. The coefficient ideal mapping maps the monomials to either $\{0\}$ or $\langle 1 \rangle$. If the residue class ring is finitely generated then only finitely many monomials will map to $\{0\}$.*

Case (ii) *$A = \Bbbk$. The case is the same as above since in a field the only possible ideals are $\{0\}$ and $\langle 1 \rangle$.*

6.2 Finitely Generated Residue Class Rings with Torsion

From the observations we have made above, it is easy to see that when the residue class ring, $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated the structure satisfies the following additional properties.

Corollary 6.16 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated. Let G be a Gröbner basis of an ideal $\mathfrak{a}$ and $\mathcal{I}^{(G)}$ the coefficient ideal mapping fixed by G. Then,*

1. *The coefficient ideal mapping* $\mathfrak{I}^{(G)}$ *is proper,*

2. *The set of weak standard monomials w.r.t* $\mathfrak{a}$ *is finite, and*

3. $A[x_1, \ldots, x_n]/\mathfrak{a}$ *has a finite weak basis.*

In Section 3.1, we saw that short reduced Gröbner basis can be used to characterize residue class polynomial rings that are finitely generated and have a free A-module representation w.r.t. a monomial order. Here we give a similar characterization for finitely generated residue class polynomial rings that are not necessarily free.

Proposition 6.17 *Let* $\mathfrak{a}$ *be an ideal in* $A[x_1, \ldots, x_n]$ *and let* $G = \{g_1, \ldots, g_t\}$ *be a short reduced Gröbner basis for* $\mathfrak{a}$*. The following statements are equivalent.*

(i) For each $i = 1, \ldots, n$ *there exists* $j = 1, \ldots, t$ *such that* $\mathrm{lt}(g_j) = {x_i}^{\nu}$ *for some* $\nu \in \mathbb{N}$*.*

(ii) The A-module $A[x_1, \ldots, x_n]/\mathfrak{a}$ *is finitely generated.*

Proof:

(i) $\Rightarrow$ (ii). Since for every $i = 1, \ldots, n$ there exists $j = 1, \ldots, n$ such that $\mathrm{lt}(g_i) = {x_i}^{\nu}$ for some $\nu \in \mathbb{N}$, there are only finitely many power products which are reduced w.r.t. G and hence $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated.
(ii) $\Rightarrow$ (i). Assume $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and for some $i \in \{1, \ldots, n\}$ there exists no $j = 1, \ldots, t$ such that $\mathrm{lt}(g_j) = {x_i}^{\nu}$, for some $\nu \in \mathbb{N}$. There are two cases here.

(i) There exists no $j = 1, \ldots, t$ such that $\mathrm{lm}(g_j) = {x_i}^{\nu}$, for some $\nu \in \mathbb{N}$. Then the powers of x_i, $1, x_i, {x_i}^2, \ldots$ are reduced w.r.t. G and $A[x_1, \ldots, x_n]/\mathfrak{a}$ is not finitely generated as an A-module, a contradiction.

(ii) There exists at least one $j = 1, \ldots, t$ such that $\mathrm{lm}(g_j) = {x_i}^{\nu}$, for some $\nu \in \mathbb{N}$. Among the leading monomials of elements in G that are powers of x_i, let ${x_i}^{\alpha}$ denote the monomial of highest degree and let $g_j \in G$ be the corresponding element in the basis. Consider the leading coefficient ideal of ${x_i}^{\alpha}$, $I_{{x_i}^{\alpha}}$. Since $\mathrm{lt}(g_j) \neq {x_i}^{\alpha}$ and G is a short reduced Gröbner basis, we have $I_{{x_i}^{\alpha}} \neq \langle 1 \rangle$. Consider the set of coset representatives of $A/I_{{x_i}^{\alpha}}$, $C_{I_{{x_i}^{\alpha}}}$. Let $c \in C_{I_{{x_i}^{\alpha}}}$. Then $1, cx_i, c{x_i}^2, \ldots$ are reduced w.r.t. G and $A[x_1, \ldots, x_n]/\mathfrak{a}$ is not finitely generated as an A-module, a contradiction.

□

In the case when $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated one can show that it satisfies a stronger set of conditions than Theorem 6.13. For this we introduce the concept of weak$^+$ basis. It also plays a crucial role in extending border bases to this case.

Definition 6.18 (Weak$^+$ basis) *Let $\mathfrak{a}$ be an ideal in $A[x_1,\ldots,x_n]$. Let $\mathcal{I}$ be a proper coefficient ideal mapping and $\mathcal{B}=\{x^{\alpha_1},\ldots,x^{\alpha_m}\}$ be a finite set of monomials of size m such that $x^\alpha \notin \mathcal{B}$ if and only if $\mathcal{I}_{x^\alpha}=\langle 1\rangle$, where $x^\alpha \in \mathrm{Mon}(A[x_1,\ldots,x_n])$. Let $C_{\mathcal{I}_{x^\alpha}}$ be the coset representatives of the equivalence classes of $A/\mathcal{I}_{x^\alpha}$. Then we say the set of residue classes of $\mathcal{B}$ forms a weak$^+$ basis for $A[x_1,\ldots,x_n]/\mathfrak{a}$ w.r.t. $\mathcal{I}$ if it satisfies the following properties.*

(i) $A[x_1,\ldots,x_n]/\mathfrak{a}=\{\sum_{i=1}^{m} a_i x^{\alpha_i}+\mathfrak{a} \mid a_i \in C_{\mathcal{I}_{x^{\alpha_i}}}, x^{\alpha_i}\in\mathcal{B}\}$.

(ii) *If $\sum_{i=1}^{m} a_i x^{\alpha_i}+\mathfrak{a}=0$, where $m\in\mathbb{N}$, $x^{\alpha_i}\in\mathcal{B}$ and $a_i\neq 0$ for all $i=1,\ldots,m$, then for some $j\in\{1,\ldots,m\}$, $a_j\in\mathcal{I}_{x^{\alpha_j}}$.*

(iii) *If there exists a coefficient ideal mapping $\mathcal{I}'$ such that $\mathcal{I}'_{x^\alpha}\subseteq\mathcal{I}_{x^\alpha}$ for some $x^\alpha\in\mathbb{N}^n$ and $\mathcal{B}'=\{x^\alpha : \mathcal{I}'_{x^\alpha}\neq\langle 1\rangle\}$ satisfies (i) and (ii) w.r.t. $\mathcal{I}'$, then $\mathcal{I}'=\mathcal{I}$.*

Remark 6.19 *It must be noted that if the set of residue classes of $\mathcal{B}$ forms a weak$^+$ basis for the A-module $A[x_1,\ldots,x_n]/\mathfrak{a}$, then it is also a weak basis for the same. But the opposite inclusion is not necessarily true.*

Corollary 6.20 *Let $G=\{g_1,\ldots,g_t\}$ be a Gröbner basis of an ideal $\mathfrak{a}$ in $A[x_1,\ldots,x_n]$ such that $A[x_1,\ldots,x_n]/\mathfrak{a}$ is finitely generated, and let $\mathcal{I}^{(G)}$ be the coefficient ideal mapping fixed by G. Let $\mathcal{B}=\{x^{\alpha_1},\ldots,x^{\alpha_m}\}$ be a finite set of monomials of size m such that if $x^\alpha\notin\mathcal{B}$, $\mathcal{I}_{x^\alpha}=\langle 1\rangle$, where $x^\alpha\in\mathrm{Mon}(A[x_1,\ldots,x_n])$. Then the set of residue classes of $\mathcal{B}$ forms a weak$^+$ basis for the A-module, $A[x_1,\ldots,x_n]/\mathfrak{a}$.*

Proof: The equality,

$$A[x_1,\ldots,x_n]/\mathfrak{a}=\{\sum_{i=1}^{m} a_i x^{\alpha_i}+\mathfrak{a} \mid a_i\in C_{\mathcal{I}_{x^{\alpha_i}}}, m\in\mathbb{N}, x^{\alpha_i}\in\mathcal{B}\}$$

follows directly from the proof of Theorem 4.3.3. in (Adams and Loustaunau, 1994). The proof that the second and third conditions of Definition 6.18 hold is along the same lines as the proof of Theorem 6.13. □

Let us look at an example for the above corollary. It is similar to Example 6.14 except that the $\mathbb{Z}$-module is finitely generated.

Example 6.21 *Let $\mathfrak{a}=\langle 3x, 4y+2x, x^2, y^2\rangle$ be an ideal in $\mathbb{Z}[x,y]$. Then $G=\{3x, 4y+2x, x^2, y^2\}$ is a short reduced Gröbner basis w.r.t. lex order with $x\prec y$. The $\mathbb{Z}$-module, $\mathbb{Z}[x,y]/\mathfrak{a}$, is finitely generated as a $\mathbb{Z}$-module. The leading coefficient ideals calculated w.r.t. G are as follows :*

$I_1 = \{0\}$, $I_x = \langle 3\rangle$, $I_y = \langle 4\rangle$, $I_{xy} = \langle 3,4\rangle = \langle 1\rangle$ and for all the other monomials, $I_{x^\alpha y^\beta} = \langle 1\rangle$, $\alpha, \beta \in \mathbb{N}$. Consider the coefficient ideal mapping fixed by G, ${\mathcal{I}^{(G)}}_{x^\alpha y^\beta} = I_{x^\alpha y^\beta}$. Let us fix the set of coset representatives as $C_{\mathcal{I}_1} = \mathbb{Z}$, $C_{\mathcal{I}_x} = \{1,2\}$, $C_{\mathcal{I}_y} = \{1,2,3\}$ and for all the other monomials, $C_{\mathcal{I}_{x^\alpha}} = \{0\}$. The set $\mathcal{B} = \{x^\alpha y^\beta : {\mathcal{I}^{(G)}}_{x^\alpha y^\beta} \neq \langle 1\rangle\}$ is a finite set given by $\mathcal{B} = \{1, y, x\}$. The set $\mathcal{B} + \mathfrak{a}$ satisfies all the conditions of Definition 6.18 w.r.t. the set of coset representatives, $C_{\mathcal{I}_{x^\alpha}}$ and therefore forms a weak$^+$ basis for $\mathbb{Z}[x,y]/\mathfrak{a}$.

We now provide a better interpretation of the mapping described by (3.1) in terms of weak$^+$ basis.

Proposition 6.22 *Let $\mathfrak{a}$ be an ideal in $A[x_1, \ldots, x_n]$. Let $\mathcal{I}$ be a proper coefficient ideal mapping and $\mathcal{B} = \{x^{\alpha_1}, \ldots, x^{\alpha_m}\}$ be a finite set of monomials of size m such that if $x^\alpha \notin \mathcal{B}$, $\mathcal{I}_{x^\alpha} = \langle 1\rangle$, where $x^\alpha \in \text{Mon}(A[x_1, \ldots, x_n])$. Consider the mapping,*

$$\begin{aligned} \phi : A[x_1, \ldots, x_n]/\mathfrak{a} &\longrightarrow A/\mathcal{I}_{x^{\alpha_1}} \times \cdots \times A/\mathcal{I}_{x^{\alpha_m}} \\ f + \mathfrak{a} &\longmapsto (c_1 + \mathcal{I}_{x^{\alpha_1}}, \cdots, c_m + \mathcal{I}_{x^{\alpha_m}}), \end{aligned}$$

where $f \in A[x_1, \ldots, x_n]$ and $c_i \in C_{\mathcal{I}_{x^{\alpha_i}}}$ for all $i \in \{1, \ldots, m\}$. Then, ϕ is an isomorphism if $\mathcal{B}$ forms a weak$^+$ basis for $A[x_1, \ldots, x_n]/\mathfrak{a}$.

Proof: Let us assume that $\mathcal{B}$ forms a weak$^+$ basis for $A[x_1, \ldots, x_n]/\mathfrak{a}$. We first show that the mapping ϕ is well defined. Consider a polynomial $f \in A[x_1, \ldots, x_n]$. Suppose

$$\begin{aligned} \phi(f + \mathfrak{a}) &= (c_1 + \mathcal{I}_{x^{\alpha_1}}, \cdots, c_m + \mathcal{I}_{x^{\alpha_m}}) \text{ and} \\ \phi(f + \mathfrak{a}) &= (c'_1 + \mathcal{I}_{x^{\alpha_1}}, \cdots, c'_m + \mathcal{I}_{x^{\alpha_m}}), \end{aligned}$$

where c_i, $c'_i \in C_{\mathcal{I}_{x^{\alpha_i}}}$, for all $i = 1, \ldots, m$. This implies $(c_i - c'_i) \in \mathcal{I}_{x^{\alpha_i}}$, $i = 1, \ldots, m$. Since the difference of two different coset representatives cannot give the zero coset, we have $c_i = c'_i$ for all $i = 1, \ldots, m$. Thus ϕ is well defined.
Clearly, ϕ is a surjective map by construction. We now have to prove that ϕ is an injective mapping. Consider a polynomial $f \in A[x_1, \ldots, x_n]$ such that $\phi(f + \mathfrak{a}) = (0, \ldots, 0)$. Let us assume that $f \notin \mathfrak{a}$. Since $\mathcal{B}$ forms a weak$^+$ basis for $A[x_1, \ldots, x_n]/\mathfrak{a}$, we can obtain $c_i \in C_{\mathcal{I}_{x^{\alpha_i}}}$, $i = 1, \ldots, m$ such that $f = \sum_{i=1}^{m} c_i x^{\alpha_i} \mod \mathfrak{a}$. Further, atleast one of the c_i, $i \in \{1, \ldots, m\}$, is nonzero. This implies that $\phi(f + \mathfrak{a})$ also maps to $(c_1, \ldots, c_m)$. Therefore, ϕ is not a well defined mapping. This is a contradiction and $f \in \mathfrak{a}$. Thus, the kernel of ϕ, $\ker(\phi) = \{0 + \mathfrak{a}\}$. This implies that ϕ is an injective mapping. Hence, it follows that ϕ is an isomorphism. □

6.3 Order Ideals and Border Prebasis Division Algorithm

Given a Noetherian commutative ring A and a proper coefficient ideal mapping, $\mathcal{I}$, we define an order ideal w.r.t. $\mathcal{I}$.

Definition 6.23 *For each $x^\alpha \in \mathbb{N}^n$ and a proper coefficient ideal mapping $\mathcal{I}$, fix $C_{x^\alpha} \subseteq A$ a set of coset representatives of $A/\mathcal{I}_{x^\alpha}$. A set of terms $\mathcal{O}_\mathcal{I} \subseteq \mathrm{Ter}(A[x_1, \ldots, x_n])$ is said to be an order ideal w.r.t. $\mathcal{I}$ if for all $x^\alpha \in \mathbb{N}^n$, $cx^\alpha \in \mathcal{O}_\mathcal{I}$ if and only if $c \in C_{x^\alpha}$.*

Example 6.24 *Consider the polynomial ring $\mathbb{Z}[x, y]$. Let the mapping $\mathcal{I}$ be such that $\mathcal{I}_1 = \{0\}$, $\mathcal{I}_x = \langle 4 \rangle$, $\mathcal{I}_y = \langle 3 \rangle$, $\mathcal{I}_{x^2} = \langle 2 \rangle$ and the rest of the monomials map to $\langle 1 \rangle$. $\mathcal{I}$ is clearly a proper coefficient ideal mapping. Let the set of coset representatives be the following, $C_1 = \mathbb{Z}, C_x = \{0, 1, 2, 3\}, C_y = \{0, 1, 2\}, C_{x^2} = \{0, 1\}$ and for all the other monomials, x^α, $C_{x^\alpha} = \{0\}$. Then, $\mathcal{O}_\mathcal{I} = \{a_1, a_2 x, a_3 y, a_4 x^2 \mid a_1 \in C_1,\ a_2 \in C_x,\ a_3 \in C_y,\ a_4 \in C_{x^2}\}$ is an order ideal corresponding to $\mathcal{I}$.*

Example 6.25 *Now consider a polynomial ring $\Bbbk[u_1, u_2][x, y, z]$. Let $\mathcal{I}$ be a coefficient ideal mapping defined by $\mathcal{I}_1 = \{0\}$, $\mathcal{I}_x = \{0\}$, $\mathcal{I}_y = \langle u_1^2 \rangle$, $\mathcal{I}_z = \langle u_2^2 - 3u_1 \rangle$, $\mathcal{I}_{x^2} = \langle 0 \rangle$, $\mathcal{I}_{xy} = \langle u_1^2, u_2^2 - 1 \rangle$, $\mathcal{I}_{xz} = \langle u_1, u_2 \rangle$ and rest of the monomials mapping to $\langle 1 \rangle$. $\mathcal{I}$ is a proper coefficient ideal mapping. Let $C_1, C_x, C_y, C_z, C_{x^2}, C_{xy}, C_{xz}$ represent the nonzero set of coset representatives. Then $\mathcal{O}'_\mathcal{I} = \{a_1, a_2 x, a_3 y, a_4 z, a_5 x^2, a_6 xy, a_7 xz \mid a_1 \in C_1,\ a_2 \in C_x,\ a_3 \in C_y,\ a_4 \in C_z,\ a_5 \in C_{x^2},\ a_6 \in C_{xy},\ a_7 \in C_{xz}\}$ is an order ideal corresponding to $\mathcal{I}$.*

In sequel, we write order ideal $\mathcal{O}_\mathcal{I}$ as $\mathcal{O}$ and the coefficient ideal mapping is implicitly assumed. Note that unlike in the case of fields, the order ideal in the case of polynomial rings over rings have both monic and nonmonic monomials.

Given an order ideal, $\mathcal{O}$ we introduce two types of borders: a monomial border, $\partial\mathcal{O}_m$ and a scalar border, $\partial\mathcal{O}_s$.

Definition 6.26 *Given an order ideal, $\mathcal{O}$ the monomial border of $\mathcal{O}$ is defined as*

$$\partial\mathcal{O}_m = \{x_1 \cdot \mathrm{Mon}(\mathcal{O}) \cup \ldots \cup x_n \cdot \mathrm{Mon}(\mathcal{O})\} \setminus \mathrm{Mon}(\mathcal{O}).$$

Definition 6.27 *Let $\mathcal{O}$ be an order ideal with respect to a proper coefficient ideal mapping, $\mathcal{I}$. For each x^α such that $\mathcal{I}_{x^\alpha} \neq \langle 1 \rangle$ define $\partial\mathcal{O}_{x^\alpha} = \{c_1 x^\alpha, \ldots, c_s x^\alpha\}$, where $\mathcal{I}_{x^\alpha} = \langle c_1, \ldots, c_s \rangle$ for some $c_1, \ldots, c_s \in A$. The scalar border of an order ideal is defined as*

$$\partial\mathcal{O}_s = \bigcup_{\substack{x^\alpha \in \mathbb{N}^n \\ \mathcal{I}_{x^\alpha} \neq \langle 1 \rangle}} \partial\mathcal{O}_{x^\alpha}.$$

Definition 6.28 *The border of the order ideal $\mathcal{O}$, denoted as $\partial\mathcal{O}$, is defined as $\partial\mathcal{O} = \partial\mathcal{O}_m \cup \partial\mathcal{O}_s$.*

Example 6.29 *Consider Example 6.24. The set of monic border terms that form the monomial border is $\partial\mathcal{O}_m = \{xy, y^2, x^3, x^2y\}$ and the scalar border is $\partial\mathcal{O}_s = \{4x, 3y, 2x^2\}$. Hence, the border of the order ideal is $\partial\mathcal{O} = \{xy, y^2, x^3, x^2y, 4x, 3y, 2x^2\}$.*

Example 6.30 *Consider Example 6.25. The monomials that form the monomial border is $\partial\mathcal{O}'_m = \{x^3, x^2y, x^2z, xy^2, xyz, xz^2, y^2, yz, z^2\}$ and the scalar border is the set*

$$\partial\mathcal{O}'_s = \{u_1^2 y, (u_2^2 - 3u_1)z, u_1^2 xy, (u_2^2 - 1)xy, u_1 xz, u_2 xz\}.$$

Hence border of the order ideal is

$$\partial\mathcal{O}' = \{x^3, x^2y, x^2z, xy^2, xyz, xz^2, y^2, yz, z^2, u_1^2 y, (u_2^2 - 3u_1)z, u_1^2 xy, (u_2^2 - 1)xy, u_1 xz, u_2 xz\}.$$

We define $\partial^0\mathcal{O} = \mathcal{O}$ and 0^{th} border closure as

$$\overline{\partial^0\mathcal{O}} = \{ax^\alpha \mid cx^\alpha \in \mathcal{O}, \text{ for some } c \in C_{x^\alpha}, c \neq 0 \text{ and } a \in c + \mathcal{I}_{x^\alpha}\}.$$

Note that in the case of fields these quantities are defined as $\partial^0\mathcal{O} = \overline{\partial^0\mathcal{O}} = \mathcal{O}$ (Kehrein and Kreuzer, 2006).

The definitions of first and higher order border closures are given below.

Definition 6.31 *The first border closure $\overline{\partial\mathcal{O}}$ of an order ideal $\mathcal{O}$ is defined as*

$$\overline{\partial\mathcal{O}} = \{ax^\alpha \mid \exists c \in A \text{ such that } cx^\alpha \in \mathcal{O} \cup \partial\mathcal{O}_s, a \in A \text{ or } x^\alpha \in \partial\mathcal{O}_m\}.$$

Proposition 6.32 *The first border closure, $\overline{\partial\mathcal{O}}$, of an order ideal, $\mathcal{O}$ is an order ideal.*

Proof: We fix $\mathcal{I}_{x^\alpha} = \{0\}$ for all $x^\alpha \in \overline{\partial\mathcal{O}}$. By Definition 6.31 three cases arises: $x^\alpha \in \partial\mathcal{O}_m$ or there exists $c \in A$ such that $cx^\alpha \in \mathcal{O}$ or $cx^\alpha \in \partial\mathcal{O}_s$. Let $x^\alpha \in \partial\mathcal{O}_m$. Suppose $x^\beta | x^\alpha$ for some $x^\beta \in \mathbb{N}^n$, then clearly, $x^\beta \in \text{Mon}(\mathcal{O}) \cup \partial\mathcal{O}_m$. If $x^\beta \in \text{Mon}(\mathcal{O})$, then there exists some $d \in C_{x^\beta}$ such that $dx^\beta \in \mathcal{O}$. Therefore, in either case $x^\beta \in \overline{\partial\mathcal{O}}$. In the second case, let $cx^\alpha \in \mathcal{O}$. Suppose $x^\beta | x^\alpha$ for some $x^\beta \in \mathbb{N}^n$. By the closure property of $\mathcal{O}$, $dx^\beta \in \mathcal{O}$ for some $d \in C_{x^\beta}$. Therefore, $x^\beta \in \overline{\partial\mathcal{O}}$. In the third case, let $cx^\alpha \in \partial\mathcal{O}_s$. Suppose $x^\beta | x^\alpha$ for some $x^\beta \in \mathbb{N}^n$. This implies that $x^\beta \in \text{Mon}(\mathcal{O})$. Thus, $x^\beta \in \overline{\partial\mathcal{O}}$. □

The monomial part of the first border closure defined as the set of monomials in $\overline{\partial\mathcal{O}}$, is a finite set and it is represented as $\text{Mon}(\overline{\partial\mathcal{O}})$. It is interesting to see that since $\mathcal{I}_{x^\alpha} = \{0\}$ for all

$x^\alpha \in \text{Mon}(\overline{\partial \mathcal{O}})$, the scalar border for $k \geq 2$ is an empty set and one needs to consider only the monomial border.

Definition 6.33 *The k^{th} border of an order ideal $\mathcal{O}$ for $k \geq 1$ is defined as*

$$\partial^k \mathcal{O} = \{x_1 \cdot \text{Mon}(\overline{\partial^{k-1}\mathcal{O}}) \cup \ldots \cup x_n \cdot \text{Mon}(\overline{\partial^{k-1}\mathcal{O}})\} \setminus \text{Mon}(\overline{\partial^{k-1}\mathcal{O}}),$$

where $\text{Mon}(\overline{\partial^{k-1}\mathcal{O}})$ is the monomial part of the $(k-1)^{th}$ border closure.

Definition 6.34 *For $k \geq 2$, the k^{th} border closure of an order ideal is defined as*

$$\overline{\partial^k \mathcal{O}} = \{ax^\alpha |\ a \in A, x^\alpha \in \partial^k \mathcal{O} \cup \overline{\partial^{k-1}\mathcal{O}_m}\}.$$

Example 6.35 *Consider Example 6.24. The set of monic border terms that form the monomial border is $\partial \mathcal{O}_m = \{xy, y^2, x^3, x^2y\}$ and the scalar border is $\partial \mathcal{O}_s = \{4x, 3y, 2x^2\}$. The second border of the order ideal, $\mathcal{O}$, is the set, $\partial^2 \mathcal{O} = \{xy^2, y^3, x^4, x^3y, x^2y^2\}$.*

Example 6.36 *Consider Example 6.25. The second border of the order ideal, $\mathcal{O}'$ is the set, $\partial^2 \mathcal{O}' = \{y^3, y^2z, yz^2, z^3, x^4, x^3y, x^3z, x^2y^2, x^2yz, x^2z^2, xy^3, xyz^2, xy^2z, xz^3\}$.*

Remark 6.37 *The k^{th} border closure is an infinite set of terms for $k \geq 0$. Further, for $k \geq 1$, $\overline{\partial^k \mathcal{O}}$ is closed under division and hence the set of monomials corresponding to it, $\text{Mon}(\overline{\partial^k \mathcal{O}})$, mimics the case of fields.*

We give below certain properties of order ideals, their borders and border closures. These properties are analogous to the case of polynomial rings over fields.

Proposition 6.38 *Let $\mathcal{O}$ be an order ideal and $\partial \mathcal{O}_m$ be its monomial border. Then*

1. *For $k \geq 1$, the k^{th} monomial border closure of $\mathcal{O}$, $\text{Mon}(\overline{\partial^k \mathcal{O}})$ is the following disjoint union, $\text{Mon}(\mathcal{O}) \cup \partial \mathcal{O}_m \cup (\cup_{i=2}^k \partial^k \mathcal{O})$.*
2. *For $k \geq 1$, $\partial^k \mathcal{O}_m = \mathbb{N}_k^n \cdot \text{Mon}(\mathcal{O}) \setminus \mathbb{N}_{<k}^n.\text{Mon}(\mathcal{O})$, where $\partial^k \mathcal{O}_m = \partial^k \mathcal{O}$ for $k \geq 2$.*
3. *A monomial, $x^\alpha \in \mathbb{N}^n$ is divisible by $x^\beta \in \partial \mathcal{O}_m$ if and only if $x^\alpha \in \mathbb{N}^n \setminus \text{Mon}(\mathcal{O})$.*

Proof: (1) The proof is by induction on k. For $k = 1$, clearly the monomials in the first border closure are elements of the set $\mathcal{O}_m \cup \partial \mathcal{O}_m$. From the definition of monomial border of $\mathcal{O}$ we have that $\mathcal{O}_m$ and $\partial \mathcal{O}_m$ are disjoint. Suppose that the claim is true for the k^{th} monomial border closure. For $k+1$, $\overline{\partial^{k+1}\mathcal{O}_m} = \overline{\partial^k \mathcal{O}_m} \cup \partial^{k+1}\mathcal{O}$. It is easy to verify that the sets $\overline{\partial^k \mathcal{O}_m}$ and

$\partial^{k+1}\mathcal{O}$ are disjoint.
(2) The claim follows from the observation that $\partial^k\mathcal{O} = \overline{\partial^k\mathcal{O}_m} \setminus \overline{\partial^{k-1}\mathcal{O}_m}$.
(3) We have $x^\beta \in \partial\mathcal{O}_m$. This implies that there exists $x^\gamma \in \mathcal{O}_m$ and an indeterminate x_{i_0} such that $x^\beta = x_{i_0}x^\gamma$. We have $x_{i_0}x^\gamma | x^\alpha$. If $x^\alpha \in \mathcal{O}_m$ then $x_{i_0}x^\gamma \in \mathcal{O}_m$ which is a contradiction. Now consider a monomial $x^\alpha \in \mathbb{T}^n \setminus \mathcal{O}$. Then, $x^\alpha \in \partial\mathcal{O}_m$ or $x^\alpha \in \partial^k\mathcal{O}$ for some $k \geq 2$. If $x^\alpha \in \partial^k\mathcal{O}$ then it implies that there exists a monomial x^γ of degree $k-1$ and a $x^\beta \in \partial\mathcal{O}_m$ such that $x^\alpha = x^\gamma x^\beta$. The claim follows. □

Now we introduce certain concepts that are essential for the division algorithm.

Definition 6.39 *Index of a term cx^α, where $c \in A$ and $x^\alpha \in \mathbb{N}^n$, w.r.t. an order ideal, $\mathcal{O}$ is defined as*

$$\mathrm{ind}_\mathcal{O}(cx^\alpha) = \min\{k \in \mathbb{N} \mid cx^\alpha \in \overline{\partial^k\mathcal{O}}\}.$$

Definition 6.40 *Let $f \in A[x_1, \ldots, x_n]$ be any nonzero polynomial with support,* $\mathrm{supp}(f)$*. Then index of f w.r.t. an order ideal, $\mathcal{O}$ is defined as*

$$\mathrm{ind}_\mathcal{O}(f) = \max_{\alpha \in \mathrm{supp}(f)} \mathrm{ind}_\mathcal{O}(c_\alpha x^\alpha).$$

Example 6.41 *Consider Example 6.24. The set of monic border terms that form the monomial border is $\partial\mathcal{O}_m = \{xy, y^2, x^3, x^2y\}$ and the scalar border is $\partial\mathcal{O}_s = \{4x, 3y, 2x^2\}$. Then* $\mathrm{ind}_\mathcal{O}(3x) = 0$, $\mathrm{ind}_\mathcal{O}(xy) = 1$ *and* $\mathrm{ind}_\mathcal{O}(xy^2 + 8x + 7y) = 2$.

Example 6.42 *Consider Example 6.25. The monomials that form the monomial border is $\partial\mathcal{O}'_m = \{x^3, x^2y, x^2z, xy^2, xyz, xz^2, y^2, yz, z^2\}$ and the scalar border is the set $\partial\mathcal{O}'_s = \{u_1^2y, (u_2^2 - 3u_1)z, u_1^2xy, (u_2^2 - 1)xy, u_1xz, u_2xz\}$. Then* $\mathrm{ind}_{\mathcal{O}'}((3u_2 + u_2)x) = 0$, $\mathrm{ind}_{\mathcal{O}'}(u_1x^2y) = \mathrm{ind}_{\mathcal{O}'}((u_1^2 + u_2)xz) = 1$ *and* $\mathrm{ind}_{\mathcal{O}'}(xy^3 + 8x) = 2$.

For any polynomial, the terms of highest index are grouped together to form a border form analogous to the leading term in Gröbner basis theory. We define this below.

Definition 6.43 *Let $f \in A[x_1, \ldots, x_n]$ be a nonzero polynomial such that the* $\mathrm{ind}_\mathcal{O}(f) = i_0$*. The border form of f w.r.t. $\mathcal{O}$ is defined as*

$$\mathrm{BF}_\mathcal{O}(f) = \sum_{\substack{\alpha \in \mathrm{supp}(f), c_\alpha \in A \\ \mathrm{ind}_\mathcal{O}(c_\alpha x^\alpha) = i_0}} c_\alpha x^\alpha \ ,$$

a polynomial in $A[x_1, \ldots, x_n]$.

Note that unlike leading term of a polynomial in Gröbner basis theory that is always a monomial, border form can be a polynomial. The concept of leading term ideal has an analogous form in border bases called the border form ideal.

Definition 6.44 *The border form ideal of an ideal* $\mathfrak{a}$ *in* $A[x_1, \ldots, x_n]$ *w.r.t. an order ideal* $\mathcal{O}$ *is defined as*

$$\mathrm{BF}_{\mathcal{O}}(\mathfrak{a}) = \langle \mathrm{BF}_{\mathcal{O}}(f) \mid f \in \mathfrak{a} \rangle.$$

Example 6.45 *Consider Example 6.24. Let* $f = xy^2 + 2x^2y^2 + xy + 3x + 2$. *Then the index of* f *w.r.t. the order ideal* $\mathcal{O}$ *is equal to 2. The border form of* f *is the polynomial,* $\mathrm{BF}_{\mathcal{O}}(f) = xy^2 + 2x^2y^2$.

Example 6.46 *Consider Example 6.25. Let* $f = 2xy^2 + (u_1 - u_2)xz + 3x + 2$. *Then the index of* f *w.r.t. the order ideal* $\mathcal{O}'$ *is equal to 2. The border form of* f *is the polynomial,* $\mathrm{BF}_{\mathcal{O}'}(f) = 2xy^2 + (u_1 - u_2)xz$.

We now give the definition of border prebasis for an order ideal, $\mathcal{O}$.

Definition 6.47 *Let* $\mathcal{O}$ *be an order ideal,* $\partial\mathcal{O} = \{c_1 x^{\alpha_1}, \ldots, c_s x^{\alpha_s}\}$ *be its border and* $C_{x^{\alpha_i}}$ *be the set of coset representatives of* $A/\mathcal{I}_{x^{\alpha_i}}$. *A finite set of polynomials* $G = \{g_1, \ldots, g_s\} \subseteq A[x_1, \ldots, x_n]$ *is said to be an* $\mathcal{O}$*-border prebasis if* $g_i = c_i x^{\alpha_i} - h_i$, *where* $h_i \in A[x_1, \ldots, x_n]$ *satisfying* $\mathrm{Ter}(h_i) \subseteq \mathcal{O} \setminus \{a x^{\alpha_i} \mid a \in C_{x^{\alpha_i}}\}$, $i = 1, \ldots, s$.

Note that unlike in fields, for a monomial in the border of $\mathcal{O}$, we can have more than one polynomial in the $\mathcal{O}$-border prebasis but only one polynomial corresponding to a term in the border. With the definition of $\mathcal{O}$-border prebasis, we now give a procedure for division of any polynomial in $A[x_1, \ldots, x_n]$ with the $\mathcal{O}$-border prebasis.

Procedure 6.48 *Let* $\mathcal{O}$ *be an order ideal. Let* $\mathrm{Mon}(\mathcal{O}) = \{x^{\alpha_1}, \ldots, x^{\alpha_t}\}$ *be its monomial part. Let* $\partial\mathcal{O}_m = \{x^{\beta_1}, \ldots, x^{\beta_{s'}}\}$ *and* $\partial\mathcal{O}_s = \{c_{s'+1} x^{\beta_{s'+1}}, \ldots, c_s x^{\beta_s}\}$ *be its monomial border and scalar border respectively. Let* $G = \{g_1, \ldots, g_s\} \subseteq A[x_1, \ldots, x_n]$ *be an* $\mathcal{O}$*-border prebasis. For* $f \in A[x_1, \ldots, x_n]$ *we perform the following steps.*

1. *Initialize* $f_1 = \ldots = f_s = 0$, $a_1 = \ldots = a_t = 0$ *and* $h = f$.
2. *If* $h = 0$ *return* $(f_1, \ldots, f_s, a_1, \ldots, a_t)$.
3. *If* $\mathrm{ind}_{\mathcal{O}}(h) = 0$ *then find* $b_1, \ldots, b_t \in A$ *such that* $h = b_1 x^{\alpha_1} + \ldots + b_t x^{\alpha_t}$. *Set* $a_i = b_i$ *for each* $1 \leq i \leq t$. *Return* $(f_1, \ldots, f_s, a_1, \ldots, a_t)$.

4. *If* $\mathrm{ind}_{\mathcal{O}}(h) = 1$ *and* h *contains a term* dx^{β} *such that* $x^{\beta} \in \partial\mathcal{O}_m$ *then goto Step 5. Else, let* $h = d_1x^{\gamma_1} + \ldots + d_jx^{\gamma_j}$ *such that* $\mathrm{ind}_{\mathcal{O}}(h) = \mathrm{ind}_{\mathcal{O}}(d_1x^{\gamma_1})$ *and* $\mathrm{ind}_{\mathcal{O}}(d_1x^{\gamma_1}) \geq \ldots \geq \mathrm{ind}_{\mathcal{O}}(d_jx^{\gamma_j})$. *Find* $b_{\mu+1}, \ldots, b_s \in A$ *such that* $d_1x^{\gamma_1} = b_{s'+1}(c_{s'+1}x^{\beta_{s'+1}}) + \ldots + b_s(c_sx^{\beta_s})$. *Subtract* $b_{s'+1}g_{s'+1} + \ldots + b_sg_s$ *from* h, *add* b_i *to* f_i *for* $s'+1 \leq i \leq s$ *and return to Step 2.*

5. *Else, if* $\mathrm{ind}_{\mathcal{O}}(h) \gneq 1$, *let* $h = d_1x^{\gamma_1} + \ldots + d_jx^{\gamma_j}$ *such that* $\mathrm{ind}_{\mathcal{O}}(h) = \mathrm{ind}_{\mathcal{O}}(x^{\gamma_1})$ *and* $\mathrm{ind}_{\mathcal{O}}(d_1x^{\gamma_1}) \geq \ldots \geq \mathrm{ind}_{\mathcal{O}}(d_jx^{\gamma_j})$. *Determine* $x^{\beta_i} \in \partial\mathcal{O}_m$ *with the smallest* i *such that* $x^{\gamma_i} = x^{\mu}x^{\beta_i}$ *and* $\deg(x^{\mu}) = \mathrm{ind}_{\mathcal{O}}(h) - 1$. *Subtract* $d_1x^{\mu}g_i$ *from* h, *add* d_1x^{μ} *to* f_i *and return to Step 2.*

This procedure over rings differs from the case of fields only in Step 4. The termination of the above method is not assured because of the possibility that for a given polynomial, f, a monomial in its support identified with index 0 in Step 3 may again have an index 1 after Step 4. Therefore, we cannot assume the reduction in index values at every step of the procedure.

6.4 Acyclic Border Prebases and Termination of Border Division Algorithm

Here, we identify a special class of $\mathcal{O}$-border prebases called acyclic $\mathcal{O}$-border prebases for which the termination of the border division algorithm can be established.

Definition 6.49 *A* $\mathcal{O}$*-border prebasis* $G = \{g_1, \ldots, g_s\}$ *is said to be acyclic if there exists a permutation of* G, $\{g_{i_1}, \ldots, g_{i_s}\}$ *such that for any* g_{i_j}, g_{i_k}, *where* $j \lneq k$, *exactly one of the following conditions are satisfied*

1. $c_j\,\mathrm{BF}_{\mathcal{O}}(g_{i_j}) = c_k\,\mathrm{BF}_{\mathcal{O}}(g_{i_k})$ *for any* $c_j, c_k \in A$ *or*

2. $d_jx^{\alpha_j} \in \partial\mathcal{O}$ *and* $d_jx^{\alpha_j} \in \mathrm{supp}(g_{i_j})$ *implies* $c_kx^{\alpha_j} \notin \mathrm{supp}(g_{i_k})$ *for some* $c_k, d_j \in A$.

The ordered set of acyclic $\mathcal{O}$-border prebasis that satisfies the permutation given above is called a 'well ordered' acyclic $\mathcal{O}$-border prebasis.

Example 6.50 *We consider Example 6.24. The set* $G = \{g_1, \ldots, g_7\}$, *where* $g_1 = xy - x$, $g_2 = y^2 - y$, $g_3 = x^3 - 2y$, $g_4 = x^2y - x^2 + 10$, $g_5 = 4x - 2y$, $g_6 = 3y - 3x$ *and* $g_7 = 2x^2 - x + 5$ *is an* $\mathcal{O}$*-border prebasis but it is not acyclic. Let* $G' = \{g'_1, \ldots, g'_7\}$ *where* $g'_1 = xy - x$, $g'_2 = y^2 - y$, $g'_3 = x^3 - x^2 + 6$, $g'_4 = x^2y - y + 5$, $g'_5 = 4x - 7$, $g'_6 = 3y - x$ *and* $g'_7 = 2x^2 - 2y - 3x$, *which is also an* $\mathcal{O}$*-border prebasis but it is acyclic since the permutation of* G', $\{g'_1, g'_2, g'_3, g'_4, g'_7, g'_6, g'_5\}$ *satisfies the acyclicity condition.*

Example 6.51 *Consider Example 6.25. The set* $G = \{g_1, \ldots, g_{15}\}$, *where* $g_1 = x^3 - 3$, $g_2 = x^2y - 3u_1y$, $g_3 = x^2z - 2z$, $g_4 = xy^2 - x + 10$, $g_5 = xyz - 11xy$, $g_6 = xz^2 - u_2u_1^2x^2$, $g_7 = y^2 - x + u_1u_2$, $g_8 = yz - 3y + 2$, $g_9 = z^2 + 5xz + 11u_1x$, $g_{10} = u_1^2y + u_2x + 3$, $g_{11} = (u_2^2 - 3u_1)z - u_2^2y$, $g_{12} = u_1^2xy + 3u_1x - 2z$, $g_{13} = (u_2^2 - 1)xy + 2x^2$, $g_{14} = u_1xz + 3u_1x^2$, $g_{15} = u_2xz + 2u_1xy + 4x^2 - 4z - 10u_1y + 14$ *is an acyclic* $\mathcal{O}$*-border prebasis since the following permutation of* G, $\{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_9, g_{14}, g_{15}, g_{13}, g_{12}, g_{11}, g_{10}\}$ *satisfies the acyclicity condition.*

We now show the correctness and termination of Algorithm 6.48 when the $\mathcal{O}$-border prebasis is acyclic.

Proposition 6.52 (Border division algorithm) *Consider a polynomial* $f \in A[x_1, \ldots, x_n]$. *If the* $\mathcal{O}$*-border prebasis* $G = \{g_1, \ldots, g_s\} \subseteq A[x_1, \ldots, x_n]$ *is acyclic, then Procedure 6.48 terminates for a polynomial,* $f \in A[x_1, \ldots, x_n]$ *and returns a tuple,*

$$(f_1, \ldots, f_s, a_1, \ldots, a_t) \in (A[x_1, \ldots, x_n])^s \times A^t$$

such that

$$f = f_1g_1 + \ldots + f_sg_s + a_1x^{\alpha_1} + \ldots + a_tx^{\alpha_t},$$

and $\deg(f_i) \leq \mathrm{ind}_{\mathcal{O}}(f)$, *for* $i = 1, \ldots, s$ *with* $f_ig_i \neq 0$.

Proof: We first describe the execution of the algorithm. In Step 4, $\mathrm{ind}_{\mathcal{O}}(d_1x^{\gamma_1}) = 1$ and $d_1x^{\gamma_1} \in \mathrm{Span}_A(\langle \partial\mathcal{O} \rangle_A)$. This implies that $d_1 \in \mathcal{I}_{x^{\gamma_1}}$, where $\mathcal{I}_{x^{\gamma_1}}$ is an ideal generated by $\langle u_1, \ldots, u_k \rangle$, $u_ix^{\gamma_1} \in \partial\mathcal{O}_s$, $1 \leq i \leq k$. Thus, there exists $l_1, \ldots, l_k \in A$ such that $d_1 = \sum_{i=1}^{k} l_iu_i$. Hence, $d_1x^{\gamma_1} = \sum_{s'+1}^{s} b_i(c_ix^{\beta_i})$, where $c_ix^{\beta_i} \in \partial\mathcal{O}_s$ and $b_i = l_j$ when $c_ix^{\beta_i} = u_jx^{\gamma_1}$ for some $j \in \{1, \ldots, k\}$, and $b_i = 0$, otherwise. The other steps, due to the absence of scalar border terms, mimic the steps of border basis division in fields and therefore the description of the execution of these steps of the algorithm is the same as in (Kehrein and Kreuzer, 2005, Proposition 3). We prove that the representation,

$$f = f_1g_1 + \ldots + f_sg_s + a_1x^{\alpha_1} + \ldots + a_tx^{\alpha_t} + h,$$

computed by the algorithm is valid in every step of the algorithm. Clearly, it is satisfied in Step 1. In Step 4 we subtract $(b_{s'+1}g_{s'+1} + \ldots + b_sg_s)$ from h. These b_is are then added to f_is, i.e. $f_i = f_i + b_i$, $s' + 1 \leq i \leq s$. Similarly in Step 5, from h we subtract $d_1x^{\mu}g_i$ and we add d_1x^{μ} to f_i. The constants $a_1, \ldots, a_t$ are modified only in Step 3. The representation of f is also valid because $\mathrm{ind}_{\mathcal{O}}(h) = 0$. If the algorithm terminates, $h = 0$ and we have a valid representation.

Now we prove that $\deg(f_i) \leq \text{ind}_{\mathcal{O}}(f)$ for all $i = 1, \ldots, s$. In Step 5 of the algorithm, where we divide using the monomial border, our choice of the term $d_1 x^{\mu}$ is such that $\deg(dx^{\mu}) = \text{ind}_{\mathcal{O}}(h) - 1$. In Step 4, where we divide using the scalar border, the index of the intermediate polynomial, h is 1. The b_i, $i = 1, \ldots, s$ are actually constants and the degree of f_i, $i = 1, \ldots, s$ are therefore zero. All the other steps in the algorithm do not affect f_i, $i = 1, \ldots, s$. Also, in the algorithm the index of the intermediate polynomial, h never increases. From the above steps, the inequality $\deg(f_i) \leq \text{ind}_{\mathcal{O}}(f) - 1$ for all $i = 1, \ldots, s$ follows.

Next, we prove that the algorithm terminates on all inputs. In Step 4, $\text{ind}_{\mathcal{O}}(h) = 1$ and the $\text{Ter}(h) \subseteq \text{Span}_A(\text{Mon}(\mathcal{O})) \cup \text{Span}_A(\partial\mathcal{O}_s) = \text{Span}_A(\text{Mon}(\mathcal{O}))$. We claim that Step 4 terminates after a finite number of steps for an acyclic $\mathcal{O}$-border prebasis. Let $h = d_1 x^{\alpha_1} + \ldots + d_t x^{\alpha_t}$. For simplicity, let us assume that the acyclic $\mathcal{O}$-border prebasis, G is well ordered. It can easily be seen that g_1 will be used atmost once in Step 4, while g_2 will be used at most twice ($h \xrightarrow{g_2} h_1 \xrightarrow{G\setminus\{g_1,g_2\}}_+ h_2 \xrightarrow{g_1} h_3 \xrightarrow{G\setminus\{g_1,g_2\}}_+ h_4 \xrightarrow{g_2} h_5$). Similarly, any g_i will be used atmost $\mathrm{O}(i^2)$ times. For the set G, therefore Step 4 is executed at most $\mathrm{O}(s^3)$ times. All the other steps of the division correspond to either order ideal, monomial border or the k^{th} order border, $k \gneq 1$ and therefore mimic the border division in fields. Hence, the termination is guaranteed by (Kehrein and Kreuzer, 2005, Proposition 3). □

Consider an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ generated by an acyclic $\mathcal{O}$-border prebasis, $G = \{g_1, \ldots, g_s\}$. The border division algorithm gives us the remainder upon division by G as a part of its output. We now give a formal definition for the remainder.

Definition 6.53 *Let $\mathcal{O}$ be an order ideal and $\text{Mon}(\mathcal{O}) = \{x^{\alpha_1}, \ldots, x^{\alpha_t}\}$, its monomial part. Let $G = \{g_1, \ldots, g_s\}$ be the $\mathcal{O}$-border prebasis. The $\mathcal{O}$-remainder of a polynomial f w.r.t. G, if it exists, is given as*

$$\text{rem}_{\mathcal{O},G}(f) = a_1 x^{\alpha_1} + \ldots + a_t x^{\alpha_t},$$

where $f = f_1 g_1 + \ldots + f_s g_s + a_1 x^{\alpha_1} + \ldots + a_t x^{\alpha_t}$, $a_i \in A$ for $i = 1, \ldots, t$ is a representation computed by the border division algorithm whenever the algorithm terminates.

6.5 Acyclic Border Bases in $A[x_1, \ldots, x_n]$

With the concept of acyclic $\mathcal{O}$-border prebasis that guarantee the termination of division algorithm, we proceed to define border basis for polynomial rings over rings.

Definition 6.54 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is a finitely generated A-module. Let $\mathcal{O}$ be an order ideal and $G = \{g_1, \ldots, g_s\}$ be an acyclic $\mathcal{O}$-border prebasis consisting of polynomials in $\mathfrak{a}$. G is an acyclic $\mathcal{O}$- border basis of $\mathfrak{a}$ if $\text{Mon}(\mathcal{O})$ is a weak$^+$ basis of $A[x_1, \ldots, x_n]/\mathfrak{a}$.*

The next proposition shows that these polynomials indeed generate the ideal in $\mathfrak{a}$.

Proposition 6.55 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated as an A-module. Let $\mathcal{O}$ be an order ideal and let $G = \{g_1, \ldots, g_s\}$ be an acyclic $\mathcal{O}$-border basis for $\mathfrak{a}$. Then $\mathfrak{a}$ is generated by G.*

Proof: Let $\mathrm{Mon}(\mathcal{O}) = \{x^{\alpha_1}, \ldots, x^{\alpha_t}\}$ be the monomial part of $\mathcal{O}$ and $G = \{g_1, \ldots, g_s\}$ be an acyclic $\mathcal{O}$-border basis of $\mathfrak{a}$. Consider, $f \in \mathfrak{a}$. By Algorithm 6.52, we have $f_1, \ldots, f_s \in A[x_1, \ldots, x_n]$ and $a_1, \ldots, a_t \in A$ such that

$$f = f_1 g_1 + \ldots + f_s g_s + a_1 x^{\alpha_1} + \ldots + a_t x^{\alpha_t}. \tag{6.1}$$

Now, $f - \sum_{i=1}^{s} f_i g_i \in \mathfrak{a}$. This implies, $\sum_{i=1}^{t} a_i x^{\alpha_i} \in \mathfrak{a}$. Let $h = \sum_{i=1}^{t} a_i x^{\alpha_i}$. Suppose $h \neq 0$, then $a_i \notin \mathcal{I}_{x^{\alpha_i}} \setminus \{0\}$, for all $i = 1, \ldots, t$. If $a_i \in \mathcal{I}_{x^{\alpha_i}}$, for all $i = 1, \ldots, t$, then $\mathrm{ind}_{\mathcal{O}}(h) = 1$. Then, (6.1) is not a valid output of Algorithm 6.52. But we are also given that G is an acyclic border basis of $\mathfrak{a}$. The weak$^+$ basis property of border bases implies that if $\sum_{i=1}^{t} a_i x^{\alpha_i} \in \mathfrak{a}$ and $a_i \neq 0$ for all $i = 1, \ldots, t$, then $a_i \in \mathcal{I}_{x^{\alpha_i}}$ for some $i \in \{1, \ldots, t\}$. This is a contradiction. Hence, $h = 0$. We have, $f = \sum_{i=1}^{s} f_i g_i$. The other inclusion follows from the fact that $G \subseteq \mathfrak{a}$. □

Now one needs to verify if an acyclic $\mathcal{O}$-border basis exists for every ideal, $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$. We first address, below, whether an acylic $\mathcal{O}$-border basis for $\mathfrak{a}$ given an order ideal, $\mathcal{O}$, exists. We also prove the uniqueness of the acyclic $\mathcal{O}$-border basis.

Theorem 6.56 *Let $\mathcal{O}$ be an order ideal, and let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is a finitely generated A-module. If $\mathrm{Mon}(\mathcal{O})$ is a weak$^+$ basis then there exists a unique acyclic $\mathcal{O}$-border basis for $\mathfrak{a}$.*

Proof: Let $\mathrm{Mon}(\mathcal{O}) = \{x^{\alpha_1}, \ldots, x^{\alpha_t}\}$ be the monomial part of $\mathcal{O}$, and let $\partial\mathcal{O} = \{c_1 x^{\beta_1}, \ldots, c_s x^{\beta_s}\}$ be the border of $\mathcal{O}$. We now prove that an $\mathcal{O}$-border basis exists for $\mathfrak{a}$. Since $\mathrm{Mon}(\mathcal{O})$ is a weak$^+$ basis, for each $c_i x^{\beta_i} \in \partial\mathcal{O}$ one can find $a_j^{(i)} x^{\alpha_i} s \in \mathcal{O}$ such that $c_i x^{\beta_i} = \sum_{j=1}^{t} a_j^{(i)} x^{\alpha_j} \bmod \mathfrak{a}$. We define G as

$$G = \{c_i x^{\beta_i} - \sum_{j=1}^{t} a_j^{(i)} x^{\alpha_j}, 1 \leq i \leq s\}.$$

Clearly, G is an acyclic $\mathcal{O}$-border prebasis. Now, $G \subseteq \mathfrak{a}$ and $A[x_1, \ldots, x_n]/\mathfrak{a} = \{\sum a_i x^{\alpha_i} + \mathfrak{a} : x^{\alpha_i} \in \mathrm{Mon}(\mathcal{O}) \text{ and } a_i \in A\}$. Hence, G is an $\mathcal{O}$-border basis of $\mathfrak{a}$.

To prove the uniqueness of $\mathcal{O}$-border basis, consider two acyclic $\mathcal{O}$-border bases for $\mathfrak{a}$. Let

$G = \{g_1, \ldots, g_t\}$ and $G = \{g'_1, \ldots, g'_t\}$ where

$$g_i = c_i x^{\beta_i} - \sum_{j=1}^{t} a_j^{(i)} x^{\alpha_j}, \text{ where each } a_j^{(i)} x^{\alpha_j} \in \mathcal{O} \text{ and,}$$

$$g'_i = c_i x^{\beta_i} - \sum_{j=1}^{t} a_j'^{(i)} x^{\alpha_j}, \text{ where each } a_j'^{(i)} x^{\alpha_j} \in \mathcal{O}.$$

We have,

$$g_i - g'_i = \sum_{j=1}^{t} a_j^{(i)} x^{\alpha_j} - \sum_{j=1}^{t} a_j'^{(i)} x^{\alpha_j} \in \mathfrak{a}.$$

This implies,

$$\sum_{j=1}^{t} (a_j^{(i)} - a_j'^{(i)}) x^{\alpha_j} \in \mathfrak{a}.$$

Since $a_j^{(i)}$ and $a_j'^{(i)}$ are coset representatives of $A/\mathcal{I}_{x^{\alpha_j}}$ and the difference of two different cosets cannot be a zero coset, we have $a_j^{(i)} = a_j'^{(i)}$. Therefore, $g_i = g'_i$. Hence, the acyclic $\mathcal{O}$-border basis of $\mathfrak{a}$ is unique. □

Thus, the question of existence of a border basis for an ideal reduces to the following questions. Given an ideal $\mathfrak{a}$, (i) does there always exist a proper coefficient ideal mapping, $\mathcal{I}$ such that the monomial part of the order ideal, Mon($\mathcal{O}$) constructed from $\mathcal{I}$ forms a weak$^+$ basis for $A[x_1, \ldots, x_n]/\mathfrak{a}$ and (ii) will the corresponding $\mathcal{O}$-border basis be acyclic. We use the theory of Gröbner bases to establish this result.

Theorem 6.57 *Given an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated as an A-module, there always exists an acyclic border basis of $\mathfrak{a}$ corresponding to some order ideal, $\mathcal{O}$.*

Proof: Let $\prec$ be a monomial order on $A[x_1, \ldots, x_n]$. Let $G' = \{g'_1, \ldots, g'_t\}$ be a Gröbner basis of $\mathfrak{a}$. Consider the coefficient ideal mapping fixed by G, $\mathcal{I}^{(G)}$. Since $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated, the mapping is proper. Let $\mathcal{O}_\prec$ be the order ideal corresponding to $\mathcal{I}^{(G)}$. It follows from Corollary 6.20 that Mon($\mathcal{O}_\prec$) forms a weak$^+$ basis. Let $\partial\mathcal{O}_\prec = \{c_1 x^{\beta_1}, \ldots, c_s x^{\beta_s}\}$ be the border of $\mathcal{O}_\prec$. Let G be the $\mathcal{O}_\prec$-border prebasis constructed along the same lines as in the proof of Theorem 6.56. Therefore, each polynomial g_i in G is of the form,

$$g_i = c_i x^{\beta_i} - \sum_{j=1}^{t} a_j^{(i)} x^{\alpha_j}, \; i = 1, \ldots, s,$$

where $c_i x^{\beta_i} \in \partial\mathcal{O}$ and each $a_j^{(i)} x^{\alpha_j} \in \mathcal{O}$.

For any $g_i \in G$, monomial ordering imposes that for every nonzero $a_j^{(i)} x^{\alpha_j}$, $x^{\alpha_j} \prec x^{\beta_i}$. Also, for two distinct border terms $c_i x^{\beta_i}$ and $c_j x^{\beta_j}$ such that $x^{\beta_i} \neq x^{\beta_j}$, either $x^{\beta_i} \prec x^{\beta_j}$ or $x^{\beta_j} \prec x^{\beta_i}$. The acyclic property of G follows from these two observations. Theorem 6.56 implies that G forms a unique acyclic $\mathcal{O}_\prec$-border basis for $\mathfrak{a}$. □

For any polynomial $f \in A[x_1, \ldots, x_n]$, given an acylic $\mathcal{O}$-border prebasis, G and an order ideal, $\mathcal{O}$, $\mathcal{O}$-remainder of f is denoted by $\mathrm{rem}_{\mathcal{O},G}(f)$ (Definition 6.53).

Proposition 6.58 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated as an A-module and $G \subseteq \mathfrak{a}$ be an acyclic $\mathcal{O}$-border basis of $\mathfrak{a}$. For any $f \in A[x_1, \ldots, x_n]$, $f \in \mathfrak{a}$ if and only if $\mathrm{rem}_{\mathcal{O},G}(f) = 0$.*

Proof: Let $\mathrm{Mon}(\mathcal{O}) = \{x^{\alpha_1}, \ldots, x^{\alpha_t}\}$ be the monomial part of $\mathcal{O}$ and $G = \{g_1, \ldots, g_s\}$ be an acyclic $\mathcal{O}$-border basis of $\mathfrak{a}$. By Algorithm 6.52, we have $f_1, \ldots, f_s \in A[x_1, \ldots, x_n]$ and $a_1, \ldots, a_t \in A$ such that

$$f = \sum_{i=1}^{s} f_i g_i + \mathrm{rem}_{\mathcal{O},\mathcal{G}}(f), \tag{6.2}$$

where $\mathrm{rem}_{\mathcal{O},G}(f) = \sum_{j=1}^{t} a_j x^{\alpha_j}$. If $\mathrm{rem}_{\mathcal{O},G}(f) = 0$ then $f = \sum_{i=1}^{s} f_i g_i$. Hence, $f \in \mathfrak{a}$.

Now let $f \in \mathfrak{a}$. Then $f - \sum_{i=1}^{s} f_i g_i \in \mathfrak{a}$. This implies, $\mathrm{rem}_{\mathcal{O},G}(f) \in \mathfrak{a}$. Suppose $\mathrm{rem}_{\mathcal{O},G}(f)$ is not equal to zero. The proof proceeds along the same lines as the proof of Proposition 6.55, where we take $h = \mathrm{rem}_{\mathcal{O},G}(f)$ and arrive at a contradiction. Hence, when $f \in \mathfrak{a}$ the remainder of f w.r.t. G is zero. □

The above proposition enables us to solve the ideal membership problem provided the acyclic border basis of the ideal is known. However, it must be noted that the remainder on division by an acyclic $\mathcal{O}$-border basis for any $f \in A[x_1, \ldots, x_n]$ is not unique.

Below we define the normal form of a polynomial w.r.t. an acyclic border basis.

Definition 6.59 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated as an A-module. Let $G \subseteq \mathfrak{a}$ be an acyclic $\mathcal{O}$-border basis for $\mathfrak{a}$. Let $\mathrm{Mon}(\mathcal{O}) = \{x^{\alpha_1}, \ldots, x^{\alpha_t}\}$ be the monomial part of $\mathcal{O}$, $C_{\mathfrak{I}_{x^{\alpha_i}}}$ be the set of coset representatives of the equivalence classes $A/\mathfrak{I}_{x^{\alpha_i}}$ and f be any polynomial in $A[x_1, \ldots, x_n]$. Let r be a polynomial given by $r = a_1 x^{\alpha_1} + \cdots + a_t x^{\alpha_t}$, where $a_i \in C_{\mathfrak{I}_{x^{\alpha_i}}}$, $1 \leq i \leq t$. Then r is said to be the normal form of f if $f = r \mod \mathfrak{a}$.*

The normal form of a polynomial is denoted by $\mathrm{NF}_{\mathcal{O},G}(f)$. We now prove that every polynomial f in $A[x_1, \ldots, x_n]$ has a unique normal form.

Proposition 6.60 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal such that $A[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated as an A-module. Let $G \subseteq \mathfrak{a}$ be an acyclic $\mathcal{O}$-border basis for $\mathfrak{a}$. For any polynomial f in $A[x_1, \ldots, x_n]$, the normal form of f is unique.*

Proof: Let $\text{Mon}(\mathcal{O}) = \{x^{\alpha_1}, \ldots, x^{\alpha_t}\}$ be the monomial part of $\mathcal{O}$. Let $s' \leq t$ be the number of monomials in the scalar border, $\partial\mathcal{O}_s$ and $G = \{g_1, \ldots, g_s\}$ be an acyclic $\mathcal{O}$-border basis of $\mathfrak{a}$. The existence of a normal form, $\text{NF}_{\mathcal{O},G}(f)$ for any polynomial $f \in A[x_1, \ldots, x_n]$ is a consequence of the following equality,

$$A[x_1, \ldots, x_n]/\mathfrak{a} = \{\sum_{i=1}^{k} a_i x^{\alpha_i} + \mathfrak{a} \mid a_i \in C_{\mathcal{I}_{x^{\alpha_i}}}\}.$$

Now, we prove the uniqueness of the normal form of f. Let r_1 and r_2 be two different normal forms for f. Then $f = r_1 \bmod \mathfrak{a}$ and $f = r_2 \bmod \mathfrak{a}$. This implies, $r_1 = r_2 \bmod \mathfrak{a}$. Therefore, $r_1 - r_2 \in \mathfrak{a}$. Let $r_1 = \sum_{i=1}^{t} b_i x^{\alpha_i}$ and $r_2 = \sum_{i=1}^{t} b'_i x^{\alpha_i}$, where b_i and b'_i are coset representatives in $C_{\mathcal{I}_{x^{\alpha_i}}}$. Then, $r_1 - r_2 = \sum_{i=1}^{t}(b_i - b'_i)x^{\alpha_i}$. If $r_1 \neq r_2$, then there is atleast one i such that $b_i \neq b'_i$. This implies that $b_i - b'_i \neq 0$. Since b_i and b'_i are coset representatives of distinct cosets, $b_i - b'_i \notin \mathcal{I}_{x^{\alpha_i}}$. Therefore, $(r_1 - r_2) \notin \mathfrak{a}$. Hence a contradiction. Thus $r_1 = r_2$ and the normal form of a polynomial is unique. □

We show below that if we can associate a monomial order to an order ideal $\mathcal{O}$, then the reduced Gröbner basis of $\mathfrak{a}$ w.r.t. to that monomial order is a subset of the acyclic border basis associated with $\mathcal{O}$.

Proposition 6.61 *Let $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$ be an ideal. Let $\prec$ be a monomial order. Let $\mathcal{O}_\prec$ be an order ideal corresponding to $\prec$ such that* Mon($\mathcal{O}$) *forms a weak$^+$ basis for $A[x_1, \ldots, x_n]/\mathfrak{a}$. Then the Pauer (2007) reduced Gröbner basis of $\mathfrak{a}$ w.r.t. $\prec$ is a subset of the acyclic $\mathcal{O}$-border basis of $\mathfrak{a}$.*

Proof: Let $\text{Mon}(\mathcal{O}_\prec) = \{x^{\alpha_1}, \ldots, x^{\alpha_t}\}$ be the monomial part of $\mathcal{O}_\prec$ and $\partial\mathcal{O}_\prec = \{c_1 x^{\beta_1}, \ldots, c_s x^{\beta_s}\}$ be the border of $\mathcal{O}_\prec$. Let $G = \{g_1, \ldots, g_s\}$ be the acyclic $\mathcal{O}_\prec$-border basis for $\mathfrak{a}$. The acyclic $\mathcal{O}_\prec$-border basis is constructed as in the proof of Theorem 6.57. Since G is an acyclic $\mathcal{O}_\prec$-border basis we have from Proposition 6.58 that for any $f \in \mathfrak{a}$, f reduces to zero. This implies that G is a Gröbner basis of $\mathfrak{a}$. Further, $\langle \text{Lt}(\mathfrak{a}) \rangle$ is generated by $\partial\mathcal{O}_\prec$. Recall that, $\langle \text{Lc}(\alpha, \mathfrak{a}) \rangle = \langle \text{Lc}(f) : f \in \mathfrak{a},\ \text{Lm}(f) = x^\alpha \rangle$ and $\langle \text{Lc}(< \alpha, \mathfrak{a}) \rangle = \langle \text{Lc}(f) : f \in \mathfrak{a},\ \alpha \in \deg(f) + \mathbb{N}^n,\ \text{Lm}(f) \neq x^\alpha \rangle$. Clearly, for each monomial x^α, in the monomial part, $\text{Mon}(\mathcal{O}_\prec)$, $\langle \text{Lc}(\alpha, \mathfrak{a}) \rangle = \mathcal{I}_{x^\alpha}$. From the definition of order ideal $\langle \text{Lc}(\alpha, \mathfrak{a}) \rangle \neq \langle 1 \rangle$. For each monomial x^α in the monomial border, $\partial\mathcal{O}_{\prec_m}$,

$\langle \mathrm{Lc}(\alpha, \mathfrak{a})\rangle = \langle 1\rangle$. Also, for each monomial $x^\alpha \in \mathrm{Lm}(G)$, we have

$$\mathrm{Gen}(\alpha, \mathfrak{a}) = \{\eta(a, \langle \mathrm{lc}(< \alpha, \mathfrak{a})\rangle) : a \in \mathrm{Gen}(\langle \mathrm{lc}(\alpha, \mathfrak{a})\rangle)\} \setminus \{0\},$$

where $\eta(a, \langle \mathrm{lc}(< \alpha, \mathfrak{a})\rangle)$ maps to an element in the coset $a + \langle \mathrm{lc}(< \alpha, \mathfrak{a})\rangle$. Consider the set, $\partial\mathcal{O}_{\prec_{\mathrm{red}}} = \{cx^\alpha \in \partial\mathcal{O}_\prec : c \notin \langle \mathrm{Lc}(< \alpha, \mathfrak{a})\rangle\}$. This set contains all the terms of the form cx^α in the border $\partial\mathcal{O}_\prec$ such that c cannot be expressed as a combination of leading coefficients of those monomials that properly divide x^α. Clearly, $\partial\mathcal{O}_{\prec_{\mathrm{red}}} \subseteq \partial\mathcal{O}_\prec$. Let $G_{\mathrm{red}} \subseteq G$ consist of polynomials in G with the border term in $\partial\mathcal{O}_{\prec_{\mathrm{red}}}$. It can easily be seen that $\langle \mathrm{Lt}(\mathfrak{a})\rangle = \langle \partial\mathcal{O}_{\prec_{\mathrm{red}}}\rangle$. Therefore, G_{red} is a Gröbner basis for $\mathfrak{a}$. Also, it is clear from the construction of $\partial\mathcal{O}_{\prec_{\mathrm{red}}}$ that $\mathrm{Gen}(\alpha, \mathfrak{a}) = \{c \ : \ cx^\alpha \in \partial\mathcal{O}_{\prec_{\mathrm{red}}}\}$. We now prove that G satisfies the two properties of Pauer's reduced Gröbner basis. The bijectivity of the map,

$$\begin{aligned} \phi : \{g \in G_{\mathrm{red}} : \deg(g) = \alpha\} &\longrightarrow \mathrm{Gen}(\alpha, \mathfrak{a}) \\ \phi(g) &\longmapsto \mathrm{Lc}(g) \end{aligned}$$

follows from the observation that corresponding to each border term $cx^\beta \in \partial\mathcal{O}_\prec$, there is exactly one polynomial $g \in G$ such that the border term in g is cx^β. If we had not considered the reduced border $\partial\mathcal{O}_{\prec_{\mathrm{red}}}$, then for all $g \in G \setminus G_{\mathrm{red}}$, $\phi(g)$ will map to zero. Also, each polynomial $g_i \in G_{\mathrm{red}}$ is of the form,

$$c_i x^{\beta_i} - \sum_{j=1}^{t} a_j^{(i)} x^{\alpha_j} \text{ where } c_i x^{\beta_i} \in \partial\mathcal{O}_\prec \text{ and } a_j^{(i)} x^{\alpha_j} \in \mathcal{O}_\prec.$$

Since for each $a_j^{(i)} x^{\alpha_j}$, $a_j^{(i)} \in A/\mathcal{I}_{x^{\alpha_j}}$ we have that $\eta(a_j^{(i)}, \langle \mathrm{lc}(\alpha_j, \mathfrak{a})\rangle) = a_j^{(i)}$. Hence, G_{red} satisfies the second condition of Pauer's reduced Gröbner basis. Therefore, G_{red} is a reduced Gröbner basis for $\mathfrak{a}$. □

From the above result we can see that for every ideal $\mathfrak{a}$, the set of all acyclic border bases contains all the reduced Gröbner bases w.r.t. any monomial order.

Theorem 6.62 *Let $\mathfrak{a}$ be a nonzero ideal in $A[x_1, \ldots, x_n]$, $\mathcal{O}$ be an order ideal and $\partial\mathcal{O} = \{c_1 x^{\beta_1}, \ldots, c_s x^{\beta_s}\}$ be its border. Let $\mathrm{Mon}(\mathcal{O}) = \{x^{\alpha_1}, \ldots, x^{\alpha_t}\}$ be the monomial part of $\mathcal{O}$ and $G = \{g_1, \ldots, g_s\}$ be an acyclic $\mathcal{O}$-border prebasis. Then the following statements are equivalent.*

(i) G is an acyclic $\mathcal{O}$-border basis for $\mathfrak{a}$.

(ii) $f \in \mathfrak{a}$ if and only if $f \xrightarrow{G}_+ 0$.

(iii) $f \in \mathfrak{a}$ *if and only if there exists* $f_1, \ldots, f_s \in A[x_1, , \ldots, x_n]$ *such that* $f = \sum_{i=1}^{s} f_i g_i$ *and* $\max\{\deg(f_i) \mid f_i g_i \neq 0, i = 1, \ldots, s\} = \mathrm{ind}_{\mathcal{O}}(f) - 1$.

(iv) The border form of $\mathfrak{a}$, $\mathrm{BF}_{\mathcal{O}}(\mathfrak{a}) = \langle c_1 x^{\beta_1}, \ldots, c_s x^{\beta_s} \rangle$.

Proof: (i) $\Rightarrow$ (ii). The claim follows from the proof of Proposition 6.58.
(ii) $\Rightarrow$ (iii). Let $f \in \mathfrak{a}$. By the border division algorithm, there exists $f_1, \ldots, f_s \in A[x_1, , \ldots, x_n]$, $\deg(f_i) \leq \mathrm{ind}_{\mathcal{O}}(f) - 1$, $1 \leq i \leq s$ such that $f = \sum_{i=1}^{s} f_i g_i$. Assume that $\max\{\deg(f_i)\} \lneq \mathrm{ind}_{\mathcal{O}}(f) - 1$. It can easily be verified that $\mathrm{ind}_{\mathcal{O}}(f_i g_i) \leq \mathrm{ind}_{\mathcal{O}}(g_i) + \deg(f_i)$. The definition of $\mathcal{O}$-border prebasis implies that $\mathrm{ind}_{\mathcal{O}}(g_i) = 1$. Thus $\mathrm{ind}_{\mathcal{O}}(f_i g_i) \leq \deg(f_i) + 1 \lneq \mathrm{ind}_{\mathcal{O}}(f) - 1 + 1$. Thus $\mathrm{ind}_{\mathcal{O}}(f_i g_i) \lneq \mathrm{ind}_{\mathcal{O}}(f)$. Also it can be seen that, $\mathrm{ind}_{\mathcal{O}}(f + g) \leq \max\{\mathrm{ind}_{\mathcal{O}}(f), \mathrm{ind}_{\mathcal{O}}(g)\}$, when either $\mathrm{ind}_{\mathcal{O}}(f) \geq 1$ or $\mathrm{ind}_{\mathcal{O}}(g) \geq 1$. Thus, $\mathrm{ind}_{\mathcal{O}}(\sum_{i=1}^{s} f_i g_i) \lneq \mathrm{ind}_{\mathcal{O}}(f)$. This is a contradiction. Hence $\max\{\deg(f_i)\} = \mathrm{ind}_{\mathcal{O}}(f) - 1$.
(iii) $\Rightarrow$ (iv) Since each $g_i \in \mathfrak{a}$ and $\mathrm{BF}_{\mathcal{O}}(g_i) = c_i x^{\beta_i}$, we have $\langle c_1 x^{\beta_1}, \ldots, c_s x^{\beta_s} \rangle \subseteq \mathrm{BF}_{\mathcal{O}}(\mathfrak{a})$. Consider a polynomial $f \in \mathfrak{a}$. Suppose $\mathrm{ind}_{\mathcal{O}}(f) \geq 1$, then by Definitions 6.40 and 6.43 each term in $\mathrm{BF}_{\mathcal{O}}(f)$ is divisible by $cx^{\beta} \in \partial\mathcal{O}$. Hence, it follows that $\mathrm{BF}_{\mathcal{O}}(f) \in \langle c_1 x^{\beta_1}, \ldots, c_s x^{\beta_s} \rangle$.
Let $\mathcal{I}$ be the proper coefficient ideal mapping associated with the order ideal $\mathcal{O}$. Now let us assume that the there exists a polynomial $f \in \mathfrak{a} \setminus \{0\}$ such that $\mathrm{ind}_{\mathcal{O}}(f) = 0$ i.e., $f = \sum_{i=1}^{t} c_i x^{\alpha_i}$ where $c_i \notin \mathcal{I}_{x^{\alpha_i}}$. Then by hypothesis, there exist f_i, $1 \leq i \leq s$, such that $f = \sum_{i=1}^{s} f_i g_i$ and $\max\{\deg(f_i) \mid f_i g_i \neq 0, i = 1, \ldots, s\} = 0 - 1 = -1$. This is not possible since $\deg(f) \geq 0$ for all $f \in \mathbb{A}[x_1, \ldots, x_n]$. This implies that $f = 0$ which is a contradiction. Therefore, $\mathrm{ind}_{\mathcal{O}}(f) \geq 1$. Thus, $\mathrm{BF}_{\mathcal{O}}(\mathfrak{a}) \subseteq \langle c_1 x^{\beta_1}, \ldots, c_s x^{\beta_s} \rangle$. The claim follows.
(iv) $\Rightarrow$ (i). Consider a polynomial $f \in A[x_1, \ldots, x_n]$. By the border division algorithm, we have $f_1, \ldots, f_s \in A[x_1, \ldots, x_n]$ and $a_1, \ldots, a_t \in A$ such that

$$f = f_1 g_1 + \cdots + f_s g_s + a_1 x^{\alpha_1} + \cdots + a_t x^{\alpha_t}.$$

Since $\sum_{i=1}^{s} f_i g_i \in \mathfrak{a}$, $f = h \bmod \mathfrak{a}$, where $h = \sum_{j=1}^{t} a_j x^{\alpha_j}$. We are given that the $\mathcal{O}$-border prebasis, G is acyclic. Without loss of generality, let us assume that G is well ordered. Find the smallest i for which the border term in g_i belongs to $\partial\mathcal{O}_s$ and assume that the monomial in the border term is x^{α_1}. Let $G_1 \subseteq G$ represent all the polynomials for which the border monomial is x^{α_1} and let $|G_1| = s_1$.

Let the ideal $\mathcal{I}_{x^{\alpha_1}}$ be generated by $\{c_1, \ldots, c_{s_1}\}$ and let $b_1 \in C_{\mathcal{I}_{x^{\alpha_1}}}$ be the coset representative of $a_1 + \mathcal{I}_{x^{\alpha_1}}$. Then there exist $d_1, \ldots, d_{s_1} \in A$ such that

$$(a_1 - b_1) = d_1 c_1 + \cdots + d_{s_1} c_{s_1}.$$

Let $h_1 = h - d_1 g_1 + \cdots + d_{s_1} g_{s_1}$. Therefore we have,

$$h_1 = b_1 x^{\alpha_1} + b_2' x^{\alpha_2} + \cdots + b_t' x^{\alpha_t},$$

where $b_i' \in A$, $i = 2, \ldots, t$. Further, $h_1 = h \bmod \mathfrak{a}$. Repeating the above process for the remaining monomials in $\partial\mathcal{O}_s$ in the same sequence as the well ordered basis, we get

$$h_{s'} = b_1 x^{\alpha_1} + \ldots + b_{s'} x^{\alpha_{s'}} + b_{s'+1} x^{\alpha_{s+1}} + \cdots + b_t x^{\alpha_t},$$

where each b_i is a coset representative in $C_{\mathcal{I}_{x^{\alpha_i}}}$. Note that for x^{α_i}, $s'+1 \leq i \leq t$, $\mathcal{I}_{x^{\alpha_i}} = \{0\}$ and $b_i \in A$. The acyclicity of the basis ensures that at each stage, i, all b_j, $j \lneq i$ will not be modified. Further, at every stage i, the intermediate polynomial, $h_i = h_{i-1} \bmod \mathfrak{a}$. Therefore, $h_{s'} = h \bmod \mathfrak{a}$ which implies that $f = h_{s'} \bmod \mathfrak{a}$. Further, each b_i is a coset representative in $C_{\mathcal{I}_{x^{\alpha_i}}}$ where $x^{\alpha_i} \in \mathrm{Mon}(\mathcal{O})$. Hence, $A[x_1, \ldots, x_n]/\mathfrak{a} = \{\sum_{i=1}^{t} a_i x^{\alpha_i} + \mathfrak{a} \mid a_i \in C_{\mathcal{I}_{x^{\alpha_i}}}\}$.
To prove the second condition of the weak$^+$ basis definition (Definition 6.18), consider a polynomial $f = \sum_{i=1}^{t} a_i x^{\alpha_i} \in \mathfrak{a}$. Then, there exists an $i \in \{1, \ldots, t\}$ such that $a_i x^{\alpha_i} \in \mathrm{BF}_{\mathcal{O}}(f)$. By hypothesis we have, $\mathrm{BF}_{\mathcal{O}}(\mathfrak{a}) = \langle c_1 x^{\beta_1}, \ldots, c_s x^{\beta_s} \rangle$. Since $\mathrm{BF}_{\mathcal{O}}(\mathfrak{a})$ is an ideal generated by terms, we have $a_i x^{\alpha_i} \in \mathrm{BF}_{\mathcal{O}}(\mathfrak{a})$. Thus, there exists terms $d_i x^{\gamma_i}$, $1 \leq i \leq s$ such that

$$a_i x^{\alpha_i} = \sum_{i=1}^{s} (d_i x^{\gamma_i})(c_i x^{\beta_i}).$$

Since for all $x^{\beta} | x^{\alpha_i}$ $\mathcal{I}_{x^{\beta}} \subseteq \mathcal{I}_{x^{\alpha_i}}$, we have $a_i \in \mathcal{I}_{x^{\alpha_i}}$.
Consider a proper coefficient ideal mapping, $\mathcal{I}'$ such that for any $x^{\alpha} \in \mathrm{Mon}(A[x_1, \ldots, x_n])$, either $\mathcal{I}'_{x^{\alpha}} \subsetneq \mathcal{I}_{x^{\alpha}}$ or $\mathcal{I}'_{x^{\alpha}} = \mathcal{I}_{x^{\alpha}}$. Let $\mathcal{O}'$ be the order ideal associated with $\mathcal{I}'$ and $\partial\mathcal{O}' = \{c_1' x^{\beta_1}, \ldots, c_l' x^{\beta_l}\}$ be the corresponding border. Assume that $\mathrm{Mon}(\mathcal{O}')$ satisfies (i) and (ii). Consider the ideal, $\mathfrak{A} = \langle c_1' x^{\beta_1}, \ldots, c_l' x^{\beta_l} \rangle$. We have, $\mathfrak{A} \subsetneq \mathrm{BF}_{\mathcal{O}}(\mathfrak{a})$ since $\mathcal{I}'_{x^{\alpha}} \subsetneq \mathcal{I}_{x^{\alpha}}$ for some x^{α}. Consider $c_\omega x^{\omega} \in \mathrm{BF}_{\mathcal{O}}(\mathfrak{a}) \setminus \mathfrak{A}$. Let h denote the $\mathrm{rem}_{\mathcal{O},G}(c_\omega x^{\omega})$. Then each non zero term in h is of the form $d_\gamma x^{\gamma}$ such that $d_\gamma \in A/\mathcal{I}_{x^{\gamma}}$ and $x^{\gamma} \in \mathrm{Mon}(\mathcal{O})$. Since $d_\gamma \notin \mathcal{I}_{x^{\gamma}}$, it is not an element of $\mathcal{I}'_{x^{\gamma}}$. Also, $c_\omega \notin \mathcal{I}'_{x^{\omega}}$. Therefore, $\mathrm{Mon}(\mathcal{O}')$ fails to satisfy Condition (ii) of the definition of weak basis for $c_\omega x^{\omega} - h$ and therefore we have a contradiction. Thus $G = \{g_1, \ldots, g_s\}$ is an $\mathcal{O}$-border basis for $\mathfrak{a}$. □

6.6 Example

In this section, we illustrate the concepts given in this chapter with an example.

Example 6.63 *Let us consider the polynomial ring, $\mathbb{Z}[x, y]$. Let $\mathcal{I}$ be a coefficient ideal mapping*

such that $\mathcal{I}_1 = \{0\}$, $\mathcal{I}_x = \{0\}$, $\mathcal{I}_y = \{0\}$, $\mathcal{I}_{xy} = \{0\}$, $\mathcal{I}_{y^2} = \{0\}$, $\mathcal{I}_{x^2} = \langle 2\rangle$, $\mathcal{I}_{x^2y} = \langle 2\rangle$ *and the rest of the monomials map to* $\langle 1\rangle$. *Therefore,* $C_{\mathcal{I}_1} = C_{\mathcal{I}_x} = C_{\mathcal{I}_y} = C_{\mathcal{I}_{xy}} = C_{\mathcal{I}_{y^2}} = \mathbb{Z}$ *and* $C_{\mathcal{I}_{x^2}} = C_{\mathcal{I}_{x^2y}} = \{0, 1\}$. *The set,*

$$\mathcal{O} = \{a_1, a_2x, a_3y, a_4xy, a_5y^2, a_6x^2, a_7x^2y \mid a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z},\ a_6, a_7 \in \{0, 1\}\}$$

is an order ideal corresponding to $\mathcal{I}$. *The monomial part of* $\mathcal{O}$ *is the set* $\mathrm{Mon}(\mathcal{O}) = \{1, x, y, x^2, y^2, xy, x^2y\}$. *The scalar border of the order ideal is* $\partial\mathcal{O}_s = \{2x^2, 2x^2y\}$ *and the monomial border is* $\partial\mathcal{O}_m = \{x^3, y^3, xy^2, x^2y^2, x^3y\}$. *Thus the border of* $\mathcal{O}$ *is the union of the scalar border and the monomial border, i.e.,*

$$\partial\mathcal{O} = \partial\mathcal{O}_m \cup \partial\mathcal{O}_s = \{x^3, y^3, xy^2, x^2y^2, x^3y, 2x^2, 2x^2y\}.$$

Consider the set $G = \{g_1, g_2, g_3, g_4, g_5, g_6, g_7\}$, *where* $g_1 = x^3 - x$, $g_2 = y^3 - y$, $g_3 = xy^2 - xy$, $g_4 = x^2y^2 - x^2y$, $g_5 = x^3y - xy$, $g_6 = 2x^2y - y^2 - y$ *and* $g_7 = 2x^2 + 2xy - y^2 - 2x - y$. *The set* G *is an* $\mathcal{O}$*-border prebasis for the ideal* $\mathfrak{a} = \langle g_1, g_2, g_3, g_4, g_5, g_6, g_7\rangle$. *It is also clear that the* $\mathcal{O}$*-border prebasis satisfies the properties of acyclicity. Hence* G *is an acyclic* $\mathcal{O}$*-border prebasis.*
The set G *is a Gröbner basis for* $\mathfrak{a}$ *with deglex order with* $x > y$. *The proof of Theorem 6.57 implies that the set* G *is an acyclic* $\mathcal{O}$*-border basis for* $\mathfrak{a}$. *Hence the border form ideal of* $\mathfrak{a}$ *is generated by the border terms i.e.,*

$$\mathrm{BF}_{\mathcal{O}}(\mathfrak{a}) = \langle x^3, y^3, xy^2, x^2y^2, x^3y, 2x^2, 2x^2y\rangle.$$

Now we demonstrate the border division algorithm (Algorithm 6.52) for a polynomial, $f = x^4 + 2x^3y^2 + x^2 + 4xy + 15$ *w.r.t.* G. *We have* $\mathrm{Mon}(\mathcal{O}) = \{x^{\alpha_1}, \ldots, x^{\alpha_7}\}$, *where* $x^{\alpha_1} = 1$, $x^{\alpha_2} = x$, $x^{\alpha_3} = y$, $x^{\alpha_4} = x^2$, $x^{\alpha_5} = y^2$, $x^{\alpha_6} = xy$ *and* $x^{\alpha_7} = x^2y$. *The monomial border is* $\partial\mathcal{O}_m = \{b_1, \ldots, b_5\}$ *and the scalar border is* $\partial\mathcal{O}_s = \{b_6, b_7\}$, *where* $b_1 = x^3$, $b_2 = y^3$, $b_3 = xy^2$, $b_4 = x^2y^2$, $b_5 = x^3y$, $b_6 = 2x^2y$ *and* $b_7 = 2xy$.

1. *Initialize* $f_1 = f_2 = f_3 = f_4 = f_5 = f_6 = f_7 = 0$, $l_1 = l_2 = l_3 = l_4 = l_5 = l_6 = l_7 = 0$ *and* $h = x^4 + 2x^3y^2 + x^2 + 4xy + 15$.

2. *Since* $\mathrm{ind}_{\mathcal{O}}(h) = 2$, *Step 5 of the algorithm is executed. We have,* $x^4 = xb_1$ *and* $\deg(x) = \mathrm{ind}_{\mathcal{O}}(h) - 1$. *Hence, we have* $f_1 = f_1 + x$ *and* $h = x^4 + 2x^3y^2 + x^2 + 4xy + 15 - x(x^3 - x)$. *Thus,* $h = 2x^3y^2 + 2x^2 + 4xy + 15$. *Return to Step 2.*

3. *Again,* $\mathrm{ind}_{\mathcal{O}}(h) = 2$ *and we return to Step 5 of the algorithm. We have* $x^3y^2 = xb_4$ *and* $\deg(x) = \mathrm{ind}_{\mathcal{O}}(h) - 1$. *After the reduction step we have* $f_4 = f_4 + 2x$ *and* $h = 2x^3y^2 + 2x^2 + 4xy + 15 - 2x(x^2y^2 - x^2y) = 2x^3y + 2x^2 + 4xy + 15$. *We return to Step 2.*

4. *In this step,* $\mathrm{ind}_{\mathcal{O}}(h) = 1$ *and the polynomial* h *has the monomial* x^3y *in its support. Since* $x^3y \in \partial\mathcal{O}_m$*, we go to Step 5. We have* $x^3y = 1 \cdot b_5$ *and* $\deg(1) = \mathrm{ind}_{\mathcal{O}}(h) - 1$*. We perform the operation* $f_5 = f_5 + 2$ *and* $h = 2x^3y + 2x^2 + 4xy + 15 - 2(x^3y - xy)$*. Hence,* $h = 2x^2 + 6xy + 15$*. We return to Step 2.*

5. *We have* $\mathrm{ind}_{\mathcal{O}}(h) = 1$ *and none of the terms in* h *are in the monomial border,* $\partial\mathcal{O}_m$*. Hence, we perform Step 4 of the algorithm. We have* $2x^2 = 1 \cdot b_1$*. Thus, we have* $f_7 = f_7 + 1$ *and* $h = 2x^2 + 6xy + 15 - 1(2x^2 + 2xy - y^2 - 2x - y)$*. Hence,* $h = 4xy + y^2 + 2x + y + 15$*.*

6. *We have* $\mathrm{ind}_{\mathcal{O}}(h) = 0$ *and Step 3 of the algorithm is executed. We have* $l_1 = l_1 + 15$*,* $l_2 = l_2 + 2$*,* $l_3 = l_3 + 1$*,* $l_4 = l_4 + 0$*,* $l_5 = l_5 + 1$*,* $l_6 = l_6 + 4$ *and* $l_7 = l_7 + 0$*. The algorithm terminates and returns* $(f_1, \ldots, f_7, l_1, \ldots, l_7)$*.*

Thus we have the following representation for f*,*

$$f = xg_1 + 0g_2 + 0g_3 + 1g_4 + 2g_5 + 0g_6 + 1g_7 + 15 + 2x + y + 0x^2 + 1y^2 + 4xy + 0x^2y.$$

The $\mathcal{O}$*-remainder of* f *is* $\mathrm{rem}_{\mathcal{O},G}(f) = 15 + 2x + y + y^2 + 4xy$*. Since the remainder is not equal to zero, by Proposition 6.58,* $f \notin \mathfrak{a}$*. For this example, the normal form of* f *is equal to the* $\mathcal{O}$*-remainder,*

$$\mathrm{NF}_{\mathcal{O},G}(f) = \mathrm{rem}_{\mathcal{O},G}(f) = 15 + 2x + y + y^2 + 4xy.$$

Chapter 7

Conclusion

7.1 Summary

The aim of this thesis has been to build an algorithmic framework for algebraic problems in polynomial ideal theory over Noetherian commutative rings. Polynomials with coefficients from Noetherian commutative rings, $A[x_1, \ldots, x_n]$, appear in several real world applications. The two important cases include polynomial rings over integers, $\mathbb{Z}[x_1, \ldots, x_n]$ and polynomial rings over polynomial rings, $(\Bbbk[y_1, \ldots, y_m])[x_1, \ldots, x_n]$. For example, integer polynomial equations appear in lattice based cryptography and polynomial parametric equations have applications in control theory. Therefore, algorithms for determining the properties of these structures will go a long way in making these applications efficient and more practical. Another reason for studying computational techniques in $A[x_1, \ldots, x_n]$ is that they allow for an algorithmic interpretation of algebraic properties, an insight that did not exist previously. An apt example is the Gröbner basis methods given in Chapter 5 to compute Krull dimension of certain A-algebras, $A[x_1, \ldots, x_n]/\mathfrak{a}$ using the concepts of combinatorial dimension and degree of the Hilbert polynomial. These methods give algorithmic steps to compute the Krull dimension of A-algebras, independent of the ideal. Though polynomial rings over rings are the underlying algebraic structures in several applications, the algorithmic theory for computational problems in $A[x_1, \ldots, x_n]$, unfortunately, has not been developed beyond extending basic definitions and techniques from fields to rings. In this thesis, we tried to fill this gap.

Buchberger (1965) introduced Gröbner bases for an ideal $\mathfrak{a} \subseteq \Bbbk[x_1, \ldots, x_n]$ to compute the $\Bbbk$-vector space basis of the corresponding residue class polynomial ring, $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ and this gave an algorithmic characterization of zero dimensional ideals. The first question we addressed in this thesis is whether one can give a Gröbner basis method to compute an A-module basis of $A[x_1, \ldots, x_n]/\mathfrak{a}$. We first characterized ideals that gave rise to free residue class polynomial rings

w.r.t. a monomial order, or equivalently a Gröbner basis (Section 3.1). For this characterization we introduced a special type of Gröbner bases called short reduced Gröbner bases. We gave a Gröbner basis algorithm to compute an A-module basis for residue class polynomial rings with a free A-module representation w.r.t. a monomial order. Thereby, we extended the Macaulay-Buchberger basis theorem to polynomial rings over rings. The characterization has several consequences which have been presented here :

1. It allowed us to extend border bases to $A[x_1, \ldots, x_n]$ (Section 3.5 and Chapter 6).
2. It can be used to locate ideal lattices in the multivariate case (Chapter 4). Using these multivariate ideal lattices collision resistant hash functions can be built.
3. It can be used to derive algorithmic relations between the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$, its combinatorial dimension and the Hilbert polynomial of $\mathfrak{a}$ for residue class polynomial rings with a free A-module representation w.r.t. either lexicographic or degree compatible monomial orderings (Chapter 5).

7.2 Possible Future Directions

7.2.1 Free A-module representation of $A[x_1, \ldots, x_n]/\mathfrak{a}$

All the results presented in this thesis rely on the characterization of ideals that give rise to residue class polynomial rings with a free A-module representation w.r.t. a monomial order. This raises the following crucial question.

Question 7.1 *Is there an algorithmic method to determine whether there exists a monomial order with respect to which $A[x_1, \ldots, x_n]/\mathfrak{a}$ has a free A-module representation?*

One way to do that is to determine the short reduced Gröbner basis of $\mathfrak{a}$ for each admissible ordering that give rise to different leading terms. If the short reduced Gröbner basis of the ideal is monic then we have the required monomial order. Given a polynomial in $\mathbb{k}[x_1, \ldots, x_n]$, there are standard techniques to determine all the admissible orderings for different combinations of monomials (Schwarz, 1991). These techniques will work for $A[x_1, \ldots, x_n]$ as well. It would be more efficient to develop a technique that does not require us to compute all possible monomial orderings.

7.2.2 Multivariate ideal lattices in cryptography

In univariate ideal lattices, the underlying ring is the residue class polynomial ring, $\mathbb{Z}[x]/\langle\phi_m(x)\rangle$, where $\phi_m(x)$ is the mth cyclotomic polynomial. From an algebraic point of view, these rings

are considered as the rings of algebraic integers in cyclotomic number fields. To prove collision resistance in hash functions built from univariate ideal lattices, Lyubashevsky and Micciancio (2006) use the hardness of determining if two number fields are isomorphic. In fact, the security guarantees of univariate ideal lattices are often based on results from algebraic number theory. Analogously, properties of multivariate ideal lattices can be mapped to algebraic function fields as shown in Chapter 4. In this thesis, the computational hardness of the underlying worst case problem, Shortest Polynomial Problem(SPP), was shown for the specific ideal,

$$\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \ldots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1 \rangle.$$

Therefore the natural question to ask at this juncture is whether one can extend the hardness results to all ideals in $\mathbb{Z}[x_1, \ldots, x_n]$ that give rise to free and finitely generated residue class polynomial rings and thus build collision resistant hash functions using them. The results in (Hess, 2004) relating to functional field isomorphism will be key in extending the results to all classes of ideals.

For multivariate ideal lattices to not remain a theoretical notion, it is vital that we explore building other cryptographic primitives such as digital signatures and identification schemes using them. The following two questions are key in building any cryptographic primitive based on multivariate ideal lattices.

Question 7.2 *1. Can we have a practical construction using multivariate ideal lattices?*

2. Which computationally hard property of algebraic function fields will give the security guarantee?

The hardness results in algebraic function fields will provide the foundation for building cryptographic primitives using multivariate ideal lattices.

7.2.3 Dimension of A-algebras

In Chapter 5, we derived a relation between Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ and its combinatorial dimension if the residue class polynomial ring has a free A-module representation w.r.t. either lexicographic or degree compatible monomial orderings (Corollary 5.18, Corollary 5.42).

Question 7.3 *Can we have the similar relation for monomial orders that are not lexicographic and degree compatible?*

In fields, it is true if we consider a reduced Gröbner basis, a consequence of (Carrà Ferro, 1987, Theorem 3.1). An affirmative answer seems likely in rings as well but we have yet to have a

formal proof. If the answer to the above question is yes, it gives us a completely algorithmic technique to compute the Krull dimension of A-algebras with a free A-module representation w.r.t. any monomial order.

7.2.4 Software implementation of algorithms in $A[x_1, \ldots, x_n]$

Most software implementations of Gröbner basis for ideals in $A[x_1, \ldots, x_n]$, including `SageMath`, `Macaulay2` and `Magma`, rely on a definition of polynomial reduction called strong reduction (Adams and Loustaunau, 1994, Definition 4.5.6), which is not flexible enough to determine the A-module representation of the residue class polynomial ring given in (3.1).

Definition 7.4 (Strong Reduction) *Let f, h and $\{f_1, \ldots, f_s\}$ be a set of nonzero polynomials in $A[x_1, \ldots, x_n]$. We say that f reduces to h w.r.t. $\{f_1, \ldots, f_s\}$, denoted as*

$$f \xrightarrow{\{f_1,\ldots,f_s\}} h,$$

if and only if

$$h = f - (c_i x^{\alpha_i} f_i),$$

for some $i \in \{1, \ldots, s\}$ where $c_i \in A$ and for $c_i \neq 0$, $\mathrm{lt}(f_i) \mid \mathrm{lt}(f)$.

The definition required for our Gröbner basis computations is given by (Adams and Loustaunau, 1994, Definition 4.1.1), which is also stated in this thesis as Definition 2.57. For building software packages that implement all the algorithms proposed in this thesis one needs to first implement a software package that calculates Gröbner bases based on this definition of reduction. The next step will be to build a software to determine the A-module representation of $A[x_1, \ldots, x_n]/\mathfrak{a}$ w.r.t. a Gröbner basis. To interpret if the residue class polynomial ring has a free A-module representation one needs to first construct a short reduced Gröbner basis. Since short reduced Gröbner basis requires a mapping that is dependent on the coefficient ring A, we will have to decide the Noetherian commutative rings that will be included in our packages. The most common rings that we encounter in real world applications are the ring of integers and the ring of polynomials. So it is paramount that we implement it for $A = \mathbb{Z}$ and $A = \Bbbk[y_1, \ldots, y_m]$. Once implemented, it can be used to locate multivariate ideal lattices and implement hash functions based on such ideal lattices. These packages will simplify computations for researchers working with either polynomial equations over integers or parametric equations over polynomial rings.

7.2.5 When $A[x_1, \ldots, x_n]/\mathfrak{a}$ is not free

Unlike in fields, polynomial rings over rings have to be studied in two parts : ideals that give rise to free residue class polynomial rings and ideals for which the residue class rings have

torsion. We have mostly explored Gröbner basis algorithms for the free case in this thesis. How does the theory of Gröbner bases look like when $A[x_1, \ldots, x_n]/\mathfrak{a}$ is not free? In Chapter 6, we generalized Macaulay-Buchberger basis theorem for residue class polynomial rings with torsion. As an application of this theorem, we extended border bases to ideals in $A[x_1, \ldots, x_n]$, where the corresponding residue class polynomial ring need not necessarily be free. The isomorphism given by (3.1) was key in developing the theory of border bases in this case. The coefficient ideal mapping (Definition 6.7), the underlying notion in this theory, is based on the leading coefficient ideals of (3.1). The two concepts coincide when we consider a coefficient ideal mapping fixed by a Gröbner basis. The isomorphism will definitely lead to more computational techniques for residue class polynomial rings with torsion and these algorithmic methods will help enrich the field of computational algebra.

Bibliography

Ackermann, P. and M. Kreuzer (2006). Gröbner Basis Cryptosystems. *Applicable Algebra in Engineering, Communication and Computing 17*(3), 173–194. 5

Adams, W. and P. Loustaunau (1994). *An Introduction to Gröbner Bases*. American Mathematical Society. 5, 6, 17, 18, 19, 34, 35, 36, 37, 38, 39, 61, 107, 125, 147

Ajtai, M. (1996). Generating Hard instances of Lattice Problems (Extended Abstract). In G. L. Miller (Ed.), *Proceedings of the 1996 ACM Symposium on the Theory of Computing, STOC*, pp. 99–108. ACM. 5, 44, 45

Ajtai, M., R. Kumar, and D. Sivakumar (2001). A Sieve Algorithm for the Shortest Lattice Vector Problem. In J. S. Vitter, P. G. Spirakis, and M. Yannakakis (Eds.), *STOC*, pp. 601–610. ACM. 43

Ananth, P. V. and A. Dukkipati (2012). Complexity of Gröbner Basis Detection and Border Basis Detection. *Theoretical Computer Science 459*, 1–15. 19

Arnold, E. A. (2003). Modular algorithms for Computing Gröbner bases. *Journal of Symbolic Computation 35*, 403–419. 40

Atiyah, M. and I. G. Macdonald (1969). *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics. 102

Bayer, D., A. Galligo, and M. Stillman (1991). Gröbner Bases and Extension of Scalars. In *Proceedings Comput. Algebraic Geom. and Commut. Algebra, Cortona, Italy*, pp. 198 – 215. 101

Becker, T., H. Kredel, and V. Weispfenning (1993). *Gröbner Bases: A Computational Approach to Commutative Algebra*. Springer-Verlag. 6, 21

Bigatti, A., R. La Scala, and L. Robbiano (1999). Computing Toric Ideals. *Journal of Symbolic Computation 27*(4), 351 – 365. 75

Buchberger, B. (1965). *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (in German).* Ph. D. thesis, University of Innsbruck, Austria. (reprinted in (Buchberger, 2006)). iii, 1, 2, 4, 15, 17, 144

Buchberger, B. (2006). Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation 41*, 475–511. 150

Byrne, E. and T. Mora (2009). Gröbner Bases over Commutative Rings and Applications to Coding Theory. In *Gröbner Bases, Coding, and Cryptography*, pp. 239–261. Springer. 5

Carrà Ferro, G. (1987). Some Properties of the Lattice Points and Their Application to Differential Algebra. *Communications in Algebra 15*(12), 2625–2632. 146

Cohen, H. (2013). *A Course in Computational Algebraic Number Theory*, Volume 138. Springer. 81

Faugère, J.-C. (1999). A New Efficient Algorithm for Computing Gröbner Bases (F4). *Journal of Pure and Applied Algebra 139*(1–3), 61–88. 16

Faugère, J.-C. (2002). A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, ISSAC '02. 16

Faugère, J.-C. and A. Joux (2003). Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner Bases. In *Advances in Cryptology-CRYPTO 2003*, pp. 44–60. Springer. 4

Francis, M. and A. Dukkipati (2014). On Reduced Gröbner Basis and Macaulay-Buchberger Basis Theorem over Noetherian Rings. *Journal of Symbolic Computation 65*, 1–14. 9, 10, 49

Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. In M. Mitzenmacher (Ed.), *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pp. 169–178. ACM. 41

Gianni, P., B. Trager, and G. Zacharias (1988). Gröbner Bases and Primary Decomposition of Polynomial Ideals. *Journal of Symbolic Computation 6*(23), 149 – 167. 75

Giovini, A., T. Mora, G. Niesi, L. Robbiano, and C. Traverso (1991). One Sugar Cube, Please or Selection Strategies in the Buchberger Algorithm. In *Proceedings of the 1991 international symposium on Symbolic and algebraic computation*, pp. 49–54. ACM. 16

Greuel, G.-M., F. Seelisch, and O. Wienand (2011). The Gröbner Basis of the Ideal of Vanishing Polynomials. *Journal of Symbolic Computation 46*(5), 561–570. 5

G.Zacharias (1978). Generalized Gröbner Bases in Commutative Polynomial Rings. Master's thesis, MIT,Cambridge,MA. 4

Hess, F. (2004). An Algorithm for Computing Isomorphisms of Algebraic Function Fields. In *Algorithmic Number Theory*, pp. 263–271. Springer. 146

Hiss, G., A. Hadj Kacem, and I. Yengui (2010). Dynamical Gröbner Bases over Dedekind Rings. *Journal of Algebra 324*(1), 12 – 24. 5

Hoffstein, J., J. Pipher, and J. Silverman (1998). NTRU: A Ring-Based Public Key Cryptosystem. In J. Buhler (Ed.), *Algorithmic Number Theory*, Volume 1423 of *Lecture Notes in Computer Science*, pp. 267–288. Springer. 5

Kalkbrener, M. (1998). Algorithmic Properties of Polynomial Rings. *Journal of Symbolic Computation 26*(5), 525–581. 5

Kalker-Kalkman, C. (1993). An Implementation of Buchberger's Algorithm with Applications to Robotics. *Mechanism and Machine Theory 28*(4), 523–537. 4

Kandri-Rody, Ä. and D. Kapur (1988). Computing a Gröbner Basis of a Polynomial Ideal over a Euclidean Domain. *Journal of symbolic computation 6*(1), 37–57. 5

Kapur, D. and K. Madlener (1989). A Completion Procedure for Computing a Canonical Basis for a k-subalgebra. In *Computers and mathematics*, pp. 1–11. Springer. 5

Katsabekis, A., M. Morales, and A. Thoma (2010). Binomial Generation of the Radical of a Lattice Ideal. *Journal of Algebra 324*(6), 1334 – 1346. 75

Kehrein, A. and M. Kreuzer (2005). Characterizations of Border Bases. *Journal of Pure and Applied Algebra 196*(2-3), 251–270. 19, 67, 118, 133, 134

Kehrein, A. and M. Kreuzer (2006). Computing Border Bases. *Journal of Pure and Applied Algebra 205*(2), 279–295. 19, 128

Kehrein, A., M. Kreuzer, and L. Robbiano (2005). An Algebraists View on Border Bases. In A. Dickenstein and I. Z. Emiris (Eds.), *Solving Polynomial Equations*, Volume 14 of *Algorithms and Computation in Mathematics*, pp. 169–202. Springer. 19, 20, 118

Kemper, G. (2011). *A Course in Commutative Algebra*. Springer Verlag. 22, 23, 25, 31, 107, 109

Kredel, H. and V. Weispfenning (1988). Computing Dimension and Independent Sets for Polynomial Ideals. *Journal of Symbolic Computation 6*(2 - 3), 231 – 247. 4, 25, 26, 91, 94, 97, 98

Kreuzer, M. and L. Robbiano (2005). *Computational Commutative Algebra 2*. Springer. 4, 19, 24, 25, 26, 32, 91, 92

Laubenbacher, R. (2003). A Computer Algebra Approach to Biological Systems. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pp. 5–6. ACM. 4

Lenstra, A., H. Lenstra, and L. Lovász (1982). Factoring Polynomials with Rational Coefficients. *Math. Ann. 261*, 515–534. 43

Lezama, O. (2008). Gröbner Bases for the Modules over Noetherian Polynomial Commutative Rings. *Georgian Mathematical Journal 15*(1), 121–137. 5

Lyubashevsky, V. (2008). Lattice Based Identification Schemes Secure Under Active Attacks. In *Proceedings of the 11th International Workshop on Practice and Theory in Public Key Cryptography, 2008*, pp. 162–179. 41, 69

Lyubashevsky, V. and D. Micciancio (2006). Generalized Compact Knapsacks Are Collision Resistant. In *ICALP (2)*, pp. 144–155. 5, 41, 45, 47, 69, 74, 77, 80, 81, 87, 88, 90, 146

Lyubashevsky, V. and D. Micciancio (2008). Asymptotically Efficient Lattice-Based Digital Signatures. In *Theory of Cryptography Conference, 2008*, pp. 37–54. 41, 69

Macaulay, F. S. (1927). Some Properties of Enumeration in the Theory of Modular Systems. *Proc. London Math. Soc 26*, 531–555. 3, 17

Madlener, K. and B. Reinert (1993). Computing Gröbner Bases in Monoid and Group Rings. In *Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation*, ISSAC '93, pp. 254–263. 5

Matsumura, H. (1980). *Commutative Algebra, 2nd Edition*. Benjamin-Cummings Pub Co. 102

Micciancio, D. (2002). Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions from Worst-Case Complexity Assumptions. In *Symposium on Foundations of Computer Science (FOCS 2002) Proceedings*, pp. 356–365. IEEE Computer Society. 5, 45, 47, 79, 89

Micciancio, D. and S. Goldwasser (2002). *Complexity of Lattice Problems: a cryptographic perspective*, Volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Boston, Massachusetts: Kluwer Academic Publishers. 42

Micciancio, D. and O. Regev (2004). Worst-case to average-case reductions based on gaussian measures. In *45th Symposium on Foundations of Computer Science (FOCS 2004) Proceedings*, pp. 372–381. IEEE Computer Society. 88

Möller, H. M. (1988). On the Construction of Gröbner Bases using Syzygies. *Journal of Symbolic Computation 6*(2-3), 345–359. 4, 38

Mora, F. and H. M. Möller (1983). The Computation of the Hilbert Function. In J. A. van Hulzen (Ed.), *Computer Algebra, EUROCAL '83*, Volume 162 of *Lecture Notes in Computer Science*, pp. 157–167. Springer. 4, 91

Mourrain, B. (1999). A New Criterion for Normal Form Algorithms. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pp. 430–442. Springer. 118

Mourrain, B. and P. Trébuchet (2005). Generalized Normal Forms and Polynomial System Solving. In *Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation*, pp. 253–260. ACM. 118

Mourrain, B. and P. Trébuchet (2008). Stable Normal Forms for Polynomial System Solving. *Theoretical Computer Science 409*(2), 229–240. 118

Mourrain, B. and P. Trébuchet (2012). Border Basis Representation of a General Quotient Algebra. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, pp. 265–272. ACM. 118

Nabeshima, K. (2009). Reduced Gröbner Bases in Polynomial Rings over a Polynomial Ring. *Mathematics in Computer Science 2*(4), 587–599. 57, 58, 61

Norton, G.H. Salagean, A. (2001). Strong Gröbner Bases for Polynomials over a Principal Ideal Ring. *Bulletin of the Australian Mathematical Society 64*(3), 505. 4

O'Shea, D., J. B. Little, and D. A. Cox (2007). *Ideals, Varieties, and Algorithms: an Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer. 6, 32, 111

Pan, L. (1989). On the D-bases of Polynomial Ideals over Principal Ideal Domains. *Journal of Symbolic Computation 7*(1), 55–69. 4

Pauer, F. (2007). Gröbner Bases with Coefficients in Rings. *Journal of Symbolic Computation 42*(11-12). 40, 41, 52, 64, 138

Pritchard, F. L. (1996). The Ideal Membership Problem in Non-commutative Polynomial Rings. *Journal of Symbolic Computation 22*(1), 27–48. 5

Pukhlikov, A. V. (1998). Birational Automorphisms of Higher-Dimensional Algebraic Varieties. *Doc. Math., J. DMV*, 97–107. 81

Robbiano, L. and M. Sweedler (1990). *Subalgebra Bases*, Volume 1430 of *Lecture Notes in Mathematics*. Springer. 5

Rutman, E. W. (1992). Gröbner Bases and Primary Decomposition of Modules. *Journal of Symbolic Computation 14*(5), 483 – 503. 5

Sato, Y., S. Inoue, A. Suzuki, K. Nabeshima, and K. Sakai (2011). Boolean Gröbner bases. *Journal of Symbolic Computation 46*(5), 622–632. 5

Schwarz, F. (1991). Monomial Orderings and Gröbner Bases. *SIGSAM Bull. 25*(1), 10–23. 145

Spear, D. A. (1977). A Constructive Approach to Commutative Ring Theory. pp. 369–376. 4

Stetter, H. J. (2004). *Numerical Polynomial Algebra*. SIAM. 19, 67

Stillman, M. and H. Tsai (1999). Using SAGBI Bases to Compute Invariants. *Journal of Pure and Applied Algebra 139*(1–3), 285 – 302. 5

Sturmfels, B. (2005). What is a Gröbner basis. *Notices Amer. Math. Soc. 52.10*, 1199–1200. 6

Sturmfels, B. and Z. Xu (2010). SAGBI Bases of Cox–Nagata Rings. *Journal of the European Mathematical Society 12*(2), 429–459. 5

Thieu, V. N. (2013). Reduction Modulo Ideals and Multivariate Polynomial Interpolation. Master's thesis, Université Bordeaux 1 U.F.R. Mathématiques et Informatique. 77

Tran, Q. and M. Y. Vardi (2007). Gröbner Bases Computation in Boolean Rings for Symbolic Model Checking. *MOAS 7*, 440–445. 4

Trinks, W. (1978). Über B. Buchbergers verfahren, systeme algebraischer Gleichungen zu Lösen. *Journal of Number Theory 10*(4), 475–488. 4

Weispfenning, V. (1989). Gröbner Bases for Polynomial Ideals over Commutative Regular Rings. In *Eurocal '87: European Conference on Computer Algebra Leipzig, GDR, June 2–5, 1987 Proceedings*, pp. 336–347. Springer Berlin Heidelberg. 5

Winkler, F. (2010). Gröbner Bases - Theory and Applications. 5th Science Training School in Symbolic Computation, RISC, Univ.Linz. 32, 111, 112

Yengui, I. (2006). Dynamical Gröbner Bases. *Journal of Algebra 301*(2), 447 – 458. 5