Insert here your thesis' task.

FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Master's thesis

Gröbner Bases and their Applications to Cryptanalysis

Marek Bielik

Department of Theoretical Computer Science
Supervisor: Mgr. Martin Jureček

March 4, 2020

Acknowledgements

THANKS (remove entirely in case you do not with to thank anyone)

Declaration

I hereby declare that the presented thesis is my own work and that I have cited all sources of information in accordance with the Guideline for adhering to ethical principles when elaborating an academic final thesis.

I acknowledge that my thesis is subject to the rights and obligations stipulated by the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular that the Czech Technical University in Prague has the right to conclude a license agreement on the utilization of this thesis as a school work under the provisions of Article 60 (1) of the Act.

In Prague on March 4, 2020 . . . . . .

Czech Technical University in Prague
Faculty of Information Technology

Citation of this thesis

Bielik, Marek. *Gröbner Bases and their Applications to Cryptanalysis.* Master's thesis. Czech Technical University in Prague, Faculty of Information Technology, 2020.

Abstrakt

V několika větách shrňte obsah a přínos této práce v českém jazyce.

Klíčová slova Replace with comma-separated list of keywords in Czech.

Abstract

Summarize the contents and contribution of your work in a few sentences in English language.

Keywords Replace with comma-separated list of keywords in English.

Contents

List of Figures

Introduction

Chapter 1

Gröbner Bases

The theory of Gröbner bases for ideals in polynomial rings was introduced by Bruno Buchberger [1], who named the concept in honor of his advisor Wolfgang Gröbner (1899–1980). Buchberger also developed the fundamental algorithm for the computation of a Gröbner basis known as Buchberger's algorithm. A similar concept for ideals in power series rings was introduced by Heisuke Hironaka [2], [3].

The theory is nowadays discussed in multiple books including [4] and [5]. We will follow these books along the way as we gradually unveil the elegance and power of Gröbner bases in solving systems of polynomial equations. Further information can be also found in [6] and [7].

1.1 Elementary algebraic structures

Let us introduce the rudiments of abstract algebra that will allow us to progress towards the application of Gröbner bases in algebraic cryptanalysis.

Definition 1.1.1. Let $A_1, \ldots, A_n$ be sets. Then the **Cartesian product** $A_1 \times \cdots \times A_n$ is the set of all ordered n-tuples $(a_a, \ldots, a_n)$ such that $a_i \in A_i$ for $1 \leq i \leq n$.

Definition 1.1.2. Let A and B be sets. A **map** is a set $\varphi \subseteq A \times B$ such that for each $a \in A$ there is exactly one $b \in B$ with $(a, b) \in \varphi$.

Definition 1.1.3. Let A be a set. A **binary operation** is a map from $A \times A$ to A.

Group theory is central to abstract algebra. We will use the definition of a group to define the structures we will operate with throughout the rest of our work — rings, ideals, and fields. Such an approach should make the definitions of these structures shorter and emphasize their relations.

Let us first start with a definition of a simpler structure than a group:

Definition 1.1.4. A **monoid** is a set M with a binary operation $(a, b) \mapsto a \circ b$ such that the following two axioms hold:

(i) $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in M$,

(ii) there is $e \in M$ such that $e \circ a = a \circ e = a$ for all $a \in M$.

A monoid is called a **commutative monoid** if, in addition to (i) and (ii), the following axiom also holds:

(iii) $a \circ b = b \circ a$ for all $a, b \in M$.

Note that since $\circ$ is a binary operation, the resulting element, $a \circ b$ is always in M for all $a, b \in M$. We say that M is closed under $\circ$ or that $\circ$ is closed on M. Also note that the first axiom is the associative property. The element e is called the **identity element** or simply the **identity**. For simplicity, we will refer to the set M as the monoid with the associated operation being implicit. We will also use this convention for all the subsequent algebraic structures, even when there will be multiple operations associated with the structure.

Definition 1.1.5. A **group** G is a monoid in which for all $a \in G$, there is $b \in G$ with $a \circ b = b \circ a = e$. A group G is an **Abelian group** if it is also a commutative monoid.

The element b in the definition above is called the **inverse** of a. Note that Abelian groups are commutative groups.

Definition 1.1.6. A **ring** is a set R with two binary operations $(a, b) \mapsto a + b$ and $(a, b) \mapsto a \cdot b$, referred to as addition and multiplication, such that the following axioms hold:

(i) the set R is an Abelian group under addition with the **additive identity** 0,

(ii) the set R is a monoid under multiplication with the **multiplicative identity** 1,

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

A ring is a **commutative ring** if, under multiplication, R is a commutative monoid.

The inverse under addition in a ring is called the **additive inverse**, and the inverse under multiplication is the **multiplicative inverse**. Note that the axiom (iii) describes the left and right distributive laws. We will usually omit the symbol for multiplication, and instead of $a \cdot b$, we will write ab.

Example 1.1.7.

(i) The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are rings with their standard addition and multiplication.

(ii) The natural numbers do not form a ring since not all elements have their additive inverse in this set.

(iii) The set of integers modulo $n \in \mathbb{Z}$, denoted $\mathbb{Z}_n$, is a ring.

Definition 1.1.8. Let R be a ring and $\emptyset \neq I \subseteq R$. Then I is an **ideal** of R if:

(i) $a + b \in I$ for all $a, b \in I$, and

(ii) $ar \in I$ for all $a \in I$ and $r \in R$.

The ideal I is **proper** if $I \neq R$.

Note that an ideal I of a ring R is closed under addition. It is also closed under multiplication by any $r \in R$.

Proposition 1.1.9. *Let I be an ideal of a commutative ring R, then:*

(i) $a \cdot 0 = 0 \cdot a = 0$ *for all* $a \in R$.

(ii) $0 \in I$, *and*

(iii) *if* $1 \in I$ *then* I *is not proper.*

Proof.

(i) Suppose $a \in R$. Then

$$\begin{aligned} a + a \cdot 0 &= a \cdot 1 + a \cdot 0 \\ &= a\,(1 + 0) \\ &= a \cdot 1 \\ &= a. \end{aligned}$$

Adding the additive inverse of a on both sides gives $a \cdot 0 = 0$. Since R is commutative, $0 \cdot a = 0$ also holds.

(ii) Considering the previous proof, by (i) of definition 1.1.6, we know that $0 \in R$ and by (ii) of definition 1.1.8, we get $0 \cdot a = 0 \in I$ for any $a \in I$.

(iii) Since 1 is the multiplicative identity, we have $1 \cdot r = r \in I$ for all $r \in R$ and thus $I = R$. □

Remark 1.1.10. There is an analogy from modular arithmetic that illustrates an intuitive view of ideals — they can be regarded as a generalization of a zero in a number set such as the integers. Consider the ring $\mathbb{Z}_n$ of integers modulo a given integer $n \in \mathbb{Z}$. The exact set of integers that we identify with 0 in $\mathbb{Z}_n$ is the set $n\mathbb{Z} = \{nm | m \in \mathbb{Z}\}$. This set meets the criteria for being an ideal ((i) and (ii) of definition 1.1.8) of $\mathbb{Z}$ and its elements "behave" like 0 in $\mathbb{Z}$: adding two elements of $n\mathbb{Z}$ yields another element of $n\mathbb{Z}$ and multiplying any element of $n\mathbb{Z}$ again yields an element of $n\mathbb{Z}$.

Considering our definition of rings, note that an ideal might not be a ring itself. For example, consider the ring of integers and its ideal consisting of even numbers. This ideal is not a ring since it has no multiplicative identity.

Definition 1.1.11. A **field** F is a ring where the set $F \setminus \{0\}$ is an Abelian group under multiplication with the **multiplicative identity** 1.

Fields with a finite number of elements are **finite fields** and are often denoted $\mathbb{F}_q$, where the number of elements q is the **order** of the field. Since we will not encounter any rings that are not commutative, we will adopt the convention that by a ring, we will mean a commutative ring. Then, the only difference between rings and fields is that in a field, every element other than 0 has its multiplicative inverse. Note that every field is a ring as well.

Example 1.1.12.

(i) The sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields with their standard addition and multiplication.

(ii) The integers do not form a field since not all elements have their multiplicative inverse in this set.

(iii) The set of integers modulo $p \in \mathbb{Z}$, denoted $\mathbb{Z}_p$, is a field whenever p is prime. The primality of p ensures that each non-zero element has its multiplicative inverse.

We will often work with the finite field $\mathbb{Z}_2$, which merits a short comment. We will denote this field $\mathbb{F}_2$. The additive and multiplicative identities are 0 and 1, respectively. The additive inverse of 0 is 0. The element 1 is also its additive and multiplicative inverse.

1.2 Multivariate Polynomials

Definition 1.2.1. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be an n-tuple of non-negative integers. A **monomial** in $x_1, \ldots, x_n$ is a product of the form

$$\prod_{i=1}^{n} x_i^{\alpha_i} = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

Let us simplify the notation by setting

$$x^\alpha = \prod_{i=1}^{n} x_i^{\alpha_i}.$$

The **total degree** of a monomial x^α is the sum $\sum_{i=1}^{n} \alpha_i$. We simplify the notation again an let $|x^\alpha|$ denote the total degree of x^α. We will call the symbols $x_1, \ldots, x_n$ indeterminates or variables, depending on which context we will need to emphasize. Note that $x^\alpha = 1$ when $\alpha = (0, \ldots, 0)$ and also when $|x^\alpha| = 0$. Also note that any monomial is fully determined by α.

Definition 1.2.2. Let x^α be a monomial and let K be a field. A **term** with a non-zero **coefficient** $c_\alpha \in K$ is the product $c_\alpha x^\alpha$.

Definition 1.2.3. A **polynomial** f with coefficients in a field K is a finite sum of terms in the form

$$f = \sum_{\alpha} c_\alpha \cdot x^\alpha, \quad c_\alpha \in K.$$

The zero polynomial will be denoted 0.

Definition 1.2.4. Let $f = \sum c_\alpha x^\alpha \neq 0$ be a non-zero polynomial. The **total degree** of f, denoted $\deg(f)$, is the maximum $|x^\alpha|$ such that the corresponding coefficient c_α is nonzero. The degree of 0 is undefined.

The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in a field K will be denoted $K[x_1, \ldots, x_n]$. When the particular indeterminates are of no relevance, we will denote the set by $K[\mathbf{x}]$ for short. We will also employ the standard letters x, y and z instead of x_1, x_2 and x_3 when we discuss illustrative polynomials.

Let $f, g \in K[\mathbf{x}]$ be polynomials. We say that f *divides* g if $g = fh$ for some polynomial $h \in K[\mathbf{x}]$. One can show that the set $K[\mathbf{x}]$ satisfies all of the ring axioms under standard polynomial addition and multiplication. We will therefore refer to $K[\mathbf{x}]$ as a *polynomial ring*. Not all polynomials in this ring have their multiplicative inverses, e.g., even the elementary polynomial x_1 does not have its multiplicative inverse and so $K[\mathbf{x}]$ does not form a field. A proof that $K[\mathbf{x}]$ forms a ring can be found in [4, Chapher 2], the authors also provide a broader outlook on polynomials by defining them in a more abstract way.

Definition 1.2.5. Let $\{f_1, \ldots, f_s\} \subset K[\mathbf{x}]$ be a set of polynomials. Then we set

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \;\middle|\; h_1, \ldots, h_s \in K[\mathbf{x}] \right\}.$$

Lemma 1.2.6. *If* $\{f_1, \ldots, f_s\} \subset K[\mathbf{x}]$ *is a set of polynomials, then* $\langle f_1, \ldots, f_s \rangle$ *is an ideal of* $K[\mathbf{x}]$.

Proof. Assume $f = \sum_{i=1}^{s} p_i f_i$ and $g = \sum_{i=1}^{s} q_i f_i$ are polynomials, and let also $h \in K[\mathbf{x}]$ be a polynomial. Then the equations

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i \quad \text{and}$$
$$hf = \sum_{i=1}^{s} (hp_i) f_i$$

show that $\langle f_1, \ldots, f_s \rangle$ meets the criteria for being an ideal of $K[\mathbf{x}]$. □

Definition 1.2.7. Let $\{f_1, \ldots, f_s\} \subset K[\mathbf{x}]$ be a set of polynomials and let I be an ideal such that $I = \langle f_1, \ldots, f_s \rangle$. The set $\{f_1, \ldots, f_s\}$ is a **basis** of I. We will also call $\langle f_1, \ldots, f_s \rangle$ the **ideal generated by** $\{f_1, \ldots, f_s\}$.

Remark 1.1.10 provides an intuitive view of ideals through modular arithmetic. Another analogy comes from linear algebra where the definition of subspaces can be likened to the definition of ideals of polynomial rings. Both are closed under addition. Subspaces are closed under multiplication by scalars while ideals of polynomial rings are closed under multiplication by polynomials. An ideal generated by a set of polynomials also shares similar properties with a span generated by a set of vectors, which is a structure similar to subspaces as well.

Definition 1.2.8. Let K be a field and n a positive integer. The n-dimensional **affine space** over K is the set

$$K^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in K\}.$$

Remark 1.2.9. A polynomial $f \in K[x_1, \ldots, x_n]$ can be regarded as a function $f : K^n \mapsto K$ that takes in points in the affine space K^n and produces elements of the field K.

Definition 1.2.10. Let K^n be an affine space and let $f = f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ be a polynomial. The **zero point** of f is a point $(a_1, \ldots, a_n) \in K^n$ such that $f(a_1, \ldots, a_n) = 0$.

Definition 1.2.11. Let $\{f_1, \ldots, f_s\} \subset K[x_1, \ldots, x_n]$ be a set of polynomials and K^n an affine space. The **affine variety** $V(f_1, \ldots, f_s)$ defined by $\{f_1, \ldots, f_s\}$ is the set

$$V(f_1, \ldots, f_s) = \left\{ (a_1, \ldots, a_n) \in K^n \;\middle|\; f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s \right\}$$

of all zero points of all the polynomials in $\{f_1, \ldots, f_s\}$.

Solving an equation that can be expressed as a polynomial in multiple variables can be seen as finding the zero points of the corresponding polynomial. Affine varieties generalize this notion to systems of polynomial equations. Considering remark 1.2.9, we may also see varieties as geometric objects, which is briefly illustrated by the following example:

Example 1.2.12. Consider the real coordinate space $\mathbb{R}^2$ and the polynomial $f = f(x^2 + y^2 - 1)$. The variety $V(f)$ is the unit circle centered at the origin.

We will use the following lemma to show that a given ideal is contained in another one. This is useful for proving the equality of two ideals in example 1.2.14.

Lemma 1.2.13. *Let $I \subseteq K[\mathbf{x}]$ be an ideal, and let $\{f_1, \ldots, f_s\} \subset K[\mathbf{x}]$ be a set of polynomials. Then $\langle f_1, \ldots, f_s \rangle \subseteq I$ if and only if $\{f_1, \ldots, f_s\} \subseteq I$.*

Proof.
$\Longrightarrow$ Assume $\langle f_1, \ldots, f_s \rangle \subseteq I$. Each $f_i \in \{f_1, \ldots, f_s\}$ can be constructed as follows: $f_i = 0 \cdot f_1 + \cdots + 1 \cdot f_i + \cdots + 0 \cdot f_s$, and hence $\{f_1, \ldots, f_n\} \subseteq I$.

$\Longleftarrow$ Assume $\{f_1, \ldots, f_n\} \subseteq I$ and choose any $f \in \langle f_1, \ldots, f_s \rangle$ so that $f = h_1 f_1 + \cdots + h_s f_s$ where each $h_i \in K[\mathbf{x}]$. We see that $f \in I$ since I is an ideal and so $\langle f_1, \ldots, f_s \rangle \subseteq I$. □

Example 1.2.14. Consider the ideals $\langle x, y \rangle$ and $\langle x + y, x - y \rangle$ in the polynomial ring $\mathbb{Q}[x, y]$. We will show that these two ideals are equal so that $\langle x, y \rangle = \langle x + y, x - y \rangle$.

We see that $x + y \in \langle x, y \rangle$ and $x - y \in \langle x, y \rangle$, so by lemma 1.2.13, $\langle x + y, x - y \rangle \subseteq \langle x, y \rangle$. Similarly, both $x = \frac{1}{2}(x + y) + \frac{1}{2}(x - y)$ and $y = \frac{1}{2}(x + y) - \frac{1}{2}(x - y)$ are in $\langle x + y, x - y \rangle$ so that by lemma 1.2.13, $\langle x, y \rangle \subseteq \langle x + y, x - y \rangle$ and the equality follows.

Proposition 1.2.15. *If $\{f_1, \ldots, f_s\}$ and $\{g_1, \ldots, g_t\}$ are two bases of the same ideal in $K[x_1, \ldots, x_n]$, so that $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, then $V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$.*

Proof. Choose any $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$. We know that all polynomials in $\{f_1, \ldots, f_s\}$ are equal to zero at $(a_1, \ldots, a_n)$. Now choose any $g \in \langle g_1, \ldots, g_t \rangle$. Since $\langle g_1, \ldots, g_t \rangle = \langle f_1, \ldots, f_s \rangle$, we can write $g = \sum_{i=1}^{s} h_i f_i$, $h_i \in K[x_1, \ldots, x_n]$. Then $g(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot f_i(a_1, \ldots, a_n) = 0$, which shows that $(a_1, \ldots, a_n) \in V(g_1, \ldots, g_t)$, which means that $V(f_1, \ldots, f_s) \subseteq V(g_1, \ldots, g_t)$. The opposite inclusion can be proved in the same way. □

Example 1.2.14 shows that an ideal may have multiple different bases while proposition 1.2.15 reveals that a variety is actually determined by the ideal generated by its basis and not by the basis itself.

A system of multivariate equations can be seen as an ideal basis. Proposition 1.2.15 then gives us a potential ability to change the original system to another one while keeping the exact same solution set. We will model our cipher as system of polynomial equations and then we will transform this system into a new one which will be solvable in linear time. We will show that a Gröbner basis is the new system and that the transformation will be the most demanding part of the computation as regards both time and memory.

1.3 Monomial Orders

A Gröbner basis always pertains to a particular order on monomials. Let us therefore introduce the most fundamental ones.

Before we actually define a monomial order, let us start with a concise discussion about binary relations so that it is convenient to prove that certain orders are in fact monomial orders.

Definition 1.3.1. Let S be a non-empty set. A **binary relation** on S is a subset r of $S \times S$. The relation $\Delta(S) = \{(a, a) \mid a \in S\}$ is the **diagonal** of S.

We will use only binary relations in our work and so we will refer to them simply as relations. In order to simplify the notation, we will also employ infix notation to denote that two elements are in a relation, i.e., if r is a binary relation on S and $a, b \in S$, then $a\ r\ b$ will mean $(a, b) \in r$.

Definition 1.3.2. Let r and s be relations on S. The relation $r^{-1} = \{(a, b) \,|\, (b, a) \in r\}$ is the **inverse** of r. The **strict part** of r is the relation $r_s = r \setminus r^{-1}$, and

$$s \circ r = \{(a, c) \mid \text{there is } b \in S \text{ such that } (a, b) \in r \text{ and } (b, c) \in s\}$$

is the **product** of r and s.

Definition 1.3.3. Let r be a relation on S. Then r is

(i) **transitive** if $r \circ r \subseteq r$,

(ii) **antisymmetric** if $r \cap r^{-1} \subseteq \Delta(S)$,

(iii) **connex** if $r \cup r^{-1} = S \times S$,

(iv) a **linear order on** S if r is transitive, antisymmetric and connex.

Definition 1.3.4. Let r be a relation on S with strict part r_s and let $R \subseteq S$. An element $a \in R$ is **minimal** if there is no $b \in R$ such that $b\ r_s\ a$. A **strictly descending** (or **strictly decreasing**) **sequence** in S is an infinite sequence of elements $a_n \in S$ such that $a_{n+1}\ r_s\ a_n$ for all $n \in \mathbb{N}$. The relation r is **noetherian** if every non-empty subset R of S has a minimal element. The relation r is a **well-order** on S if it is a noetherian linear order on S.

A natural way to think about the strict part of a relation is to consider the natural order on $\mathbb{N}$, which is a linear order, where for each $m, n \in \mathbb{N}$; $m > n$ means $m \geq n$ and $m \neq n$. The symbol $>$ denotes the strict part of the relation $\geq$. We will also denote our orders on monomials by $\succeq$, the inverse will be $\preceq$ and the strict parts will be denoted $\succ$ and $\prec$.

We will denote by $\mathcal{M}(x_1, \ldots, x_n)$, or simply $\mathcal{M}$, the set of all monomials in the indeterminates $x_1, \ldots, x_n$. It turns out that $\mathcal{M}$ forms an Abelian monoid

under natural multiplication where we add corresponding exponents of the indeterminates. The multiplicative identity is the monomial 1. Note that we can associate any monomial $x^\alpha \in \mathcal{M}(x_1, \ldots, x_n)$ with its n-tuple of exponents $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ in a one-to-one fashion. Thus, we can use the sets $\mathcal{M}$ and $\mathbb{N}_0^n$ interchangeably.

Lemma 1.3.5. *A linear order $\geq$ on S is a well-order if and only if there is no strictly descending sequence in S.*

Proof. Let us turn the lemma into its contrapositive form: $\geq$ is not a well-order if and only if there is a strictly descending sequence in S; and prove this version of the lemma.

$\Longrightarrow$ Suppose $\geq$ is not a well-order. Then there is a non-empty subset $R \subseteq S$ that has no minimal element. We can choose $a \in R$ and since a is not the minimal element, we can choose again $b \in R$ such that $a > b$, which leads to a strictly descending sequence.

$\Longleftarrow$ Suppose there is a strictly descending sequence in S. The elements of such a sequence form a non-empty subset R of S that has no minimal element. Hence, $\geq$ is not a well-order. □

Definition 1.3.6. A **monomial order** $\succeq$ is a well-order on $\mathcal{M}$, which satisfies the **property of respecting multiplication**: if $m_1 \succeq m_2$, then $n \cdot m_1 \succeq n \cdot m_2$ for all $m_1, m_2, n \in \mathcal{M}$.

The purpose of the property of respecting multiplication is that the relative ordering of monomials in a polynomial does not change when we multiply the polynomial by a monomial. Such behavior is necessary for the division algorithm described in the next section.

Definition 1.3.7 (Lexicographic order). Let $x^\alpha, x^\beta \in \mathcal{M}(x_1, \ldots, x_n)$ be monomials. We say $x^\alpha \succeq_{lex} x^\beta$ if $\alpha = \beta$ or if there is $1 \leq i \leq n$ such that $\alpha_j = \beta_j$ for $1 \leq j < i$ and $\alpha_i > \beta_i$.

Note that $\succ_{lex}$ compares the exponent n-tuples $\alpha, \beta \in \mathbb{N}_0^n$ so that $x^\alpha \succ_{lex} x^\beta$ if the left-most non-zero component of the difference $\alpha - \beta \in \mathbb{N}_0^n$ is positive.

Remark 1.3.8. Also note that the lexicographic order depends on how the underlying indeterminates $x_1, x_2, \ldots, x_n$ are ordered. In general, there are $n!$ ways to order n indeterminates and each of these orders has its respective lexicographic order. We will only assume the standard order where $x_1 > x_2 > \cdots > x_n$, or the alphabetical order where $x > y > z$.

Example 1.3.9.

(i) Let xy^2z^3 and xy^3 be monomials in $\mathcal{M}(x,y,z)$. Then $xy^3 \succ_{lex} xy^2z^3$ since there is $i = 2$ and $j = 1$ such that $\alpha_j = \beta_j$ and $\alpha_i > \beta_i$, where $\alpha = (1,3,0)$ and $\beta = (1,2,3)$. Also, the left-most non-zero component of the difference $\beta - \alpha = (0,1,-3)$ is positive.

(ii) Let x, y, z be monomials in $\mathcal{M}(x,y,z)$. Then considering remark 1.3.8 and example (i), we get $x \succ_{lex} y \succ_{lex} z$.

(iii) In the lexicographic order, note that a monomial that contains the most significant indeterminate (as regards the underlying order) is greater than any other monomial that does not contain such an indeterminate. For example, if x and y^3z^2 are monomials in $\mathcal{M}(x,y,z)$, then $x \succ_{lex} y^3z^2$. The reasoning is the same as in (i) and (ii).

The intuitive outlook on the lexicographic order is that it looks for the most significant indeterminate that appears in one of the monomials and then gives preference to the monomial in which this indeterminate has greater power.

Proposition 1.3.10. *The lexicographic order $\succeq_{lex}$ on $\mathcal{M}$ is a monomial order.*

Proof. Following the definition of the lexicographic order and the fact that the regular numerical order on $\mathbb{N}_0$ is a linear order, it is straightforward to show that for any monomials $x^\alpha, x^\beta, x^\gamma \in \mathcal{M}(x_1,\dots,x_n)$ and $\alpha,\beta,\gamma \in \mathbb{N}_0^n$, the following conditions hold:

(transitivity) if $x^\alpha \succeq_{lex} x^\beta$ and $x^\beta \succeq_{lex} x^\gamma$, then $x^\alpha \succeq_{lex} x^\gamma$;

(antisymmetry) if $x^\alpha \succeq_{lex} x^\beta$ and $x^\alpha \preceq_{lex} x^\beta$, then $x^\alpha = x^\beta$; and

(connexity) either $x^\alpha \succeq_{lex} x^\beta$ or $x^\alpha \preceq_{lex} x^\beta$.

These properties show that $\succeq_{lex}$ is a linear order on $\mathcal{M}$.

Let us prove the property of respecting multiplication explicitly. If $x^\alpha \succeq_{lex} x^\beta$, then either $\alpha = \beta$, or there is $1 \le i \le n$ such that $\alpha_i - \beta_i > 0$ with $\alpha_j = \beta_j$ for $1 \le j < i$. Also, $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ and $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. Comparing the results gives us $(\alpha+\gamma) - (\beta+\gamma) = \alpha - \beta$ and we see that $\alpha_i - \beta_i > 0$ with $\alpha_j = \beta_j$ for $1 \le j < i$ again; or if $\alpha = \beta$, then $(\alpha+\gamma) = (\beta+\gamma)$. This shows that also $x^{\alpha+\gamma} \succeq_{lex} x^{\beta+\gamma}$.

The last part to prove is to show that $\succeq_{lex}$ is also noetherian, i.e a well-order. We will prove this by the following contradiction:

By lemma 1.3.5, if $\succeq_{lex}$ is not a well-order, then there is a strictly decreasing sequence

$$x^{\alpha_{(1)}} \succ_{lex} x^{\alpha_{(2)}} \succ_{lex} \cdots$$

of elements in $\mathcal{M}(x_1,\dots,x_n)$, where each $\alpha_{(i)} = (\alpha_1,\dots,\alpha_n) \in \mathbb{N}_0^n$. By the definition of $\succeq_{lex}$, we also know that there exists a j such that all the first

components of the n-tuples $\alpha_{(k)}$ with $k \geq j$ are equal. Continuing further, there is an $l \geq j$ such that all the second components of the n-tuples $\alpha_{(m)}$ with $m \geq l$ are all equal. We see that there must be a $p \geq l$, for which the whole n-tuples $\alpha_{(p)} = \alpha_{(p+1)} = \cdots$ are all equal. This means that the sequence is not strictly decreasing, which contradicts the lemma. □

Definition 1.3.11 (Reverse Colexicographic Order). Let $x^\alpha, x^\beta \in \mathcal{M}(x_1, \ldots, x_n)$ be monomials. We say $x^\alpha \succeq_{rclex} x^\beta$ if $\alpha = \beta$ or if there is $1 \leq i \leq n$ such that $\alpha_j = \beta_j$ for $i < j \leq n$ and $\alpha_i < \beta_i$.

Observe that $\succ_{rclex}$ compares the exponent n-tuples $\alpha, \beta \in \mathbb{N}_0^n$ so that $x^\alpha \succ_{rclex} x^\beta$ if the right-most non-zero component of the difference $\alpha - \beta \in \mathbb{N}_0^n$ is negative. Remark 1.3.8 also applies.

Example 1.3.12.

(i) Let xy^2z^3 and xy^3 be monomials in $\mathcal{M}(x, y, z)$. Then $xy^3 \succ_{rclex} xy^2z^3$ as well as in example 1.3.9 (i), but for a different reason. There is $i = 3$ such that $\alpha_i < \beta_i$, where $\alpha = (1, 3, 0)$ and $\beta = (1, 2, 3)$. Also, the right-most non-zero component of the difference $\beta - \alpha = (0, 1, -3)$ is negative.

(ii) The lexicographic order coincides with the reverse colexicographic order for monomials in one and two indeterminates. These orders may differ for monomials in three and more variables, as shown by the following example: let xz and y^2 be monomials in $\mathcal{M}(x, y, z)$. Then $xz \succ_{lex} y^2$, as explained in example 1.3.9 (i), but $y^2 \succ_{rclex} xz$, as explained in example (i).

The intuitive outlook on the reverse colexicographic order is that it looks for the least significant indeterminate that appears in one of the monomials and then gives preference to the monomial in which this indeterminate has lesser power. It can be thought of as a double reversal of the lexicographic order — we first reverse the underlying order of the indeterminates and then their powers.

Equivalently to the lexicographic order, it is straightforward to show that the reverse colexicographic order is a linear order as well. However, it is not a well-order since it is possible to define the following strictly decreasing sequence

$$x_1x_2 \succ_{rclex} x_1x_2^2 \succ_{rclex} x_1x_2^3 \succ_{rclex} \cdots$$

of monomials in $\mathcal{M}(x_1, x_2)$. In this sequence, let $x^\alpha = x^{(1,n)}$ and $x^\beta = x^{(1,n+1)}$ for $n \in \mathbb{N}_{>0}$. We see that it is always the case that $x^\alpha \succ_{rclex} x^\beta$ since $\alpha_1 = \beta_1$ and $\alpha_2 < \beta_2$, and we get a strictly decreasing sequence. Hence, by lemma 1.3.5, $\succeq_{rclex}$ is not a well-order and by definition 1.3.6, $\succeq_{rclex}$ cannot be a monomial order either. For this reason, we will not use it to order monomials

on its own, but we will use it as a "sub-order" in the definition of the next order, which will be a monomial order.

Examples 1.3.9 and 1.3.12 show that the lexicographic and reverse colexicographic orders do not take into consideration the total degree of monomials. Later in our work, we will see that in certain cases, it is desirable to order the monomials in a polynomial according to their total degree. Let us therefore introduce the following order, which allows for the total degree.

Definition 1.3.13 (Graded Reverse Lexicographic Order). Let $x^\alpha, x^\beta \in \mathcal{M}(x_1, \ldots, x_n)$ be monomials. We say $x^\alpha \succeq_{grlex} x^\beta$ if $|x^\alpha| > |x^\beta|$, or $|x^\alpha| = |x^\beta|$ and $x^\alpha \succeq_{rclex} x^\beta$.

Notice that despite its name, the graded reverse lexicographic order actually makes use of the reverse colexicographic order. There is a general consensus on such a name, so we will follow it.

Example 1.3.14.

(i) Let $x, y^2, xz \in \mathcal{M}(x, y)$ be monomials. Then $y^2 \succeq_{grlex} x$ since $|y^2| = 2 > |x| = 1$; and $y^2 \succeq_{grlex} xz$ since $|xz| = |y^2|$ and $y^2 \succeq_{rclex} xz$.

(ii) Let $x, y, z \in \mathcal{M}(x, yz)$ be monomials. Then $x \succeq_{grlex} y \succeq_{grlex} z$ since $|x| = |y| = |z|$ and $x \succeq_{rclex} y \succeq_{rclex} z$.

Proposition 1.3.15. *The graded reverse lexicographic order $\succeq_{grlex}$ on $\mathcal{M}$ is a monomial order.*

Proof. Since $\succeq_{grlex}$ first uses the usual well-order order on the total degree of monomials $|x^\alpha| \in \mathbb{N}_0$ and when $|x^\alpha| = |x^\beta|$, it decides ties using the reverse colexicographic order (which is a linear order), grlex is also linear.

It is also straightforward to show that $\succeq_{grlex}$ is a well-order since we consider only the strict part $\succ_{grlex}$, which is solely the well-order on $|x^\alpha| \in \mathbb{N}_0$.

In order to show that the property of respecting multiplication holds, consider the monomials $x^\alpha, x^\beta, x^\gamma \in \mathcal{M}(x_1, \ldots, x_n)$ with the n-tuples $\alpha, \beta, \gamma \in \mathbb{N}_0^n$. Also, $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ and $x^\beta \cdot x^\gamma = x^{\alpha+\gamma}$. Assume $x^\alpha \succeq_{grles} x^\beta$. If $|x^\alpha| > |x^\beta|$, then $x^{\alpha+\gamma} \succ_{grlex} x^{\beta+\gamma}$ since $|x^{\alpha+\gamma}| = |x^\alpha| + |x^\gamma| > |x^\beta| + |x^\gamma| = |x^{\beta+\gamma}|$. Also, if $|x^\alpha| = |x^\beta|$, we get $|x^{\alpha+\gamma}| = |x^{\beta+\gamma}|$ by the same argument as above and we use the reverse colexicographic order. So if $|x^\alpha| = |x^\beta|$, then $x^\alpha \succeq_{rclex} x^\beta$ (since we have assumed that $x^\alpha \succeq_{grlex} x^\beta$), which means that either $\alpha = \beta$, or there is $1 \leq i \leq n$ such that $\alpha_i - \beta_i < 0$ with $\alpha_j = \beta_j$ for $i < j \leq n$. As in the proof of proposition 1.3.10, comparing the results gives us $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$ and we see that $\alpha_i - \beta_i < 0$ with $\alpha_j = \beta_j$ for $i < j \leq n$ again; or if $\alpha = \beta$, then $(\alpha + \gamma) = (\beta + \gamma)$. This shows that $x^{\alpha+\gamma} \succeq_{grlex} x^{\beta+\gamma}$ and completes the proof. □

1.4 Multivariate Division

Conclusion

Bibliography

[1] Buchberger, B. 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*, volume 41, no. 3-4, 2006: pp. 475–511.

[2] Hironaka, H. Resolution of Singularities of an Algebraic Variety Over a Field of Characteristic Zero: I. *Annals of Mathematics*, volume 79, no. 1, 1964: pp. 109–203, ISSN 0003486X. Available from: http://www.jstor.org/stable/1970486

[3] Hironaka, H. Resolution of Singularities of an Algebraic Variety Over a Field of Characteristic Zero: II. *Annals of Mathematics*, volume 79, no. 2, 1964: pp. 205–326, ISSN 0003486X. Available from: http://www.jstor.org/stable/1970547

[4] Becker, T. *Gröbner bases : a computational approach to commutative algebra*. New York: Springer-Verlag, 1993, ISBN 0-387-97971-9.

[5] Cox, D. *Ideals, varieties, and algorithms : an introduction to computational algebraic geometry and commutative algebra*. Cham: Springer, 2015, ISBN 9783319167206.

[6] Adams, W. *An introduction to Gröbner bases*. Providence, R.I: American Mathematical Society, 1994, ISBN 978-0-8218-3804-4.

[7] Hibi, T. *Gröbner bases : statistics and software systems*. Tokyo New York: Springer, 2013, ISBN 978-4-431-54573-6.

Appendix **A**

Abbreviations and Symbols

$\mathbb{N}_0 =$ the set of natural numbers including zero

$\mathbb{N}_{>0} =$ the set of natural numbers excluding zero

$\mathbb{Z} =$ the set of integers

$\mathbb{Q} =$ the set of rational numbers (fractions)

$\mathbb{R} =$ the set of real numbers

$\mathbb{C} =$ the set of complex numbers

$\square$ indicates the end of a proof

e.g. (Latin *exempli gratia*) for example

i.e. (Latin *id est*) that is

Appendix B

Contents of enclosed CD

- `readme.txt` ..... the file with CD contents description
- `exe` ..... the directory with executables
- `src` ..... the directory of source codes
  - `wbdcm` ..... implementation sources
  - `thesis` ..... the directory of LaTeX source codes of the thesis
- `text` ..... the thesis text directory
  - `thesis.pdf` ..... the thesis text in PDF format
  - `thesis.ps` ..... the thesis text in PS format