Technische Universität München
Institut für Mathematik

Degree Bounds and Complexity of Gröbner Bases of Important Classes of Polynomial Ideals

Stephan Ritscher

Vollständiger Abdruck der von der Fakultät für Mathematik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

genehmigten Dissertation.

Vorsitzender:		Univ.-Prof. Dr. Raymond Hemmecke
Prüfer der Dissertation:	1.	Univ.-Prof. Dr. Ernst W. Mayr
	2.	Univ.-Prof. Dr. Gregor Kemper
	3.	Prof. Chee K. Yap, Ph.D. New York University / USA (schriftliche Beurteilung)

Die Dissertation wurde am 23.12.2010 bei der Technischen Universität München eingereicht und durch die Fakultät für Mathematik am 24.07.2012 angenommen.

Acknowledgments

I want to emphatically thank Prof. Ernst Mayr from Technische Universität München who supervised me from my third year of studies until the end of the PhD. He guided and instructed me constantly while always leaving enough space for my own interests. With well-thought suggestions he supported me when I did not know what to do next, challenging me to find my own way at the same time. He encouraged me to go abroad and helped organizing my studies at North Carolina State University and an internship at Wolfram Research.

During my studies at North Carolina State University, Prof. Hoon Hong was so kind to supervise me in cooperation with Prof. Mayr. He was a great teacher and introduced me into research and tools that turned out crucial for my work. His intuitive explanations were invaluable and could not have been replaced by text books.

The TopMath program by the Elitenetzwerk Bayern at Technische Universität München organized my studies beginning with the third year. It focused my concentration such that I could finish my studies in a tight schedule. Because of the financial support, I was able to visit conferences and seminars related to my research. Moreover, regular get-togethers of the students enriched my studies with some pleasant hours.

Last but not least, I owe to the scholarships of Max-Weber-Program by the Elitenetzwerk Bayern, the Studienstiftung des deutschen Volkes, and the TUM Graduate School. These equipped me with chances to visit seminars of various kinds which I repeatedly took. I learned languages in foreign countries, discussed in politics seminars, and improved my soft skills from rhetoric to leadership. The biggest financial supporter was the Studienstiftung des deutschen Volkes which sent me to the USA and gave me financial aid during the PhD.

Abstract

Polynomial ideals have been intensely studied by computer scientists. The method of Buchberger allows to effectively solve the membership problem to which a variety of other interesting problems can be reduced. Mayr and Meyer showed that these computations are very expensive in the worst case. As a consequence, special ideal classes have to be identified for which the membership problem can be solved more efficiently.

As previous results show, the complexity of the membership problem is mainly related to the degrees of the representation problem and Gröbner bases. Thus the first part of the thesis studies degree bounds for various ideal classes. The main contributions are upper and lower bounds for Gröbner bases depending on the ideal dimension and some results for toric ideals.

In the second part, these findings are applied to questions of complexity. The presentation comprises an incremental space-efficient algorithm for the computation of Gröbner bases, an algorithm in polylogarithmic space for the membership problem in toric ideals and the space-efficient computation of the radicals of low-dimensional ideals.

Contents

Introduction

In polynomial algebra, most questions are motivated by very basic operations. In the algebraic theory, they might seem trivial themselves, but effective (and especially efficient) solutions require deep knowledge of ring theory and related topics. Being viewed as the abstraction per se, algebra is usually rather descriptive than manipulative, rather existential than constructive. The ambitious goal of computer algebra is to bridge two worlds — the abstract world of algebra and the constructive world of computer science. The results are tremendous — while the methods are still generally applicable, using modern computers allows for automation and computation in scales that were unthinkable before.

However, generality usually comes at a high cost: slowness. While domain-specific methods will always win in production environments, general methods will play a crucial role in prototyping environments. The largest such environment is obviously science itself. Likewise, science has very high requirements to the used methods — rather in terms of quality, flexibility, and scalability than in terms of throughput.

Beyond the actual computations, more work is necessary in the theoretical foundations. With computer science being relatively young, many fundamental questions remain open. These mostly evolve around the complexity of problems and their settlement involves lower bounds just as well as upper bounds. While implementing a known algorithm more efficiently may increase the running time by a factor of 10 or 100, finding a method of lower complexity will make a difference in which instances are feasible or not. Lower bounds, however, may show that the problem has to be reformulated or specialized for efficient computations.

This is just how polynomial algebra defines itself. On the one hand it is a tool which is widely used in other branches of scientific research, mainly mathematics and computer science. Using Gröbner bases, one can do automated reasoning which is most suitable for geometry, one can find global optima in polynomial systems or integral linear systems, one can study properties of differential equations, compute reachable positions for robot arms, and solve certain logical formulas. It is also used in other computational research, e.g. for the computation of Frobenius numbers. On the other hand, polynomial algebra approaches fundamental questions of complexity which then help re-factoring the computational tools. This includes the study of the membership problem complexity for various ideal classes which will shed light on the structure of the problem and focus the research in two directions: finding better algorithms for ideal classes with low complexity and categorizing the ideals that occur in applications into the studied classes. Both will finally contribute to increased efficiency.

This thesis deals with the second part — the complexity of problems. Previous research mostly measured the complexity in the number of indeterminates in the ring and the degrees of the ideal generators. Mayr and Meyer showed in [33] that the membership problem is exponential space hard. Later, Kühnle and Mayr presented an algorithm [28] which solves the problem in space which is exponential in the number of indeterminates. Both proofs and thus the complexity of the membership problem are tightly connected to the degrees of Gröbner bases. While [33] implies a double exponential lower degree bound which was sharpened by Yap [44], a similar upper degree bound was proved by Dubé in [12]. Also the representation degree is important in the algorithm by Kühnle and Mayr. The lower bound for it is in [33]. The upper bound is much older and goes back to Hermann [19].

There has been some work on special ideal classes before. Various authors studied homogeneous and zero-dimensional ideals as well as toric ideals. While the membership problem for homogeneous ideals can be solved in polynomial space [32], their Gröbner bases also have double exponential degrees. For zero-dimensional ideals, the degrees of Gröbner bases are known to be smaller by a magnitude. Already the famous theorem of Bézout can be used for proving this in the homogeneous case. For the inhomogeneous case, the proofs are slightly more involved and many of the bounds in literature are not tight. While Caniglia et al. [6] give a degree bound which is not tight either, one of the intermediate results can be used for the proof of a tight single exponential bound as will be shown later. While the representation degrees evolve in the same magnitude, the business of tight bounds is even harder. The best bound known to the author is due to Dickenstein et al. in [11] and probably not tight.

One of the large themes in this thesis is the dependence of the complexity on the ideal dimension. This was started by Kratzer [24] who gave an algorithm for the membership problem in space polynomial in the number of variables and exponential in the ideal dimension using a respective bound for the representation degree. In this thesis, upper and lower bounds for Gröbner bases will be presented which are double exponential in the ideal dimension. The proof is based on the construction by Dubé in [12]. These bounds will be applied to an algorithm for the computation of the radical of an ideal by [30] achieving a space complexity which is exponential in the ideal dimension.

Furthermore, toric ideals will be analyzed. Starting from results by Sturmfels [42], single exponential degree bounds for Gröbner bases and the representation problem will be given. Moreover, a polylogarithmic algorithm for the membership problem will be deduced.

Finally, the space-efficient algorithm for the computation of Gröbner bases by Kühnle and Mayr [28] will be improved. By adding a S-polynomial criterion, it will be made adaptive such that it only achieves the worst case behavior for hard examples.

The thesis is divided in three parts. The first provides the theoretical background for the proofs and algorithms. Most of it is common knowledge in the field of computer algebra, but it is included for the sake of completeness. Inexperienced readers, however, might prefer to start off with a text book since there are few explanations for the interpretation of the theorems. Starting off, chapter 1 introduces concepts of abstract algebra like rings, ideals, modules and some of their properties. Chapter 2 focuses on rings of polynomials and their ideals. Although Gröbner bases are introduced, the presentation is still rather algebraic (i.e. most proofs will not use algorithms). There will be many definitions of the ideal dimension, and connected tools like Hilbert polynomials, cone decompositions and regular sequences are introduced. A dedicated section will cover toric ideals. In chapter 3, several computational models and basic complexity results will be introduced. These are Thue systems, Turing machines, Boolean circuits, and some results about space-efficient methods, especially in linear algebra.

The second part covers degree bounds. It contains both new results and an overview of the best known results. Chapter 4 will treat the representation problem, chapter 5 is about the Gröbner basis degrees. Both cover various ideal classes, ranging from arbitrary (polynomial) ideals via zero-dimensional ideals and arbitrary ideals parametrized by the dimension to toric ideals. As mentioned before, the main contributions in this part are the dimension-dependent bounds for Gröbner bases and the bounds for toric ideals.

Finally, the third part is about consequences of the degree bounds. All of the presented results are contributions of this thesis (partly based on previous results). Chapter 6 explains an incremental space-efficient algorithm for the computation of Gröbner bases. In chapter 7, the membership problem for toric ideals is solved in polylogarithmic space. Last, but not least, chapter 8 analyzes an algorithm for the computation of radicals improving the space-efficiency for low-dimensional ideals.

Part I.

Preliminaries

In the first part of this thesis, a mostly self-contained introduction into the theory of Gröbner bases and the necessary algebraic foundations will be given. Moreover, fundamentals of the theory of computation will be treated. However, the objectives are neither completeness nor comprehensive explanations. Readers not familiar with the topic might prefer reading a textbook prior to this thesis. Good introductions to computational polynomial algebra are available in [9] and [10] respectively [26] and [27], for abstract algebra [13] provides a great reference.

The author considers most of the results in this part to be well-known and therefore will only give spare references. Most of the results can be found in the above text books, although the proofs might differ. Less known results will be cited to the best of the knowledge of the author.

1. Abstract Algebra

1.1. Vector Spaces

Vector spaces are introduced in every first year course. Due to the (more or less) widespread terminology, the definitions and well-known results do not have to be repeated in this thesis before they can be used. Thus, a good knowledge of linear algebra will be assumed.

Still, some variants of Cramer's rule for solving linear systems will be used that might not be known to the reader. They will be stated and proved in this section.

Lemma 1.1 (Cramer's Rule). *Let $A = (a_1, \dots, a_n)$ be a $(n-1) \times n$ matrix over a field $\mathbb{K}$ of rank $n-1$. Then the one-dimensional kernel is generated by*

$$\sum_{i=1}^{n} (-1)^i \det(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n) e_i$$

where e_i denotes the i-th unit vector in $\mathbb{K}^n$.

Proof. Let $A' \in \mathbb{K}^{n \times n}$ be the matrix A extended by the k-th row of A for some $k \in \{1, \dots, n-1\}$, i.e. $A' = (a'_1, \dots, a'_n)$ with $a'_i = \begin{pmatrix} a_i \\ a_{k,i} \end{pmatrix}$ for $a_i = (a_{1,i}, \dots, a_{n-1,i})^T$ and $i = 1, \dots, n$. Then obviously $\det(A') = 0$. Now calculate $\det(A')$ expanding along the last row:

$$0 = \det(A') = \sum_{i=1}^{n} (-1)^{i+n} a_{k,i} \det(A_i) \text{ with } A_i = (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n) \text{ for } i = 1, \dots, n$$

Combining the equations for $k = 1, \dots, n-1$ yields $\sum_{i=1}^{n} a_i (-1)^{i+n} \det(A_i) = 0$ which proves the claim. □

Lemma 1.1 can be generalized to matrices of arbitrary rank. Actually, this formalizes the standard way to solve underdetermined systems of linear equations while avoiding the transformation into triangular form. Some special notation will be necessary.

Definition 1.2. *Let $v = (v_i)_i \in \mathbb{K}^n$ be a vector and $I \subseteq \{1, \dots, n\}$ a set of indices. Then v_I denotes the vector $v_I = (v_i)_{i \in I} \in \mathbb{K}^{\#I}$ where $\#I$ denotes the cardinality of the set I. Also, let $\operatorname{supp}(v) = \{i \in \{1, \dots, n\} : v_i \neq 0\}$ denote the* support *of v.*

Let $A = (a_{i,j})_{i,j} \in \mathbb{K}^{m \times n}$ be a matrix and $I \subseteq \{1, \dots, m\}$, $J \subseteq \{1, \dots, n\}$ be sets of indices. Then $A_{I,J}$ denotes the submatrix $A_{I,J} = (a_{i,j})_{i \in I, j \in J} \in \mathbb{K}^{\#I \times \#J}$. Furthermore let

$$\ker_J(A_{I,J}) = \{v \in \mathbb{K}^n : A_{I,J} \cdot v_J = 0, \operatorname{supp}(v) \subseteq J\}.$$

Lemma 1.3. *Let A be an $m \times n$ matrix of rank r over $\mathbb{K}$. Define $\mathcal{B}$ as the set of $r \times (r+1)$ matrices $A_{I,J}$ of rank r with $I \subseteq \{1, \ldots, m\}$, $J \subseteq \{1, \ldots, n\}$. Then* $\ker(A) = \sum_{A_{I,J} \in \mathcal{B}} \ker_J(A_{I,J})$.

Proof. If $m > r$, then there is a $r \times n$ submatrix A' of A with $\ker(A') = \ker(A)$. Thus it suffices to consider the case $m = r$.

In this proof the abbreviation $A_J = A_{\{1,\ldots,r\},J}$ will be used. Consider a quadratic submatrix A_K of A with rank r for some $K \subseteq \{1, \ldots, n\}$. Let $\tilde{\mathcal{B}}$ be the set of $r \times (r+1)$ submatrices A_J of A with $J \supseteq K$. Obviously those A_J have rank r, such that $\tilde{\mathcal{B}} \subseteq \mathcal{B}$. The claim is that $\ker(A) = \sum_{A_J \in \tilde{\mathcal{B}}} \ker_J(A_J)$ which proves the statement.

Clearly $\dim_{\mathbb{K}}(\ker(A)) = n - r$. Since $\#\tilde{\mathcal{B}} = n - r$ and each kernel $\ker_J(A_J)$ is generated by a single nonzero vector $v^{(J)}$, it suffices to show that these vectors are linearly independent. Note $\operatorname{supp}(v^{(J)}) \subseteq J$ and $\#(J \setminus K) = 1$. Thus, if $v_j^{(J)} \neq 0$ for $j \in J \setminus K$ for all $A_J \in \tilde{\mathcal{B}}$, the vectors $\left\{v^{(J)} : A_J \in \tilde{\mathcal{B}}\right\}$ are linearly independent. According to lemma 1.1, $v_j^{(J)} = \det(A_K) \neq 0$ which completes the proof. □

1.2. Rings

The best-known objects in algebra probably are groups and fields. In this thesis, the focus, however, is on rings which are somewhat in between. One could — roughly speaking — describe a ring as group with a second binary operation, the multiplication, or as field without division. The following is a precise definition:

Definition 1.4. *A set R with two binary operations $+ : R \times R \longrightarrow R$ and $\cdot : R \times R \longrightarrow R$ is a* ring *iff*

1. *$(R, +)$ is an Abelian group, i.e.*
   - *a)* $(a + b) + c = a + (b + c)$ *for all* $a, b, c \in R$ (associativity),
   - *b)* $\exists 0 \in R : a + 0 = a = 0 + a$ *for all* $a \in R$ (neutral element),
   - *c)* $\forall a \in R\ \exists (-a) \in R : a + (-a) = 0 = (-a) + a$ (inverse elements),
   - *d)* $a + b = b + a$ *for all* $a, b \in R$ (commutativity),
2. *$(R, \cdot)$ is a commutative monoid, i.e.*
   - *a)* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all* $a, b, c \in R$ (associativity),
   - *b)* $a \cdot 1 = a = 1 \cdot a$ *for all* $a \in R$ (neutral element),
   - *c)* $a \cdot b = b \cdot a$ *for all* $a, b \in R$ (commutativity), *and*
3. $(a + b) \cdot c = a \cdot c + b \cdot c$ *for all* $a, b, c \in R$ (distributivity).

If there are no zero-divisors, *i.e.* $a \cdot b = 0$ *implies* $a = 0$ *or* $b = 0$ *for all* $a, b \in R$, *R is called* domain. *R is said to be* reduced *if* $a^k = 0$ *for any* $k \in \mathbb{N}$ *implies* $a = 0$.

Note that this is not the most general definition of a ring. It might be more exact to call R *commutative ring with 1*. However, since only commutative rings with 1 are treated here, commutativity and neutral elements are included into the definition of a ring in order to make the presentation more succinct.

The elements of rings which are not invertible are usually characterized as representation of irreducible factors. However, this is not possible in all rings.

Definition 1.5. *Let R be a ring and $r \in R$. If there is $r^{-1} \in R$ such that $r^{-1}r = 1$, r is called* invertible *or* unit*. r is called* reducible *if there are non-units $a, b \in R$ such that $r = ab$. Otherwise r is called* irreducible*. $r = a_1 \cdots a_t$ is called* factorization *of r if $a_1, \ldots, a_t \in R$ are irreducible non-units.*

Definition 1.6. *A domain R is called* factorial *or* unique factorization domain *iff each non-unit in $R \setminus \{0\}$ has a unique factorization.*

As usual, the multiplication sign will be omitted as in $ab = a \cdot b$ if the context is clear. The order of evaluation is PEMDAS, i.e. parentheses, exponentiation, multiplication, division, addition, subtraction.

The natural functions on rings are homomorphism which respect the ring operations.

Definition 1.7. *Let Q and R be rings with neutral elements $1_Q \in Q$ and $1_R \in R$ and $\varphi : Q \longrightarrow R$ be a function such that*

1. *$\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in Q$,*
2. *$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ for all $a, b \in Q$, and*
3. *$\varphi(1_Q) = 1_R$.*

Then φ is a (ring) homomorphism*. If φ is injective, it is called* endomorphism *or* embedding*, if it is surjective, it is called* epimorphism*, and, if it is bijective, it is called* isomorphism*.*

Note that usually one would write $1 = 1_R = 1_Q$ since it is clear from the context which neutral element is referred to. Using homomorphisms, one can characterize the subrings of a ring.

Corollary 1.8. *Let R be a ring. Then $Q \subseteq R$ is a ring iff it is image of a (ring) homomorphism, i.e. iff there are a ring P and a homomorphism $\varphi : P \longrightarrow R$ with*

$$Q = \operatorname{im}(\varphi) = \{\varphi(r) : r \in P\}.$$

In this case, Q is called subring *of R.*

Especially when working with polynomials, the concept of gradings will be very important. It represents the ring as direct sum of sets that are assigned to an integer. Gradings play a crucial role in termination proofs and in converting polynomial systems into linear systems.

Definition 1.9. *Let R be a ring. Then $(R_d)_{d\in\mathbb{Z}}$ is a* grading *of R iff the ring equals the (inner) direct sum $R = \ldots \oplus R_{-1} \oplus R_0 \oplus R_1 \oplus \ldots$, i.e. each ring element is a* finite *sum of elements of $\ldots, R_{-1}, R_0, R_1, \ldots$. In this case, the ring R is called* graded.

The elements of R_d are called homogeneous *of* degree *d. By definition, each element $0 \neq r \in R$ can be written as finite sum $r = r_c + \ldots + r_d$ with $c \leq d \in \mathbb{Z}$ and $r_k \in R_k$ for all $k = c, \ldots, d$ and $r_c, r_d \neq 0$ where $\deg(r) = d$ is called the* degree *of r. The elements $r_c, \ldots, c_d$ are called* homogeneous components *of r.*

A set $S \subseteq R$ is called homogeneous *iff $r \in S$ implies $r_k \in S$ for all $k \in \mathbb{Z}$.*

Example 1.10.

1. *The integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ form a factorial domain.*

2. *The sets of the form $k\mathbb{Z} = \{ka : a \in \mathbb{Z}\}$ for $k \geq 2$ are* no *rings since $1 \notin k\mathbb{Z}$.*

3. *The natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ are* no *ring since there are no inverse elements of the positive numbers.*

4. *Any field $\mathbb{K}$ is a factorial domain.*

5. *The integers $\mathbb{Z}$ are a subring of the rational numbers $\mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z}, 0 \neq b \in \mathbb{N}\}$.*

6. *The set of invertible matrices over a field ($A \in \mathbb{K}^{n\times n}$ with $\det(A) \neq 1$ for a fixed $n \geq 2$) is* no *ring (in the above sense) since the multiplication is non-commutative.*

In section 1.5, the ring of polynomials, another prominent example, will be defined and studied in detail.

1.3. Modules

Modules are a generalization of vector spaces. Instead of being field elements, the scalars are elements of a ring. As for rings, only the commutative case will be treated.

Definition 1.11. *Let R be a ring. Then M is a* module *over R iff there are two operations $+ : M \times M \longrightarrow M$ and $\cdot : R \times M \longrightarrow M$ such that*

1. *$(M, +)$ is an Abelian group,*

2. *$a \cdot (b \cdot m) = (a \cdot b) \cdot m$ for all $a, b \in R, m \in M$* (associativity),

3. *$(a + b) \cdot m = a \cdot m + b \cdot m$ for all $a, b \in R, m \in M$* (distributivity),

4. *$a(m + n) = a \cdot m + a \cdot n$ for all $a \in R, m, n \in M$* (distributivity), *and*

5. *$1 \cdot m = m$ for all $m \in M$.*

The natural functions on modules are very similar to ring homomorphisms.

Definition 1.12. *Let M and N be modules over a ring R and $\varphi : M \longrightarrow N$ be a function such that*

1. *$\varphi(m+n) = \varphi(m) + \varphi(n)$ for all $m, n \in M$ and*

2. *$\varphi(r \cdot m) = r\varphi(m)$ for all $r \in R, m \in M$.*

Then φ is a (module) homomorphism.

Corollary 1.13. *Let M be module over a ring R. Then $N \subseteq M$ is a module over R iff it is image of a (module) homomorphism, i.e. iff there are a module L over R and a homomorphism $\varphi : L \longrightarrow M$ with $N = \mathrm{im}(\varphi)$. In this case, N is called R-*submodule *of M.*

An equivalent of the vector space dimension is the module length.

Definition 1.14. *Let M be module over a ring R. Then the* length *of M is the supremum of the lengths of chains of R-modules $M_0 \subsetneq \ldots \subsetneq M_t = M$ and denoted by* $\mathrm{length}_R(M) = t$.

If the ring is clear from the context, $\mathrm{length}(M)$ will be written instead of $\mathrm{length}_R(M)$.

Exact sequences are a very powerful tool in algebra. They are defined as sequences of modules which are connected by homomorphisms with special properties.

Definition 1.15. *Let*

$$M_0 \xrightarrow{\varphi_1} M_1 \xrightarrow{\varphi_2} \ldots \xrightarrow{\varphi_k} M_k$$

be a sequence of homomorphisms φ_i on modules M_i. If $\mathrm{im}(\varphi_{i-1}) = \ker(\varphi_i)$ for all $i = 2, \ldots, k$, the sequence is called exact. *The sequence*

$$0 \longrightarrow M_1 \xrightarrow{\varphi_2} M_2 \xrightarrow{\varphi_3} M_3 \longrightarrow 0$$

is called short sequence. *It is exact iff φ_2 is injective, φ_3 is surjective, and $\mathrm{im}(\varphi_2) = \ker(\varphi_3)$.*

In the context of toric ideals, the following modules will be of particular interest.

Definition 1.16. *Let N be a submodule of M over the ring R. If $r \cdot m \in N$ implies $m \in N$ for all $0 \neq r \in R, m \in M$, N is called* saturated *R-submodule of M.*

Example 1.17.

- *For any ring R, R^n is a R-module with component-wise addition and scalar multiplication.*

- *$\mathbb{Z}\left(1,3,5\right)^T$ and $\mathbb{Z}\left(1,-1,3\right)^T$ are saturated $\mathbb{Z}$-submodules of $\mathbb{Z}^3$.*

- *$N = \mathbb{Z}\left(1,3,5\right)^T + \mathbb{Z}\left(1,-1,3\right)^T$ is not a saturated $\mathbb{Z}$-submodule of $\mathbb{Z}^3$ since $\left(2,2,8\right) \in N$ but $\left(1,1,4\right) \notin N$.*

1.4. Ideals

Ideals are subsets of rings which can be characterized and represented in various ways, the most common of which will be presented here. One could say that ideals are for rings what normal subgroups are for groups. After the definitions, there will be some structure theorems covering both the decomposition of ideals and the construction of new ideals.

Definition 1.18. *A nonempty subset I of a ring R is called* ideal *iff*

1. $a + b \in I$ *for all* $a, b \in I$ *and*

2. $r \cdot a \in I$ *for all* $r \in R, a \in I$.

Corollary 1.19. *Let R be a ring. Then $I \subseteq R$ is an ideal iff I is a R-submodule of R.*

The similarity to normal subgroup becomes obvious in the following characterization.

Corollary 1.20. *Let R be a ring. A subset I of R is an ideal iff it is the kernel of a (ring) homomorphism, i.e. iff there are a ring Q and a homomorphism $\varphi : R \longrightarrow Q$ such that*

$$I = \ker(\varphi) = \{r \in R : \varphi(r) = 0\}.$$

There are two equivalent ways to describe the ideal associated to a set of ring elements — the inner method describes it as span of the elements, the outer method as intersection of all ideals containing the elements. For computations, the inner method with a finite set of generating elements will be preferred.

Definition 1.21. *Let R be a ring and B be a subset of R. Then $\langle B \rangle$ is the smallest ideal containing B, i.e.*

$$\langle B \rangle_R = \bigcap_{\substack{I \text{ ideal} \\ B \subseteq I \subseteq R}} I = \left\{ \sum_{i=1}^{s} a_i b_i : s \in \mathbb{N}, a_i \in R, b_i \in B \text{ for } i = 1, \ldots, s \right\}.$$

If $B = \{b_1, \ldots, b_s\}$ is finite, it is called basis *of $\langle B \rangle_R$. If the ring R is clear from the context, the simpler notation $\langle B \rangle$ will be preferred over $\langle B \rangle_R$.*

There are various possibilities to operate on ideals in order to produce new ideals. The most important ones are listed in the following corollary.

Corollary 1.22. *Let R be a ring and $I, J \subseteq R$ ideals. Then*

1. $I \cap J$ *is an ideal.*

2. $I + J$ *is an ideal.*

3. $I : J = \{a \in R : a \cdot J \subseteq I\}$ *is an ideal, the so-called* ideal quotient *of I and J.*

4. $I : J^\infty = \left\{a \in R : a \cdot J^k \subseteq I \text{ for some } k \in \mathbb{N}\right\}$ *is an ideal, the so-called* saturation *of I w.r.t. J.*

5. $\sqrt{I} = \left\{a \in R : a^k \in I \text{ for some } k \in \mathbb{Z}\right\}$ *is an ideal, the so-called* radical *of I.*

The union of two ideals is, in general, no ideal.

Example 1.23. *Let $I = \langle x \rangle$ and $J = \langle y \rangle$ be ideals in the ring $\mathbb{K}[x, y]$. Then $I \cup J$ is no ideal since $x, y \in I \cup J$ but $x + y \notin I \cup J$.*

There are some classes of ideals worth mentioning. Some of these can be viewed as elementary ideals into which one can decompose other ideals (compare with simple groups). Others have special properties which make computations easier as will be seen in the main parts of the thesis.

Definition 1.24. *Let R be a ring and $I \subseteq R$ be an ideal.*

1. *I is called* radical *iff $I = \sqrt{I}$.*
2. *I is called* maximal *iff $I \neq R$ and there is no ideal $I \subsetneq J \subsetneq R$.*
3. *I is called* prime *iff $I \neq R$ and $a \cdot b \in I$ implies $a \in I$ or $b \in I$.*
4. *I is called* primary *iff $a \cdot b \in I$ implies $a \in I$ or $b^k \in I$ for some $k \in \mathbb{N}$.*
5. *I is called* principal *iff $I = \langle r \rangle$ for some $r \in R$.*

Moreover the ideals $\{0\}$ and R are called trivial *and all ideals $\{0\} \subsetneq I \subsetneq R$ are called* proper.

The following corollary explains the hierarchy of radical, primary, prime, and maximal ideals and connects the ideal classes with the properties of their factor rings.

Corollary 1.25. *Let I be an ideal in the ring R.*

1. *If I is maximal, it is prime, primary and radical.*
2. *If I is prime, it is primary and radical.*
3. *If I is primary, $\sqrt{I}$ is prime.*
4. *Let R be a domain. Then R/I is a field iff I is maximal and R/I is a domain iff I is prime.*

As mentioned before, finite generating sets are very important for computations. Most of the theory therefore restricts to rings in which all ideals have a basis.

Definition 1.26. *A ring R is called* Noetherian *iff each ideal $I \subseteq R$ has a basis.*

The use of this property will be demonstrated by the following lemma.

Lemma 1.27. *Let I be a ideal in a Noetherian ring R. Then $\sqrt{I}^k \subseteq I$ for some $k \in \mathbb{N}$.*

Proof. Since R is Noetherian, $\sqrt{I}$ has a basis $B = \{b_1, \ldots, b_s\}$. By the definition of the radical, $b_i^{k_i} \in I$ for each $i = 1, \ldots, s$ and some $k_i \in \mathbb{N}$. Thus $\sqrt{I}^k \subseteq I$ for $k = \sum_{i=1}^{s} (k_i - 1) + 1$. □

Given an ideal, it is desirable to decompose it into simpler parts. These simpler parts turn out to be primary ideals. Their radicals (which are prime ideals by corollary 1.25) play a vital role in connection with zero-divisors of the factor ring and thus deserve special treatment.

Lemma 1.28. *Let I be an ideal in a Noetherian ring R. Then there is a minimal* primary decomposition *of I, i.e. there are primary ideals $Q_1, \ldots, Q_t$ such that*

1. *$I = Q_1 \cap \ldots \cap Q_t$ and*

2. *t is minimal.*

This decomposition also fulfills:

3. *The intersection is* irredundant, *i.e. $I \subsetneq Q_1 \cap \ldots \cap Q_{k-1} \cap Q_{k+1} \cap \ldots \cap Q_t$ for all $k = 1, \ldots, t$.*

4. *The prime ideals $\sqrt{Q_1}, \ldots, \sqrt{Q_t}$ are pairwise distinct.*

Proof. See [9], §4.7. □

This primary decomposition is not necessarily unique.

Corollary 1.29. *Let I be an ideal in a Noetherian ring R with a minimal primary decomposition $I = Q_1 \cap \ldots \cap Q_t$. Then a (not necessarily minimal) prime decomposition of the radical is given by $\sqrt{I} = \sqrt{Q_1} \cap \ldots \cap \sqrt{Q_t}$.*

Example 1.30. *(from [9], §4.7) Let $I = \langle x^2, xy \rangle$ be an ideal in the ring $\mathbb{K}[x, y]$. Then $I = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle$ and $I = \langle x \rangle \cap \langle x^2, y \rangle$ are two distinct minimal primary decompositions. Applying the radical yields the redundant prime decomposition $\sqrt{I} = \langle x \rangle \cap \langle x, y \rangle$.*

Lemma 1.31. *Let I and J be ideals in a Noetherian ring R. If $I = Q_1 \cap \ldots \cap Q_t$ is a primary decomposition of I, then*

$$I : J^\infty = \bigcap_{\substack{i=1 \\ J \not\subseteq \sqrt{Q_i}}}^{t} Q_i.$$

Proof. First let $f \in I : J^\infty$ and consider any Q_i with $J \not\subseteq \sqrt{Q_i}$ for $i \in \{1, \ldots, t\}$. Then $f \cdot J^k \subseteq I \subseteq Q_i$ for some $k \in \mathbb{N}$. Since Q_i is primary, $f \in Q_i$ follows.

Now assume $f \in \bigcap_{J \not\subseteq \sqrt{Q_i}} Q_i$ and choose $k \in \mathbb{N}$ such that $J^k \subseteq Q_i$ for all $i = 1, \ldots, t$ with $J \subseteq \sqrt{Q_i}$. Then $f \cdot J^k \subseteq I$ and thus $f \in I : J^\infty$. □

Definition 1.32. *Let M be a module over a ring R. Then the* annihilator *of an element $m \in M$ is the ideal*

$$\operatorname{ann}_R(m) = \{r \in R : rm = 0\}.$$

Definition 1.33. *Let M be a module over a ring R. Then*

$$\operatorname{ass}_R(M) = \{P \subseteq R : P \textit{ prime ideal}, P = \operatorname{ann}_R(m) \textit{ for some } 0 \neq m \in M\}$$

is the set of associated primes *of M.*

If I is an ideal in R, it is common to write $\operatorname{ass}_R(I) = \operatorname{ass}_R(R/I)$ and call the elements *associated primes* of I. In this context, $\operatorname{ann}_R(r) = I : r$ for all $r \in R/I$.

First note that primary ideals have exactly one associated prime.

Lemma 1.34. *Let Q be a primary ideal in a Noetherian ring R and $\{0\} \neq M \subseteq R/Q$ a non-empty submodule. Then $\operatorname{ass}_R(M) = \{\sqrt{Q}\}$.*

Proof. Choose $0 \neq m \in M$. Viewing m as element of R, $\operatorname{ann}_R(m) \cdot m \subseteq Q$ implies together with Q primary and $m \notin Q$ that $\operatorname{ann}_R(m) \subseteq \sqrt{Q}$. On the other hand $Q \cdot m \subseteq Q$ and hence $Q \subseteq \operatorname{ann}_R(m)$. Thus, if $\operatorname{ann}_R(m)$ is prime, $\operatorname{ann}_R(m) = \sqrt{Q}$ and therefore $\operatorname{ass}_R(M) \subseteq \{\sqrt{Q}\}$.

For the converse inclusion, again choose $0 \neq m \in M$, assume $\sqrt{Q} \cdot m \neq 0$, and let $\{b_1, \ldots, b_s\}$ be a basis of $\sqrt{Q}$. Then there is some b_k for $k \in \{1, \ldots, s\}$ such that $b_k m \notin Q$. Since $b_i^{e_i} \in Q$ for some $e_i \in \mathbb{N}$ and each $i = 1, \ldots, s$, by induction there is a multiple n of m with $n \neq 0$ and $\sqrt{Q} \cdot n = 0$ which proves $\sqrt{Q} \subseteq \operatorname{ann}_R(n)$. By the above, $\operatorname{ann}_R(n) = \sqrt{Q}$ and thus $\operatorname{ass}_R(M) = \sqrt{Q}$. □

Lemma 1.35. *Let I be an ideal in a Noetherian domain R with a minimal primary decomposition $I = Q_1 \cap \ldots \cap Q_t$. Then $\operatorname{ass}_R(I) = \{\sqrt{Q_1}, \ldots, \sqrt{Q_t}\}$.*

Proof. (from [13], §3.1 - §3.3) Given a minimal primary decomposition $I = Q_1 \cap \ldots \cap Q_t$ and $k \in \{1, \ldots, t\}$, let $I_k = \bigcap_{i \neq k} Q_i$. Since the decomposition is irredundant, $I_k/I \neq \{0\}$. Observe $\operatorname{ass}_R(I_k/I) \subseteq \operatorname{ass}_R(R/I)$. By the second isomorphism theorem,

$$I_k/I = I_k/(I_k \cap Q_k) \cong (I_k + Q_k)/Q_k.$$

Since I_k/I is non-empty, so is $(I_k + Q_k)/Q_k$ and lemma 1.34 yields $\operatorname{ass}_R((I_k + Q_k)/Q_k) = \sqrt{Q_k}$. By the isomorphism and $Q_k \subseteq \sqrt{Q_k}$, $\sqrt{Q_k} \in \operatorname{ass}_R(R/I)$ as desired.

For the converse, let $I = Q_1 \cap \ldots \cap Q_t$ be a primary decomposition and consider the canonical embedding $R/I \longrightarrow M = \bigoplus_{i=1}^t R/Q_i$. By lemma 1.34, $\operatorname{ass}_R(R/Q_i) = \sqrt{Q_i}$ for $i = 1, \ldots, t$. So it suffices to show $\operatorname{ass}_R(R/I) \subseteq \bigcup_{i=1}^t \operatorname{ass}_R(R/Q_i)$. The proof is by induction on t. The case $t = 1$ is trivial, so assume $t > 1$ and $P \in \operatorname{ass}_R(R/I) \setminus \operatorname{ass}_R(R/Q_t)$, i.e. $\operatorname{ann}_R(m) = P$ for some $0 \neq m \in R/I$. Let $n = n_1 \oplus \ldots \oplus n_t \in M$ be the image of m under the embedding. Then $\operatorname{ann}_R(n) = P$ and, since P is prime, $Rn \cong R/P$ is a domain. Thus any non-zero multiple rn for $r \in R$ has the annihilator $\operatorname{ann}_R(rn) = P$ and cannot be contained in (the embedding in M of) R/Q_t. Hence $rn \neq 0$ and $\operatorname{ann}_R(n_t) \supsetneq P$ imply $r(n_1 \oplus \ldots \oplus n_{t-1}) \neq 0$, for all $r \in R$, and therefore $P = \operatorname{ann}_R(n_1 \oplus \ldots \oplus n_{t-1}) \in \bigcup_{i=1}^{t-1} \operatorname{ass}_R(R/Q_i)$. □

The primary decomposition of an ideal also allows to decompose its factor ring.

Lemma 1.36. *Let I be an ideal in a ring R and $I = Q_1 \cap \ldots \cap Q_t$ be a minimal primary decomposition of I. Then*

$$R/I \cong R/Q_1 \oplus \ldots \oplus R/Q_t.$$

Proof. Consider the canonical homomorphisms $R/I \longrightarrow R/Q_i$ for $i = 1, \ldots, t$. These are obviously surjective since $I \subseteq Q_i$ for $i = 1, \ldots, t$. On the other hand, $f - g \in I$ iff $f - g \in Q_i$ for all $i = 1, \ldots, t$ since the primary decomposition is minimal. □

Example 1.37.

- *In the ring of integers, the ideals are exactly the subsets of the form $k\mathbb{Z}$. They are prime ideals iff k is a prime and primary iff k is the power of a prime.*
- $(a\mathbb{Z}) : (b\mathbb{Z}) = \frac{a}{\gcd(a,b)}\mathbb{Z}$.
- *If I is an ideal in the ring R, $I : I = R$ and $I : R = I$.*
- $\sqrt{p_1^{e_1} \cdots p_s^{e_s}\mathbb{Z}} = p_1 \cdots p_s\mathbb{Z}$ *for primes $p_1, \ldots, p_s$ and integral exponents $e_1, \ldots, e_s \geq 1$. The primary decomposition of $p_1^{e_1} \cdots p_s^{e_s}\mathbb{Z}$ is $p_1^{e_1}\mathbb{Z} \cap \cdots \cap p_s^{e_s}\mathbb{Z}$.*
- *A field $\mathbb{K}$ has only two ideals, namely $\{0\}$ and $\mathbb{K}$. This is because all elements but 0 are invertible.*

1.5. Polynomials

Polynomials can be considered as generalization of the linear functions studied in linear algebra. They form a ring which is the prototype of a purely transcendent extension of the coefficient ring. In the following, only polynomials with commuting indeterminates will be considered — just as all rings are assumed to be commutative.

The term polynomial actually is used for two slightly different objects, the abstract polynomial and the induced polynomial function. However it will not be necessary to accentuate this distinction too much for the purposes of this thesis.

Definition 1.38. *Let R be a ring and M be monoid generated by a set B. Then an* (abstract) polynomial *over M is a function*

$$f : M \longrightarrow R, m \mapsto f_m$$

with finite support $\operatorname{supp}(f) = \{m \in M : f_m \neq 0\}$. *The set of all polynomials over M is denoted by $R[M]$ or $R[B]$. It forms a ring with the operations $(f+g)(m) = f(m)+g(m)$ and $(f \cdot g)(m) = \sum_{\substack{m_1,m_2 \in M \\ m_1 m_2 = m}} f(m_1) \cdot g(m_2)$ for all $m \in M$ and $f, g \in R[M]$. Note that, by definition, those sums are finite. The elements of M are called* monomials *and the f_m are called* coefficients.

If there is a grading of the monoid $M = (M_d)_{d \in \mathbb{Z}}$, this induces a grading of $R[M]$ by $R[M]_d = \{f \in R[M] : \operatorname{supp}(f) \subseteq M_d\}$.

The most common polynomials are those over the monoid generated by a set of (algebraically independent) indeterminates $X = \{x_1, \ldots, x_n\}$. In the following, the notion *polynomial* will refer to elements of $R[X]$. All monomials have the form $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for some $\alpha \in \mathbb{N}^n$. Thus any polynomial $f \in R[X]$ can be represented as

$$f = \sum_{\alpha \in \mathbb{N}^n} f_\alpha x^\alpha.$$

Here the sum sign is understood as separator. As mentioned above, any polynomial $f \in R[X]$ induces a function by

$$f : R^n \longrightarrow R, (y_1, \ldots, y_n) \mapsto \sum_{\alpha \in \mathbb{N}^n} f_\alpha y^\alpha.$$

In this case, the sum sign is the operator in R.

The polynomials over the monoid generated by $\left\{x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}\right\}$ are called *Laurent polynomials*. They occur in the study of toric ideals.

This thesis will mainly be concerned with polynomial rings over fields. Still, the definitions will be held general if this causes no extra work. As for notations, for any polynomial $f \in R[M]$, the coefficient of a monomial $m \in M$ will by denoted by f_m.

Definition 1.39. *Let $R[X]$ be a polynomial ring.*

1. *Let $F \subseteq \{x^\alpha \in R[X] : \alpha \in \mathbb{N}^n\}$. Then $\langle F \rangle$ is called* monomial ideal.
2. *Let $F \subseteq \left\{x^\alpha - x^\beta \in R[X] : \alpha, \beta \in \mathbb{N}^n\right\}$. Then $\langle F \rangle$ is called* binomial ideal.

It was already mentioned that finite generating sets of ideals are very important for computations. Thus it is nice to notice that polynomial rings over Noetherian rings are Noetherian, again.

Theorem 1.40 (Hilbert Basis Theorem)**.** *Let R be a* Noetherian *ring. Then $R[X]$ is Noetherian.*

Proof. See [13], §1.4. □

Moreover, factorization in polynomial rings is unique.

Lemma 1.41 (Gauß's Lemma)**.** *Let R be a factorial domain. Then the ring of polynomials $R[X]$ is factorial.*

Proof. See [26], theorem 1.2.13. □

Polynomials in one indeterminate play a special role. There are a couple of neat properties which make handling them about as easy as handling integers. The next few lemmas collect the most important properties. The much more delicate task is to study multivariate polynomials and how these properties generalize or do not generalize. Chapter 2 will be dedicated to the resulting theory.

Lemma 1.42. *Let $\mathbb{K}[x]$ be a ring of polynomials with one indeterminate x over a field $\mathbb{K}$. Then for any $f, g \in \mathbb{K}[x]$ with $g \neq 0$, there are $a, r \in \mathbb{K}[x]$ such that $f = ag + r$ and $\deg(r) < \deg(g)$.*

Proof. Let $f = \sum_{i=0}^{d} f_i x^i$ and $g = \sum_{i=0}^{e} g_i x^i$ with $f_d \neq 0 \neq g_e$. If $d \geq e$, then $f = \frac{f_d}{g_e} x^{d-e} g + r$ for some $r \in \mathbb{K}[x]$ with $\deg(r) < d$. The claim now follows by induction on $\deg(f)$. □

In general, domains that have the property of lemma 1.42 are called *Euclidean*. In these, one can use the Euclidean algorithm for the calculation of the greatest common divisor. Unfortunately, this is not possible for multivariate polynomials.

Lemma 1.43. *Let $\mathbb{K}[x]$ be a ring of polynomials in one variable x over a field $\mathbb{K}$. Then any ideal I is principal.*

Proof. Lemma 1.42 yields $f_{s-1} = af_s + r$. Thus $I = \langle f_1, \ldots, f_{s-2}, f_s, r \rangle$. Since $\deg(r) < \deg(f_s)$, iteration yields $I = \langle f_1, \ldots, f_{s-2}, h, 0 \rangle$ for $h = \gcd(f_{s-1}, f_s)$. By induction on the number of generators, one obtains $I = \langle \gcd(f_1, \ldots, f_s) \rangle$. □

Another consequence of the division algorithm is that, for polynomials over infinite fields, the distinction between abstract polynomials and polynomial functions is unnecessary. This is true for multivariate polynomials as well.

Lemma 1.44. *Let $0 \neq f \in \mathbb{K}[X]$ and $S \subseteq \mathbb{K}$ such that $\#S > \deg(f)$. Then $f(y_1, \ldots, y_n) \neq 0$ for some $(y_1, \ldots, y_n) \in S^n$.*

Proof. The proof is by induction on n. For any $n \geq 1$, consider the polynomial f as element of $\mathbb{K}(x_1, \ldots, x_{n-1})[x_n]$. Since this ring is univariate, lemma 1.42 yields that $(x_n - y_n) \mid f$ iff $f(y_n) = 0$. Since $\#S > \deg(f)$, there must be $y_n \in S$ such that $(x_n - y_n) \nmid f$ and thus $0 \neq f(y_n) \in \mathbb{K}[x_1, \ldots, x_{n-1}]$. By induction, there are $(y_1, \ldots, y_{n-1}) \in S^{n-1}$ such that $f(y_1, \ldots, y_n) \neq 0$. □

Corollary 1.45. *Let $\mathbb{K}$ be an infinite field and $f \in \mathbb{K}[X]$ be a polynomial. Then $f(y_1, \ldots, y_n) = 0$ for all $(y_1, \ldots, y_n) \in \mathbb{K}^n$ iff $f = 0$.*

There is an interesting relationship between ideals in the polynomial ring $R[X]$ and special subsets of R^n. These subsets are the sets of common zeros of the polynomials in the ideals.

Definition 1.46. *Let I be an ideal in $R[X]$. Then the corresponding* variety *is defined by*

$$\boldsymbol{V}_R(I) = \{y \in R^n : f(y) = 0 \, \textit{for all } f \in I\}.$$

Conversely, the ideal which annihilates a variety V is denoted by

$$\boldsymbol{I}_{R[X]}(V) = \{f \in R[X] : f(y) = 0\}.$$

If R and $R[X]$ are clear from the context, the shorter notations $\boldsymbol{V}(I) = \boldsymbol{V}_R(I)$ and $\boldsymbol{I}(V) = \boldsymbol{I}_{R[X]}(V)$ will be preferred.

Many ideal operations can be translated into the language of varieties.

Corollary 1.47. *Let I and J be ideals in $R[X]$. Then*

- *$I \subseteq J$ iff $\mathbf{V}(I) \supseteq \mathbf{V}(J)$,*
- *$\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$, and*
- *$\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$.*

Consider a variety $\mathbf{V}(I)$ generated by an ideal I in $R[X]$. It is obvious that $I \subseteq \mathbf{I}(\mathbf{V}(I))$. If R is reduced, $f^k(y) = 0$ iff $f(y) = 0$ for all $k > 0$ and $y \in R^n$. Thus $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(I))$. Could $\mathbf{I}(\mathbf{V}(I))$ be even larger? The answer is yes and no — depending on R.

Example 1.48. *Consider the radical ideal $I = \langle x^2 + 1 \rangle$ in the ring $\mathbb{Q}[x]$. Since $y^2 + 1 > 0$ for all $y \in \mathbb{Q}$, $\mathbf{V}(I) = \emptyset$ and thus $\mathbf{I}(\mathbf{V}(I)) = \mathbb{Q}[x]$.*

This result would not hold if the field of coefficients $\mathbb{Q}$ was replaced by $\mathbb{C}$. This is generalized by Hilbert's Nullstellensatz.

Theorem 1.49 (Hilbert's Nullstellensatz)**.** *Let I be an ideal in the polynomial ring $\mathbb{K}[X]$ over an algebraically closed field $\mathbb{K}$. Then $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.*

Proof. See [9], §4.1. □

In the following, some nice identities for polynomial ideals will be proved. They make up the foundation for the application of Gröbner bases for the computation of basic ideal operations.

Lemma 1.50 (cf. [30])**.** *Let I and J be ideals in $\mathbb{K}[X]$ generated by polynomials $f_1, \ldots, f_s$ respectively $g_1, \ldots, g_t$. If x_0 is a new indeterminate,*

$$I \cap J = \langle x_0 f_1, \ldots, x_0 f_s, (1 - x_0)g_1, \ldots, (1 - x_0)g_t \rangle \cap \mathbb{K}[X].$$

Proof. Let $f \in I \cap J \subseteq \mathbb{K}[X]$. Then $f = \sum_{i=1}^{s} a_i f_i = \sum_{j=1}^{t} b_j g_j$ for $a_i, b_j \in \mathbb{K}[X]$, $i = 1, \ldots, s$, and $j = 1, \ldots, t$. Hence $f = \sum_{i=1}^{s} a_i x_0 f_i + \sum_{j=1}^{t} b_j (1 - x_0) g_j$.

Conversely, let $f = \sum_{i=1}^{s} a_i x_0 f_i + \sum_{j=1}^{t} b_j (1 - x_0) g_j \in \mathbb{K}[X]$ for $a_i, b_j \in \mathbb{K}[X \cup \{x_0\}]$, $i = 1, \ldots, s$, and $j = 1, \ldots, t$. Substituting x_0 with 0 yields $f = \sum_{j=1}^{t} \tilde{b}_j g_j \in J$ with $\tilde{b}_j \in \mathbb{K}[X]$ for $j = 1, \ldots, t$ and substituting x_0 with 1 yields $f = \sum_{i=1}^{s} \tilde{a}_i f_i \in I$ with $\tilde{a}_i \in \mathbb{K}[X]$ for $i = 1, \ldots, s$. □

Lemma 1.51 (cf. [30])**.** *Let I and J be ideals in $\mathbb{K}[X]$ and assume J is generated by polynomials $f_1, \ldots, f_s$. If x_0 is a new indeterminate and $g = f_1 + x_0 f_2 + \ldots + x_0^{s-1} f_s$, $I : J^\infty = (I : g^\infty) \cap \mathbb{K}[X]$.*

Proof. If $h \in I : J^\infty$, then $f_i^{k_i} h \in I$ for some $k_i \in \mathbb{N}$ and each $i = 1, \ldots, s$. Thus $g^k h \in I$ for $k = \sum_{i=1}^s (k_i - 1) + 1$.

For the opposite direction, assume $h \in I : g^\infty$, i.e. $g^k h \in I$ for some $k \in \mathbb{N}$. Assume $i \in \{1, \ldots, s\}$ is maximal such that $f_i^k h \notin I$. Therefore $0 \equiv g^k h \equiv (f_1 + x_0 f_2 + \ldots + x_0^{i-1} f_i)^k h \bmod I$. Since $h, f_1, \ldots, f_s \in \mathbb{K}[X]$ and $I \subseteq \mathbb{K}[X]$, comparing the coefficients of $x_0^{(i-1)k}$ yields $f_i^k h \in I$ which contradicts the choice of i and proves the claim. □

Lemma 1.52 (Rabinovich Trick, cf. [30]). *Let I be an ideal in $\mathbb{K}[X]$ generated by polynomials $f_1, \ldots, f_s$ and $g \in \mathbb{K}[X]$. If x_0 is a new indeterminate, $I : g^\infty = \langle f_1, \ldots, f_s, 1 - x_0 g\rangle \cap \mathbb{K}[X]$.*

Proof. Let $h \in I : g^\infty$, i.e. $g^k h \in I$. Then

$$h = (1 + x_0 g + \ldots + x_0^{k-1} g^{k-1}) h (1 - x_0 g) + x_0^k g^k h.$$

On the other hand, if $h = \sum_{i=1}^s a_i f_i + b(1 - x_0 g)$ for $a_1, \ldots, a_s, b \in \mathbb{K}[X \cup \{x_0\}]$, one can substitute x_0 with $\frac{1}{g}$ and then multiply with the common denominator. This yields $g^k h = \sum_{i=1}^s \tilde{a}_i f_i$ for some $k \in \mathbb{N}$ and $\tilde{a}_1, \ldots, \tilde{a}_s \in \mathbb{K}[X]$ and thus $h \in I : g^\infty$. □

Example 1.53.

- *Since any field $\mathbb{K}$ is Noetherian, such is $\mathbb{K}[X]$.*
- $\langle x^3 + x^2 + 2x, x^4 - x\rangle = \langle x\rangle \subseteq \mathbb{K}[x]$ *is a principal ideal.*
- $\langle x_1, x_2\rangle \subseteq \mathbb{K}[x_1, x_2]$ *is* not *principal.*

1.6. Localization

Given a ring without zero-divisors, it is possible to make some of its elements invertible. The original ring will be a subset of the new construct.

Definition 1.54. *Let R be a domain and $S \subseteq R$ be a set with $S \cdot S \subseteq S$, $0 \notin S$ and $1 \in S$. Let $R_S = (R \times S)/\!\sim$ be the set of equivalence classes of pairs $(r, s) \in R \times S$ w.r.t. the relation $(r_1, s_1) \sim (r_2, s_2)$ iff $r_1 s_2 = r_2 s_1$ for all $r_1, r_2 \in R$ and $s_1, s_2 \in S$. With addition and multiplication defined by $(r_1, s_1) + (r_2, s_2) = (r_1 s_2 + r_2 s_1, s_1 s_2)$ and $(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$, R_S forms a domain which is called* localization *of R at S. R is embedded into R_S by the homomorphism $\varphi : R \longrightarrow R_S, r \mapsto (r, 1)$. A pair $(r, s) \in R_S$ is also denoted by $\frac{r}{s}$ or $r \cdot s^{-1}$. Moreover, if $(R_d)_{d \in \mathbb{Z}}$ is a grading of R, one can assign degrees to elements of R_S by $\deg(\frac{r}{s}) = \deg(r) - \deg(s)$ for all $r \in R, s \in S$.*

Note that R_S is usually not graded since a decomposition into homogeneous components might not be possible.

Definition 1.55. *Let I be an ideal in a domain R and let R_S be a localization of R. Then I_S denotes the ideal $I_S = I \cdot R_S$ generated by I in R_S.*

Definition 1.56. *If P is a prime ideal in a domain R, $S = R \setminus P$ is multiplicatively closed. The localization R_S is called localization by the prime ideal P. This is often denoted by $R_P = R_S$.*

Lemma 1.57. *Let R be a domain. Then there is a unique minimal field $\mathbb{K} \supseteq R$. It is called the* field of fractions *of R and denoted by $\mathbf{Q}(R) = \mathbb{K}$.*

Proof. Since R has no zero-divisors, $S = R \setminus \{0\}$ is multiplicatively closed and R_S is a domain in which all non-zero elements are invertible. Thus $\mathbb{K} = R_S$ is a field. Since any field containing R must contain the inverse elements of all elements in R, R_S is minimal w.r.t. inclusion and unique (up to isomorphisms). □

On localization of an ideal, the primary components with invertible elements disappear.

Lemma 1.58. *Let I be an ideal in a domain R, $I = Q_1 \cap \ldots \cap Q_t$ be the primary decomposition of I, and consider any localization R_S of R. Then*

$$I_S \cap R = \bigcap_{\substack{i=1 \\ Q_i \cap S = \emptyset}}^{t} Q_i.$$

Proof. Let $r \in I_S \cap R$ and thus $sr \in I$ for some $s \in S$. Let $i = 1, \ldots, t$ such that $Q_i \cap S = \emptyset$. Since S is multiplicatively closed, $s^k \notin Q_i$ for each $k \in \mathbb{N}$. Therefore Q_i primary yields $r \in Q_i$.

Conversely, consider $r \in \bigcap_{Q_i \cap S = \emptyset} Q_i$. For any $i \in \{1, \ldots, t\}$ such that $Q_i \cap S \neq \emptyset$, let $s_i \in Q_i \cap S$. Then $r \cdot \prod_{Q_i \cap S \neq \emptyset} s_i \in I$. Since $\prod_{Q_i \cap S \neq \emptyset} s_i$ is invertible in R_S, $r \in I_S \cap R$. □

Localization can also be used in order to proof the existence of elimination polynomials.

Lemma 1.59. *Let f, g be polynomials in $\mathbb{K}[X]$ with $\gcd(f, g) = 1$. Then $\langle f, g \rangle \cap \mathbb{K}[X \setminus \{x\}] \neq \{0\}$ for each $x \in X$.*

Proof. Choose $x \in X$, let $U = X \setminus \{x\}$, and consider the localization $\mathbb{K}(U)[x]$. First let $h \in \mathbb{K}(U)[x]$ be a common divisor of f and g in $\mathbb{K}(U)[x]$, i.e. $h \mid f$ and $h \mid g$. Then $hs \mid fs$ and $hs' \mid gs'$ in $\mathbb{K}[X]$ for some $s, s' \in \mathbb{K}[U]$. Since $\gcd_{\mathbb{K}[X]}(f, g) = 1$, $h \in \mathbb{K}(U)$ and thus $\gcd_{\mathbb{K}(U)[x]}(f, g) = 1$. Iterated application of lemma 1.42 yields a Bézout relation $af + bg = \gcd_{\mathbb{K}(U)[x]}(f, g) = 1$ with $a, b \in \mathbb{K}(U)[x]$. Multiplying with the common denominator $0 \neq s \in \mathbb{K}[U]$ of the coefficients of a and b, one obtains $0 \neq saf + sbg = s \in \langle f, g \rangle \cap \mathbb{K}[U]$. □

Example 1.60.

- *Let $r \in R$. Then $S = \{1, r, r^2, \ldots\}$ is multiplicatively closed. One writes $R_r = R_S$.*

1.7. Transcendence Degree

This section considers extensions of fields and provides means to measure their size.

Definition 1.61. *Let $\mathbb{L} \supseteq \mathbb{K}$ be fields and $S \subseteq \mathbb{L}$. Then $\mathbb{L}$ is called* field extension *of $\mathbb{K}$. Furthermore*

$$\mathbb{K}(S) = \bigcap_{\mathbb{K} \cup S \subseteq \mathbb{L}' \subseteq \mathbb{L} \text{ field}} \mathbb{L}' = \left\{ \frac{f}{g} \in \mathbb{L} : f, g \in \mathbb{K}[S], g \neq 0 \right\} = \boldsymbol{Q}(\mathbb{K}[S])$$

denotes the field that is obtained by the adjunction *of the elements of S to $\mathbb{K}$. If $\mathbb{L} = \mathbb{K}(S)$ and S is minimal, S is called* transcendence basis *of $\mathbb{L}$ over $\mathbb{K}$.*

The following definitions will be put into a slightly more general context. The objects of interest will be a domain R over a subdomain Q. Then the field of fractions $\mathbf{Q}(R)$ is a field extension of $\mathbf{Q}(Q)$.

Definition 1.62. *Let $Q \subseteq R$ be domains. A set $S \subseteq R$ is called* algebraically independent *over Q iff for any finite subset $\{s_1, \ldots, s_t\} \subseteq S$ and any polynomial $0 \neq h \in Q[x_1, \ldots, x_t]$, $h(s_1, \ldots, s_t) \neq 0$. A set S which is algebraically independent over Q is called* maximal algebraically independent *over Q iff none of the sets $S \subsetneq S' \subseteq R$ is algebraically independent over Q.*

Corollary 1.63. *Let $Q \subseteq R$ be domains. A set $S \subseteq R$ is algebraically independent over Q iff $S \subseteq \boldsymbol{Q}(R)$ is algebraically independent over $\boldsymbol{Q}(Q)$.*

The algebraically independent sets behave as nicely as bases of vector spaces do. Especially, maximal algebraically independent sets all have the same cardinality.

Lemma 1.64. *Let $Q \subseteq R$ be domains. If $B, B' \subseteq R$ are (w.r.t. inclusion) maximal algebraically independent sets over Q and $b' \in B'$, then there is some $b \in B$ such that $(B' \setminus \{b'\}) \cup \{b\}$ is maximal algebraically independent over Q.*

Proof. (from [13], appendix A1) By corollary 1.63, one can assume that Q and R are fields and thus factorial.

Let $B = \{b_1, \ldots, b_r\}$ and $B' = \{b'_1, \ldots, b'_t\}$. By the maximality of B', there are irreducible polynomials $0 \neq f_k \in Q[x_k, y_1, \ldots, y_t]$ such that $f_k(b_k, b'_1, \ldots, b'_t) = 0$ for $k = 1, \ldots, r$. Assume w.l.o.g. $b' = b'_1$. If none of the f_k involves y_1 (i.e. b'_1), $B \cup \{b'_1\}$ is algebraically independent over Q which contradicts the maximality of B. Otherwise there was some irreducible $0 \neq f \in Q[x_1, \ldots, x_r, y_1]$ with $\deg_{y_1}(f) > 0$ and $f(b_1, \ldots, b_r, b'_1) = 0$ and therefore relatively prime to $f_1, \ldots, f_r$ and one could use lemma 1.59 inductively in order to eliminate the variables $x_1, \ldots, x_r$ from $f, f_1, \ldots, f_r$ and obtain a non-zero polynomial in $Q[y_1, \ldots, y_t]$ which vanishes on $b'_1, \ldots, b'_t$. This cannot be happen since B' is algebraically independent over Q.

Thus f_k involves y_1 for some $k \in \{1, \ldots, r\}$. The claim is that $(B' \setminus \{b'_1\}) \cup \{b_k\}$ is maximal algebraically independent over Q. Assume for contradiction that there is some irreducible $0 \neq f \in Q[x_k, y_2, \ldots, y_t]$ with $f(b_k, b'_2, \ldots, b'_t) = 0$. Now lemma 1.59 applied to f and f_k yields a non-zero polynomial in $Q[y_1, \ldots, y_t]$ with $f(b'_1, \ldots, b'_t) = 0$. But this is a contradiction since B' is algebraically independent. The maximality of $(B' \setminus \{b'_1\}) \cup \{b_k\}$ follows from the maximality of B'. □

Definition 1.65. *Let $Q \subseteq R$ be domains. Then the transcendence degree* $\operatorname{trdeg}(R, Q)$ *of R over Q is the supremum of the cardinalities of subsets of R which are algebraically independent over Q. If* $\operatorname{trdeg}(R, Q) = 0$*, the extension is called* algebraic*, otherwise it is called* transcendent.

Lemma 1.66. *Let $Q \subseteq R$ be domains. Then all subsets of R which are maximal algebraically independent over Q have the same cardinality, namely* $\operatorname{trdeg}(R, Q)$.

Proof. (from [13], appendix A1) Let $B \subseteq R$ be maximal algebraically independent over Q with minimal cardinality $\#B$ and assume there is $B' \subseteq R$ maximal algebraically independent over Q with $\#B' < \#B$ and $\#(B \cap B')$ maximal. If $\#(B \cap B') = \#B$, $B = B'$ by the maximality of B which contradicts $\#B' > \#B$. If $\#(B \cap B') < \#B$, choose $b' \in B' \setminus B$. By lemma 1.64, there is some $b \in B$ such that $\tilde{B} = (B' \setminus \{b'\}) \cup \{b\}$ is maximal algebraically independent over Q and $\#(B \cap \tilde{B}) > \#(B \cap B')$. This contradicts the maximality of $\#(B \cap B')$ and finishes the proof. □

This claim even can be strengthened to

Lemma 1.67. *Let $Q \subseteq R$ be domains. Then set $\mathcal{S}$ of algebraically independent sets of R over Q has a* matroid structure*, i.e.*

1. *$\emptyset \in \mathcal{S}$,*
2. *If $S \in \mathcal{S}$ and $S' \subseteq S$ then $S' \in \mathcal{S}$, and*
3. *If $S, S' \in \mathcal{S}$ and $\#S > \#S'$, then there is some $s \in S \setminus S'$ such that $S' \cup \{s\} \in \mathcal{S}$.*

Proof. This follows from lemma 1.64 and [37], §1.2. □

Corollary 1.68. *Let $P \subseteq Q \subseteq R$ be domains. Then* $\operatorname{trdeg}(R, P) = \operatorname{trdeg}(Q, P) + \operatorname{trdeg}(R, Q)$.

Example 1.69. *The field of rational functions $\mathbb{K}(x_1, \ldots, x_n)$ has transcendence degree n.*

2. Polynomial Algebra

2.1. Monomial Orderings

For one indeterminate, there is only one well-ordering of the monomials which is compatible with multiplication, namely $x^k \prec x^l$ iff $k < l$ for all $k, l \in \mathbb{N}$. Having more indeterminates, there are plenty of choices. These will be employed by a couple of applications such that the definition of a monomial ordering has to be kept general. However compatibility with multiplication and well-orderedness are crucial for many proofs and algorithms, e.g. Buchberger's algorithm for computing Gröbner bases.

Definition 2.1. *A total ordering $\prec$ of the monomials is called* admissible *iff*

1. $x^\alpha \prec x^\beta$ *implies* $x^{\alpha+\gamma} \prec x^{\beta+\gamma}$ *for all* $\alpha, \beta, \gamma \in \mathbb{N}^n$ *and*
2. $1 \prec x^\alpha$ *for all* $0 \neq \alpha \in \mathbb{N}^n$.

Definition 2.2. *Given a monomial ordering $\prec$, the largest monomial in the support of a polynomial $f \in R[X]$ is called* leading monomial *and denoted by* $\operatorname{lm}_\prec(f) = \max_\prec(\operatorname{supp}(f))$. *If* $\operatorname{lm}_\prec(f) = x^\alpha$ *for* $\alpha \in \mathbb{N}^n$, $\operatorname{lc}_\prec(f) = f_\alpha$ *is the* leading coefficient *of f and* $\operatorname{lt}_\prec(f) = f_\alpha x^\alpha$ *is the* leading term. *If $I \subseteq R[X]$ is an ideal,* $\operatorname{lm}_\prec(I)$ *denotes the ideal* $\langle \operatorname{lm}(f) : f \in I \rangle$.

If the monomial ordering is fixed, it will be omitted in the notation as in $\operatorname{lm}(f) = \operatorname{lm}_\prec(f)$.

Lemma 2.3. *Let $\prec$ be an admissible monomial ordering. Then $\prec$ is a well-ordering of the monomials, i.e. any set of monomials has a smallest element w.r.t. $\prec$.*

Proof. Consider a set S of monomials in the variables X. This set generates an ideal I in $\mathbb{Q}[X]$. Since this ring is Noetherian, I has a basis $F \subseteq S$. Moreover I is a monomial ideal such that one can assume that F only contains monomials. Since F is finite and $\prec$ is total, the set has a smallest element x^α w.r.t. $\prec$. Since 1 is the smallest monomial and $\prec$ is compatible with multiplication, x^α is the smallest monomial in S. □

If the ring R is ordered, e.g. $R = \mathbb{Z}$ or $R = \mathbb{Q}$, the monomial ordering can be easily extended to polynomials. For terms $ax^\alpha, bx^\beta \in R[X]$ with $a \neq 0 \neq b$, $ax^\alpha \prec bx^\beta$ iff $x^\alpha \prec x^\beta$ or $x^\alpha = x^\beta$ and $a < b$. For non-zero polynomials $f, g \in R[X]$, $f \prec g$ iff $\operatorname{lt}_\prec(f) \prec \operatorname{lt}_\prec(g)$ or $\operatorname{lt}_\prec(f) = \operatorname{lt}_\prec(g)$ and $f - \operatorname{lt}_\prec(f) \prec g - \operatorname{lt}_\prec(g)$. Finally $0 \prec f$ for all non-zero polynomials $0 \neq f \in R[X]$.

If the ring R is not ordered, one can still extend the ordering to the support of polynomials (respectively finite sets of monomials).

Lemma 2.4. *Let $R[X]$ be a polynomial ring and $\prec$ be an admissible ordering. Then there is an induced well-ordering on the finite sets of monomials defined by*

$$M \prec N \Leftrightarrow \max_{\prec}(M \setminus N) \prec \max_{\prec}(N \setminus M) \qquad \textit{for all finite } M, N \subseteq \{x^\alpha \in R[X] : \alpha \in \mathbb{N}^n\}$$

and $\emptyset \prec M$ for all $\emptyset \neq M \subseteq \{x^\alpha \in R[X] : \alpha \in \mathbb{N}^n\}$.

Proof. The ordering $\prec$ on the finite sets of monomials is clearly well-defined and total. To see it is a well-ordering, consider $(M_i)_{i \in I}$ for an arbitrary index set I and finite $M_i \subseteq \{x^\alpha \in R[X] : \alpha \in \mathbb{N}^n\}$ for all $i \in I$. If $M_k = \emptyset$ for some $k \in I$, $M_k = \min_\prec \{M_i : i \in I\}$.

Otherwise, since all sets are finite, there exists $x^{\alpha_i} = \max_\prec(M_i)$ for all $i \in I$. Since $\prec$ is a well-ordering, there is $x^\beta = \min_\prec \{x^{\alpha_i} : i \in I\}$. The proof will be by induction on x^β (w.r.t. $\prec$), the smallest maximal element.

With the notation from above, define $J = \left\{i \in I : \max_\prec(M_i) = x^\beta\right\}$ and $N_i = M_i \setminus \left\{x^\beta\right\}$ for all $i \in J$. By the definition of the induced ordering, $M_j \prec M_i$ for all $j \in J$, $i \in I \setminus J$, and $M_j \prec M_i$ iff $N_j \prec N_i$ for all $i, j \in J$. Thus $M_k = \min_\prec \{M_i : i \in I\}$ iff $N_k = \min_\prec \{N_i : i \in J\}$ for all $k \in I$. The maximal elements of $(N_i)_{i \in J}$, however, are strictly smaller than x^β. Thus, by induction, a minimal set N_k with $k \in J$ exists which implies $M_k = \min_\prec \{M_i : i \in I\}$. □

Example 2.5. *Define an ordering $<_{lex}$ on number vectors by $\alpha <_{lex} \beta$ iff there is a $1 \leq k \leq n$ such that $\alpha_i = \beta_i$ for all $1 \leq i < k$ and $\alpha_k < \beta_k$ for all $\alpha, \beta \in \mathbb{R}^n$. Analogously define $<_{rev}$ by $\alpha <_{rev} \beta$ iff there is a $1 \leq k \leq n$ such that $\alpha_i = \beta_i$ for all $k < i \leq n$ and $\alpha_k > \beta_k$ for all $\alpha, \beta \in \mathbb{R}^n$.*

- *The* lexicographic ordering *$\prec_{lex}$ is defined by $x^\alpha \prec_{lex} x^\beta$ iff $\alpha <_{lex} \beta$. $\prec_{lex}$ is admissible.*
- *The* reverse-lexicographic ordering *$\prec_{rev}$ is defined by $x^\alpha \prec_{rev} x^\beta$ iff $\alpha <_{rev} \beta$. $\prec_{rev}$ is* not *admissible.*
- *The* graded reverse-lexicographic ordering *$\prec_{grl}$ is defined by $x^\alpha \prec_{grl} x^\beta$ iff $\deg(x^\alpha) < \deg(x^\beta)$ or $\deg(x^\alpha) = \deg(x^\beta)$ and $x^\alpha \prec_{rev} x^\beta$. $\prec_{grl}$ is admissible.*
- *A weight matrix $W \in \mathbb{R}^{n \times n}$ represents the monomial ordering $\prec$ defined by $x^\alpha \prec x^\beta$ iff $W\alpha <_{lex} W\beta$ (note $W\alpha, W\beta \in \mathbb{R}^n$).*

2.2. Gröbner Bases

In a univariate polynomial ring, there is a well-known division algorithm which was sketched in lemma 1.42. The generalization to multivariate polynomials is not completely straightforward. Considering a fixed monomial ordering, a first try could be the following definition:

Definition 2.6. *Given a polynomial $h \in \mathbb{K}[X]$ and a set of polynomials F, h is* reducible *w.r.t. F iff there is a* reductor *$f \in F$ such that $\operatorname{lm}(f) \mid x^\alpha$ for some $x^\alpha \in \operatorname{supp}(h)$. Then $h' = h - \frac{h_\alpha x^\alpha}{\operatorname{lt}(f)} f$ is called the* reduct. *The reduction is written as $h \xrightarrow{F} h'$. $\xrightarrow[*]{F}$ is the transitive closure of $\xrightarrow{F}$. Otherwise h is called* irreducible *w.r.t. F.*

Note that this definition is a little more general than in lemma 1.42 since not only the leading term of h can be reduced but any of its terms. Thus, there might be very long reduction sequences where the same term is reduced many times (with some other reductions in between). Still, each sequence of reductions $h = h_0 \xrightarrow{F} h_1 \xrightarrow{F} h_2 \xrightarrow{F} \dots$ terminates after a finite number of steps in an irreducible polynomial. This follows from lemma 2.4 applied to $\{\operatorname{supp}(h_i) : i \in \mathbb{N}\}$.

As noted before, ideals in polynomial rings with several indeterminates are — in general — not principal. Hence a polynomial h might reduce to two different irreducible polynomials, depending on the choice of the reductors. This behavior is obviously unwanted.

Example 2.7. *Consider the basis $F = \{x^2y - 1, xy^2 - x\}$ of an ideal I in the ring $\mathbb{Q}[x, y]$. Then the polynomial $h = x^2y^2 - y$ can be reduced by $h \xrightarrow{x^2y-1} 0$, which proves $h \in I$, or by $h \xrightarrow{xy^2-x} x^2 - y$, which yields an irreducible non-zero reduct.*

Looking at the univariate case, one notices that a division with remainder yields 0 iff the dividend is a multiple of the divisor, i.e. the dividend is an element of the ideal generated by the divisor. For multivariate ideals, the use of special bases is necessary to obtain a similar result:

Definition 2.8. *A basis G of an ideal I over a polynomial ring $\mathbb{K}[X]$ is called* Gröbner basis *iff $\langle \operatorname{lm}(G) \rangle = \operatorname{lm}(I)$.*

Definition 2.9. *Let I be an ideal in $\mathbb{K}[X]$. Then the* normal form *of a polynomial $h \in \mathbb{K}[X]$ w.r.t. the ideal I is defined as the unique polynomial $\operatorname{nf}_I(h) = \min_\prec(h + I)$ where $f \prec g$ iff $\operatorname{supp}(f) \prec \operatorname{supp}(g)$ for all $f, g \in \mathbb{K}[X]$. The set of all normal forms (w.r.t. I) is denoted by $N_I = \{\operatorname{nf}(h) : h \in \mathbb{K}[X]\}$ and also called* complement *of I.*

Note that $\prec$ is a partial ordering of the polynomials. One could define a total ordering if $\mathbb{K}$ was ordered, but this is generally not the case and not needed for the uniqueness of the normal form: assume there are $f, g \in h + I$, $f \neq g$ with $\operatorname{supp}(f) = \operatorname{supp}(g) = \min_\prec(\operatorname{supp}(h + I))$, then $0 \neq f - g \in I$. For $x^\beta = \operatorname{lm}(f - g)$, $f - \frac{f_\beta}{\operatorname{lc}(f-g)}(f - g) \in h + I$ is a polynomial whose support is smaller than $\operatorname{supp}(f) = \operatorname{supp}(g)$ which contradicts the assumption.

Lemma 2.10. *Let G be a Gröbner basis of the ideal I in the polynomial ring $\mathbb{K}[X]$. Then $h \xrightarrow[*]{G} \operatorname{nf}_I(h)$ for all $h \in \mathbb{K}[X]$ and $\operatorname{nf}_I(h)$ is irreducible.*

Proof. Let $h \xrightarrow[*]{G} \tilde{h}$ for some $h, \tilde{h} \in \mathbb{K}[X]$. By definition of the reduction, $\tilde{h} \prec h$ and thus $\mathrm{nf}_I(h)$ is irreducible. Since G is a Gröbner basis, h is reducible w.r.t. G iff it is reducible w.r.t. I. Given any polynomial $h \in \mathbb{K}[X]$ with $h \neq \mathrm{nf}_I(h)$, $h \xrightarrow{I} \mathrm{nf}_I(h)$ and thus h is reducible w.r.t. I and also w.r.t. G. By lemma 2.4, any reduction sequence of h terminates (after a finite number of steps) in an irreducible polynomial, hence $h \xrightarrow[*]{G} \mathrm{nf}_I(h)$. □

Corollary 2.11. *Let I be an ideal in $\mathbb{K}[X]$. Then*

1. $\mathrm{nf}_I(f+g) = \mathrm{nf}_I(f) + \mathrm{nf}_I(g)$ *for all* $f, g \in \mathbb{K}[X]$.
2. $\mathrm{nf}_I(f \cdot g) = \mathrm{nf}_I(\mathrm{nf}_I(f) \cdot \mathrm{nf}_I(g))$ *for all* $f, g \in \mathbb{K}[X]$.
3. $\mathrm{nf}_I(f) = 0$ *iff* $f \in I$.
4. N_I *is a* $\mathbb{K}$*-vector space.*
5. $(N_I, +, *)$ *is a ring with multiplication* $f * g = \mathrm{nf}_I(f \cdot g)$.
6. $I \oplus N_I = \mathbb{K}[X]$.
7. $N_I \cong \mathbb{K}[X]/I$ *as* $\mathbb{K}$*-vector space and as ring.*

Gröbner bases can also be used to define a unique finite representation of an ideal, assuming a monomial ordering was fixed first. Therefore superfluous polynomials in the basis have to be eliminated.

Definition 2.12. *A Gröbner basis G of an ideal I in $\mathbb{K}[X]$ is called* reduced *iff*

1. *each polynomial $g \in G$ is irreducible w.r.t. $G \setminus \{g\}$ and*
2. $\mathrm{lc}(g) = 1$ *for all* $g \in G$.

Lemma 2.13. *Each ideal I in $\mathbb{K}[X]$ has a unique reduced Gröbner basis $G = \{x^\alpha - \mathrm{nf}_I(x^\alpha) \in \mathbb{K}[X] : x^\alpha$ minimally reducible w.r.t. $I\}$. Here $x^\alpha \in \mathbb{K}[X]$ is* minimally reducible *w.r.t. I if it is reducible w.r.t. I but none of its proper divisors is reducible w.r.t. I.*

Proof. First look at $B = \{x^\alpha \in \mathbb{K}[X] : x^\alpha$ minimally reducible w.r.t. $I\}$. For any monomial $x^\alpha \in \mathbb{K}[X]$, $x^\alpha \in \mathrm{lm}(I)$ iff x^α is reducible w.r.t. I. Thus $\langle B \rangle = \mathrm{lm}(I)$ and, since $\mathbb{K}[X]$ is Noetherian, the irredundant basis B is finite.

To show the existence of the Gröbner basis, choose $G = \{x^\alpha - \mathrm{nf}_I(x^\alpha) \in \mathbb{K}[X] : x^\alpha$ minimally reducible w.r.t. $I\}$ as above and note $\langle \mathrm{lm}(G) \rangle = \langle B \rangle = \mathrm{lm}(I)$ and $\#G = \#B < \infty$. Thus G is a Gröbner basis of I. For any $g \in G$, $g - \mathrm{lt}(g)$ is irreducible w.r.t. G and thus g is irreducible w.r.t. $G \setminus \{g\}$. Hence G is reduced.

For uniqueness, consider any reduced Gröbner basis G. By definition, $B = \mathrm{lm}(G)$ and $\#B = \#G$. For any $g \in G$, g is irreducible w.r.t. $G \setminus \{g\}$ and therefore $g - \mathrm{lt}(g)$ is irreducible w.r.t. G. Hence $\mathrm{lt}(g) - g = \mathrm{nf}_G(\mathrm{lt}(g)) = \mathrm{nf}_I(\mathrm{lt}(g))$. □

The unique reduced Gröbner basis of an ideal generated by polynomials F will be denoted by $\mathrm{GB}_{\prec}(F)$ respectively $\mathrm{GB}(F)$ if $\prec$ is fixed.

For the computation of Gröbner bases, Buchberger came up with a criterion for Gröbner bases in [5]. Basically, it says that, if a basis is not a Gröbner basis, this must be due to some non-leading monomials of the basis elements which can become leading monomials by cancellation. The important insight is that it suffices to consider cancellations between two polynomials.

Definition 2.14. *Let $f, g \in \mathbb{K}[X]$. Then the* S-polynomial *of f and g is defined as*

$$\mathrm{S}(f,g) = \frac{\mathrm{lt}(g)}{\gcd(\mathrm{lm}(f), \mathrm{lm}(g))} f - \frac{\mathrm{lt}(f)}{\gcd(\mathrm{lm}(f), \mathrm{lm}(g))} g.$$

Note that the leading terms of $\frac{\mathrm{lt}(g)}{\gcd(\mathrm{lm}(f),\mathrm{lm}(g))} f$ and $\frac{\mathrm{lt}(f)}{\gcd(\mathrm{lm}(f),\mathrm{lm}(g))} g$ are identical and therefore cancel out.

Lemma 2.15. *Let I be an ideal in $\mathbb{K}[X]$, $G = \{g_1, \dots, g_t\}$ a basis of I, and $\prec$ be an admissible monomial ordering. Then G is a Gröbner basis of I w.r.t. $\prec$ iff*

$$\mathrm{S}(g_k, g_l) = \sum_{i=1}^{t} a_i g_i \quad \textit{for some } a_i \in \mathbb{K}[X] \textit{ with } \mathrm{lm}(a_i g_i) \preceq \mathrm{lm}(S(g_k, g_l)) \textit{ and } i, k, l = 1, \dots, t.$$

Proof. See [9], §2.9. □

One of the nice properties of Gröbner basis is that they allow to compute elimination ideals. Here the lexicographic monomial ordering is necessary (actually, this could be slightly generalized).

Theorem 2.16 (Elimination Theorem). *Let I be an ideal in $\mathbb{K}[X]$ and G a Gröbner basis of I w.r.t. to the lexicographic monomial ordering $\prec$ with $x_1 \succ \ldots \succ x_n$. Then $G \cap \mathbb{K}[x_k, \dots, x_n]$ is a Gröbner basis of $I \cap \mathbb{K}[x_k, \dots, x_n]$ for $k = 1, \dots, n$.*

Proof. (cf. [9], §3.1) Obviously $G \cap \mathbb{K}[x_k, \dots, x_n] \subseteq I \cap \mathbb{K}[x_k, \dots, x_n]$. Moreover, a polynomial $f \in \mathbb{K}[X]$ is contained in $\mathbb{K}[x_k, \dots, x_n]$ iff $\mathrm{lm}(f) \in \mathbb{K}[x_k, \dots, x_n]$. Hence

$$\mathrm{lm}(G \cap \mathbb{K}[x_k, \dots, x_n]) = \mathrm{lm}(G) \cap \mathbb{K}[x_k, \dots, x_n] = \mathrm{lm}(I) \cap \mathbb{K}[x_k, \dots, x_n] = \mathrm{lm}(I \cap \mathbb{K}[x_k, \dots, x_n])$$

proves the claim. □

Given a basis of an ideal I in a polynomial ring $\mathbb{K}[X]$ and $U \subseteq X$, the very same basis also generates the localized ideal $I \cdot \mathbb{K}(U)[X \setminus U]$. The converse direction is not as easy and requires the computation of a Gröbner basis.

Lemma 2.17. *Let I be an ideal in ring $\mathbb{K}[X]$, $U \subseteq X$, and $G = \{g_1, \dots, g_t\} \subseteq \mathbb{K}[X]$ a Gröbner w.r.t. a lexicographic monomial ordering $\prec$ such that $u \prec x$ for all $u \in U$, $x \in X \setminus U$. Furthermore let $h_i = \mathrm{lc}(g_i) \in \mathbb{K}[U]$ be the leading coefficient of g_i as polynomial in $\mathbb{K}(U)[X \setminus U]$ for $i = 1, \dots, s$ and $h = \mathrm{lcm}(h_1, \dots, h_t)$. Then $(I \cdot \mathbb{K}(U)[X \setminus U]) \cap \mathbb{K}[X] = \langle g_1, \dots, g_t \rangle : h^{\infty}$.*

Proof. $\langle g_1,\dots,g_t\rangle : h^\infty \subseteq (I\cdot\mathbb{K}(U)[X\setminus U])\cap\mathbb{K}[X]$ is obvious since h is invertible in $\mathbb{K}(U)[X\setminus U]$. For the opposite direction, let $f\in(I\cdot\mathbb{K}(U)[X\setminus U])\cap\mathbb{K}[X]$. Since the leading monomial of any polynomial $g_i\in\mathbb{K}[X]$ w.r.t. $\prec$ equals the leading monomial of g_i as element of $\mathbb{K}(U)[X\setminus U]$ up to a unit of $\mathbb{K}(U)[X\setminus U]$ for $i=1,\dots,t$, G is also a Gröbner basis of $I\cdot\mathbb{K}(U)[X\setminus U]$. Thus, in $\mathbb{K}(U)[X\setminus U]$, f reduces to 0 w.r.t. G. Note that the leading coefficients of $g_1,\dots,g_t$ in $\mathbb{K}(U)[X\setminus U]$ are not invertible in $\mathbb{K}[X]$. But there are $e_1,\dots,e_t\in\mathbb{N}$ such that $h_1^{e_1}\cdots h_t^{e_t}f$ reduces to 0 w.r.t. G in $\mathbb{K}[X]$. □

2.3. Homogenization

Definition 2.18. *Let $f=\sum_{i=0}^d f_i$, $f_d\neq 0$ be the decomposition into homogeneous components of a polynomial f in $R[X]$ and x_0 be a new indeterminate. Then the* homogenization *of f is defined by ${}^h0=0$ and otherwise*

$$ {}^hf = x_0^d f_0 + x_0^{d-1} f_1 + \ldots + f_d. $$

${}^hf$ is homogeneous of degree d in $R[X_0]$ for $X_0=\{x_0,\dots,x_n\}$. Given a set of polynomials S, ${}^hS=\left\{{}^hf : f\in S\right\}$. The converse operation, the substitution of x_0 by 1, is called dehomogenization *and denoted by*

$$ {}^dg(x_1,\dots,x_n)=g(1,x_1,\dots,x_n) \qquad \text{for } g\in R[X_0]. $$

The homogenization of an ideal I in $R[X]$ is denoted by

$$ {}^hI=\left\langle {}^hf : f\in I\right\rangle. $$

Let $f:g^\infty$ denote the saturation of $f\in R[X]$ w.r.t. $g\in R[X]$, i.e. $f:g^\infty=h=\frac{f}{g^k}$ for $f=hg^k$ such that $g\nmid h$, $k\in\mathbb{N}$, and $h\in R[X]$. Then ${}^d({}^hf)=f$ for any polynomial $f\in R[X]$, but ${}^h({}^dg)=g:x_0^\infty$ for a homogeneous polynomial $g\in R[X_0]$. Moreover, all homogeneous polynomials in ${}^hI$ have the form $x_0^k\cdot{}^hf$ with $k\in\mathbb{N}$, $f\in I$.

Of course, the relation of homogenization, ideals, and Gröbner bases is of special interest here. Unfortunately, the homogenization of the basis of an ideal does (in general) not generate the homogenization of the ideal. However, the polynomials in the two ideals are the same up to a power of the new variable.

Example 2.19. *Consider the ideal I in $\mathbb{K}[x,y]$ generated by $F=\{x^2-y,x^2-1\}$. Then $y-1\in I$. Now consider the homogenization of F w.r.t. t, i.e. ${}^hF=\{x^2-yt,x^2-t^2\}$, and let $J=\left\langle{}^hF\right\rangle$. Then $t^k(y-t)\in J$ iff $k\geq 1$.*

Lemma 2.20. *Let $I=\langle f_1,\dots,f_s\rangle$ be an ideal in $R[X]$. Then ${}^hI=\left\langle{}^hf_1,\dots,{}^hf_s\right\rangle:x_0^\infty$.*

Proof. Since both ${}^hI$ and $\left\langle{}^hf_1,\dots,{}^hf_s\right\rangle$ are homogeneous, it suffices to reason about homogeneous polynomials.

If $f\in\left\langle{}^hf_1,\dots,{}^hf_s\right\rangle:x_0^\infty$ is homogeneous, $x_0^kf=\sum_{i=1}^s a_i\cdot{}^hf_i$ for some $k\in\mathbb{N}$ and homogeneous $a_i\in R[X_0]$ for $i=1,\dots,s$. Thus ${}^df={}^d(x_0^kf)=\sum_{i=1}^s{}^da_if_i\in I$. Now ${}^h({}^df)\in{}^hI$ and ${}^h({}^df)\mid f$ imply $f\in{}^hI$.

For the converse, let $f \in {}^hI$ be homogeneous and thus ${}^df = \sum_{i=1}^s a_i f_i \in I$ for some $a_i \in R[X]$ and $i = 1, \dots, s$. Let $d = \max\{\deg(f), \deg(a_i f_i) : i = 1, \dots, s\}$. Hence

$$x_0^{d-\deg(f)} f = x_0^{d-\deg({}^df)} \cdot {}^h({}^df) = \sum_{i=1}^{s} x_0^{d-\deg(a_i f_i)} \cdot {}^ha_i \cdot {}^hf_i$$

and $f \in \left\langle {}^hf_1, \dots, {}^hf_s \right\rangle : x_0^\infty$. □

Before considering Gröbner bases, it is necessary to specify how the monomial ordering should behave on homogenization. It is most desirable that the monomial ordering of the homogenization mirrors the original monomial ordering.

Definition 2.21. *Let $\prec$ be a monomial ordering on $R[X]$ and let $\prec'$ be the graded monomial ordering on $R[X_0]$ defined by $x^\alpha \prec' x^\beta$ for $\alpha, \beta \in \mathbb{N}^{n+1}$ iff $\deg(x^\alpha) < \deg(x^\beta)$ or $\deg(x^\alpha) = \deg(x^\beta)$ and ${}^dx^\alpha \prec {}^dx^\beta$. Then $\prec'$ is called the* homogenization *of $\prec$ and also denoted by $\prec$.*

Unless explicitly mentioned, the homogenization of the fixed monomial ordering on $R[X]$ will be used in $R[X_0]$.

Corollary 2.22. *Let $\prec$ be an admissible monomial ordering on $R[X]$. Then its homogenization $\prec$ on $R[X_0]$ is admissible and ${}^d\mathrm{lm}(f) = \mathrm{lm}({}^df)$ for all homogeneous $f \in R[X_0]$.*

Lemma 2.23. *Let I be an ideal in $R[X]$ and fix an admissible monomial ordering. Then $\mathrm{lm}(I) = \mathrm{lm}({}^hI) : x_0^\infty$.*

Proof. $f \in I$ iff ${}^hf \in {}^hI$. Now $\mathrm{lm}({}^hf) = x_0^k \cdot \mathrm{lm}(f)$ for some $k \geq 0$ by corollary 2.22, which proves the claim. □

Lemma 2.24. *Let $I = \langle f_1, \dots, f_s \rangle$ be an ideal in $R[X]$ and $\prec$ be a monomial ordering on $R[X]$. Then any homogeneous Gröbner basis G of $J = \left\langle {}^hf_1, \dots, {}^hf_s \right\rangle$ w.r.t. the homogenization of $\prec$ yields a Gröbner basis ${}^dG$ of I.*

Proof. By lemma 2.20, ${}^dG \subseteq {}^dJ \subseteq I$. Since J is homogeneous, it suffices to consider homogeneous polynomials and corollary 2.22 implies ${}^d\mathrm{lm}(J) = \mathrm{lm}({}^dJ)$. Thus

$$\mathrm{lm}(I) = \mathrm{lm}({}^d(J : x_0^\infty)) = \mathrm{lm}({}^dJ) = {}^d\mathrm{lm}(J) = {}^d\langle \mathrm{lm}(G) \rangle = \left\langle \mathrm{lm}({}^dG) \right\rangle.$$

□

Note that applying the above lemma to a reduced Gröbner basis of J does not necessarily generate a reduced Gröbner basis of I.

Example 2.25. *Consider the ideal $I = \langle x^3 - x, x^2 - y^3 \rangle$ w.r.t. the lexicographic monomial ordering with $x \succ y$. The reduced Gröbner basis of $\left\langle x^3 - xt^2, x^2t - y^3 \right\rangle$ is given by $G = \{x^3 - xt^2, x^2t - y^3, xy^3 - xt^3, y^6 - y^2t^4\}$ which dehomogenizes to ${}^dG = \{x^3 - x, x^2 - y^3, xy^3 - x, y^6 - y^2\}$. While ${}^dG$ is a Gröbner basis of I, $x^3 - x$ is superfluous and thus ${}^dG$ is not reduced.*

Many ideal classes are stable under homogenization.

Corollary 2.26. *Let I be an ideal in $R[X]$.*

1. *I is radical iff ${}^hI$ is radical.*
2. *I is prime iff ${}^hI$ is prime.*
3. *I is primary iff ${}^hI$ is primary.*
4. *I is principal iff ${}^hI$ is principal.*

Example 2.27.

1. *Let $f_1, \dots, f_s$ be homogeneous polynomials in $R[X]$. Then $I = \langle f_1, \dots, f_s \rangle$ is a homogeneous set.*
2. *The reduced Gröbner basis of a homogeneous ideal I in $\mathbb{K}[X]$ contains only homogeneous polynomials.*
3. *Let I be a homogeneous ideal and f be a homogeneous polynomial in $\mathbb{K}[X]$. Then all reducts of f w.r.t. I according to definition 2.6 (especially $\mathrm{nf}_I(f)$) are homogeneous of the same degree.*
4. *If I is a homogeneous ideal in $R[X]$, the grading of $R[X]$ induces a grading of the quotient ring $R[X]/I = \bigoplus_{d \in \mathbb{N}} (R[X]_d + I)/I \cong \bigoplus_{d \in \mathbb{N}} R[X]_d/I_d$. The last congruence holds since the map $R[X]_d/I_d \longrightarrow (R[X]_d + I)/I$ has a zero kernel for any $d \in \mathbb{N}$.*

2.4. Hilbert Function, Hilbert Polynomial, and Hilbert Series

The idea behind the Hilbert function is to make a quantitative analysis of an ideal using linear algebra, especially the vector space dimension. Since the ring $\mathbb{K}[X]$ is infinite-dimensional, it is necessary to cut the ideal into slices. The canonical way is to use the grading induced by the degrees of the polynomials. For inhomogeneous ideal, however, some care has to be taken.

Let T be a linear subspace of $\mathbb{K}[X]$. Then the elements of degree at most z are given by

$$T_{\leq z} = \{f \in T : \deg(f) \leq z\}.$$

The degree of freedom in degree exactly z then can be measured by the dimension of $T_z = T_{\leq z}/T_{\leq z-1}$. With these definitions, the vector space T is isomorphic to the (inner) direct sum

$$T \cong T_0 \oplus T_1 \oplus T_2 \oplus \dots.$$

Remember that only finite sums belong to the space spanned by this infinite direct sum. For a homogeneous vector space T, the definition can be slightly simplified since T_z is isomorphic to $T_z \cong \{f \in T : f \text{ homogeneous}, \deg(f) = z\} \cup \{0\}$.

Definition 2.28. *Let $T \subseteq \mathbb{K}[X]$ be a $\mathbb{K}$-vector space. Then*

$$\mathrm{HF}_T(z) = \dim_{\mathbb{K}}(T_z)$$

is the Hilbert function *of T and*

$$^{\mathrm{a}}\mathrm{HF}_T(z) = \dim_{\mathbb{K}}(T_{\leq z})$$

is the affine Hilbert function *of T.*

Note that this the definition of HF_T works not only for homogeneous case and sometimes allows to unify the results. Actually, using one or the other Hilbert function barely matters:

Corollary 2.29. *Let $T \subseteq \mathbb{K}[X]$ be a $\mathbb{K}$-vector space. Then $\mathrm{HF}_T(z) = {}^{\mathrm{a}}\mathrm{HF}_T(z) - {}^{\mathrm{a}}\mathrm{HF}_T(z-1)$ for all $z \in \mathbb{N}$.*

So all values of HF_T can be computed from $^{\mathrm{a}}\mathrm{HF}_T$ and all values of $^{\mathrm{a}}\mathrm{HF}_T$ except $^{\mathrm{a}}\mathrm{HF}_T(0)$ can be computed from HF_T.

Lemma 2.30. *Let I be an ideal in $\mathbb{K}[X]$ and fix an admissible monomial ordering. Then there is a polynomial HP_{N_I}, called* Hilbert polynomial, *and some $z_0 \in \mathbb{N}$ such that $\mathrm{HP}_{N_I}(z) = \mathrm{HF}_{N_I}(z)$ for all $z \geq z_0$. The smallest possible value of z_0 is called* (Castelnuovo-Mumford) regularity *of I and denoted by $\mathrm{reg}(I)$.*

Proof. Since $N_I = N_{\mathrm{lm}(I)}$ as $\mathbb{K}$-vector spaces, this follows from [9], §9.2. An independent proof can be derived from the results in section 2.5. □

Analogously there is an affine Hilbert polynomial $^{\mathrm{a}}\mathrm{HP}_{N_I}(z) = {}^{\mathrm{a}}\mathrm{HF}_{N_I}(z)$ for sufficiently large $z \in \mathbb{N}$.

Corollary 2.31. *Let I be an ideal in $\mathbb{K}[X]$ and fix a monomial ordering. Then $\mathrm{HF}_{N_I} = \mathrm{HF}_{N_{\mathrm{lm}(I)}}$.*

Usually, the Hilbert function of the quotient ring $\mathbb{K}[X]/I$ is considered instead of the normal forms N_I. Under certain conditions, this is equivalent. First, one has to think about how to define $(\mathbb{K}[X]/I)_{\leq z}$. There are two possibilities that come to mind: $\mathbb{K}[X]_{\leq z}/I_{\leq z}$ and $(\mathbb{K}[X]_{\leq z}+I)/I$. It turns out that both spaces are isomorphic since $f-g \in I$ for $f, g \in \mathbb{K}[X]_{\leq z}$ iff $f-g \in I_{\leq z}$. Thus it suffices to consider $(\mathbb{K}[X]/I)_{\leq z} = \mathbb{K}[X]_{\leq z}/I_{\leq z}$.

Now compare HP_{N_I} and $\mathrm{HP}_{\mathbb{K}[X]/I}$. The first observation is $(N_I)_{\leq z} \subseteq (\mathbb{K}[X]/I)_{\leq z}$. But in general, both sets differ since f might have lower degree than $\mathrm{nf}_I(f)$. Yet fixing a graded monomial ordering yields $\deg(\mathrm{nf}_I(f)) \leq \deg(f)$ for all $f \in \mathbb{K}[X]$ and thus an isomorphism of $(\mathbb{K}[X]/I)_{\leq z}$ and $(N_I)_{\leq z}$.

Corollary 2.32. *Let I be an ideal in $\mathbb{K}[X]$ and fix a graded admissible monomial ordering $\prec$. Then $\mathrm{HF}_{N_I} = \mathrm{HF}_{\mathbb{K}[X]/I}$ and $\mathrm{HF}_{\mathbb{K}[X]} = \mathrm{HF}_I + \mathrm{HF}_{N_I}$. Thus there is a Hilbert polynomial HP_I which agrees with HF_I for sufficiently large parameters.*

Corollary 2.33. *Let I be an ideal in $\mathbb{K}[X]$ and fix a graded admissible monomial ordering. Then ${}^{a}\mathrm{HF}_{\mathbb{K}[X]/I} = \mathrm{HF}_{\mathbb{K}[X_0]/{}^{h}I}$.*

This corollary shows, that ${}^{a}\mathrm{HF}_{\mathbb{K}[X]/I}$ (respectively $\mathrm{HF}_{\mathbb{K}[X]/I}$) is the same function for any graded admissible monomial ordering.

For a homogeneous ideal I in $\mathbb{K}[X]$, one can replace an arbitrary admissible monomial ordering $\prec$ by the graded admissible monomial ordering $\prec'$ defined by $x^\alpha \prec' x^\beta$ iff $\deg(x^\alpha) < \deg(x^\beta)$ or $\deg(x^\alpha) = \deg(x^\beta)$ and $x^\alpha \prec x^\beta$ for $x^\alpha, x^\beta \in \mathbb{K}[X]$. Then $\mathrm{nf}_{I,\prec'}(f) = \mathrm{nf}_{I,\prec}(f)$ for all homogeneous $f \in \mathbb{K}[X]$ and the Hilbert functions of $N_{I,\prec'}$ and $N_{I,\prec}$ agree. Thus the previous corollary holds for homogeneous ideals and arbitrary admissible monomial orderings.

By lemma 1.36, the Hilbert function of a homogeneous ideal can be computed in parts using a primary decomposition of the ideal.

Corollary 2.34. *Let I be a homogeneous ideal in $\mathbb{K}[X]$ and $I = Q_1 \cap \ldots \cap Q_t$ be a minimal primary decomposition of I. Then*

$$\mathrm{HF}_{\mathbb{K}[X]/I} = \sum_{i=1}^{t} \mathrm{HF}_{\mathbb{K}[X]/Q_i}.$$

Note that the above does not generalize to inhomogeneous ideals with graded monomial orderings straight forward. The projections of an element in $\mathbb{K}[X]/I$ to the rings $\mathbb{K}[X]/Q_i$ might all have lower degree than the element itself.

Example 2.35. *Consider the ideal $I = \langle x_1^2x_2x_4 - x_1x_2x_5 - x_1x_3x_4 + x_3x_5\rangle$ with minimal primary decomposition $I = Q_1 \cap Q_2$ for $Q_1 = \langle x_1x_2 - x_3\rangle$ and $Q_2 = \langle x_1x_4 - x_5\rangle$ in the ring $\mathbb{K}[x_1, \ldots, x_5]$ with the graded reverse lexicographic ordering $\prec$ such that $x_1 \succ \ldots \succ x_n$. Then the polynomial $f = x_1x_2x_4$ is irreducible w.r.t. I, but $\mathrm{nf}_{Q_1}(f) = x_3x_4$ and $\mathrm{nf}_{Q_2}(f) = x_4x_5$ have lower degree.*

Another encoding of the Hilbert function is the Hilbert series. It will be useful for computations with regular sequences.

Definition 2.36. *Let $T \subseteq \mathbb{K}[X]$ be a $\mathbb{K}$-vector space. Then the* Hilbert series *of T is defined as*

$$\mathrm{HS}_T(y) = \sum_{z\geq 0} \mathrm{HF}_T(z)y^z.$$

Analogously

$${}^{a}\mathrm{HS}_T(y) = \sum_{z\geq 0} {}^{a}\mathrm{HF}_T(z)y^z.$$

Example 2.37.

1. *The polynomial ring $\mathbb{K}[X]$ has the Hilbert function*

$$\mathrm{HP}_{\mathbb{K}[X]}(z) = \mathrm{HF}_{\mathbb{K}[X]}(z) = \binom{z+n-1}{n-1}.$$

2. *Fix a graded admissible monomial ordering. Then, for any ideal I in $\mathbb{K}[X]$,* $\mathrm{HF}_I(z) = \mathrm{HP}_I(z)$ *iff* $\mathrm{HF}_{N_I}(z) = \mathrm{HP}_{N_I}(z)$ *for any $z \geq 0$ since $\mathbb{K}[X]_{\leq z} = I_{\leq z} \oplus (N_I)_{\leq z}$.*

3. *Let R, S, T be homogeneous subspaces of $\mathbb{K}[X]$ and*

$$0 \longrightarrow R_z \longrightarrow S_z \longrightarrow T_z \longrightarrow 0$$

be a short exact sequence for each $z \geq 0$. Then

$$\mathrm{HS}_R(y) - \mathrm{HS}_S(y) + \mathrm{HS}_T(y) = 0.$$

2.5. Cone Decompositions

Vector spaces $T \subseteq \mathbb{K}[X]$ that are generated by monomials — like (leading) monomial ideals and sets of normal forms — can be nicely represented on a n-dimensional grid, by marking all dots $\alpha \in \mathbb{N}^n$ which represent a monomial $x^\alpha \in T$. Since T is assumed to be generated by monomials, this representation is a bijection.

For counting dots in the grid respectively the dimension of subspaces of T, a finite representation is desirable. While monomial ideals contain all multiples of their elements, sets of normal forms contain no multiples of monomials which are not normal forms themselves. Thus, it is appropriate to combine the monomials to sets of a monomial and multiples of it. It is necessary to avoid overlaps by specifying the multiples belonging to the set. Otherwise, counting would be hard and sets of normal forms could not even be represented.

In the following, the basic structures and theorems used in [12] are described. This formalizes the idea which was sketched above in a general setting (allowing for certain vector spaces which are not generated by monomials).

Definition 2.38. *Let $h \in \mathbb{K}[X]$ and $U \subseteq X$. Then $C = \mathbf{C}(h, U) = h \cdot \mathbb{K}[U]$ is the* cone *with* point *h. Its* degree *is defined by $\deg(C) = \deg(h)$ and its* dimension *by $\dim(C) = \#U$.*

One of the advantages of working with cones is that their Hilbert functions can be easily calculated.

Corollary 2.39. *Let C be a cone in $\mathbb{K}[X]$. If $\dim(C) = 0$,*

$$\mathrm{HF}_C(z) = \begin{cases} 0 & \text{for } z \neq \deg(C) \\ 1 & \text{for } z = \deg(C) \end{cases},$$

otherwise,

$$\mathrm{HF}_C(z) = \begin{cases} 0 & \text{for } z < \deg(C) \\ \binom{z-\deg(C)+\dim(C)-1}{\dim(C)-1} & \text{for } z \geq \deg(C) \end{cases}.$$

Note that in the above corollary the following definition of the binomial coefficients is used:

$$\mathrm{HP}_C(z) = \binom{z - \deg(C) + \dim(C) - 1}{\dim(C) - 1} = \frac{(z - \deg(C) + \dim(C) - 1) \cdots (z - \deg(C) + 1)}{(\dim(C) - 1) \cdots 1}$$

Definition 2.40. *Let T be a subspace of $\mathbb{K}[X]$. If $T = \mathbf{C}(h_1, U_1) \oplus \ldots \oplus \mathbf{C}(h_t, U_t)$, then $P = \{\mathbf{C}(h_1, U_1), \ldots, \mathbf{C}(h_t, U_t)\}$ is called* cone decomposition *of T. The* degree *of a cone decomposition refers to* $\deg(P) = \max\{\deg(C) : C \in P\}$.

As already seen in the formulas for the Hilbert function of cones, it will be necessary to distinguish cones of dimension 0.

Definition 2.41. *Let P be a cone decomposition. Then $P^+ = \{C \in P : \dim(C) > 0\}$.*

For computations with Hilbert functions, special cone decompositions are necessary.

Definition 2.42. *Let T be a subspace of $\mathbb{K}[X]$. A decomposition $T = T_1 \oplus \ldots \oplus T_t$ is called* degree-compatible *iff $T_{\leq z} = (T_1)_{\leq z} \oplus \ldots \oplus (T_t)_{\leq z}$ for all $z \in \mathbb{N}$. A cone decomposition P of T is called* degree-compatible *iff $T = \bigoplus_{C \in P} C$ is a degree-compatible decomposition.*

Corollary 2.43. *Let T be a subspace of $\mathbb{K}[X]$ and P be a degree-compatible cone decomposition of T. Then $\mathrm{HF}_T = \sum_{C \in P} \mathrm{HF}_C$ and $\mathrm{HP}_T = \sum_{C \in P^+} \mathrm{HP}_C$.*

Definition 2.44. *Let T be a subspace of $\mathbb{K}[X]$ and $P = \{\mathbf{C}(h_1, U_1), \ldots, \mathbf{C}(h_t, U_t)\}$ be a cone decomposition of T. Then P is called* homogeneous *iff $h_1, \ldots, h_t$ are homogeneous.*

Corollary 2.45. *Any homogeneous cone decomposition P of a subspace T of $\mathbb{K}[X]$ is degree-compatible.*

Definition 2.46. *A cone decomposition P is* q-standard *for some $q \in \mathbb{N}$ if*

- *$C \in P^+$ implies $\deg(C) \geq q$ and*
- *for each $C \in P^+$ and each $q \leq d \leq \deg(C)$, there exists a cone $C' \in P$ with degree $\deg(C') = d$ and dimension $\dim(C') \geq \dim(C)$.*

Note that P is q-standard for all $q \in \mathbb{N}$ iff $P^+ = \emptyset$. Otherwise it can be q-standard for at most one q, namely the minimal degree of the cones in P^+. Furthermore, the union of q-standard decompositions is q-standard, again.

Definition 2.47. *Let $C = \mathbf{C}(h, U)$ be a cone in $\mathbb{K}[X]$ with $U = \{u_1, \ldots, u_t\}$. Then the* fan *of the cone C is defined as*

$$\boldsymbol{F}(C) = \{\mathbf{C}(h, \emptyset)\} \cup \{\mathbf{C}(u_i h, \{u_1, \ldots, u_i\} : i = 1, \ldots, t)\}.$$

The fan is a way to split a cone into smaller cones. The direct sum of the cones in the fan represents the original vector space, i.e. $C = \bigoplus_{C' \in \mathbf{F}(C)} C'$. Note that this decomposition is homogeneous if C is homogeneous. The definition of the fan, however, is not unique since it depends on the order of the elements of U. This will not matter in the following.

Lemma 2.48 (Dubé 1990)**.** *Every q-standard cone decomposition P of a vector space T in $\mathbb{K}[X]$ may be refined into a $(q+1)$-standard cone decomposition Q of T with $\deg(P) \leq \deg(Q)$ and $\deg(P^+) \leq \deg(Q^+)$. If P is degree-compatible respectively homogeneous, then Q is also degree-compatible respectively homogeneous.*

Proof. (from [12], lemma 3.1) By the previous remark about fans,

$$Q = \{C \in P : \deg(P) \neq q\} \cup \bigcup_{C \in P, \deg(C) = q} \mathbf{F}(C)$$

is a cone decomposition of the same vector space T. Note that, for any zero-dimensional cone C, $\mathbf{F}(C) = \{C\}$, so actually only the cones of positive dimension and minimal degree q are replaced by their fans. It is easy to see that Q is $(q+1)$-standard and the degree bounds hold obviously. Since, for any cone C, $\mathrm{HF}_C(z) = \sum_{C' \in \mathbf{F}(C)} \mathrm{HF}_{C'}(z)$, Q is degree-compatible if P is. Furthermore, the points of the cones of the fan are monomial multiples of the original point. Thus Q inherits homogeneity and degree-compatibility from P. □

Remember that the set of normal forms is spanned by monomials as vector space. In the following, a cone decomposition of this set shall be computed. Thus one chooses monomials as points of the cones. For any variable, one can split the space of normal forms into two subspaces, namely the multiples of the variable and the polynomials avoiding the variable. Since all monomials (and thus the generators of the space) are in one of both sets, this splitting yields a direct decomposition. Moreover, the cone decomposition of the normal forms will be homogeneous. Last but not least, by avoiding a maximal independent set (i.e. a set of variables of maximal cardinality whose subring has zero intersection with the ideal) when choosing the variable, the cones of higher dimension will obtain smaller degrees making the cone decomposition 0-standard.

In order to avoid computation with arbitrary polynomials, one can employ the fact that the set of normal forms only depends on the leading monomials of an ideal. Thus a Gröbner basis of the leading monomial ideal suffices for the computations. In the following, it will be assumed that the ideal is monomial.

For reading algorithm 1, note that for $F \subseteq \mathbb{K}[X]$ and $g \in \mathbb{K}[X]$, $F : g$ is defined by $\{f : g \in \mathbb{K}[X] : f \in F\}$ where $f : g = \frac{f}{\gcd(f,g)}$ for $f, g \in \mathbb{K}[X]$.

Postpone the proof of termination and correctness for a moment and first prove a central property of the cone decompositions computed by `Split` (algorithm 1).

Lemma 2.49 (Dubé 1990)**.** *Fix any admissible monomial ordering in the polynomial ring $\mathbb{K}[X]$. Let $P = \texttt{Split}(h, U, G)$ for some monomial $h \in \mathbb{K}[X]$, $U \subseteq X$, and a monomial basis G of an ideal $I : h$ in $\mathbb{K}[X]$. If $\mathbf{C}(g, U') \subseteq \mathbf{C}(h, U) \cap N_I$ for some polynomial $g \in \mathbb{K}[X]$ and some $U' \subseteq X$, then $\mathbf{C}(h, S) \in P$ for some $S \subseteq U$ with $\#S \geq \#U'$.*

Algorithm 1: `Split`(h, U, G)

```
Data: $h$ monomial, $U \subseteq X$, $G$ monomial basis of $I : h$
Result: Cone decomposition $P$ of $N_I \cap \mathbf{C}(h, U)$
if $1 \in G$ then return $\emptyset$.
else if $G \cap \mathbb{K}[U] = \emptyset$ then return $\{\mathbf{C}(h, U)\}$.
else
    Choose $S \subseteq U$ with $G \cap \mathbb{K}[S] = \emptyset$ and maximal $\#S$.
    Choose $x_k \in U \setminus S$.
    return Split$(h, U \setminus \{x_k\}, G) \cup$ Split$(x_k h, U, G : x_k)$.
end
```

Proof. (from [12], lemma 4.6) First note that $\mathbf{C}(g, U') \subseteq \mathbf{C}(h, U)$ implies $h \mid g$ and $U' \subseteq U$. Since divisors of irreducible polynomials are in N_I, $\mathbf{C}(h, U') \subseteq \mathbf{C}(h, U) \cap N_I$ and $G \cap \mathbb{K}[U'] = \emptyset$.

The rest of the proof is by induction on $\#(U \setminus U')$. If $U' = U$, $\mathbf{C}(h, U) \in P$ which proves the claim. Otherwise consider $S \subseteq U$ of maximal cardinality such that $G \cap \mathbb{K}[S] = \emptyset$ and $x_k \in U \setminus S$ as in `Split`. Since $\mathbf{C}(h, S) \subseteq \mathbf{C}(h, U \setminus \{x_k\}) \cap N_I$, by induction the recursive call `Split`$(h, U \setminus \{x_k\}, G)$ returns a cone $\mathbf{C}(h, S')$ with $\#S' \geq \#S \geq \#U'$ which proves the claim. □

Lemma 2.50 (Dubé 1990). *Let h be a monomial in $\mathbb{K}[X]$ and fix any admissible monomial ordering. If $U \subseteq X$ and G is a monomial basis of a monomial ideal $I : h$ in $\mathbb{K}[X]$, then $P =$ `Split`(h, U, G) is a homogeneous $\deg(h)$-standard cone decomposition P of $\mathbf{C}(h, U) \cap N_I$.*

Proof. (from [12], §4) First convince yourself of the termination of algorithm 1 and consider the potential $\#U + \sum_{g \in G} \deg(g)$. By the maximality of $\#S$, some element of G contains the variable x_k and thus the potential is reduced in both recursive calls. Since the potential can only obtain integral values and the recursion ends at latest for the potential 0, the termination of `Split` is clear.

In the extreme cases $1 \in G$ and $G \cap \mathbb{K}[U] = \emptyset$, `Split` obviously computes correct cone decompositions of $\mathbf{C}(h, U) \cap N_I$. Otherwise, S and x_k can be chosen as stated and, for any $x_k \in U$, the equality $\mathbf{C}(h, U) \cap N_I = (\mathbf{C}(h, U \setminus \{x_k\}) \cap N_I) \oplus (\mathbf{C}(x_k h, U) \cap N_I$ holds because N_I has a monomial basis. This leads to the two recursive calls in the algorithm. The only thing to note is that $G : x_k = \{g : x_k \in \mathbb{K}[X] : g \in G\}$ is a monomial basis of the ideal $I : x_k$.

The cone decomposition is obviously homogeneous. Thus it remains to show that P is $\deg(h)$-standard. This can be done by induction on the number of recursions. If the recursion terminates, the returned cone decomposition $\emptyset$ respectively $\{\mathbf{C}(h, U)\}$ is obviously $\deg(h)$-standard. Otherwise assume by induction that $P_1 =$ `Split`$(h, U \setminus \{x_k\}, G)$ and $P_2 =$ `Split`$(x_k h, U, G : x_k)$ are $\deg(h)$-standard respectively $(\deg(h) + 1)$-standard cone decompositions. It suffices to show that for each cone $C \in P_2^+$ there is a cone

$C' \in P = P_1 \cup P_2$ with $\deg(C') = \deg(h)$ and $\dim(C') \geq \dim(C)$. The existence of such a cone is proved by lemma 2.49 applied to the cone $C \subseteq \mathbf{C}(h, U) \cap N_I$. □

Example 2.51. *Consider the monomial ideal $I = \langle x^2 \rangle$ in the ring $\mathbb{K}[x, y, z]$ and use `Split` in order to compute a cone decomposition P of N_I. Thus the algorithm has to be called with the parameters `Split`$(1, \{x, y, z\}, \{x^2\})$. Since none of the termination condition holds, the algorithm chooses an independent set $S = \{y, z\}$ of maximal cardinality and $x \in \{x, y, z\} \setminus S$. Then it calls `Split`$(1, \{y, z\}, \{x^2\})$ and `Split`$(x, \{x, y, z\}, \{x\})$. The first call terminates returning $\{\mathbf{C}(1, \{y, z\})\}$. The second call chooses the same independent set S and the variable x and recurses into `Split`$(x, \{y, z\}, \{x\})$ and `Split`$(x^2, \{x, y, z\}, \{1\})$. These both calls terminate returning $\{\mathbf{C}(x, \{y, z\})\}$ respectively $\emptyset$. Collecting the cones along the way yields the cone decomposition $P = \{\mathbf{C}(1, \{y, z\}), \mathbf{C}(x, \{y, z\})\}$ of N_I.*

Dubé found out that more restrictions were needed in order to be able to express the Hilbert functions of cone decompositions nicely. While it was already granted that the cones of small dimensions have rather low degrees, the actual distribution could vary immensely. Since he was interested in a worst case bound, he refined the cone decompositions such that, in each degree, there was only one cone of positive dimension. The resulting cone decomposition obtains the highest degree possible according to the definition of standard cone decompositions.

Definition 2.52. *A q-standard cone decomposition P is q-*exact *if $\deg(C) \neq \deg(C')$ for all $C \neq C' \in P^+$.*

Since q-exact cone decompositions are also q-standard, the cones of higher degrees have lower dimensions, i.e. $C, C' \in P, \deg(C) > \deg(C')$ implies $\dim(C) \leq \dim(C')$.

The computation of exact cone decompositions is pretty easy — simply replace cones which contradict the definition by their fans. The interesting part is the proof of the termination.

Note that algorithm 2 is a reformulation of SHIFT and EXACT in [12] and does essentially the same.

Lemma 2.53 (Dubé 1990). *Every q-standard cone decomposition P of a vector space T in $\mathbb{K}[X]$ may be refined into a q-exact cone decomposition Q of T with $\deg(P) \leq \deg(Q)$ and $\deg(P^+) \leq \deg(Q^+)$. If P is degree-compatible respectively homogeneous, then Q is also degree-compatible respectively homogeneous.*

Proof. (from [12], lemma 6.3) The claim is that `Shift` always terminates and returns a cone decomposition $Q =$ `Shift`(P) with the desired properties. First consider correctness. It is obvious from the code and the definition of the fan that $S = \{C \in Q^+ : \deg(C) = d\}$ after each while-loop. Since no cones with degree smaller than d are added to Q, in the end Q^+ contains at most one cone per degree. Since a cone C with minimal dimension is chosen from S, Q is q-standard at any time by induction. Hence it is q-exact on termination.

Algorithm 2: `Shift`(P)

```
Data: $q$-standard cone decomposition $P$ of $T$
Result: $q$-exact cone decomposition $Q$ of $T$
$Q \leftarrow P$
for $d \leftarrow q, \dots, \deg(Q^+)$ do
    $S \leftarrow \{C \in Q^+ : \deg(C) = d\}$
    while $\#S > 1$ do
        Choose $C \in S$ with minimal dimension $\dim(C)$.
        $S \leftarrow S \setminus \{C\}$
        $Q \leftarrow Q \setminus \{C\} \cup \mathbf{F}(C)$
    end
end
return $Q$.
```

The proof of termination involves a potential function on Q. Let $v \in \mathbb{Z}^n$ be the vector with entries $v_i = \#\{C \in Q^+ : \deg(C) \geq d, \dim(C) = n + 1 - i\} - 1$ for $i = 1, \dots, n$. It counts the number of cones that still have to be processed grouped by their dimensions. Within the for-loop, the first positive entry of v stays the same, as each fan $\mathbf{F}(C)$ contains exactly one cone of dimension $\dim(C)$ and none with higher dimension. When d is increased, the first positive entry of v decreases by 1 since Q is q-standard at any time.

Finally, $\deg(P) \leq \deg(Q)$ and $\deg(P^+) \leq \deg(Q^+)$ are obvious from the construction and Q is degree-compatible respectively homogeneous by the same reasoning as in lemma 2.48. □

Example 2.54. *Start with the cone decomposition $P = \{\mathbf{C}(1, \{y, z\}), \mathbf{C}(x, \{y, z\})\}$ in the ring $\mathbb{K}[x, y, z]$ and try to compute a 2-exact cone decomposition of the same vector space. First note that P is 0-standard as it was computed by `Split`$(1, \{x, y, z\}, \{x^2\})$ in example 2.51. To make it 2-standard, employ lemma 2.48 and replace some of the cones by their fans. With*

$$\begin{aligned} \boldsymbol{F}(\mathbf{C}(1, \{y, z\})) &= \{\mathbf{C}(1, \emptyset), \mathbf{C}(y, \{y\}), \mathbf{C}(z, \{y, z\})\}, \\ \boldsymbol{F}(\mathbf{C}(x, \{y, z\})) &= \{\mathbf{C}(x, \emptyset), \mathbf{C}(xy, \{y\}), \mathbf{C}(xz, \{y, z\})\}, \\ \boldsymbol{F}(\mathbf{C}(y, \{y\})) &= \left\{\mathbf{C}(y, \emptyset), \mathbf{C}(y^2, \{y\})\right\}, \text{ and} \\ \boldsymbol{F}(\mathbf{C}(z, \{y, z\})) &= \left\{\mathbf{C}(z, \emptyset), \mathbf{C}(yz, \{y\}), \mathbf{C}(z^2, \{y, z\})\right\}, \end{aligned}$$

one obtains a 2-standard cone decomposition

$$\begin{aligned} Q = \{&\mathbf{C}(1, \emptyset), \mathbf{C}(x, \emptyset), \mathbf{C}(xy, \{y\}), \mathbf{C}(xz, \{y, z\}), \mathbf{C}(y, \emptyset), \\ &\mathbf{C}(y^2, \{y\}), \mathbf{C}(z, \emptyset), \mathbf{C}(yz, \{y\}), \mathbf{C}(z^2, \{y, z\})\right\} . \end{aligned}$$

Then the desired result is computed by $\tilde{Q}$ = `Shift`(Q). Since it is too large, only the positive *cones are listed here.*

$$\tilde{Q}^+ = \left\{\mathbf{C}(xz, \{y,z\}), \mathbf{C}(z^3, \{y,z\}), \mathbf{C}(y^2z^2, \{y\}), \mathbf{C}(xy^4, \{y\}), \mathbf{C}(y^6, \{y\}), \mathbf{C}(y^6z, \{y\})\right\}$$

2.6. Ideal Dimension

The intuition of the ideal dimension comes from the variety of an ideal $\mathbf{V}(I)$. For a lot of simple examples, it is clear which geometric dimension one would assign to $\mathbf{V}(I)$ (and thus to I). However, an algebraic definition is necessary for computations.

Definition 2.55. *Let R be a ring. Then the* (Krull) dimension $\dim(R)$ *of R is the supremum of the lengths r of chains of prime ideals $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_r$ in R.*

Definition 2.56. *Let R be a ring and $I \subsetneq R$ be an ideal. Then the* (Krull) dimension $\dim(I)$ *of I is defined as the (Krull) dimension of the factor ring $\dim(I) = \dim(R/I)$.*

Corollary 2.57. *Let R be a ring and $I \subseteq J \subsetneq R$ be ideals. Then $\dim(I) \geq \dim(J)$.*

The following corollary uses the fact that prime ideals $P \supseteq I$ correspond to prime ideals $P \subseteq R/I$.

Corollary 2.58. *Let R be a ring and $I \subsetneq R$ be an ideal. Then*

$$\dim(I) = \sup\left\{\dim(P) : I \subseteq P \subseteq R, P \textit{ prime ideal}\right\}.$$

The dimension also can be defined in terms of the transcendence degree of the ring. Since prime ideals are the only ideals whose factor ring is a domain, corollary 2.58 will be used to compute the dimension of arbitrary ideals.

Theorem 2.59. *If R is a reduced, finitely generated domain over a field $\mathbb{K}$, $\dim(R) = \operatorname{trdeg}(R, \mathbb{K})$. Moreover, all (w.r.t. inclusion) maximal chains of prime ideal have length $\dim(R)$.*

Proof. See [13], §13.1. □

Corollary 2.60. *Let R be a reduced, finitely generated domain over a field $\mathbb{K}$ and $P \subsetneq R$ be a prime ideal. Then $\dim(P) = \operatorname{trdeg}(R/P, \mathbb{K})$.*

Another closely related notion is the height of ideals.

Definition 2.61. *Let P be a prime ideal in a ring R. Then the* height $\operatorname{ht}(P)$ *is the number r of strict inclusions in the longest chains of prime ideals $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_r \subseteq P$.*

Definition 2.62. *Let I be an arbitrary ideal in R. Then $\operatorname{ht}(I)$ is the infimum of the heights of the prime ideals containing I, or equivalently (by lemma 1.35) $\operatorname{ht}(I) = \inf\{\operatorname{ht}(P) : P \in \operatorname{ass}(I)\}$.*

Lemma 2.63. *Let R be a reduced, finitely generated domain over a field $\mathbb{K}$ and $I \subsetneq R$ be an ideal. Then $\dim(I) = \dim(R) - \operatorname{ht}(I)$.*

Proof. By corollary 2.58 and the definition of the ideal height, it suffices to prove the lemma for prime ideals.

$R \longrightarrow R/I$ induces a bijection of the prime ideals containing I and the prime ideals in R/I. If I is prime, there are a chain of prime ideals $P_0 \subsetneq \ldots \subsetneq P_{\dim(I)} \subseteq R/I$ in R/I and a chain of prime ideals $P'_0 \subsetneq \ldots \subsetneq P'_{\mathrm{ht}(I)} \subseteq I$. Since these chains are maximal by assumption, $P_0 = \{0\}$ and $P'_{\mathrm{ht}(I)} = I$. This yields a chain of prime ideals $P'_0 \subsetneq \ldots \subsetneq P'_{\mathrm{ht}(I)} = P_0 + I \subsetneq \ldots \subsetneq P_{\dim(I)} + I$ of length $\mathrm{ht}(I) + \dim(I)$ in R. The maximality of the chains in I and in R/I implies the maximality of the chain w.r.t. inclusion in R. Now theorem 2.59 implies $\dim(R) = \mathrm{ht}(I) + \dim(I)$. □

Note that any polynomial ring over a field fulfills the conditions of theorem 2.59 and has a finite dimension. Thus the above lemma holds. Moreover, one can give a slightly easier characterization of the dimension for this special case.

Definition 2.64. *Let I be an ideal in $\mathbb{K}[X]$ and $U \subseteq X$. Then U is called* independent set *w.r.t. I iff $I \cap \mathbb{K}[U] = \{0\}$.*

Lemma 2.65. *Let $I \subsetneq \mathbb{K}[X]$ be an ideal. Then*

$$\dim(I) = \max\{\#U : U \subseteq X, U \textit{ independent set w.r.t. } I\}.$$

Proof. (from [25], lemma 1.3) By corollary 2.58, there is a prime ideal $P \supseteq I$ with $\dim(P) = \dim(I)$. By corollary 2.60 and since X is a transcendence basis of $\mathbb{K}(X)$, there is a subset $U \subseteq X$ of cardinality $\dim(P)$ whose image in $\mathbb{K}[X]/P$ is algebraically independent. Hence U is an independent set w.r.t. $I \subseteq P$ of size $\dim(I)$.

Conversely, let $U \subseteq X$ be independent w.r.t. I. Then $S = \mathbb{K}[U] \setminus \{0\}$ is multiplicatively closed and disjoint to I. Let $I = Q_1 \cap \ldots \cap Q_t$ be a minimal primary decomposition of I. Localization w.r.t. S yields a proper ideal $I_S \subsetneq \mathbb{K}[X]_S$. Thus $(Q_k)_S \neq \mathbb{K}[X]_S$ for some $k = 1, \ldots, t$. Hence $\sqrt{Q_k} \subseteq \mathbb{K}[X] \setminus S$, U is algebraically independent in $\mathbb{K}[X]/\sqrt{Q_k}$, and $\dim(I) \geq \dim(\sqrt{Q_k}) \geq \#U$. □

Unfortunately, the independent sets modulo an arbitrary ideal do not form a matroid structure, as the following example explains.

Example 2.66. *(from [25], example 1.4) Consider the ideal $I = \langle xy, xz \rangle$ in the ring $\mathbb{K}[x, y, z]$. Then $\{x\}$ and $\{y, z\}$ are both maximal independent sets w.r.t. I, but their cardinalities differ.*

The following corollary of lemma 2.65 and Hilbert's Nullstellensatz (theorem 1.49) indicates that the definition of the ideal dimension has a geometric interpretation.

Corollary 2.67. *Let $I \subsetneq \mathbb{K}[X]$ be and ideal. Then $\dim(I) = \dim(\sqrt{I})$.*

This motivates the definition of the dimension of a variety.

Definition 2.68. *Let $V \neq \emptyset$ be a variety in $\mathbb{K}^n$. Then the* dimension *of V is defined as $\dim(V) = \dim(\boldsymbol{I}(V))$.*

Lemma 2.69 (Kredel, Weispfenning 1988)**.** *Let $I \subsetneq \mathbb{K}[X]$ be an ideal and fix an admissible monomial ordering. Then* $\dim(I) = \dim(\mathrm{lm}(I))$.

Proof. (from [25], theorems 1.9 and 2.1, and [16], theorem 3.1) First assume I is prime and choose a (w.r.t. inclusion) maximal independent set U w.r.t. $\mathrm{lm}(I)$. Since I is prime, $\mathbf{Q}(\mathbb{K}[X]/I)$ exists and, since $\mathbb{K}[U] \subseteq N_{\mathrm{lm}(I)} = N_I$, $\mathbb{K}(U) \subseteq \mathbf{Q}(\mathbb{K}[X]/I)$ is a field extension. To make this explicit, note that lemma 1.58 and I prime imply $\mathbf{Q}(\mathbb{K}[X]/I) = \mathbf{Q}(\mathbb{K}(U)[X \setminus U]/(I \cdot \mathbb{K}(U)[X \setminus U]))$. Now look at the ideal $I \cdot \mathbb{K}(U)[X \setminus U]$ in the ring $\mathbb{K}(U)[X \setminus U]$. The leading monomials of this ideal are $\mathrm{lm}(I \cdot \mathbb{K}(U)[X \setminus U]) = \mathrm{lm}(I) : U^\infty$. Since U is maximal, $x^k \in \mathrm{lm}(I) : U^\infty$ for all $x \in X \setminus U$ and some $k \in \mathbb{N}$, $N_{I \cdot \mathbb{K}(U)[X \setminus U]} = N_{\mathrm{lm}(I \cdot \mathbb{K}(U)[X \setminus U])}$ is a finite-dimensional vector space, and

$$\begin{aligned}\dim(I) = \mathrm{trdeg}(\mathbf{Q}(\mathbb{K}[X]/I), \mathbb{K}) = \\ \mathrm{trdeg}(\mathbf{Q}(\mathbb{K}[X]/I), \mathbb{K}(U)) + \mathrm{trdeg}(\mathbf{Q}(\mathbb{K}(U)/\mathbb{K})) = 0 + \dim(\mathrm{lm}(I)).\end{aligned}$$

For arbitrary I, choose a prime ideal $P \supseteq I$ with $\dim(P) = \dim(I)$. Then $\mathrm{lm}(P) \supseteq \mathrm{lm}(I)$ and hence $\dim(\mathrm{lm}(I)) \geq \dim(\mathrm{lm}(P)) = \dim(P) = \dim(I)$ by the above reasoning. The converse inequality follows since U independent w.r.t. $\mathrm{lm}(I)$ implies U independent w.r.t. I. □

Having a couple of neat characterizations of the ideal dimension at hand, turn to the dimension of the homogenization of an ideal next. Since this ideal is contained in a larger ring, the more natural language is the one of the ideal height. This is expected to remain the same on homogenization since the homogenization represents the ideal in a canonical way.

Lemma 2.70. *Let $I \subsetneq \mathbb{K}[X]$ be an ideal. Then* $\mathrm{ht}({}^hI) = \mathrm{ht}(I)$.

Proof. Since $\dim(\mathbb{K}[X_0]) = \dim(\mathbb{K}[X]) + 1$, it is equivalent to prove $\dim({}^hI) = \dim(I) + 1$. Recall that ${}^hI = \mathrm{span}_{\mathbb{K}}\left\{x_0^k \cdot {}^hf : k \geq 0, f \in I\right\}$. Thus U is an independent set w.r.t. I iff $U \cup \{x_0\}$ is an independent set w.r.t. ${}^hI$. □

Note that lemma 2.70 is not true for $I = \mathbb{K}[X]$ even if the height is defined in this case. While $\mathrm{ht}(\mathbb{K}[X]) = n$, $\mathrm{ht}({}^h\mathbb{K}[X]) = \mathrm{ht}(\mathbb{K}[X_0]) = n + 1$.

Another characterization of the ideal dimension uses the Hilbert polynomial.

Lemma 2.71. *Let $I \subsetneq \mathbb{K}[X]$ be an ideal and fix an arbitrary monomial ordering. Then*

$$\dim(I) = \deg(\mathrm{HP}_{N_I}) + 1.$$

Here one defines $\deg(0) = -1$.

Proof. By corollary 2.31 and lemma 2.69, it suffices to show $\dim(\mathrm{lm}(I)) = \deg(\mathrm{HP}_{N_{\mathrm{lm}(I)}}) + 1$. Now $N_{\mathrm{lm}(I)}$ is a finite union of monomial cones by lemma 2.50 and the degree of $\mathrm{HP}_{N_{\mathrm{lm}(I)}}$ equals the largest dimension of the cones. This cone yields an independent set w.r.t. $\mathrm{lm}(I)$

whose cardinality equals the cone dimension. On the other hand, if U is an independent set w.r.t. $\mathrm{lm}(I)$, then $\mathbf{C}(1, U) \subseteq N_{\mathrm{lm}(I)}$. By lemma 2.49, the cone decomposition of $\mathrm{lm}(U)$ contains a cone of dimension at least $\#U$ and the claim follows. □

Lemma 2.72. *Let I be an ideal in $\mathbb{K}[X]$ and $f \in \mathbb{K}[X]$ such that $I + \langle f \rangle \subsetneq \mathbb{K}[X]$. If f is not a zero-divisor in $\mathbb{K}[X]/I$, then* $\dim(I + \langle f \rangle) \leq \dim(I) - 1$. *If I and f are homogeneous, even* $\dim(I + \langle f \rangle) = \dim(I) - 1$.

Proof. (from [27], §5.6) Fix a graded monomial ordering, so, by lemma 2.71 and corollary 2.32, $\dim(I) = \deg(\mathrm{HP}_{\mathbb{K}[X]/I}) + 1$. First note, that $I_{\leq z} + \langle f \rangle_{\leq z} = (I + \langle f \rangle)_{\leq z}$ if I and f are homogeneous and $I_{\leq z} + \langle f \rangle_{\leq z} \subseteq (I + \langle f \rangle)_{\leq z}$ otherwise.

Consider the exact sequence

$$0 \to \ker(m_f)_{\leq z-d} \longrightarrow (\mathbb{K}[X]/I)_{\leq z-d} \xrightarrow{m_f} (\mathbb{K}[X]/I)_{\leq z} \longrightarrow \mathbb{K}[X]_{\leq z}/(I_{\leq z} + \langle f \rangle_{\leq z}) \to 0$$

where m_f denotes the multiplication with f and $d = \deg(f)$. If f is not a zero-divisor in $\mathbb{K}[X]/I$, $\ker(m_f) = \{0\}$ and thus

$$\dim_{\mathbb{K}}(\mathbb{K}[X]_{\leq z}/(I_{\leq z} + \langle f \rangle_{\leq z})) = \dim_{\mathbb{K}} (\mathbb{K}[X]/I)_{\leq z} - \dim_{\mathbb{K}} (\mathbb{K}[X]/I)_{\leq z-d}.$$

Since $\mathrm{HP}_{\mathbb{K}[X]/I}(z) = \dim_{\mathbb{K}} (\mathbb{K}[X]/I)_{\leq z} - \dim_{\mathbb{K}} (\mathbb{K}[X]/I)_{\leq z-1}$, $\dim_{\mathbb{K}}(\mathbb{K}/(I_{\leq z} + \langle f \rangle_{\leq z}))$ agrees with a polynomial of degree $\deg(\mathrm{HP}_{\mathbb{K}[X]/I})$ for sufficiently large z. In the homogeneous case, this yields $\deg(\mathrm{HP}_{\mathbb{K}[X]/(I+\langle f \rangle)}) = \deg(\mathrm{HP}_{\mathbb{K}[X]/I}) - 1$, otherwise $\deg(\mathrm{HP}_{\mathbb{K}[X]/(I+\langle f \rangle)}) \leq \deg(\mathrm{HP}_{\mathbb{K}[X]/I}) - 1$. □

Theorem 2.73 (Krull's Principal Ideal Theorem)**.** *Let $I = \langle f_1, \ldots, f_s \rangle$ be a proper ideal in a ring R. Then* $\mathrm{ht}(I) \leq s$.

Proof. See [13], §10. □

2.7. Regular Sequences

Regular sequences appear in the study of exact sequences like those in lemma 2.72. A regular sequence incrementally defines an ideal such that the no element is a zero-divisor modulo the ideal of the previous generators. Just like in lemma 2.72 many calculations with Hilbert functions and Hilbert polynomials simplify, especially in the homogeneous case.

Definition 2.74. *A sequence $(g_1, \ldots, g_t)$ of polynomials in $R[X]$ is called* regular *iff*

1. *g_k is no zero-divisor in $R[X]/\langle g_1, \ldots, g_{k-1} \rangle$ for $k = 1, \ldots, t$ and*
2. *$\langle g_1, \ldots, g_t \rangle \subsetneq R[X]$.*

The ideal $I = \langle g_1, \ldots, g_t \rangle$ is called complete intersection.

The length of a regular sequences is bounded by the number of indeterminates. This is because lemma 2.72 and theorem 2.73 imply

Corollary 2.75. *Let $(g_1, \dots, g_t)$ be a regular sequence in $\mathbb{K}[X]$ and $J = \langle g_1, \dots, g_t\rangle \subsetneq \mathbb{K}[X]$. Then $\mathrm{ht}(J) = t$. Moreover, any homogeneous sequence $(g_1, \dots, g_t)$ in $\mathbb{K}[X]$ such that $J = \langle g_1, \dots, g_t\rangle \subsetneq \mathbb{K}[X]$ and $\mathrm{ht}(J) = t$ is a regular sequence.*

It is important to memorize that the order of regular sequences is important. This is illustrated by the following example.

Example 2.76. *(from [26], tutorial 33) It will be shown that $(g_1, g_2, g_3) = (x^2 - x, xy - 1, xz)$ is a regular sequence in the ring $\mathbb{K}[x, y, z]$ but its permutation $(g_1', g_2', g_3') = (x^2 - x, xz, xy - 1)$ is not.*

To show the first part, note that the second condition for regular sequences is fulfilled since $\langle x^2 - x, xy - 1, xz\rangle = \langle x - 1, y - 1, z\rangle \subsetneq \mathbb{K}[x, y, z]$. To see the first condition, observe $g_1 = x^2 - x \neq 0$, $\gcd(g_1, g_2) = \gcd(x^2 - x, xy - 1) = 1$, and that $\langle g_1, g_2\rangle = \langle x - 1, y - 1\rangle$ is prime. However, $g_2' = xz$ is a zero-divisor modulo $\langle g_1'\rangle = \langle x^2 - x\rangle$.

This can only happen in the affine case. In the homogeneous setting, regular sequences behave much more nicely.

Lemma 2.77. *Let $(g_1, \dots, g_t)$ be a homogeneous sequence in the polynomial ring $\mathbb{K}[X]$ with degrees $d_1, \dots, d_t$, fix an arbitrary monomial ordering, and let $J = \langle g_1, \dots, g_t\rangle$. Iff $(g_1, \dots, g_t)$ is regular, N_J has the Hilbert series*

$$\mathrm{HS}_{N_J}(y) = \frac{\prod_{i=1}^t (1 - y^{d_i})}{(1 - y)^n}.$$

In this case, its Hilbert function HP_{N_J} only depends on n, t, and $d_1, \dots, d_t$ and the regularity is $\mathrm{reg}(J) = d_1 + \ldots + d_t - n + 1$.

Proof. (from [27], §5.2B and §5.4B) The formula for $\mathrm{HS}_{N_J}(y) = \mathrm{HS}_{\mathbb{K}[X]/J}(y)$ will be proved by induction on t. The base case $t = 0$ follows from the definition of the Hilbert series:

$$\mathrm{HS}_{\mathbb{K}[X]}(y) = \sum_{z \geq 0} \binom{z + n - 1}{n - 1} y^z = \frac{1}{(1 - y)^n}.$$

The second equality can be shown by

$$\frac{1}{z!}\partial_y^z (1 - y)^{-n} \mid_{y=0} = \frac{n \cdot (n + 1) \cdots (n + z - 1)}{z \cdots 1} (1 - y)^{-n-z} \mid_{y=0} = \binom{z + n - 1}{n - 1}.$$

For the induction step, consider the exact sequence

$$0 \to \ker(m_{g_t}) \longrightarrow \mathbb{K}[X]/\langle g_1, \dots, g_{t-1}\rangle \xrightarrow{m_{g_t}} \mathbb{K}[X]/\langle g_1, \dots, g_{t-1}\rangle \longrightarrow \mathbb{K}[X]/\langle g_1, \dots, g_t\rangle \to 0,$$

where m_{g_t} denotes multiplication by g_t. Now use the additivity of the Hilbert series on exact sequences. The factor y^{d_t} appears since m_{g_t} increases the degree by d_t.

$$y^{d_t}\mathrm{HS}_{\ker(m_{g_t})}(y) - y^{d_t}\mathrm{HS}_{\mathbb{K}[X]/\langle g_1,\ldots,g_{t-1}\rangle}(y) + \mathrm{HS}_{\mathbb{K}[X]/\langle g_1,\ldots,g_{t-1}\rangle}(y) - \mathrm{HS}_{\mathbb{K}[X]/\langle g_1,\ldots,g_t\rangle}(y) = 0.$$

If $(g_1,\ldots,g_t)$ is regular, $\mathrm{HS}_{\ker(m_{g_t})} = 0$ and the formula for the Hilbert series follows by solving the equation for $\mathrm{HS}_{\mathbb{K}[X]/\langle g_1,\ldots,g_t\rangle}(y)$ and applying the induction hypothesis. Since $\mathrm{HF}_{N_J}(z)$ is the coefficient of y^z in the series expansion of $\mathrm{HS}_{N_J}(y)$, it only depends on z, n, t, and $d_1,\ldots,d_t$.

For the regularity, define $\mathrm{HS}_f(y) = \sum_{z\geq 0} f(z)y^z$ for a sequence $(f(i))_{i\in\mathbb{N}}$, let $(\Delta f)(y) = f(y) - f(y-1)$ for all $y \in \mathbb{N}$ with $f(z) = 0$ for $z < 0$ and $\Delta^q f = \Delta\Delta^{q-1}f$. Then $\mathrm{HS}_{\Delta f}(y) = (1-y)\mathrm{HS}_f(y)$ for all $y \in \mathbb{N}$ follows. Also let

$$\mathrm{reg}(f) = \min\{k \in \mathbb{N} : \exists h \in \mathbb{Q}[x] : f(y) = h(y) \text{ for all } y \geq k\}.$$

Then $\mathrm{reg}(\Delta f) = \mathrm{reg}(f) + 1$. For $f(z) = \mathrm{HF}_{N_J}(z)$, one obtains $\mathrm{HS}_{\Delta^n f}(y) = \prod_{i=1}^{t}(1-y^{d_i})$ and $\mathrm{reg}(J) = \mathrm{reg}(f) = \mathrm{reg}(\Delta^n f) - n = \deg(\mathrm{HS}_{\Delta^n f}) + 1 - n$ since $(\Delta^n f)(z) = 0$ for $z > \deg(\mathrm{HS}_{\Delta^n f})$.

If $(g_1,\ldots,g_t)$ is not regular, let z be minimal such that $\ker(m_{g_k})_z \neq \{0\}$ for some $1 \leq k \leq t$. Thus $\mathrm{HF}_{\mathbb{K}[X]/\langle g_1,\ldots,g_t\rangle}(z)$ is strictly larger than for a regular sequence and the formula for the Hilbert series does not hold. □

Corollary 2.78. *Let $(g_1,\ldots,g_t)$ be a homogeneous regular sequence in the polynomial ring $\mathbb{K}[X]$. Then, for any permutation σ of $\{1,\ldots,t\}$, $(g_{\sigma(1)},\ldots,g_{\sigma(t)})$ is a regular sequence.*

It is well-known, that most sequences $(g_1,\ldots,g_t)$ of length $t \leq n$ are regular. But there is a result which is even stronger and crucial to later proofs in this thesis. Given an arbitrary ideal I of height r, one can "approximate" I by a regular sequence of length r which is completely contained in the ideal. As nice giveaway, the degrees of the sequence are bounded by the degrees of arbitrary generators of I. The so-called unmixedness theorem is essential for the proof given below.

Theorem 2.79 (Unmixedness Theorem). *Let I be an ideal in $\mathbb{K}[X]$ generated by $\mathrm{ht}(I)$ polynomials. Then $\mathrm{ht}(P) = \mathrm{ht}(I)$ for all associated primes $P \in \mathrm{ass}_{\mathbb{K}[X]}(I)$ of I.*

Proof. See [13], §18.2. □

Lemma 2.80. *Let $\mathbb{K}$ be an infinite field and $I \subsetneq \mathbb{K}[X]$ be an ideal generated by polynomials $f_1,\ldots,f_s$ with degrees $d_1 \geq \ldots \geq d_s$ such that $\mathrm{ht}(I) \geq r$. Then there are an injective map $\sigma : \{1,\ldots,r\} \longrightarrow \{1,\ldots,s\}$ and $a_{k,i} \in \mathbb{K}$ such that*

$$g_k = \sum_{i=\sigma(k)}^{s} a_{k,i}f_i \qquad \textit{for } k = 1,\ldots,r$$

form a regular sequence, and $\deg(g_k) \leq d_{\sigma(k)}$.

Proof. (from [38], lemma 2.2) The proof is by induction on r. The case $r = 0$ is trivial, and for $r = 1$, simply pick $\sigma(1)$ maximal such that $g_1 = f_{\sigma(1)} \neq 0$.

Now let $r > 1$. By induction, there are a regular sequence $(g_1, \ldots, g_{r-1})$ and a map σ on $\{1, \ldots, r-1\}$ of the stated form. Let $J = \langle g_1, \ldots, g_{r-1} \rangle$ and $\operatorname{ass}_{\mathbb{K}[X]}(J) = \{P_1, \ldots, P_t\}$ be the associated primes of J. The Unmixedness Theorem 2.79 implies that all associated primes of J have the same height $r-1$. Consider the vector spaces

$$S_k = \left\{ (b_1, \ldots, b_s) \in \mathbb{K}^s : \sum_{i=1}^{s} b_i f_i \in P_k \right\} \qquad \text{for } k = 1, \ldots, t.$$

These must be proper subspaces since I cannot be contained in an ideal of height $r-1$. Since $\mathbb{K}$ is infinite, also $S_1 \cup \ldots \cup S_t \neq \mathbb{K}^s$, and it is possible to choose

$$(b_1, \ldots, b_s) \in \mathbb{K}^s \setminus (S_1 \cup \ldots \cup S_t) .$$

Thus $h = \sum_{i=1}^{s} b_i f_i \notin P_1 \cup \ldots \cup P_t$. So h is no zero-divisor in $\mathbb{K}[X]/J$ by definition of the associated primes. Furthermore, $\langle g_1, \ldots, g_{r-1}, h \rangle \subseteq I \subsetneq \mathbb{K}[X]$, which implies that $(g_1, \ldots, g_{r-1}, h)$ is a regular sequence.

Now choose $\sigma(r)$ maximal such that there is a polynomial $g_r = \sum_{i=\sigma(r)}^{s} a_{r,i} f_i$ with $a_{r,i} \in \mathbb{K}$ such that $(g_1, \ldots, g_r)$ is a regular sequence. Then $\deg(g_r) \leq d_{\sigma(r)}$. Moreover $a_{r,\sigma(r)} \neq 0$ by maximality of $\sigma(r)$.

It remains to show that (the extended) σ is injective. Assume for contradiction that $\sigma(r) = \sigma(k)$ for some $k = 1, \ldots, r-1$. Let $h = a_{k,\sigma(k)} g_r - a_{r,\sigma(r)} g_k$ and consider the sequence $(g_1, \ldots, g_{r-1}, h)$. Since $h - a_{k,\sigma(k)} g_r \in \langle g_1, \ldots, g_{r-1} \rangle$ and $a_{k,\sigma(k)} \neq 0$ as noted above, this is a regular sequence in I, too. However h is a linear combination of only $f_{\sigma(k)+1}, \ldots, f_s$ which contradicts the maximality of $\sigma(r)$. □

Actually, a homogeneous version of the above will be needed. The statement will be slightly stricter since all permutations of homogeneous regular sequences are regular.

Lemma 2.81. *Let $\mathbb{K}$ be an infinite field and $I \subsetneq \mathbb{K}[X]$ an ideal generated by homogeneous polynomials $f_1, \ldots, f_s$ with degrees $d_1 \geq \ldots \geq d_s$ such that $\operatorname{ht}(I) \geq r$. Then there are a strictly decreasing sequence $s \geq j_1 > \ldots > j_r \geq 1$ and homogeneous $a_{k,i} \in \mathbb{K}[X]$ such that*

$$g_k = \sum_{i=j_k}^{s} a_{k,i} f_i \qquad \textit{for } k = 1, \ldots, r$$

form a homogeneous regular sequence, $\operatorname{ht}\langle f_{j_k}, \ldots, f_s \rangle = k$ and $\deg(g_k) = d_{j_k}$.

Proof. The proof is by induction on r. The case $r = 0$ is trivial, and for $r = 1$, simply pick j_1 maximal such that $g_1 = f_{j_1} \neq 0$. Then $\operatorname{ht}\langle f_{j_1}, \ldots, f_s \rangle = 1$.

Now let $r > 1$. By induction, there is a homogeneous regular sequence $(g_1, \ldots, g_{r-1})$ with $g_k \in I_{j_k} = \langle f_{j_k}, \ldots, f_s \rangle$ for $k = 1, \ldots, r-1$ and $\operatorname{ht}(I_{j_{r-1}}) = r-1$. Thus there exists a maximal $j_r < j_{r-1}$ such that $\operatorname{ht}(I_{j_r}) > r-1$. By lemma 2.72, $\operatorname{ht}(I_{j_r}) = r$. Let

$J = \langle g_1, \dots, g_{r-1} \rangle$ and $\operatorname{ass}_{\mathbb{K}[X]}(J) = \{P_1, \dots, P_t\}$ be the associated primes of J. The Unmixedness Theorem 2.79 implies that all associated primes of J have the same height $r-1$. Let $T = \prod_{i=j_r}^{s} \mathbb{K}^{\binom{d_{j_r}-d_i+n-1}{n-1}}$ the vector space of coefficients of the homogeneous $a_{r,i}$ for $i = j_r, \dots, s$ and consider the subspaces

$$S_k = \left\{ (b_{i,\alpha})_{j_r \le i \le s, |\alpha| = d_{j_r} - d_i} \in T : \sum_{i=j_r}^{s} \left(\sum_{|\alpha| = d_{j_r} - d_i} b_{i,\alpha} x^\alpha \right) f_i \in P_k \right\} \qquad \text{for } k = 1, \dots, t.$$

These must be proper subspaces since I_{j_r} cannot be contained in an ideal of height $r-1$. Since $\mathbb{K}$ is infinite, also $S_1 \cup \ldots \cup S_t \neq T$, and it is possible to choose

$$(b_{i,\alpha})_{i,\alpha} \in T \setminus (S_1 \cup \ldots \cup S_t)\,.$$

Thus $a_{r,i} = \sum_{|\alpha| = d_r - d_i} b_{i,\alpha} x^\alpha$ for $i = j_r, \dots, s$ and $g_r = \sum_{i=j_r}^{s} a_{r,i} f_i$ define a homogeneous polynomial $g_r \notin P_1 \cup \ldots \cup P_t$. So g_r is no zero-divisor in $\mathbb{K}[X]/J$ by definition of the associated primes. Furthermore, $\langle g_1, \dots, g_r \rangle \subseteq I \subsetneq \mathbb{K}[X]$, which implies that $(g_1, \dots, g_r)$ is a regular sequence of the desired form. □

These lemmas will be sufficient for theoretical purposes. For computations, however, sparse regular sequences would be preferable as they are constructed in [14].

Lemma 2.82. *Let I be an ideal in $\mathbb{K}[X]$ and $f \in \mathbb{K}[X]$. Then f is a zero-divisor in $\mathbb{K}[X]/I$ iff ${}^h\!f$ is a zero-divisor in $\mathbb{K}[X_0]/{}^h I$.*

Proof. Assume f is zero-divisor in $\mathbb{K}[X]/I$. Then $fg \in I$ for some $g \notin I$ and therefore ${}^h\!f \cdot {}^h g = {}^h(fg) \in {}^h I$ and ${}^h g \notin {}^h I$. Hence f is zero-divisor in $\mathbb{K}[X_0]/{}^h I$.

Conversely, assume ${}^h\!f$ is zero-divisor in $\mathbb{K}[X_0]/{}^h I$. Then ${}^h\!f \cdot g \in {}^h I$ for some $g \notin {}^h I$. Let $g = g_0 + \ldots + g_d$ be the decomposition into homogeneous components. Then ${}^h\!f \cdot g_k \in {}^h I$ for all $k = 0, \dots, d$ and $g_k \notin {}^h I$ for some $k \in \{0, \dots, d\}$. Therefore $f \cdot {}^d g_k = {}^d({}^h\!f \cdot g_k) \in I$ and ${}^d g_k \notin I$. Hence f is zero-divisor in $\mathbb{K}[X_0]/I$. □

Although regular sequences are tightly connected to the ideal height which does not change on homogenization, the height of the homogenization of a regular sequence may be quite different. This also means that the homogenization of a regular sequence is, in general, no regular sequence.

Example 2.83. *Consider the sequence given by $g_k = x^{t-k+1} y^k - z_k^t$ for $k = 1, \dots, t$ in the ring $\mathbb{K}[x, y, z_1, \dots, z_t]$. This sequence is regular since g_k has a monomial from $\mathbb{K}[z_k]$ and z_k does not appear in $g_1, \dots, g_{k-1}$. The homogenization of the sequence w.r.t. a new variable z_0, ${}^h g_k = x^{t-k+1} y^k - z_k^t z_0$, is not regular for $t > 2$. This is obvious since $\left\langle {}^h g_1, \dots, {}^h g_t \right\rangle \subseteq \langle x, z_0 \rangle$ and thus $\operatorname{ht}\left\langle {}^h g_1, \dots, {}^h g_t \right\rangle \le 2$.*

2.8. Degree of Varieties

If a variety of dimension r over an algebraically closed field is intersected with an affine space of dimension $n - r$, the intersection generically contains a certain finite number of points. This number is called the degree of the variety.

Example 2.84. *In a ring $\mathbb{K}[x]$ over an algebraically closed field $\mathbb{K}$, each radical ideal I is generated by one square-free polynomial $f \in \mathbb{K}[x]$ of positive degree $\deg(f) \geq 1$. The corresponding variety $\boldsymbol{V}(I) = \boldsymbol{V}(f)$ is finite and contains exactly $\deg(f)$ points. Thus $\dim(I) = 0$. The only affine space of dimension 1 is $\mathbb{K}$ such that the degree of the variety is $\#\boldsymbol{V}(I) = \deg(f)$.*

During the discussion of the ideal dimension it became apparent that one can define the dimension on prime ideals and then lift the definition to arbitrary ideals. The same approach will be used for the degree of varieties. First the definitions and results about prime ideals have to be translated into the language of varieties. Begin with the equivalent of prime ideals, the irreducible varieties.

Definition 2.85. *Let V be a variety in $\mathbb{K}^n$. V is called* reducible *if there are nonempty varieties $\emptyset \neq V_1, V_2 \subsetneq V$ such that $V = V_1 \cup V_2$. Otherwise V is called* irreducible.

Corollary 2.86. *Let V be a variety in $\mathbb{K}^n$. Then V is irreducible iff $\boldsymbol{I}(V)$ is prime.*

Thus it is possible to formulate the primary decomposition of lemma 1.28 for varieties. Note that varieties correspond to radical ideals which in turn are decomposed into prime ideals. The uniqueness of this decomposition follows from lemma 1.35.

Corollary 2.87. *Let V be a variety in $\mathbb{K}^n$. Then there is a unique (up to reordering) decomposition $V = V_1 \cup \ldots \cup V_t$ into irreducible varieties $V_i \neq \emptyset$ with $V_i \not\subseteq V_j$ for all $1 \leq i \neq j \leq t$.*

When dealing with ideals and varieties, there is a canonical way of defining a topology, the so-called *Zariski topology*. In this topology, the closed sets are exactly the varieties, their complements are the open sets.

Definition 2.88. *Let V be an arbitrary subset of $\mathbb{K}^n$. Then $\overline{V}$ denotes the smallest variety in $\mathbb{K}^n$ containing V and is called* Zariski closure *of V.*

The closures of projections are of special interest as they are related to elimination.

Theorem 2.89 (Closure Theorem). *Let I be an ideal in $\mathbb{K}[X]$ and $\pi_S : \mathbb{K}^n \longrightarrow \mathbb{K}^k$ the projection onto the coordinates indexed by $S = \{i_1, \ldots, i_k\}$. Then*

$$\overline{\pi_S(\boldsymbol{V}(I))} = \boldsymbol{V}(I \cap \mathbb{K}[x_{i_1}, \ldots, x_{i_k}]).$$

Proof. See [9], §3.2. □

These notions suffice for the definition of the degree of a variety. The following is a summary of results from [18]. The usage of (more general) constructible sets instead of varieties, however, will be avoided.

Definition 2.90. *Let $V \subseteq \mathbb{K}^n$ be an irreducible variety of dimension r. Then the* degree *of V is denoted by*

$$\deg(V) = \sup\left\{\#(V \cap A) : A \subseteq \mathbb{K}^n \textit{ affine subspace}, \dim_{\mathbb{K}}(A) = n - r, \#(V \cap A) < \infty\right\}.$$

For an arbitrary variety $V \subseteq \mathbb{K}^n$, let $V = V_1 \cup \ldots \cup V_t$ be the decomposition into irreducible components. Then $\deg(V) = \sum_{i=1}^{t} \deg(V_i)$.

Lemma 2.91. *Let $\mathbb{K}$ be an algebraically closed field and $\varphi : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ be an affine linear map and V be a variety in $\mathbb{K}^n$. Then $\deg(\overline{\varphi(V)}) \leq \deg(V)$.*

Proof. See [18], lemma 2. □

Theorem 2.92 (Bézout's Theorem). *Let $\mathbb{K}$ be an algebraically closed field and V_1 and V_2 be varieties in $\mathbb{K}^n$. Then $\deg(V_1 \cap V_2) \leq \deg(V_1) \cdot \deg(V_2)$.*

Proof. See [18], theorem 1. □

This can be used in order to bound the degree of a variety by the product of the degrees of generators of the ideal. If the number of generators is large, one can do better. The proof technique is very similar to lemma 2.80.

Lemma 2.93. *Let $\mathbb{K}$ be an infinite field and $I \subsetneq \mathbb{K}[X]$ be an ideal generated by polynomials $f_1, \ldots, f_s$ with degrees $d_1 \geq \ldots \geq d_s$. Then there are an injective map $\sigma : \{1, \ldots, r\} \longrightarrow \{1, \ldots, s\}$ and $a_{k,i} \in \mathbb{K}$ such that*

$$g_k = \sum_{i=\sigma(k)}^{s} a_{k,i} f_i \qquad \textit{for } k = 1, \ldots, n+1$$

generate ideals $J_k = \langle g_1, \ldots, g_k \rangle$ such that all minimal primes $P \supseteq J_k$ with $P \not\supseteq I$ have height $\operatorname{ht}(P) \geq k$ for $k = 0, \ldots, n+1$. Moreover $\deg(g_k) \leq d_{\sigma(k)}$ for $k = 1, \ldots, n+1$.

Proof. (from [7], proposition 1.3) The proof is by induction on k. The case $k = 0$ is trivial. Thus assume $k \geq 1$ and let $P_1, \ldots, P_t$ be the minimal primes over J_{k-1}. This is a finite set since $P_i \in \operatorname{ass}(J_{k-1})$ for all $i = 1, \ldots, t$. Let $S = \{P_i : i = 1, \ldots, t, P_i \not\supseteq I\}$. By induction, $\operatorname{ht}(P) \geq k - 1$ for all $P \in S$.

Now construct $g_k \in I$ such that the minimal primes of J_k have height at least k. Consider the vector spaces

$$T_P = \left\{(b_1, \ldots, b_s) \in \mathbb{K}^s : \sum_{i=1}^{s} b_i f_i \in P\right\} \qquad \text{for } P \in S.$$

These must be proper subspaces of $\mathbb{K}^s$ since $I \not\subseteq P$ for all $P \in S$. Since $\mathbb{K}$ is infinite and S is finite, also $\bigcup_{P \in S} T_P \neq \mathbb{K}^s$, and it is possible to choose

$$(b_1, \ldots, b_s) \in \mathbb{K}^s \setminus \bigcup_{P \in S} T_P.$$

Thus $h = \sum_{i=1}^{s} b_i f_i \notin \bigcup_{P \in S} P$. Let $Q_1, \ldots, Q_l$ be the minimal primes over $J_{k-1} + \langle h \rangle$. Obviously $Q_i \supseteq J_{k-1}$ for each $i = 1, \ldots, l$. Assume $Q_i \not\supseteq I$ for some $i = 1, \ldots, l$ and let P be a minimal prime such that $J_{k-1} \subseteq P \subseteq Q_i$. Since P is minimal over J_{k-1} and $Q_i \not\supseteq I$, $P \in S$. Hence $h \in Q_i \setminus P$ which implies $\mathrm{ht}(Q_i) \geq \mathrm{ht}(P) + 1 \geq k$.

Now choose $\sigma(k)$ maximal such that there is a polynomial $g_k = \sum_{i=\sigma(k)}^{s} a_{k,i} f_i$ with $a_{k,i} \in \mathbb{K}$ such that all minimal primes $P \supseteq J_k$ with $P \not\supseteq I$ have height $\mathrm{ht}(P) \geq k$. Then $\deg(g_k) \leq d_{\sigma(k)}$. Moreover $a_{k,\sigma(k)} \neq 0$ by maximality of $\sigma(k)$.

It remains to show that (the extended) σ is injective. Assume for contradiction that $\sigma(k) = \sigma(l)$ for some $l = 1, \ldots, k-1$. Let $h = a_{l,\sigma(l)} g_k - a_{k,\sigma(k)} g_l$. Since $a_{i,\sigma(i)} \neq 0$ for all $i = 1, \ldots, k$, $\langle g_1, \ldots, g_{k-1}, h \rangle = J_k$ also fulfills the claim. However h is a linear combination of only $f_{\sigma(k)+1}, \ldots, f_s$ which contradicts the maximality of $\sigma(k)$. □

This translates into the language of varieties as follows.

Corollary 2.94. *Let $\mathbb{K}$ be an infinite field and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[X]$ with degrees $d_1 \geq \ldots \geq d_s$. Then there are $a_{k,i} \in \mathbb{K}$ such that*

$$g_k = \sum_{i=k}^{s} a_{k,i} f_i \qquad \text{for } k = 1, \ldots, n+1$$

and $\boldsymbol{V}(f_1, \ldots, f_s) = \boldsymbol{V}(g_1, \ldots, g_{n+1})$ with $\deg(f_k) \leq d_k$ for $k = 1, \ldots, n+1$.

The following application to Bézout's theorem is even slightly sharper.

Lemma 2.95. *Let $\mathbb{K}$ be an algebraically closed field $V \subseteq \mathbb{K}^n$ be the variety of an ideal generated by polynomials $f_1, \ldots, f_s$ of degrees $d_1 \geq \ldots \geq d_s$. Then $\deg(V) \leq d_1 \cdots d_\mu$ for $\mu = \min\{n, s\}$.*

Proof. For $s \leq n$ the claim is a direct consequence of theorem 2.92. Thus assume $s > n$. By lemma 2.93, there is an ideal $J = \langle g_1, \ldots, g_n \rangle \subseteq I$ with $\deg(g_k) \leq d_k$ for $k = 1, \ldots, n$ such that all minimal primes $P \supseteq J$ with $P \not\supseteq I$ have height $\mathrm{ht}(P) \geq n$. For such P, $\mathbf{V}(P)$ is an irreducible zero-dimensional variety, i.e. a single point and $\deg(\mathbf{V}(P)) = 1$.

Now let $Q_1, \ldots, Q_t]$ be the minimal primes over $I = \langle f_1, \ldots, f_s \rangle$. Then $\deg(\mathbf{V}(I)) = \sum_{i=1}^{t} \deg(\mathbf{V}(Q_i))$. For each Q_i, $i = 1, \ldots, t$, there is a minimal prime $J \subseteq P_i \subseteq Q_i$. Assume $P_i \subsetneq Q_i$ for some $i \in \{1, \ldots, t\}$. Then $P_i \not\supseteq I$ by the minimality of Q_i and hence $\mathrm{ht}(P_i) = n$ by the construction of J. Then $\mathrm{ht}(P_i) > \mathrm{ht}(Q_i) = n$ and $P_i \subsetneq \mathbb{K}[X]$ contradict each other. Hence $Q_1, \ldots, Q_t$ are minimal over J, and there might by extraneous minimal primes over J. This implies $\deg(\mathbf{V}(I)) \leq \deg(\mathbf{V}(J)) \leq \deg(\mathbf{V}(g_1)) \cdots \deg(\mathbf{V}(g_n)) \leq d_1 \cdots d_n$. □

Lemma 2.96. *Let $I \subsetneq \mathbb{K}[X]$ be an ideal of height 1 and $\overline{\mathbb{K}}$ be the algebraic closure of $\mathbb{K}$. Then $\sqrt{I} = \langle f \rangle$ for some $f \in \mathbb{K}[X]$ with $\deg(f) = \deg(\boldsymbol{V}_{\overline{\mathbb{K}}}(I))$.*

Proof. Since $\mathrm{ht}(I) = 1$, there is no ideal $\{0\} \subsetneq J \subsetneq I$. Therefore I must be principal, i.e. $I = \langle g \rangle$ for some $g \in \mathbb{K}[X]$. Then $\sqrt{I} = \langle f \rangle$ where $f = \frac{g}{\gcd(g,g')}$ is the square-free part of g. The degree of $\mathbf{V}_{\overline{\mathbb{K}}}(f)$ is exactly $\deg(f)$. □

2.9. Multiplicities

The algebraic equivalent of the degree of a variety is the multiplicity of an ideal. Bézout's theorem can be generalized to this setting providing sharp bounds for ideals that are not radical. This field is covered in text books like [45], [13], [27], and [36] as well as the articles [43], [2], and [22]. The interested reader, however, must cope with wildly varying notations and definitions. In the following, confusion with the previous chapter shall be avoided.

Definition 2.97. *Let I be an ideal in $\mathbb{K}[X]$ and fix a graded admissible monomial ordering. Then the* (Samuel) multiplicity *of I is defined as* $\operatorname{mult}(I) = \deg({}^{a}\mathrm{HP}_{\mathbb{K}[X]/I})! \cdot \operatorname{lc}({}^{a}\mathrm{HP}_{\mathbb{K}[X]/I})$.

Remember, that ${}^{a}\mathrm{HF}_{\mathbb{K}[X]/I}$ is the same function for any graded admissible monomial ordering. Thus $\operatorname{mult}(I)$ is well-defined. Note that $\operatorname{mult}(I)$ is the leading coefficient of ${}^{a}\mathrm{HP}_{\mathbb{K}[X]/I}$ in the vector space basis $\{\binom{z}{0}, \binom{z}{1}, \binom{z}{2}, \ldots\}$ of $\mathbb{K}[z]$.

Lemma 2.98. *Let $I \subseteq J \subsetneq \mathbb{K}[X]$ be ideals of the same dimension. Then* $\operatorname{mult}(I) \geq \operatorname{mult}(J)$*.*

Proof. Fix a graded admissible monomial ordering. If $I \subseteq J$, ${}^{a}\mathrm{HP}_{\mathbb{K}[X]/I}(z) \geq {}^{a}\mathrm{HP}_{\mathbb{K}[X]/J}(z)$ for each $z \in \mathbb{N}$. Since both ideals have the same dimension r, their Hilbert polynomials have the same degree $r-1$. Hence

$$\operatorname{lc}({}^{a}\mathrm{HP}_{\mathbb{K}[X]/I}(z)) = \lim_{z\to\infty} \frac{{}^{a}\mathrm{HP}_{\mathbb{K}[X]/I}(z)}{z^{r-1}} \geq \lim_{z\to\infty} \frac{{}^{a}\mathrm{HP}_{\mathbb{K}[X]/J}(z)}{z^{r-1}} = \operatorname{lc}({}^{a}\mathrm{HP}_{\mathbb{K}[X]/J}(z)).$$

□

Lemma 2.99. *Let I be an ideal in $\mathbb{K}[X]$. Then* $\operatorname{mult}(I) = \operatorname{mult}({}^{h}I)$*.*

Proof. Fix a graded admissible monomial ordering. Then ${}^{a}\mathrm{HP}_{\mathbb{K}[X]/I}(z) = {}^{a}\mathrm{HP}_{\mathbb{K}[X_0]/{}^{h}I}(z) - {}^{a}\mathrm{HP}_{\mathbb{K}[X_0]/{}^{h}I}(z-1)$ by corollaries 2.33 and 2.29. If ${}^{a}\mathrm{HP}_{\mathbb{K}[X_0]/{}^{h}I}(z) = \sum_{d=0}^{r} a_i z^d$, then

$${}^{a}\mathrm{HP}_{\mathbb{K}[X]/I}(z) = \sum_{d=0}^{r} a_i z^d - \sum_{d=0}^{r} a_i (z-1)^d = \sum_{d=0}^{r} a_i \sum_{i=0}^{d-1} \binom{d}{i} z^i$$

and

$$\begin{aligned}\operatorname{mult}(I) = \deg({}^{a}\mathrm{HP}_{\mathbb{K}[X]/I})! \cdot \operatorname{lc}({}^{a}\mathrm{HP}_{\mathbb{K}[X]/I}) = (r-1)! \cdot a_r \binom{r}{r-1} = \\ = r! \cdot a_r = \deg({}^{a}\mathrm{HP}_{\mathbb{K}[X_0]/{}^{h}I})! \cdot \operatorname{lc}({}^{a}\mathrm{HP}_{\mathbb{K}[X_0]/{}^{h}I}) = \operatorname{mult}({}^{h}I).\end{aligned}$$

□

Note that some authors define the multiplicity of a homogeneous ideal I by $\operatorname{mult}(I) = (\deg(\mathrm{HP}_{\mathbb{K}[X]/I})! \cdot \operatorname{lc}(\mathrm{HP}_{\mathbb{K}[X]/I})$. The above lemma shows the equivalence of this definition. However, the definition using $\mathrm{HP}_{\mathbb{K}[X]/I}$ does not make sense for zero-dimensional (non-homogeneous) ideals because $\mathrm{HP}_{\mathbb{K}[X]/I} = 0$ and $\deg(\mathrm{HP}_{\mathbb{K}[X]/I}) = -1$ in this case.

By corollary 2.34, the multiplicity of a homogeneous ideal can be computed from the primary decomposition. This corresponds to the definition of the degree of a reducible variety.

Corollary 2.100. *Let I be a homogeneous ideal in $\mathbb{K}[X]$ with minimal primary decomposition $I = Q_1 \cap \ldots \cap Q_t$. Then*

$$\operatorname{mult}(I) = \sum_{\substack{i=1 \\ \dim(Q_i)=\dim(I)}}^{t} \operatorname{mult}(Q_i).$$

This can be sharpened to the so-called *associativity formula*:

Lemma 2.101. *Let I be a homogeneous ideal in $\mathbb{K}[X]$. Then*

$$\operatorname{mult}(I) = \sum_{P \supseteq I \text{ minimal prime}} \operatorname{length}_{\mathbb{K}[X]_P}(\mathbb{K}[X]_P/I_P) \cdot \operatorname{mult}(P).$$

Proof. See [43], §5. □

This can be used to construct polynomials in an unmixed ideal.

Definition 2.102. *An ideal I in a ring R is called* unmixed *iff all associated primes $P \in \operatorname{ass}_R(P)$ have the same dimension* $\dim(P) = \dim(I)$.

Lemma 2.103. *Let I be a homogeneous unmixed ideal in $\mathbb{K}[X]$, $P_1, \ldots, P_t$ the minimal primes over I and $f_i \in P_i$ with $\deg(f_i) \leq \operatorname{mult}(P)$ for $i = 1, \ldots, t$. Then $g = f_1^{e_1} \cdots f_t^{e_t} \in I$ for $e_i = \operatorname{length}(\mathbb{K}[X]_{P_i}/I_{P_i})$ and $i = 1, \ldots, t$ and $\deg(g) \leq \operatorname{mult}(I)$.*

Proof. Since I is unmixed, all associated primes of I are minimal over I. Thus let $I = Q_1 \cap \ldots \cap Q_t$ be a primary decomposition of I and $P_i = \sqrt{Q_i}$ for $i = 1, \ldots, t$ be the minimal primes. By lemma 1.58 and the unmixedness of I, $I_{P_i} \cap \mathbb{K}[X] = Q_i$ follows for $i = 1, \ldots, t$. Since $P_i \supseteq Q_i \supseteq I$, there is a one-to-one correspondence of the $(\mathbb{K}[X]_{P_i}/I_{P_i})$-modules in $\mathbb{K}[X]_{P_i}/I_{P_i} = \mathbb{K}[X]_{P_i}/(Q_i)_{P_i}$ and the $(\mathbb{K}[X]/Q_i)$-modules in $\mathbb{K}[X]/Q_i$. For simplicity, the latter will be considered. There is a chain of modules $(\mathbb{K}[X]/(Q_i)) \cdot f^k \supseteq (\mathbb{K}[X]/(Q_i))f^{k+1}$ for $k = 0, 1, 2, \ldots$ with equality iff $f^k \in Q_i$. By the definition of the module length, this happens for some $e_i = k \leq \operatorname{length}(\mathbb{K}[X]_{P_i}/I_{P_i})$. Then $g = f_1^{e_1} \cdots f_t^{e_t} \in I = Q_1 \cap \ldots \cap Q_t$. Lemma 2.101 finally implies the bound for the degree. □

The multiplicity of a homogeneous complete intersection are determined by the degree sequence.

Lemma 2.104. *Let I be an ideal in $\mathbb{K}[X]$ generated by a homogeneous regular sequence $g_1, \ldots, g_t$ of degrees $d_1, \ldots, d_t$. Then* $\operatorname{mult}(I) = d_1 \cdots d_t$.

Proof. The proof is by induction on t. The case $t = 0$ is trivial. Hence assume $t \geq 1$ and consider the exact sequence

$$0 \longrightarrow \mathbb{K}[X]/\langle g_1, \ldots, g_{t-1}\rangle \xrightarrow{m_{g_t}} \mathbb{K}[X]/\langle g_1, \ldots, g_{t-1}\rangle \longrightarrow \mathbb{K}[X]/\langle g_1, \ldots, g_t\rangle \longrightarrow 0$$

where m_{g_t} denotes multiplication by g_t. This implies

$$^{\mathrm{a}}\mathrm{HP}_{\mathbb{K}[X]/\langle g_1,\ldots,g_t\rangle}(z) = {}^{\mathrm{a}}\mathrm{HP}_{\mathbb{K}[X]/\langle g_1,\ldots,g_{t-1}\rangle}(z) - {}^{\mathrm{a}}\mathrm{HP}_{\mathbb{K}[X]/\langle g_1,\ldots,g_{t-1}\rangle}(z - d_t).$$

If $^{\mathrm{a}}\mathrm{HP}_{\mathbb{K}[X]/\langle g_1,\ldots,g_{t-1}\rangle}(z) = \sum_{d=0}^{r} a_i z^d$, then

$$^{\mathrm{a}}\mathrm{HP}_{\mathbb{K}[X]/\langle g_1,\ldots,g_t\rangle}(z) = \sum_{d=0}^{r} a_i z^d - \sum_{d=0}^{r} a_i (z - d_t)^d = \sum_{d=0}^{r} a_i \sum_{i=0}^{d-1} \binom{d}{i} z^i d_t^{d-i}$$

and

$$\begin{aligned} \mathrm{mult}\langle g_1, \ldots, g_t\rangle =& \deg({}^{\mathrm{a}}\mathrm{HP}_{\mathbb{K}[X]/\langle g_1,\ldots,g_t\rangle})! \cdot \mathrm{lc}({}^{\mathrm{a}}\mathrm{HP}_{\mathbb{K}[X]/\langle g_1,\ldots,g_t\rangle}) = \\ =&(r-1)! \cdot a_r \binom{r}{r-1} d_t = d_t \cdot r! \cdot a_r = \\ =&d_t \cdot \deg({}^{\mathrm{a}}\mathrm{HP}_{\mathbb{K}[X]/\langle g_1,\ldots,g_{t-1}\rangle})! \cdot \mathrm{lc}({}^{\mathrm{a}}\mathrm{HP}_{\mathbb{K}[X]/\langle g_1,\ldots,g_{t-1}\rangle}) = \\ =&d_t \cdot \mathrm{mult}\langle g_1, \ldots, g_{t-1}\rangle. \end{aligned}$$

□

One can also derive an exact formula for the multiplicity of the sum of two unmixed ideals for the case the height of the sum of the ideals is the sum of the heights of the single ideals. Since the notion of intersection multiplicity would be needed, this result will not be stated exactly (cf. [22], theorem 2.8). Note that there will be no references to the theory of multiplicities in the remaining thesis. It is included as impulse for researchers who want to improve work that is presented in this thesis.

2.10. Toric Ideals

Toric ideals arise from algebraic approaches to integer linear programming. They are binomial ideals whose exponent vectors correspond to relations of a linear map.

Definition 2.105. *Consider the homomorphism of free $\mathbb{Z}$-modules*

$$\varphi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^m : (\alpha_1, \ldots, \alpha_n)^T \mapsto \alpha_1 v_1 + \ldots + \alpha_n v_n \qquad \textit{for } v_1, \ldots, v_n \in \mathbb{Z}^m$$

The toric ideal *in $\mathbb{K}[X]$ corresponding to φ is*

$$I_\varphi = I_M = \left\langle x^{\alpha^+} - x^{\alpha^-} \in \mathbb{K}[X] : \alpha \in M \right\rangle$$

where $M = \ker(\varphi)$ and, for $k = 1, \dots, n$,

$$\alpha_k^+ = \begin{cases} \alpha_k & \textit{for } \alpha_k \geq 0 \\ 0 & \textit{for } \alpha_k < 0 \end{cases} \qquad \alpha_k^- = \begin{cases} 0 & \textit{for } \alpha_k \geq 0 \\ -\alpha_k & \textit{for } \alpha_k < 0. \end{cases}$$

Furthermore define the vector $\alpha \vee \beta$ by $(\alpha \vee \beta)_k = \min\{\alpha_k, \beta_k\}$ for $\alpha, \beta \in \mathbb{N}^n$.

So actually I_M is defined by a submodule M of $\mathbb{Z}^n$ which is saturated w.r.t. $\mathbb{Z}^n$. Since the module $\mathbb{Z}^n$ has no zero-divisors, the saturated submodules are exactly the submodules that appear as kernels of homomorphisms and studying toric ideals is equivalent to considering arbitrary saturated submodules M of $\mathbb{Z}^n$ and the corresponding ideals I_M. The latter point of view will be preferred in this thesis. The following lemma provides a vector space basis for toric ideals.

Lemma 2.106 (Sturmfels 1996)**.** *Let I_M be a toric ideal in $\mathbb{K}[X]$. Then I_M is generated as $\mathbb{K}$-vector space by $F = \left\{x^\alpha - x^\beta \in \mathbb{K}[X] : (\alpha - \beta) \in M\right\}$.*

Proof. (from [42], lemma 4.1) By the definition of I_M, any $f \in I_M$ can be written as polynomial combination $f = \sum_{i=1}^s a_i(x^{\alpha_i^+} - x^{\alpha_i^-})$ with $s \in \mathbb{N}$, $\alpha_i \in M$ and $a_i \in \mathbb{K}[X]$, for $i = 1, \dots, s$. But $a_i = \sum_{\beta \in \mathbb{N}^n} a_{i,\beta} x^\beta$ with $a_{i,\beta} \in \mathbb{K}$, for $i = 1, \dots, s$ and $\beta \in \mathbb{N}^n$, and hence

$$f = \sum_{i=1}^{s} \sum_{\beta \in \mathbb{N}^n} a_{i,\beta}(x^{\alpha^+ + \beta} - x^{\alpha^- + \beta}).$$

Here $(\alpha^+ + \beta) - (\alpha^- + \beta) = \alpha \in M$ and thus f is a linear combination of elements of F. □

Studying representations of members of toric ideals a little further is definitely worthwhile. Since the module M is closed under addition, one can compensate cancellations by other elements of the binomial basis. Therefore each polynomial can be represented as linear combination of binomial ideal members in which no cancellation occurs.

Lemma 2.107. *Let I_M be a toric ideal in $\mathbb{K}[X]$ and $h \in I_M$ be an arbitrary ideal member. Then there is a representation*

$$h = \sum_{i=1}^{s} a_i(x^{\alpha_i} - x^{\beta_i}) \qquad \textit{with } a_i \in \mathbb{K}, \alpha_i - \beta_i \in M, x^{\alpha_i}, x^{\beta_i} \in \operatorname{supp}(h) \textit{ for } i = 1, \dots, s.$$

Proof. By lemma 2.106, h is of the form $h = \sum_{i=1}^s f_i$ with $f_i = a_i(x^{\alpha_i} - x^{\beta_i})$,$a_i \in \mathbb{K}$, and $\alpha_i - \beta_i \in M$. Among all such representations choose one with minimal s. Obviously this implies $a_i \neq 0$ for $i = 1, \dots, s$.

Now assume that $\operatorname{supp}(f_k) \not\subseteq \operatorname{supp}(h)$ for some $k = 1, \dots, s$. Then there is some $x^\gamma \in \operatorname{supp}(f_k)$ such that $0 = h_\gamma = \sum_{f_{i,\gamma} \neq 0} f_{i,\gamma}$. The goal is now to rewrite the sum of binomials f_i with $f_{i,\gamma} \neq 0$ for $i = 1, \dots, s$. For $f_{i,\gamma} \neq 0$, let x^{δ_i} be the single monomial in $\operatorname{supp}(f_i) \setminus \{x^\gamma\}$, observe $f_{i,\gamma} = -f_{i,\delta_i}$, and define

$$g_i = f_i - \frac{f_{i,\gamma}}{f_{k,\gamma}} f_k = f_{i,\delta_i}(x^{\delta_i} - x^{\delta_k})$$

such that

$$\sum_{\substack{i=1\\f_{i,\gamma}\neq 0}}^{s} g_i = \sum_{\substack{i=1\\f_{i,\gamma}\neq 0}}^{s} \left(f_i - \frac{f_{i,\gamma}}{f_{k,\gamma}} f_k\right) = \sum_{\substack{i=1\\f_{i,\gamma}\neq 0}}^{s} f_i.$$

Since $\gamma - \delta_i = \pm(\alpha_i - \beta_i) \in M$ for $f_{i,\gamma} \neq 0$, also

$$(\delta_i - \delta_k) = (\gamma - \delta_k) - (\gamma - \delta_i) \in M$$

which shows that the g_i are of the desired form. However $g_k = 0$ such that

$$h = \sum_{\substack{i=1\\f_{i,\gamma}=0}}^{s} f_i + \sum_{\substack{i=1\\f_{i,\gamma}\neq 0\\i\neq k}}^{s} g_i$$

is a shorter representation which contradicts minimality of s and proves the claim. □

Toric ideals can be characterized neatly. This can be very useful for proving that a given ideal is toric.

Lemma 2.108 (Eisenbud, Sturmfels 1996). *Let I be an ideal in $\mathbb{K}[X]$. Then I is toric iff it is a prime ideal generated by binomials.*

Proof. (from [15], corollary 2.6) First assume $I = I_\varphi$ is toric. By definition, it is binomial. Furthermore the module homomorphism $\varphi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ extends to a homomorphism of rings

$$\widehat{\varphi} : \mathbb{K}[X] \longrightarrow \mathbb{K}[t_1, \dots, t_m, t_1^{-1}, \dots, t_m^{-1}], x_k \mapsto t^{\varphi(e_k)}$$

with the standard basis $e_1, \dots, e_n$ of $\mathbb{Z}^n$. The claim is that $I_\varphi = \ker(\widehat{\varphi})$ which implies that I_φ is prime. First of all, I_φ is generated by $x^\alpha - x^\beta \in I_\varphi$ with $\alpha - \beta \in \ker(\varphi)$ and therefore $\widehat{\varphi}(x^\alpha - x^\beta) = t^{\varphi(\alpha)} - t^{\varphi(\beta)} = 0$. Hence $I_\varphi \subseteq \ker(\widehat{\varphi})$. For the converse, choose $f = \sum_{i=1}^{s} f_i x^{\alpha_i} \in \ker(\widehat{\varphi})$ with $f_i \neq 0$ for $i = 1, \dots, s$, i.e. $\sum_{i=1}^{s} f_i x^{\varphi(\alpha_i)} = 0$. Then for each $\beta \in \mathbb{Z}^m$, the corresponding coefficient $\sum_{\varphi(\alpha_i)=\beta} f_i = 0$ must vanish. If this sum is non-empty, there must be at least two summands f_k and f_l. This means $\alpha_k - \alpha_l \in \ker(\varphi)$, $g = f - f_k(x^{\alpha_k} - x^{\alpha_l}) \in f + I_\varphi$ has strictly less terms than f, and $g \in \ker(\widehat{\varphi})$. By induction, $f \in I_\varphi$ which proves $I_\varphi = \ker(\widehat{\varphi})$.

Now assume I is a prime ideal in $\mathbb{K}[X]$ which is generated by the binomials $F = \left\{x^{\alpha_i} - x^{\beta_i} \in \mathbb{K}[X] : i = 1, \dots, s\right\}$ and define $M = \left\{\alpha \in \mathbb{Z}^n : x^{\alpha^+} - x^{\alpha^-} \in I\right\}$. Obviously $I_M \subseteq I$, so define $\gamma_i = \alpha_i - \beta_i$ and thus $x^{\alpha_i} - x^{\beta_i} = x^{\alpha_i \vee \beta_i}(x^{\gamma_i^+} - x^{\gamma_i^-})$. Since I is prime and contains no monomials, $x^{\gamma_i^+} - x^{\gamma_i^-} \in I$ follows. Hence $I_M = I$.

In order to prove that I is toric it remains to show that M is a saturated submodule of $\mathbb{Z}^n$. $\alpha \in M$ implies $k\alpha \in M$ for any $k \in \mathbb{Z}$ since $x^{\alpha^-} - x^{\alpha^+} \in I$ and

$$x^{k\alpha^+} - x^{k\alpha^-} = (x^{(k-1)\alpha^+} + x^{(k-2)\alpha^+ + \alpha^-} + \dots + x^{(k-1)\alpha^-})(x^{\alpha^+} - x^{\alpha^-}) \in I. \tag{2.1}$$

Furthermore, $\alpha, \beta \in M$ implies $x^{\alpha^+ + \beta^-} - x^{\alpha^- + \beta^+} = x^{\beta^+}(x^{\alpha^+} - x^{\alpha^-}) - x^{\alpha^+}(x^{\beta^+} - x^{\beta^-}) \in I$. As above, it is possible to divide by common factors and thereby derive $\alpha - \beta = (\alpha^+ + \beta^-) - (\alpha^- + \beta^+) \in M$. Hence M is a module.

It remains to show that M is saturated w.r.t. $\mathbb{Z}^n$. Assume $k\alpha \in M$ for some $k \in \mathbb{Z}$, $\alpha \in \mathbb{Z}^n$ and consider (2.1). Since I is generated by pure binomials, the sum of the coefficients of each ideal member is 0. Since I is prime, one of the two factors in (2.1) must be in I. Together one concludes $\alpha \in M$. □

Lemma 2.108 tells that the module $M = \mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_s \subseteq \mathbb{Z}^n$ is saturated w.r.t. $\mathbb{Z}^n$ if $\left\langle x^{\beta_i^+} - x^{\beta_i^-} : i = 1, \ldots, s \right\rangle$ is a toric ideal. The converse implication is not true in general.

Example 2.109. *Consider the ideal $I = \langle x^2 - z, xy - z \rangle$ in the ring $\mathbb{K}[x, y, z]$. The corresponding module $M = \mathbb{Z}(2, 0, -1)^T + \mathbb{Z}(1, 1, -1)^T = \mathbb{Z}(1, -1, 0)^T + \mathbb{Z}(1, 1, -1)^T$ is saturated. However, $x - y \in I_M$ and $x - y \notin I$ show that I is not a toric ideal.*

3. Theory of Computation

3.1. Thue systems

Thue systems are a way to describe certain languages. Commutative Thue systems can be viewed as different representation of binomial ideals and will be very useful later on.

Definition 3.1. *Let X be a finite alphabet and $X^* = \bigcup_{i\in\mathbb{N}} X^i$. Then a* semi-Thue system *consists of a finite set of* productions $\mathcal{P} = \{l_i \to r_i : l_i, r_i \in X^*, i = 1, \ldots, s\}$. *A word $\beta \in X^*$ is derived from $\alpha \in X^*$ w.r.t. $\mathcal{P}$ in one step iff $\alpha = \delta l_i \varepsilon$ and $\beta = \delta r_i \varepsilon$ for some $\delta, \varepsilon \in X^*$ and $i = 1, \ldots, s$. This is denoted by $\alpha \to \beta$ $(\mathcal{P})$. The reflexive transitive closure of $\to$ is denoted by $\overset{*}{\to}$. If $\alpha \overset{*}{\to} \beta$ $(\mathcal{P})$, any sequence $\alpha = \gamma_0 \to \gamma_1 \to \ldots \to \gamma_t = \beta$ $(\mathcal{P})$ is called* derivation *of β from α w.r.t. $\mathcal{P}$. A* Thue system *is a symmetric semi-Thue system, i.e.*

$$(l \to r) \in \mathcal{P} \;\Leftrightarrow\; (r \to l) \in \mathcal{P}.$$

In this case $\overset{*}{\to}$ constitutes an equivalence relation which is denoted by $\alpha \equiv \beta$ $(\mathcal{P})$. Furthermore a Thue system is called commutative *iff all symbols commute, i.e.*

$$\forall x, y \in X : (xy \to yx) \in \mathcal{P}.$$

Speaking of a commutative Thue system generated by $\mathcal{P}$, one understands that the rules in $\mathcal{P}$ are supplemented to fulfill the above criteria.

One can easily define an ideal corresponding to a commutative Thue system by treating the alphabet of the Thue system as indeterminates of a polynomial ideal.

Definition 3.2. *Let $\mathcal{P}$ be a commutative Thue system over the alphabet X and denote by*

$$I_{\mathcal{P}} = \langle l - r \in \mathbb{K}[X] : (l \to r) \in \mathcal{P} \rangle$$

the ideal corresponding to $\mathcal{P}$ in the polynomial ring $\mathbb{K}[X]$. In the above formula, the words $l, r \in X^*$ are canonically interpreted as monomials over $\mathbb{K}[X]$.

In [33], Mayr and Meyer use this setting to prove a lower degree bound for the representation problem of polynomial ideals, among others. The essential reduction is given by

Lemma 3.3 (Mayr, Meyer 1982). *Let $\mathcal{P} = \{l_i \to r_i : l_i, r_i \in X^*, i = 1, \ldots, s\}$ be a commutative Thue system over X. For any words $\alpha, \beta \in X^*$, $\alpha \equiv \beta$ $(\mathcal{P})$ iff $\alpha - \beta \in I_{\mathcal{P}}$. Then the minimal degree $d = \max\{\deg(\gamma_i) : i = 0, \ldots, t\}$ of a derivation $\alpha = \gamma_0 \to \ldots \to \gamma_t = \beta$ $(\mathcal{P})$ with $\gamma_i \in X^*$ for $i = 0, \ldots, t$ equals the minimal degree $d' = \max\{\deg(a_i(l_i - r_i)) : i = 1, \ldots, s\}$ of a polynomial representation $\alpha - \beta = \sum_{i=1}^{s} a_i(l_i - r_i)$ with $a_i \in \mathbb{K}[X]$.*

Proof. (from [33], lemma 3.1 and lemma 3.2) First assume there is a derivation $\alpha = \gamma_0 \to \ldots \to \gamma_t = \beta$ with $\deg(\gamma_i) \leq d$ for $i = 0, \ldots, t$. For each $i = 1, \ldots, t$, there is a production $l_{k_i} \to r_{k_i}$ with $k_i \in \{1, \ldots, s\}$ such that $\gamma_{i-1} = \delta_i l_{k_i}$ and $\gamma_i = \delta_i r_{k_i}$ for some word $\delta_i \in X^*$. Then

$$\alpha - \beta = \sum_{i=1}^{t} \delta_i (l_{k_i} - r_{k_i}) \text{ with } \deg(\delta_i(l_{k_i} - r_{k_i})) \leq d.$$

For the converse, assume $\alpha - \beta = \sum_{i=1}^{t} c_i \delta_i (l_{k_i} - r_{k_i}) \in I_{\mathcal{P}}$ for some $0 \neq c_i \in \mathbb{K}$, $\delta_i \in X^*$, $k_i \in \{1, \ldots, s\}$, and $\deg(\delta_i(l_{k_i} - r_{k_i})) \leq d'$ for $i = 1, \ldots, t$. Consider the graph with vertices $V = \{\delta_i l_{k_i}, \delta_i r_{k_i} : i = 1, \ldots, t\}$ and (directed) edges $E = \{(\delta_i l_{k_i}, \delta_i r_{k_i}) : i = 1, \ldots, t\} \cup \{(\beta, \alpha)\}$ whose weights are $w(\delta_i l_{k_i}, \delta_i r_{k_i}) = c_i$ for $i = 1, \ldots, t$ and $w(\beta, \alpha) = 1$. Since any path in this graph is a derivation in $\mathcal{P}$ whose degree is bounded by d', it suffices to show that α and β lie in a common (directed) cycle (repeated nodes are allowed). Since $v \subseteq \mathbb{K}[X]$, one can calculate the sum

$$\sum_{(v,u) \in E} w(v,u)(v - u) = \sum_{i=1}^{t} c_i \delta_i (l_{k_i} - r_{k_i}) + (\beta - \alpha) = 0. \tag{3.1}$$

Now use induction on the number of edges in E. By (3.1) and since $c_i \neq 0$ for all $i = 1, \ldots, t$, no node has degree 1, so there must by a cycle $C \subseteq E$. Let $0 \neq c = w(v_0, u_0)$ for some $(v_0, u_0) \in C$. Then define $w'(v,u) = w(v,u) - c$ for all $(v,u) \in C$ and $w'(v,u) = w(v,u)$ otherwise. Moreover let $E' = \{(v,u) \in E : w'(v,u) \neq 0\}$. Then (V, E') is a graph with less edges and, since C is a cycle,

$$\sum_{(v,u) \in E'} w'(v,u) \cdot (v - u) = \sum_{(v,u) \in E} w(v,u) \cdot (v - u) - \sum_{(v,u) \in C} c \cdot (v - u) = 0.$$

By induction, every edge must be contained in a cycle. Since one of the edges in E is (α, β), α and β are in the same cycle which proves the claim. □

Please note that this proof works for arbitrary fields, opposed to the original reasoning by Mayr and Meyer which requires $\mathbb{K} = \mathbb{Q}$.

3.2. Turing Machines

The definitions of Turing machines in literature slightly differ, while the computing power is the same for all of them (at least as far as computability is regarded, but essentially this is true for complexity, too). The simplest variants of Turing machines only have one tape which contains the input at first, serves as working space, and to which the output is written in the end. This is somewhat impractical as far as space complexity measurements are concerned. There are algorithms whose working space is smaller by magnitudes than the length of the input. However, not being able to determine the exact space requirements, it is common to use the O-notation. If only one tape is available, space consumption of $O(n)$

in unavoidable where n denotes the length of the input. So it is impossible to distinguish between algorithms that need linear working space and algorithms with sublinear (e.g. logarithmic) working space using the O-notation and a one-tape Turing machine.

Instead of using more complicated notations for the complexity (and therefore longer calculations), one can work with a three-tape Turing machine. Note that this is computationally equivalent and, moreover, a standard definition in complexity theory. The three tapes have different capabilities and functions. The *input tape* contains the input at the beginning and only allows for reading operations. The *output tape* only allows for writing-operations and is empty at the start. The algorithm has to fill this tape with the answer to the given problem (encoded in the input on the input tape). Finally, the third tape is called *working tape*. It is general purpose, so reading and writing operations are allowed. In the beginning, it is empty and in the end, its contents are ignored. However, the space complexity of the algorithm is measured as the length of the part of the working-tape that was touched by the algorithm.

Definition 3.4. *Let Σ be an* alphabet. *A* problem *P is a function $P : \Sigma^* \longrightarrow \Sigma^*$ which shall be computed by an algorithm. The restriction of P to inputs $w \in X^*$ of length $|w| = n$ is denoted by $P_n : \Sigma^n \longrightarrow \Sigma^*$.*

Definition 3.5. *A* Turing machine *is described by an alphabet Σ, a set Q of* states, *an* initial state *$q_0 \in Q$, a* final state *$f \in Q$, and a (partial)* transition function *$\delta : (Q \setminus \{f\}) \times \Sigma^2 \longrightarrow Q \times (\Sigma \cup \{\varepsilon\})^2 \times \{L, R\}^3$.*

Assume, the Turing machine is in state $q_k \in Q \setminus \{f\}$ after k steps and the three heads are at the positions $i_{k,j}$ where $j = 1$ corresponds to the input tape, $j = 2$ to the working tape, and $j = 3$ to the output tape. Let $c_{k,j} \in \Sigma$ be the character on tape j at position $i_{k,j}$. Then $\delta(q_k, c_{k,1}, c_{k,2})$ describes the next transition. The first entry denotes the new state, the following two the values are written at the current positions to the working respectively output tape (ε means that nothing is written), and the remaining three entries describe the movements of the three heads (L for left, R for right).

At the beginning, the Turing machine is in state q_0 and all heads are at position $i_{0,j} = 0$. If the Turing machine reaches state $q_k = f$, the computation stops. The output of the computation is the content of the working tape after k steps. The length (or time) of the computation is k.

A Turing machine is called $f(n)$-space bounded if the working tape has length $f(n)$ where n denotes the length of the input tape. Such a Turing machine fails if the head of the working tape moves beyond the limit of the tape.

Definition 3.6. *A Turing machine* computes *a problem P iff for all words $w \in \Sigma^*$, the computation of the Turing machine with the input tape w stops without failure and outputs $P(w)$.*

Definition 3.7. *SPACE($f(n)$) is the class of all problems which can be computed by a $c \cdot f(n)$-space bounded Turing machine for some $c \in \mathbb{N}$.*

Lemma 3.8. *The length of computation and output of any terminating $f(n)$-space bounded Turing machine with $f(n) \geq \log(n)$ is bounded by $2^{c \cdot f(n)}$ for some $c \in \mathbb{N}$.*

Proof. If the Turing machine $(\Sigma, Q, q_0, f, \delta)$ terminates, no configuration may be reached twice. The number of configurations is bounded by the possible contents of the working tape, the positions of the heads of the input and working tapes, and the state of the Turing machine. This is bounded in order by

$$\#\Sigma^{f(n)} \cdot n \cdot f(n) \cdot \#Q = O(\#\Sigma^{f(n)} \cdot 2^{f(n)} \cdot 2^{\log(f(n))}) = 2^{O(f(n))}.$$

□

3.3. Boolean Circuits

Just like Turing machines, Boolean circuits are a machine model. While Turing machines are a standard model for sequential computations, Boolean circuits are used to describe parallel computations.

Definition 3.9. *A* Boolean circuit *C is a directed acyclic graph. The nodes with in-degree zero are* input nodes, *the nodes with out-degree zero are* output nodes *and have in-degree one. The inner nodes (also called* gates*) are labeled by the binary operations AND, OR, and the unary operation NOT. The number of nodes is called* size *of the circuit and denoted by* $\operatorname{size}(C)$, *the longest path in the graph (from an input node to an output node) is called* depth *and denoted by* $\operatorname{depth}(C)$.

Since all gates are labeled by unary respectively binary operations, the in-degree of the circuit is bounded (actually by 2) while the out-degree is arbitrary. The input of the circuit is an assignment of Boolean values to the input nodes. The values of the gates are determined by the operations indicated by their labels applied to the values of their predecessor nodes. The output nodes inherit the values of their predecessors. Since the graph is acyclic, this recursive evaluation is well-defined and unique for given input values. By numbering the n input and m output nodes, one can view C as a function $C : \{0,1\}^n \mapsto \{0,1\}^m$. Since the gates are viewed as independent processing units, the depth of the circuit is a measure of the time the (parallel) evaluation takes.

Using a topological ordering, one can encode C in a straight-forward way as string in $\{0,1\}^*$. This string will be denoted by $\overline{C}$. Note that $|\overline{C}| \geq c \cdot \operatorname{size}(C) \cdot \log(\operatorname{size}(C))$ for some $c > 0$ if the output depends on all input bits. This is because the representation of a node index takes $\Theta(\log(\operatorname{size}(C)))$ bits.

Definition 3.10. *A problem P is* realized *by a family of Boolean circuits $(C_n)_{n\in\mathbb{N}}$ iff $C_n(y) = P_n(y)$ for all inputs $y \in \{0,1\}^n$ of length n. Here P_n is assumed to have a fixed output length (otherwise it must be padded to the maximal length).*

Up to now, there is a big difference between Turing machines and families of Boolean circuits. While the description of a Turing machine is finite, a family of Boolean circuits can have an independent definition for each input length. This non-uniformity causes an unbalance of the computing power when comparing space-bounded Turing machines and depth-bounded circuits.

Definition 3.11. *A family of Boolean circuits $(C_n)_{n\in\mathbb{N}}$ is SPACE($f(n)$)-*uniform *iff $\overline{C}_n$ can be computed in SPACE($f(n)$).*

Definition 3.12. *The class of all problems which can be realized by a family of SPACE*$(\log(n))$*-uniform Boolean circuits $(C_n)_{n\in\mathbb{N}}$ with* $\mathrm{depth}(C_n) = O(\log^k(n))$ *and* $\mathrm{size}(C_n) = n^{O(1)}$ *is denoted by NC^k.*

Be aware that the definitions of the class NC^k in literature vary slightly. Sometimes, uniformity is not required or a slightly different kind of uniformity is chosen.

Uniform Boolean circuits can be easily simulated by Turing machines. The depth of the circuit, which is a measure of the parallel computation time, determines the space requirements of the Turing machine.

Theorem 3.13 (Borodin 1977)**.** *Let $(C_n)_{n\in\mathbb{N}}$ be a family of SPACE($f(n)$)-uniform Boolean circuits with* $\mathrm{depth}(C_n) = O(f(n))$ *for some function $f(n) \geq \log(n)$. Then $(C_n)_{n\in\mathbb{N}}$ can be simulated by a Turing machine in SPACE($f(n)$).*

Proof. (from [3], theorem 4) Since $(C_n)_{n\in\mathbb{N}}$ is SPACE($f(n)$)-uniform, $\overline{C}_n$ (respectively any bit of this string) can be computed in SPACE($f(n)$). $f(n) \geq \log(n)$ is necessary here because the length of the input n has to be determined.

Knowing this, the idea is to recursively evaluate the circuit using a fixed ordering of the children of each node. In a straightforward implementation, one would store the index of the node and the status of the evaluation at each level of the recursion. Since the status of a recursion level is given by the return values of one or two recursive calls which can be "true", "false", or "unevaluated", it only needs a constant number of bits. So the total space consumption would be $O(\mathrm{depth}(C_n)\log(\mathrm{size}(C_n)))$.

This can be improved by only storing the node index of the current recursion level while keeping the status of the recursion at each level. The address of the parent node can be computed from the root of the recursion using the status entries at each recursion level. This yields a space complexity of $O(\mathrm{depth}(C_n) + \log(\mathrm{size}(C_n)))$. Remembering that $\overline{C}_n$ can be computed in SPACE($f(n)$), one deduces that the size of the circuit is bounded by $\mathrm{size}(C_n) \leq 2^{c\cdot f(n)}$ for some $c > 0$. Thus one can simulate the family of circuits in space $O(f(n) + \log(2^{c\cdot f(n)})) = O(f(n))$. □

Borodin's simulation result will be used on a number of Boolean circuits. But before more complex algorithms are considered, it is necessary to cover the basic ring operations. Borodin et al. introduced the concept of well-endowed ring for this purpose [4].

Definition 3.14. *Let R be a ring and $\alpha : R \longrightarrow \mathbb{N}$ be a* length function*, i.e. $\alpha(a + b) \leq \max\{\alpha(a), \alpha(b)\} + O(1)$ and $\alpha(a \cdot b) \leq \alpha(a) + \alpha(b) + O(\log(\max\{\alpha(a), \alpha(b)\}))$. Then $R_n = \{r \in R : \alpha(r) \leq n\}$. (l, r) is a* representation *of (R, α) iff $l : \mathbb{N} \longrightarrow \mathbb{N}$ and $r_n : \{0, 1\}^{l(n)} \longrightarrow R_n$ such that $R_n \subseteq r_n(\{0, 1\}^{l(n)})$. It is called* succinct *iff $l(n) = n^{O(1)}$, i.e. all ring elements of length n can be represented as strings of bitsize polynomial in n. The representation is* uniform *iff, for arbitrary $k \in \mathbb{N}$, a $(l(n) + k)$-bit representation of any element of R_n can be computed in NC^1 (i.e.*

with depth $O(\log(l(n)+k)))$. If (R,α) has a succinct uniform representation such that addition is in NC^0 and multiplication is in NC^1, the ring is called well-endowed.

The ring operations of well-endowed rings are fast enough such that the complexity of the considered algorithms is not essentially influenced. Also many operations on the fields of fractions can be computed efficiently. This yields to the following definition.

Definition 3.15. *Let R be a well-endowed domain. Then its field of fractions $\mathbf{Q}(R)$ is also called* well-endowed.

First consider the integers. The input and output numbers are usually stored in the binary representation. Sometimes, however, a redundant representation is preferable (cf. [4]).

Definition 3.16. *Choose $p \geq 2$. For any $n \in \mathbb{N}$, let $(a_0,\dots,a_n) \in \{-(p-1),\dots,(p-1)\}^{n+1}$ represent the number $r(a_0,\dots,a_n) = \sum_{i=0}^{n} a_i p^i$. Since each coefficient a_i uses space $\lceil\log(2p-1)\rceil$, one defines $l(n) = \lceil\log(2p-1)\rceil n$ and obtains a succinct uniform representation (l,r) of $\mathbb{Z}$ for the length function $\alpha(k) = \lceil\log_p(|k|+1)\rceil$ for all $k \in \mathbb{Z}$. This representation is called* balanced p-ary representation.

Lemma 3.17. *The addition of two integers in balanced p-ary representation is in NC^0 for $p \geq 3$.*

Proof. (from [4], §2) The task is to add two integers which are represented by $(a_0,\dots,a_n)$ and $(b_0,\dots,b_n)$ with $n \in \mathbb{N}$ and $a_i, b_i \in \{-(p-1),\dots,(p-1)\}$ for $i = 0,\dots,n$. Since $|a_k|, |b_k| \leq p-1$ for all $k = 0,\dots,n$, $|a_k+b_k| \leq 2p-2$. Since $p \geq 3$, there are x_k, y_k such that $a_k + b_k = x_k p + y_k$ and $|x_k| \leq 1$, $|y_k| \leq p-2$. Thus $(y_0, y_1+x_0, \dots, y_n+x_{n-1}, x_n)$ is a balanced p-ary representation of the sum which can be computed uniformly in constant depth. □

Lemma 3.18. *The addition of n integers with n bits each in balanced p-ary representation is in NC^1 for $p \geq 3$.*

Proof. (from [4], §3) The key is to use a balanced tree representation of the arithmetic expression. The depth of the tree is $O(\log(n))$ and each operation is in NC^0 which yields a circuit of depth $O(\log(n))$. If $2^{e-1} < n \leq 2^e$ for some $e \in \mathbb{N}$, one can call the input numbers $a_{2^e},\dots,a_{2^e+n-1} \in \mathbb{Z}$ and let $a_k = 0$ for $k = 2^e+n,\dots,2^{e+1}-1$. A circuit computing $a_k = a_{2k} + a_{2k+1}$ for $k = 1,\dots,2^e-1$ can certainly be constructed uniformly and a_1 is the sum of all input numbers. □

Lemma 3.19. *The multiplication of two integers in balanced p-ary representation is in NC^1 for $p \geq 3$.*

Proof. (from [4], §2) The product of two n-bit integers can be computed as the sum of n integers with $2n$ bits each. Those integers are either 0 or a shift of one of the two input numbers — depending on the respective bit of the other input number. Thus multiplication is in NC^1. □

Lemma 3.20. *The multiplication of n integers with n bits each in balanced p-ary representation is in NC^2 for $p \geq 3$.*

Proof. (from [4], §3) Again, use a balanced tree representation of the arithmetic expression with depth $O(\log(n))$. Since each operation is in NC^1 the whole circuit has depth $O(\log^2(n))$. □

Obviously, this non-standard representation requires efficient conversions.

Lemma 3.21. *Conversion from binary to balanced 4-ary representation is in NC^0 and conversion from balanced 4-ary representation to binary representation is in NC^1.*

Proof. (from [4], §2) Starting with binary representation, the only thing that has to be done is to group the bits in chunks of two and assign the proper sign. This is obviously in NC^0. For the converse, apply the technique of [29]. Let $(a_0, \dots, a_n)$ be the balanced 4-ary representation and compute the standard 4-ary representation $\sigma(b_0, \dots, b_{n+1})$ with sign $\sigma \in \{-1, 1\}$ and coefficients $b_k \in \{0, 1, 2, 3\}$ for $k = 0, \dots, n+1$. The binary representation is obtained by reinterpreting each digit as two bits.

In order to compute the sign σ, define the function $v_{a_k}(c_k)$ which computes the carry-over $c_{k+1} \in \{-1, 0, 1\}$ such that $b_k = a_k + c_k - 4c_{k+1} \in \{0, 1, 2, 3\}$ for $k = 0, \dots, n$. This can be implemented in NC^0. Then $\sigma_{k+1} = (v_{a_k} \circ \ldots \circ v_{a_0})(0)$. Since the concatenation of functions is associative and the functions have only finitely many values, one can compute this concatenation as balanced binary tree and then plug in 0 in order to obtain the sign $\sigma = c_{n+1}$ in NC^1. For the computation of the digits, the same technique can be used. □

Independently, Chiu used the Chinese remainder representation and efficient conversions to show that integer comparison can be realized efficiently.

Lemma 3.22 (Chiu 1995)**.** *The comparison of two integers in binary representation is in NC^1.*

Proof. See [8], §3.3. □

The combination of these lemmas yields a comparison circuit for scalar products in NC^1 using binary representation. Applying theorem 3.13, this can be simulated by a logspace-bounded Turing machine. Since Chiu's results about integer comparison is rather involved, a direct proof of the corollary will be given here.

Corollary 3.23. *Given vectors $u, v, w \in \mathbb{Q}^n$ with q-bit entries, $u \cdot w < v \cdot w$ can be decided by a SPACE$(\log^2(nq))$-bounded Turing machine.*

Proof. First consider the case $u, v, w \in \mathbb{N}^n$. It was already shown that $u \cdot w$ and $v \cdot w$ can be computed in NC^1 and, by theorem 3.13, in SPACE$(\log(nq))$. It remains to cover the integer comparison. While it is rather involved to design a family of uniform circuits with logarithmic depth, it is straight forward to program a Turing machine with logarithmic space. Starting at the most significant bits, compare the bits of both numbers sequentially.

It suffices to store the index of the bit which is currently compared which only requires space $O(\log(n))$. Since the numbers cannot be stored on the working tape, the required bits are computed on demand.

If $u, v, w \in \mathbb{Q}^n$, first multiply each vector with the product of all denominators in u, v, w. For each coefficient, these $O(n)$ multiplications can be done by a family of circuits in NC^2. The bitsize of the input blows up by a factor of $O(n)$ which can be neglected due to the logarithm in the formula of the space complexity. □

Borodin et al. also prove similar results for larger, derived rings. The following lemma only lists some examples.

Lemma 3.24 (Borodin et al. 1983)**.** *$\mathbb{Z}$, $\mathbb{Z}[X]$, and $\mathbb{Z}^{n,m}$ are well-endowed rings.*

Proof. See [4], §§2-3. □

A rather surprising result of complexity theory is about solving systems of linear equations. Borodin et al. [4] constructed a family of Boolean circuits that solves various problems for linear systems over a well-endowed field in NC^2.

Theorem 3.25 (Borodin et al. 1983)**.** *Let $A \in \mathbb{K}^{n\times n}$ be a matrix over a well-endowed field. Then the computation of its determinant, characteristic polynomial, rank, and adjoint matrix are in NC^2.*

Proof. See [4], corollary 4.3, proposition 2.1, and proposition 2.2. □

The rank of a matrix can be determined from the characteristic polynomial since the corank equals the exponent of the highest power of the indeterminate that divides the characteristic polynomial. In order to compute the rank of a rectangular rational matrix, multiply it with its transpose to obtain a square matrix with the same rank. Finally, the adjoint matrix can be computed by a polynomial number of uniform determinant computations. Thus all these algorithms are in NC^2. Again, applying theorem 3.13 yields space bounded Turing machines for the respective problems.

Corollary 3.26. *Let $n \geq m$, $A \in \mathbb{K}^{n\times m}$ a matrix over a well-endowed with q-bit numerators and denominators. Then the computation of its rank and adjoint matrix, and, if $n = m$, its determinant and characteristic polynomial are in SPACE$(\log^2(nq))$.*

Part II.

Degree Bounds

As mentioned previously, Gröbner bases can be used to effectively solve problems in polynomial rings, e.g. the membership problem. Thus a certain interest in the difficulty of their computation is self-evident. Their size is of similar importance since the complexity of most further computations will depend on it.

The degree of the Gröbner basis turned out to be an appropriate measure of both the effort of computation and the size of Gröbner basis. Knowing the degree will suffice for determining the complexity of the Gröbner basis computation and the further computations, as will be shown later.

The representation problem is more or less an explicit version of the membership problem. For an arbitrary ideal basis, the objective is to find a polynomial combination of the basis elements which equals a given polynomial. Again it is possible to ask for a bound of the degree of the representation. This makes the reduction of the representation problem (and thus the ideal membership problem) to a system of linear equations possible.

In this part of the thesis, the focus is on degree bounds for Gröbner bases and the representation problem. While the following two chapters list a lot of previously known results for both problems, the contributions of the author are explored in detail and self-contained. Both chapters are organized in sections which correspond to classes of ideals or — in the case of radical membership — to a variant of the original problem. Formally, the problems can be stated as

Problem (Representation Basis Degree)**.** *Given an ideal basis $F \subseteq \mathbb{K}[X]$, find lower and upper bounds for the maximal degree $R(h, F)$ of a minimal representation of an ideal member $h \in \langle F \rangle$, i.e.*

$$R(h,F) = \min \left\{ d \in \mathbb{N} : h = \sum_{f \in F} a_f f \textit{ with } a_f \in \mathbb{K}[X], \deg(a_f f) \leq d \textit{ for all } f \in F \right\}.$$

Problem (Gröbner Basis Degree)**.** *Given an ideal basis $F \subseteq \mathbb{K}[X]$, find lower and upper bounds for the maximal degree $G(F)$ of polynomials in the reduced Gröbner basis (w.r.t. any monomial ordering) of $\langle F \rangle$, i.e.*

$$G(F) = \max \{\deg(g) : g \in \mathrm{GB}_{\prec}(F), \prec \textit{ admissible}\}.$$

4. Representation Degree

The representation degree has been studied in various situations and a couple of bounds have been given by previous authors. The following is a comprehensive summary of the tightest bounds that are known to the author at the time of writing. This means, that the historic development of the bounds will not be analyzed. Besides the exposition of known results, the chapter includes a single exponential lower bound for the representation degree in toric ideals which is completely new.

4.1. Arbitrary Ideals

Long before the first people thought about computations in polynomial rings and Gröbner bases were defined, mathematicians considered the representation problem. Already back in 1926, Hermann proved a double exponential upper degree bound. The original proof has flaws, but they have been resolved later on using the same basic idea.

Theorem 4.1 (Hermann 1926)**.** *Let I be an ideal in $\mathbb{K}[X]$ generated by a set of polynomials $F = \{f_1, \dots, f_s\}$ of maximal degree d and let $h \in I$. Then the representation degree is bounded by*

$$R(h, F) \leq \deg(h) + d + (sd)^{2^n}.$$

Proof. The original proof in [19] is well-known to be incorrect. In the appendix of [33], there is a self-contained proof of the result. □

On the other hand, there is a well-known lower bound, also double exponential but with smaller constants, which was first proved by Mayr and Meyer in [33] and later improved by Yap.

Theorem 4.2 (Yap 1991)**.** *There are a family of ideals $I_n \subseteq \mathbb{K}[X]$ with $n \in \mathbb{N}$, generated by $O(n)$ polynomials F_n of degrees bounded by d and polynomials $h_n \in I_n$ of degree 1 such that each representation of h by F_n has degree at least*

$$R(h, F_n) \geq d^{2^{(1/2-\varepsilon)n}} \text{ for any } \varepsilon > 0 \text{ and sufficiently large } d, n \in \mathbb{N}.$$

Proof. See [44], §8. □

Summarizing, the situation is rather well understood for arbitrary polynomial ideals with upper and lower bounds matching up to a factor of 2 in the highest exponent.

4.2. Radical Membership

The following results also apply to arbitrary ideal and contrast the previous section in an astonishing way. One might think that powers of a polynomial $f \in \mathbb{K}[X]$ will have higher representation degrees since $\deg(f^k) = k \deg(f)$ for any $k \in \mathbb{N}$. But just the opposite of this expectation is true — at least in the worst case. There are many bounds for the radical membership problem. Jelonek was able to remove a limitation of Kollár's bound which renders his result optimal in the use cases of this thesis.

Theorem 4.3 (Jelonek 2005)**.** *Let I be an ideal in $\mathbb{K}[X]$ generated by polynomials $f_1, \ldots, f_s$ of degrees $d_1 \geq \ldots \geq d_s$. Then*

$$\sqrt{I}^k \in I \qquad \textit{for some } k \leq \begin{cases} d_1 \cdots d_s & \textit{if } 1 \leq s \leq n \\ d_1 \cdots d_{n-1} d_s & \textit{if } 1 < n \leq s \\ d_s & \textit{if } n = 1 \end{cases}$$

Proof. See [21], theorem 1.3. Note that the field does *not* have to be algebraically closed. This can be seen by a standard reasoning which reduces $f^k \overset{?}{\in} I$ for given $f \in \mathbb{K}[X]$ and $k \in \mathbb{N}$ to a system of linear equations which has a solution over the algebraic closure $\overline{\mathbb{K}}$ iff it is solvable over $\mathbb{K}$. □

The following example proves that the bound given in theorem 4.3 is tight.

Example 4.4 (Kollár 1988)**.** *(from [23], example 2.3) Consider the ideal I generated by the polynomials $x_1^{d_1}, x_1 - x_2^{d_2}, \ldots, x_{s-1} - x_s^{d_s}$ in $\mathbb{K}[X]$ for $s \leq n$. It is well-known and easy to verify, that $x_s^{d_1 \cdots d_s} \in I$ but $x_s^{d_1 \cdots d_s - 1} \notin I$. This provides a matching lower bound for the exponent of the radical membership problem. As generalization, note that, for any $f \in I$ and $k \geq 1$, $(f + x_s)^k \in I$ iff $x_s^k \in I$.*

Due to the importance of this example, the implication is stated as theorem.

Theorem 4.5 (Kollár 1988)**.** *For any $s \leq n \in \mathbb{N}$ and $d, d_1, \ldots, d_s \in \mathbb{N}$, there are an ideal I in $\mathbb{K}[X]$ generated by polynomials $f_1, \ldots, f_s$ of degrees $d_1, \ldots, d_s$ and a polynomial $h \in \sqrt{I}$ of degree d such that $h^k \notin I$ for all $k < d_1 \cdots d_s$.*

4.3. Zero-Dimensional Ideals

Apart from arbitrary ideals, ideals of dimension 0 have been studied most intensely. They appear in many applications on the one side and proved to be less complex on the other side. Still the bounds for the representation problem of zero-dimensional ideals are not tight. This is in contrast to the Gröbner basis degree as section 5.2 will show.

Theorem 4.6 (Dickenstein, Fitchas, Giusti, Sessa 1991)**.** *Let $I \subsetneq \mathbb{K}[X]$ be a zero-dimensional ideal generated by polynomials $F = \{f_1, \dots, f_s\}$ of maximal degree d and let $h \in I$. Then the representation degree is bounded by*

$$R(h, F) \leq \deg(h) + (nd)^{2n} + d^n + d.$$

Proof. See [11], corollary 3.4. □

4.4. Complete Intersections

Complete intersections were introduced in section 2.7 as ideals which are generated by regular sequences. Since these are defined as nicely behaving ideals in some sense, it comes at no surprise that the representation degrees are low for such ideals.

Theorem 4.7 (Dickenstein, Fitchas, Giusti, Sessa 1991)**.** *Let I be a complete intersection ideal in $\mathbb{K}[X]$ generated by polynomials $F = \{f_1, \dots, f_s\}$ of maximal degree d and let $h \in I$. Then the representation degree is bounded by*

$$R(h, F) \leq \deg(h) + d^s.$$

Proof. See [11], theorem 5.1. □

4.5. Dimension-Dependent Bounds

In his Bachelor's thesis, Kratzer uses Bézout's theorem and Kollár's bound for the radical membership in order to proof a representation bound depending on the ideal dimension. As tool he uses an effective version of the well-known Noether normalization by Dickenstein, Fitchas, Guisti, and Sessa. Their proof will be revisited in the following in order to obtain a slightly tighter bound.

Theorem 4.8 (Noether Normalization)**.** *Let $\mathbb{K}$ be an infinite field and $I \subsetneq \mathbb{K}[X]$ be an ideal of dimension r generated by polynomials $F = \{f_1, \dots, f_s\}$ of degrees $d_1 \geq \ldots \geq d_s$. Then there is an invertible linear change of coordinates*

$$\sigma : \mathbb{K}[X] \longrightarrow \mathbb{K}[X], x_i \mapsto a_{i,1}x_1 + \ldots + a_{i,n}x_n \qquad \textit{with } a_{i,j} \in \mathbb{K} \textit{ for } i, j = 1, \dots, n$$

such that $\{x_1, \dots, x_r\}$ is a maximal independent set w.r.t. $\sigma(I)$ and, for each $i = r+1, \dots, n$, there is a polynomial $h_i \in \sigma(I) \cap \mathbb{K}[x_1, \dots, x_i]$ which is monic in x_i, i.e. $\deg_{x_i}(h_i) = \deg(h_i) > 0$. Then $\sigma(I)$ is said to be in Noether position. *The degrees can be bounded by* $\deg(h_i) \leq (d_1 \cdots d_{n-r})^2$.

Proof. (from [11], §1) By the definition of the ideal dimension, there is a w.r.t. I maximal independent set of cardinality $r = \dim(I)$. Hence, permuting the variables with σ one can assume $\sigma(I) \cap \mathbb{K}[x_1, \dots, x_r] = \{0\}$. The rest of the construction is by induction.

Let $r < k \leq n$, assume there are $h_i \in \sigma(I) \cap \mathbb{K}[x_1, \ldots, x_i]$ monic in x_i for $i = k + 1, \ldots, n$, and construct a polynomial $h_k \in \sigma(I)$ and an invertible change of coordinates $\sigma' = \tilde{\sigma} \circ \sigma$ such that $\tilde{\sigma}(h_i) \in \mathbb{K}[x_1, \ldots, x_i]$ is monic in x_i for $i = k, \ldots, n$ and $\{x_1, \ldots, x_r\}$ is independent modulo $\sigma'(I)$.

By lemma 2.80, there is a complete intersection $J \subseteq I$ generated by polynomials $g_1, \ldots, g_{n-r}$ of degrees $d_1 \geq \ldots \geq d_{n-r}$. Since $\dim(J) = \dim(I) = r$, $\{x_1, \ldots, x_r\}$ is a maximal independent set w.r.t. $\sigma(J)$ and $K = \sigma(J) \cap \mathbb{K}[x_1, \ldots, x_r, x_k] \neq \{0\}$. This implies $\operatorname{ht}(\sqrt{K}) = \operatorname{ht}(K) = 1$ as ideal of $\mathbb{K}[x_1, \ldots, x_r, x_k]$. Now let $\overline{\mathbb{K}}$ be the algebraic closure of $\mathbb{K}$. By the closure theorem 2.89, $\overline{\pi(\mathbf{V}_{\overline{\mathbb{K}}}(\sigma(J)))} = \mathbf{V}_{\overline{\mathbb{K}}}(K)$ where π is the projection onto the coordinates $\{1, \ldots, r, k\}$. Applying lemma 2.91 and Bézout's theorem 2.92,

$$\deg(\mathbf{V}_{\overline{\mathbb{K}}}(K)) \leq \deg(\mathbf{V}_{\overline{\mathbb{K}}}(\sigma(J))) \leq d_1 \cdots d_{n-r}.$$

By lemma 2.96, there is $0 \neq h \in \sqrt{K} = \sqrt{\sigma(J)} \cap \mathbb{K}[x_1, \ldots, x_r, x_k]$ with $\deg(h) \leq d_1 \cdots d_{n-r}$. Since $\{x_1, \ldots, x_r\}$ is independent w.r.t. $\sigma(J)$, $\deg_{x_k}(h) > 0$. Finally, by theorem 4.3, $h^e \in \sigma(J) \subseteq \sigma(I)$ for some $e \leq d_1 \cdots d_{n-r}$. This yields $h_k = h^e \in \sigma(J) \cap \mathbb{K}[x_1, \ldots, x_r, x_k]$ with $\deg(h_k) \leq (d_1 \cdots d_{n-r})^2$ and $\deg_{x_k}(h_k) > 0$.

For the construction of $\tilde{\sigma}$, let $\tilde{h}$ be the homogeneous component of h_k of highest degree. Since $\tilde{h} \neq 0$ is homogeneous and $\mathbb{K}$ is infinite, there are values $y_1, \ldots, y_r \in \mathbb{K}$ such that $\tilde{h}(y_1, \ldots, y_r, 1) \neq 0$. Define $\tilde{\sigma}$ by $\tilde{\sigma}(x_i) = x_i + y_i x_k$ for $i = 1, \ldots, r$ and $\tilde{\sigma}(x_i) = x_i$ for $i = r + 1, \ldots, n$ which certainly is invertible. Then $\tilde{\sigma}(h_i) \in \mathbb{K}[x_1, \ldots, x_i]$ for all $i = k, \ldots, n$. Moreover, $\deg_{x_k}(\tilde{h}) = \deg(\tilde{h})$ shows that $\tilde{\sigma}(h_k)$ is monic in x_k. Since $\deg_{x_i}(h_i) = \deg(h_i)$, $\tilde{\sigma}(x_i) = x_i$ for $i = k + 1, \ldots, n$, and $\tilde{\sigma}$ preserves the total degree, $\tilde{\sigma}(h_i)$ is also monic in x_i.

It remains to show that $\{1, \ldots, x_r\}$ is independent w.r.t. $\sigma'(I)$. Assume to the contrary $0 \neq f \in \sigma'(I) \cap \mathbb{K}[x_1, \ldots, x_r]$. Then $\tilde{\sigma}^{-1}(f) \in \sigma(I)$. The inverse of the coordinate change is defined by $\tilde{\sigma}^{-1}(x_i) = x_i$ for $i \neq k$ and $\tilde{\sigma}^{-1}(x_k) = x_k - \sum_{i=1}^{r} y_i x_i$ and hence $\tilde{\sigma}^{-1}(f) \in \mathbb{K}[x_1, \ldots, x_r]$. This contradicts the assumption that $\{1, \ldots, x_r\}$ is independent w.r.t. $\sigma(I)$. □

Note that the above result is a weak version of the Noether normalization. One can even obtain monic polynomials $h_i \in \sigma(I) \cap \mathbb{K}[x_1, \ldots, x_r][x_i]$ for $i = r + 1, \ldots, n$.

Theorem 4.9 (Kratzer 2008). *Let I be an ideal of dimension $\dim(I) = r$ in the polynomial ring $\mathbb{K}[X]$ over an infinite field $\mathbb{K}$, and let I be generated by polynomials $F = \{f_1, \ldots, f_s\}$ of maximal degree d and $h \in I$. Then the representation degree is bounded by*

$$R(h, F) \leq \deg(h) + \left(d\left((n+1)\max\left\{\deg(h), (n+2)^2\left(d^\mu + 1\right)^{\mu+2}\right\} + 1\right)^{n-r}\right)^{2^r}$$

for $\mu = \min\{n, s\}$.

Proof. See [24], theorem 5. □

Theorem 4.10. *There are a family of ideals $I_{r,n} \subseteq \mathbb{K}[X]$ with $r \leq n \in \mathbb{N}$, generated by $O(n)$ polynomials F_n of degrees bounded by d and polynomials $h_n \in I_n$ of degree 1 such that each representation of h by $F_{r,n}$ has degree at least*

$$R(h, F_{r,n}) \geq d^{2^{(1/2-\varepsilon)r}} \text{ for any } \varepsilon > 0 \text{ and sufficiently large } d, r, n \in \mathbb{N}.$$

Proof. Let F_r be as defined in theorem 4.2 and $F_{r,n} = F_r \cup \{x_{r+1}, \dots, x_n\}$. Then $I_{r,n}$, the ideal generated by $F_{r,n}$ in $\mathbb{K}[X]$, has dimension $\dim(I_{r,n}) \leq r$ and the degree bound is exactly as in theorem 4.2. □

4.6. Toric Ideals

The lower bound for the representation degree in toric ideals is not surprising. The proof, however, does not lack some kind of technical complexity. The approach is similar to the construction by Mayr and Meyer [33] in using a commutative Thue system. Since toric ideals are binomial by definition and commutative Thue systems also correspond to binomial ideals, the approach seems to be particularly suited. Note that the commutative Thue systems constructed by Mayr and Meyer are *not* toric. They use state variables to force the production into a certain direction. Toric ideals, however, are prime and so state variables factor out leaving much more flexibility for derivations. One main difficulty in the construction as well as in the proof will be to show that the ideal corresponding to the commutative Thue system is prime (and hence toric).

Instead of using state variables (or more general monomial factors) as canalization, it is necessary to keep the number of occurrences of the single variables very low (only in one or two productions). This diminishes the achieved degree bound by an order of magnitude compared to the Mayr-Meyer construction. Despite of the lack of non-trivial upper bounds for the representation degree, it seems unlikely that the presented bound can be improved dramatically. The better understood situation of the Gröbner basis degree exhibits single exponential upper and lower bounds which will be presented in section 5.4.

Example 4.11. *Consider the commutative Thue system over the alphabet $X_n = \{x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n\}$, which is given by the productions $\mathcal{P}_n$:*

$$\begin{aligned}
1 &\equiv x_1 y_1 & & \textit{(I)}\\
x_i^d &\equiv x_{i+1} y_{i+1} & (i = 1, \dots, n-1) & \quad \textit{(II)}\\
y_n &\equiv z_n & & \textit{(III)}\\
z_{i+1} y_i^d &\equiv z_i^d & (i = 1, \dots, n-1) & \quad \textit{(IV)}\\
z_1 &\equiv 1 & & \textit{(V)}
\end{aligned}$$

The first, obvious remark is that y_n and z_n can be merged to one variable and z_1 can be eliminated, as well. This yields an ideal in $3n-2$ variables. For the proofs, however, the above, redundant presentation will be beneficial. The following derivation will be of main interest:

Lemma 4.12. $x_n \equiv 1\ (\mathcal{P}_n)$

Proof.

$$1 \overset{\text{(I)}}{\equiv} x_1^{d^{n-1}} y_1^{d^{n-1}} \overset{\text{(II)}}{\equiv} x_n y_1^{d^{n-1}} y_2^{d^{n-2}} \cdots y_n \overset{\text{(III)}}{\equiv} x_n y_1^{d^{n-1}} y_2^{d^{n-2}} \cdots y_{n-1}^{d} z_n \equiv$$
$$\overset{\text{(IV)}}{\equiv} x_n z_1^{d^{n-1}} \overset{\text{(V)}}{\equiv} x_n\ (\mathcal{P}_n)$$

□

The claim is that there is no derivation of $x_n \equiv 1$ with much lower degree. Unfortunately, the derivation does not have strong uniqueness properties as derivations in the Mayr-Meyer ideals have. But it is possible to predict the structure of certain derivations.

Lemma 4.13. *Let $a_0 \to a_1 \to \ldots \to a_t$ be a derivation using rules (I), (II), (IV), (V). Then*

$$\deg_{y_k}(a_t) - \deg_{y_k}(a_0) = \sum_{j\geq 0}\Big(\deg_{x_{k+j}}(a_t) - \deg_{x_{k+j}}(a_0)\Big)\, d^j + \sum_{j\geq 1}\Big(\deg_{z_{k+j}}(a_t) - \deg_{z_{k+j}}(a_0)\Big)\, d^j \quad (4.1)$$

for $k = 1, \ldots, n$.

Proof. The proof is by induction on the length of the derivation t. Obviously, the statement is true for $t = 0$. For the induction step, assume the formula to be true for a_{t-1} and consider all allowed rules.

(I) The right-hand side of (4.1) only changes for $k = 1$ which is according to the change of the exponent of y_1.

(II, i) For $k > i + 1$ nothing changes. For $k < i + 1$ the changes of the exponents of x_i and x_{i+1} equal out. For $k = i + 1$ the exponents of x_{i+1} and y_{i+1} both change by 1.

(IV, i) For $k > i$ nothing changes. For $k < i$ the changes of the exponents of z_i and z_{i+1} equal out in (4.1). For $k = i$ the exponents of y_i and z_{i+1} change by d respectively 1 which is according to (4.1).

(V) None of the variables involved in (4.1) is changed.

□

Using this result, one can prove that all derivations of $1 \equiv x_n\ (\mathcal{P}_n)$ have exponentially high degrees.

Lemma 4.14. *All derivations of $x_n \equiv 1$ $(\mathcal{P}_n)$ have degree at least $\sum_{i=0}^{n} d^i = \frac{d^{n+1}-1}{d-1}$.*

Proof. Consider a derivation $1 = a_0 \to a_1 \to \ldots \to a_t = x_n$ and let k be minimal such that $a_{k-1} \to a_k$ is an application of rule (II) with $i = n-1$. Since $a_0 = 1$ and only rule (II) with $i = n-1$ involves x_n, a_k is the first word that contains x_n. Remember that y_n only appears in rule (II) with $i = n-1$ and rule (III). By the choice of k, y_n is not needed by any rule which is applied in the derivation $a_0 \to \ldots \to a_k$, so one can w.l.o.g. assume that rule (III) is not applied in the first k steps of the derivation (otherwise one could move the applications of rule (III) behind step k which does not change the degrees). Thus lemma 4.13 applies and yields

$$\deg(a_k) \geq \deg_{x_n}(a_k) + \sum_{i=1}^{n} \deg_{y_i}(a_k) \geq 1 + \sum_{i=1}^{n} d^i.$$

□

It remains to show that $I_{\mathcal{P}_n}$ is toric or, by lemma 2.108, that $I_{\mathcal{P}_n}$ is prime. The following lemma will provide a strategy to simplify the ideal.

Lemma 4.15. *Let I be an ideal in $\mathbb{K}[X]$, $x_n - h \in I$ for a polynomial $h \in \mathbb{K}[x_1, \ldots, x_{n-1}]$ and $I \cap \mathbb{K}[x_1, \ldots, x_{n-1}]$ be prime. Then I is prime, too.*

Proof. Let $f = f_1 f_2 \in I$. Define the polynomial

$$\tilde{f}(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, h(x_1, \ldots, x_{n-1}))$$

and $\tilde{f}_1$, $\tilde{f}_2$ analogously. Thus $\tilde{f} = \tilde{f}_1 \tilde{f}_2$ with $\tilde{f}, \tilde{f}_1, \tilde{f}_2 \in \mathbb{K}[x_1, \ldots, x_{n-1}]$ and, since $x_n - h \in I$, $f - \tilde{f}, f_1 - \tilde{f}_1, f_2 - \tilde{f}_2 \in I$.

First assume $\deg(\tilde{f}_1) \geq 1$ and $\deg(\tilde{f}_2) \geq 1$. Since $\tilde{f} \in J = I \cap \mathbb{K}[x_1, \ldots, x_{n-1}]$ and J is prime, either $\tilde{f}_1 \in J$ or $\tilde{f}_2 \in J$, which implies $f_1 \in I$ respectively $f_2 \in I$.

If $\deg(\tilde{f}_1) = 0$, i.e. $\tilde{f}_1$ is a non-zero constant, then $\tilde{f} = \tilde{f}_1 \tilde{f}_2 \in J$ implies $\tilde{f}_2 \in J$ and thus $f_2 \in I$. The case $\deg(\tilde{f}_2) = 0$ is analogous.

Lastly, if $\tilde{f}_1 = 0$ (or, analogously, $\tilde{f}_2 = 0$), $f_1 \in I$. Therefore I is prime. □

Note that one obtains generators of $I \cap \mathbb{K}[x_1, \ldots, x_{n-1}]$ in this scenario by substituting h for x_n in all generators of I. Before applying this to $I_{\mathcal{P}_n}$, it is beneficial to get more familiar with the ideal by proving the following equivalences.

Lemma 4.16. *$z_{k+1} \equiv x_k^d$ $(\mathcal{P}_n)$ for $k = 1, \ldots, n-1$.*

Proof. First derive (similar to the first part of lemma 4.12)

$$\begin{aligned} x_k^d \overset{\text{(I)}}{\equiv} x_k^d x_1^{d^{n-1}-d^k} y_1^{d^{n-1}-d^k} \overset{\text{(II)}}{\equiv} x_k^{d^{n-k}} y_1^{d^{n-1}-d^k} \cdots y_k^{d^{n-k}-d} \equiv \\ \overset{\text{(II)}}{\equiv} x_n y_1^{d^{n-1}-d^k} \cdots y_k^{d^{n-k}-d} y_{k+1}^{d^{n-k-1}} \cdots y_n \ (\mathcal{P}_n). \end{aligned}$$

Now remember $x_n \equiv 1$ $(\mathcal{P}_n)$ and continue with

$$\begin{aligned} x_k^d &\overset{\text{(III)}}{\equiv} y_1^{d^{n-1}-d^k} \cdots y_k^{d^{n-k}-d} y_{k+1}^{d^{n-k-1}} \cdots y_{n-1}^{d} z_n \overset{\text{(IV)}}{\equiv} y_1^{d^{n-1}-d^k} \cdots y_k^{d^{n-k}-d} z_{k+1}^{d^{n-k-1}} \equiv \\ &\overset{\text{(IV)}}{\equiv} y_1^{d^{n-1}-d^k} \cdots y_{k-1}^{d^{n-k+1}-d^2} z_k^{d^{n-k}-d} z_{k+1} \overset{\text{(IV)}}{\equiv} z_1^{d^{n-1}-d^k} z_{k+1} \overset{\text{(V)}}{\equiv} z_{k+1} \ (\mathcal{P}_n). \end{aligned}$$

□

Now apply lemma 4.15 to the ideal $I_{\mathcal{P}_n}$ using the polynomials $x_n - 1$, $y_n - z_n$, $z_1 - 1$, and $z_{i+1} - x_i^d$ for $i = 1, \dots, n-1$ and obtain generators for $I'_n = I_{\mathcal{P}_n} \cap \mathbb{K}[x_1, \dots, x_{n-1}, y_1, \dots, y_{n-1}]$. Note that the polynomial $x_{n-1}^d - x_n y_n$ vanishes on substitution.

$$\begin{aligned} I'_n = &\left\langle x_1 y_1 - 1, x_{i+1} y_{i+1} - x_i^d : i = 1, \dots, n-2 \right\rangle + \\ &\left\langle x_1^d y_1^d - 1, x_i^d y_i^d - x_{i-1}^{d^2} : i = 2, \dots, n-1 \right\rangle. \end{aligned}$$

Since $(x_1 y_1 - 1) \mid (x_1^d y_1^d - 1)$ and $(x_{i+1} y_{i+1} - x_i^d) \mid (y_{i+1}^d x_{i+1}^d - x_i^{d^2})$ for $i = 1, \dots, n-1$, this simplifies to

$$I'_n = \left\langle x_1 y_1 - 1, x_{i+1} y_{i+1} - x_i^d : i = 1, \dots, n-2 \right\rangle.$$

Due to lemma 4.15 it suffices to show that I'_n is prime. This will imply that $I_{\mathcal{P}_n}$ is prime and therefore toric.

Rather than dealing with ideals, return to commutative Thue system. The productions ${\mathcal{P}'}_n = \left\{ x_1 y_1 \equiv 1, x_i^d \equiv x_{i+1} y_{i+1} : i = 1, \dots, n-2 \right\}$ represent the ideal I' and thus are also equivalences of $\mathcal{P}_n$. Therefore the following is an extension the of lemma 4.13 for ${\mathcal{P}'}_n$.

Lemma 4.17.

$$x_1^{c_1} \cdots x_{n-1}^{c_{n-1}} y_1^{d_1} \cdots y_{n-1}^{d_{n-1}} \equiv x_1^{e_1} \cdots x_{n-1}^{e_{n-1}} y_1^{f_1} \cdots y_{n-1}^{f_{n-1}} \ ({\mathcal{P}'}_n)$$

if and only if

$$f_j = d_j + \sum_{i=0}^{n-j-1} (e_{j+i} - c_{j+i}) d^i \text{ and } c_j, d_j, e_j, f_j \geq 0 \quad \text{for } j = 1, \dots, n-1. \tag{4.2}$$

Proof. Since the rules in ${\mathcal{P}'}_n$ are (a subset of) the rules (I) and (II) in $\mathcal{P}_n$, lemma 4.13 applies. Thus (4.2) must hold for all equivalent words. It remains to show that this condition is sufficient. The proof is by induction on n. The case $n = 2$ is clear.

Postulate the statement for $n - 1$ and prove it for n. Since the equivalence is symmetric, assume w.l.o.g. $c_{n-1} < e_{n-1}$.

Remember the proof of lemma 4.12 derived (with n shifted by 1)

$$1 \equiv x_{n-1} y_1^{d^{n-2}} y_2^{d^{n-3}} \cdots y_{n-1} \ ({\mathcal{P}'}_n)$$

by only using rules in ${\mathcal{P}'}_n$. Repeating this $e_{n-1} - c_{n-1}$ times yields

$$x_1^{c_1} \cdots x_{n-1}^{c_{n-1}} y_1^{d_1} \cdots y_{n-1}^{d_{n-1}} \equiv x_1^{c_1} \cdots x_{n-2}^{c_{n-2}} x_{n-1}^{e_{n-1}} y_1^{\tilde{d}_1} \cdots y_{n-1}^{\tilde{d}_{n-1}} \; ({\mathcal{P}'}_n)$$

with $\tilde{d}_j = d_j + (e_{n-1} - c_{n-1}) d^{n-1-j} \geq 0$ for $j = 1, \ldots, n-1$. Therefore $\tilde{d}_{n-1} = f_{n-1}$ by (4.2) and

$$f_j = \tilde{d}_j + \sum_{i=0}^{n-j-2} (e_{j+i} - c_{j+i}) d^i.$$

The rest of the derivation exists by induction. □

This structure analysis suffices to prove the wanted result.

Lemma 4.18. *$I_{{\mathcal{P}'}_n} \subseteq \mathbb{K}[X]$ is prime.*

Proof. Since $I_{{\mathcal{P}'}_n}$ is a binomial ideal, it is prime if and only if it is toric (lemma 2.108). So it suffices to show for arbitrary monomials $m_1, m_2 \in \mathbb{K}[X]$ that $m_1 - m_2 \in I_{{\mathcal{P}'}_n}$ implies $m_1' - m_2' \in I_{{\mathcal{P}'}_n}$ for $m_i' = \frac{m_i}{\gcd(m_1, m_2)}$ $(i = 1, 2)$, and that $m_1^k - m_2^k \in I_{{\mathcal{P}'}_n}$ implies $m_1 - m_2 \in I_{{\mathcal{P}'}_n}$ for any $k \geq 1$.

If $m_1 - m_2 \in I_{\mathcal{P}'}$, $m_1 = x_1^{c_1} \cdots x_{n-1}^{c_{n-1}} y_1^{d_1} \cdots y_{n-1}^{d_{n-1}}$ and $m_2 = x_1^{e_1} \cdots x_{n-1}^{e_{n-1}} y_1^{f_1} \cdots y_{n-1}^{f_{n-1}}$, lemma 4.17 yields

$$f_j = d_j + \sum_{i=0}^{n-j-1} (e_{j+i} - c_{j+i}) d^i \text{ and } c_j, d_j, e_j, f_j \geq 0 \qquad \text{for } j = 1, \ldots, n-1.$$

Assume $m = x_1^{g_1} \cdots x_{n-1}^{g_{n-1}} y_1^{h_1} \cdots y_{n-1}^{h_{n-1}}$ divides m_1 and m_2. Then, for $j = 1, \ldots, n-1$,

$$\tilde{c}_j = c_j - g_j \geq 0, \qquad \tilde{d}_j = d_j - h_j \geq 0, \qquad \tilde{e}_j = e_j - g_j \geq 0, \qquad \tilde{f}_j = f_j - h_j \geq 0,$$

and

$$\tilde{f}_j = \tilde{d}_j + \sum_{i=0}^{n-j-1} (\tilde{e}_{j+i} - \tilde{c}_{j+i}) d^i.$$

Hence, using lemma 4.17 again,

$$\frac{m_1}{m} - \frac{m_2}{m} = x_1^{\tilde{c}_1} \cdots x_{n-1}^{\tilde{c}_{n-1}} y_1^{\tilde{d}_1} \cdots y_{n-1}^{\tilde{d}_{n-1}} - x_1^{\tilde{e}_1} \cdots x_{n-1}^{\tilde{e}_{n-1}} y_1^{\tilde{f}_1} \cdots y_{n-1}^{\tilde{f}_{n-1}} \in I_{{\mathcal{P}'}_n}.$$

Now let $m_1^k - m_2^k \in I_{{\mathcal{P}'}_n}$ for some monomials $m_1 = x_1^{c_1} \cdots x_{n-1}^{c_{n-1}} y_1^{d_1} \cdots y_{n-1}^{d_{n-1}}$ and $m_2 = x_1^{e_1} \cdots x_{n-1}^{e_{n-1}} y_1^{f_1} \cdots x_{n-1}^{f_{n-1}}$ and $k \geq 1$. Lemma 4.17 implies

$$k f_j = k d_j + \sum_{i=0}^{n-j-1} (k e_{j+i} - k c_{j+i}) d^i \text{ and } c_j, d_j, e_j, f_j \geq 0 \qquad \text{for } j = 1, \ldots, n-1,$$

and thus

$$f_j = d_j + \sum_{i=0}^{n-j-1} (e_{j+i} - c_{j+i})d^i \text{ and } c_j, d_j, e_j, f_j \geq 0 \qquad \text{for } j = 1, \ldots, n-1.$$

This results in $m_1 - m_2 \in I_{\mathcal{P}'_n}$ and proves that $I_{\mathcal{P}'_n}$ is prime. □

Summing up the results, $\mathcal{P}_n$ is prime since $\mathcal{P}'_n$ is prime, and since it is binomial, it is a toric ideal. This finishes the proof of the single exponential lower bound for the representation degree in toric ideals.

Theorem 4.19. *There are a family of toric ideals $I_{\mathcal{P}_n}$ in $3n-2$ variables for each $n \in \mathbb{N}$, generated by $O(n)$ binomials $\mathcal{P}_n$ of degrees bounded by d and binomials $h_n \in I_{\mathcal{P}_n}$ of degree 1 such that each representation of h_n by $\mathcal{P}_n$ has degree at least*

$$R(h_n, \mathcal{P}_n) \geq \sum_{i=0}^{n} d^i.$$

5. Gröbner Basis Degree

In the second chapter about degree bounds, the degrees of polynomials in Gröbner bases will be analyzed. The algorithm in chapter 6 will motivate these elaborate studies and show that these bounds essentially determine the worst case complexity of the Gröbner basis computation. Just like the previous chapter, the following will be an extensive compilation of the tightest bounds to the best of the author's knowledge.

There are two contributions of the author of this thesis to this topic. The first is the previously published dimension-dependent bound improving on Dubé's bound for arbitrary ideals. The first publication contains a mistake which is uncovered and fixed (yielding a slightly worse upper bound). On the other hand, the lower bound is improved in comparison with the previous publication. The second contribution is a degree bound for toric ideals which is derived from a similar bound by Sturmfels for a different type of ideal representation.

5.1. Arbitrary Ideals

Most previous authors considered arbitrary ideals parametrized by the number of variables n and the degrees $d_1, \ldots, d_s$ of the polynomials $f_1, \ldots, f_s$ which generate the ideal. [1], [17], and [35] provide a double exponential upper bound for the Gröbner basis degree as explained in the introduction of [12]. [12] gives a combinatorial proof of an improved upper bound.

Theorem 5.1 (Dubé 1990)**.** *Let I be an ideal in $\mathbb{K}[X]$ generated by polynomials $F = \{f_1, \ldots, f_s\}$ of maximal degree d. Then the Gröbner basis degree is bounded by*

$$G(F) \leq 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}.$$

Proof. See [12]. □

Dubé's result is contrasted by a lower degree bound which also exhibits double exponential growth.

Theorem 5.2 (Yap 1991)**.** *Fix an admissible monomial ordering $\prec$. Then there are a family of ideals $I_n \subseteq \mathbb{K}[X]$ for $n \in \mathbb{N}$, generated by $O(n)$ polynomials F_n of degrees bounded by d such that each Gröbner basis has a maximal degree of at least*

$$\deg(\mathrm{GB}_{\prec}(F_n)) \geq d^{2^{(1/2-\varepsilon)n}} \textit{ for any } \varepsilon > 0 \textit{ and sufficiently large } d, n \in \mathbb{N}.$$

Proof. See [44], §8 and [44], ”Notes added in proof” for the proof for graded monomial orderings and [44], §1 for the reduction to arbitrary monomial orderings. □

The result is an improvement of the bounds derived by Möller and Mora [35] respectively by Huynh in [20] which both use the ideal which was presented by Mayr and Meyer in [33].

5.2. Zero-Dimensional Ideals

A special focus in research was on the class of zero-dimensional ideals. Here the bounds are smaller by a magnitude. The well-known theorem of Bézout (cf. [40]) immediately implies a singly exponential upper degree bound for radical ideals. Another approach using the theory of multiplicities yields the same bound for arbitrary homogeneous ideals. The generalization for inhomogeneous ideals is a bit more involved.

Lemma 5.3 (Caniglia, Galligo, Heintz 1989)**.** *Let $I \subsetneq \mathbb{K}[X]$ be a zero-dimensional ideal generated by polynomials $F = \{f_1, \ldots, f_s\}$ of degrees $d_1 \geq \ldots \geq d_s$. Then*

$$\dim_{\mathbb{K}}(\mathbb{K}[X]/I) \leq d_1 \cdots d_n.$$

Proof. See [6], theorem 17. □

Theorem 5.4. *Let $I \subsetneq \mathbb{K}[X]$ be a zero-dimensional ideal generated by polynomials $F = \{f_1, \ldots, f_s\}$ of degrees $d_1 \geq \ldots \geq d_s$. Then the Gröbner basis degree is bounded by*

$$G(F) \leq d_1 \cdots d_n.$$

Proof. There are two key observations. First of all, N_I is isomorphic to $\mathbb{K}[X]/I$ as vector space, so the bound of lemma 5.3 applies. Secondly, if any monomial $x^\alpha \in N_I$, also its divisors are irreducible. Thus $T = \operatorname{span}_{\mathbb{K}}\left\{x^\beta \in \mathbb{K}[X] : x^\beta \mid x^\alpha\right\} \subseteq N_I$. Now $\dim_{\mathbb{K}}(T) \geq \deg(x^\alpha) + 1$ yields an upper bound for the degree of the irreducible monomials. Finally, lemma 5.3 implies

$$G(F) \leq \max\left\{\deg(x^\alpha) + 1 : x^\alpha \in N_{I,\prec}, \prec \text{ admissible}\right\} \leq \dim(N_I) \leq d_1 \cdots d_n.$$

□

Note that [6], theorem 20 actually proves the bound nd^n for $d = \max\{d_1, \ldots, d_s\}$ which was also achieved by Dickenstein et al. in [11], theorem 3.3. Well-known examples show that the bound of theorem 5.4 is tight. One of them will be presented below.

Example 5.5. *This is a slight variation of [35], proposition 2.2. For any $n \in \mathbb{N}$ and $d_1, \ldots, d_n$, let $I \subseteq \mathbb{K}[X]$ be the ideal generated by*

$$\begin{aligned} f_1 &= x_1^{d_1} \\ f_2 &= x_1 + x_2^{d_2} \\ f_3 &= x_2 + x_3^{d_3} \\ &\vdots \\ f_n &= x_{n-1} + x_n^{d_n} \end{aligned}$$

Note that $(f_1, \ldots, f_n)$ is a regular sequence and thus $\dim(I) = 0$. For the lexicographic monomial ordering with $x_1 \prec \ldots \prec x_n$, it is easy to verify that $x_n^{d_1 \cdots d_n - 1}$ is irreducible. Hence every Gröbner basis contains an element of degree at least $d_1 \cdots d_n$.

Theorem 5.6 (cf. [35])**.** *For any $n \in \mathbb{N}$ and $d_1, \ldots, d_n \in \mathbb{N}$, there is a zero-dimensional ideal I in $\mathbb{K}[X]$ generated by polynomials $F = \{f_1, \ldots, f_n\}$ of degrees $d_1, \ldots, d_n$ such that*

$$G(F) \geq d_1 \cdots d_n.$$

For special monomial orderings, there is a better upper bound by Lazard. However, it does not apply to all zero-dimensional ideals. In this context one should recall example 2.76.

Theorem 5.7 (Lazard 1983)**.** *Let $I \subsetneq \mathbb{K}[X]$ be an ideal which is generated by polynomials $F = \{f_1, \ldots, f_s\}$ of degrees $d_1 \geq \ldots \geq d_s$. Fix a graded monomial ordering $\prec$ and assume $\dim \left\langle {}^h f_1, \ldots, {}^h f_s \right\rangle = 0$. Then there is a Gröbner basis w.r.t. $\prec$ with degree bounded by*

$$\deg(\mathrm{GB}_\prec(F)) \leq (d_1 - 1) + \ldots + (d_{n+1} - 1).$$

Here one defines $d_{n+1} = 1$ if $s = n$.

Proof. See [31], theorem 3. □

Lazard's bound is also tight and it is rather simple to come up with an example.

Example 5.8. *For any $n \in \mathbb{N}$ and $d_1, \ldots, d_n \in \mathbb{N}$, let $I \subseteq \mathbb{K}[X]$ be the ideal generated by*

$$\begin{aligned} f_1 &= x_1^{d_1} \\ f_2 &= x_1 x_2^{d_2 - 1} + x_2^{d_2} \\ f_3 &= x_2 x_3^{d_3 - 1} + x_3^{d_3} \\ &\vdots \\ f_n &= x_{n-1} x_n^{d_n - 1} + x_n^{d_n} \end{aligned}$$

Again, it is easy to see that $(f_1, \ldots, f_n)$ is a regular sequence and $\dim(I) = 0$ (actually, this is equivalent by corollary 2.75). For an arbitrary graded monomial ordering $\prec$ with $x_1 \succ \ldots \succ x_n$, a Gröbner basis of I contains the monomial $x_n^{(d_1-1)+\ldots+(d_n-1)}$.

Theorem 5.9. *For any $n \in \mathbb{N}$, $d_1, \ldots, d_n \in \mathbb{N}$, and any graded monomial ordering $\prec$, there is an ideal I in $\mathbb{K}[X]$ generated by polynomials $F = \{f_1, \ldots, f_n\}$ of degrees $d_1, \ldots, d_n$ such that* $\dim \left\langle {}^h f_1, \ldots, {}^h f_n \right\rangle = 0$ *and any Gröbner basis w.r.t. $\prec$ has a maximal degree of at least*

$$\deg(\mathrm{GB}_{\prec}(F)) \geq (d_1 - 1) + \ldots + (d_n - 1).$$

5.3. Dimension-Dependent Bounds

The bounds for arbitrary ideals and zero-dimensional ideals suggest that the actual reason for double exponential degrees in the reduced Gröbner bases is the dimension of an ideal, not the number of variables. One would hope that the behavior mirrors the bounds for the representation degree which were presented in section 4.5. So the results in this section will be no great surprise. Still the proofs use an interesting combination of tools reaching from the cone decompositions introduced by Dubé to regular sequences and an effective version of the Noether normal form which are used to handle the dimension of an ideal.

Unfortunately, the first publication [34] of this result contains an error in the proof of the upper degree bound. While the proof for the homogeneous case is correct, the reduction to inhomogeneous ideals in corollary 3.21 is incorrect. This is illustrated by example 2.83 in which the dimension of the ideal changes dramatically on homogenization. It will be shown how to avoid this using polynomials from the Noether normal form. Unfortunately, the resulting bound is slightly weaker than the one in [34].

In the homogeneous case, the space of normal forms will be represented as cone decomposition similar to [12]. Instead of computing a cone decomposition of the ideal, as well, a regular sequence will be embedded into the ideal using lemma 2.81. The corresponding complete intersection ideal approximates a large part of the original ideal and even has the same dimension. The cone decomposition of the normal forms will be extended to a cone decomposition with the same Hilbert function as the complement of the complete intersection. The formula for the Hilbert function of regular sequences from lemma 2.77 and an independence argument from the following section will reduce the calculations to a special case for which one can give an explicit construction and bound the degrees along the way. This yields a bound for homogeneous ideals. The general case will be reduced to this using an effective version of the Noether normal form. This way one can construct polynomials in the ideal whose homogenizations generate an ideal of the same height. Then the above reasoning can be applied. Unfortunately, the degrees of these polynomials are exponential in the number of variables. While the resulting degree bound is worse than in the homogeneous case, it still is double exponential only in the dimension of the ideal.

Cone Decompositions First recall section 2.5 where cone decompositions were introduced and some existence results were proved. In the following, some of Dubé's results from [12] will be presented which connect the degree of cone decompositions to the Gröbner basis degree. Moreover, the Hilbert polynomial of exact cone decompositions will be calculated in terms of the so-called Macaulay constants which also fix the degree of the cone decomposition. Finally, an independence argument will be given in order to simplify the calculation of the Macaulay constants.

Lemma 5.10 (Dubé 1990). *Let I be an ideal in $\mathbb{K}[X]$ and fix a graded admissible monomial ordering $\prec$. Then there is a homogeneous 0-standard cone decomposition P of N_I and the degree of the reduced Gröbner basis of I w.r.t. $\prec$ is bounded by* $\deg(\mathrm{GB}_{\prec}(I)) \leq \deg(P) + 1$.

Proof. (from [12], theorem 4.11) First remember that $N_{\mathrm{lm}(I)} = N_I$ and $G = \mathrm{lm}(\mathrm{GB}(I))$ is a reduced monomial basis of $\mathrm{lm}(I)$. Thus, by lemma 2.50, $P = \mathtt{Split}(1, X, G)$ is a homogeneous 0-standard cone decomposition of N_I. It remains to prove the degree bound. Note that, since $\prec$ is graded, $\deg(\mathrm{GB}(I)) = \deg(G)$.

Pick any $g \in G$ and consider $\mathtt{Split}(h, U, G : h)$ for $U \subseteq X$ and a monomial $h \in \mathbb{K}[X]$ such that $g \in \mathrm{lm}(I) \cap \mathbf{C}(h, U)$. Note that this especially holds for $U = X$ and $h = 1$.

If none of the termination condition holds, there are two recursive calls $\mathtt{Split}(h, U \setminus \{x_k\}, G : h)$ and $\mathtt{Split}(h, U, G : (x_k \cdot h))$. Since g and h are monomials and $\mathbf{C}(h, U) = \mathbf{C}(h, U \setminus \{x_k\}) \oplus \mathbf{C}(x_k \cdot h, U)$, either $g \in \mathrm{lm}(I) \cap \mathbf{C}(h, U \setminus \{x_k\})$ or $g \in \mathrm{lm}(I) \cap \mathbf{C}(x_k \cdot h, U)$.

Thus there is a call $\mathtt{Split}(h, U, G : h)$ with $g \in \mathrm{lm}(I) \cap \mathbf{C}(h, U)$ where one of the two termination conditions $1 \in G : h$ and $(G : h) \cap \mathbb{K}[U] = \emptyset$ holds. However, $g \in \mathbf{C}(h, U)$ implies $(G : h) \cap \mathbb{K}[U] \neq \emptyset$ which excludes the second termination condition.

Hence $1 \in G : h$ and, since G was assumed to be reduced, $h = g$. For the parent call $\mathtt{Split}(g', U', G : g')$ of $\mathtt{Split}(g, U, G : g)$, none of the termination conditions may hold. Since $1 \notin G : g'$, the parent call has the form $\mathtt{Split}(x_k^{-1} g, U, G : (x_k^{-1} g))$. Since $\mathbf{C}(x_k^{-1} g, U) \cap N_{\mathrm{lm}(I)} \neq \{0\}$, there must be a cone $C \in P$ with $\deg(C) \geq \deg(x_k^{-1} g) = \deg(g) - 1$. □

Definition 5.11. *Let P be a q-exact cone decomposition in $\mathbb{K}[X]$. If $P^+ = \emptyset$, let $q = 0$. Then the* Macaulay constants *of P are defined as*

$$a_k = \max\{q, \deg(C) + 1 : C \in P, \dim(C) \geq k\} \qquad \textit{for } k = 0, \ldots, n+1.$$

Note that $a_0 = \deg(P) + 1$, $a_1 = \deg(P^+) + 1$, and $a_{n+1} = q$, so it suffices to bound the Macaulay constants (actually a_0) in order to get a bound of the Gröbner basis degree using lemmas 5.10 and 2.53.

In the following, the Hilbert polynomial of an exact cone decomposition will be expressed by the Macaulay constants. Later, it will be discussed how to extend a cone decomposition such that the Hilbert function of the resulting cone decomposition is known thus yielding an approach for the calculation of the Macaulay constants.

Lemma 5.12 (Dubé 1990). *Let P be a q-exact degree-compatible cone decomposition of a vector space T in $\mathbb{K}[X]$ and $a_0, \ldots, a_{n+1}$ the Macaulay constants of P. Then*

$$\mathrm{HP}_T(z) = \binom{z - a_{n+1} + n}{n} - 1 + \sum_{i=1}^{n} \binom{z - a_i + i - 1}{i}.$$

Proof. (from [12], §7) Since P is q-exact, P^+ contains exactly one cone for each degree between q and $\deg(P^+)$. More precisely, for each degree $d = a_{i+1}, \dots, a_i - 1$, there is exactly one cone in P^+ which has dimension i for $i = 1, \dots, n$. Thus

$$\mathrm{HP}_T(z) = \sum_{C \in P^+} \mathrm{HP}_C(z) = \sum_{i=1}^{n} \sum_{d=a_{i+1}}^{a_i - 1} \binom{z - d + i - 1}{i - 1}.$$

Now one use the binomial identity

$$\binom{z-d+i-1}{i-1} = \binom{z-d+i}{i} - \binom{z-d+i-1}{i}$$

in order to obtain a telescoping sum which condenses to

$$\begin{aligned} \mathrm{HP}_T(z) &= \sum_{i=1}^{n} \left[\binom{z - a_{i+1} + i}{i} - \binom{z - a_i + i}{i} \right] \\ &= \binom{z - a_{n+1} + n}{n} - \binom{z - a_1 + 1}{1} + \sum_{i=2}^{n} \left[\binom{z - a_i + i - 1}{i - 1} - \binom{z - a_i + i}{i} \right] \\ &= \binom{z - a_{n+1} + n}{n} - 1 - \binom{z - a_1}{1} - \sum_{i=2}^{n} \binom{z - a_i + i - 1}{i}. \end{aligned}$$

□

The formula provided by lemma 5.12 still can be terrifying in computations, especially if the Macaulay constants are to be determined from a complicated Hilbert function. Such general computations will be avoided by the reduction to a special case. The essential insight is provided by the following lemma.

Lemma 5.13 (Dubé 1990). *Let P be a degree-compatible q-exact cone decomposition of a subspace T of $\mathbb{K}[X]$ for any $q \geq 1$. Then the Macaulay constants $a_1, \dots, a_{n+1}$ are uniquely determined by HP_T and q.*

Proof. (from [12], §7) The coefficients of a polynomial can be reconstructed by evaluating the derivatives at 0. The following is a discrete analogon. Define the *backwards difference operator* $(\nabla p)(z) = p(z) - p(z-1)$ for any function $p : \mathbb{Z} \longrightarrow \mathbb{Z}$ and all $z \in \mathbb{Z}$ and its iteration $\nabla^k p = \nabla(\nabla^{k-1} p)$ for any $k > 1$. The backward difference of binomial coefficients is easily computed. Assuming $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ and using the identity $\binom{z+a}{b} - \binom{(z-1)+a}{b} = \binom{z+a-1}{b-1}$, one obtains:

$$\nabla \binom{z+a}{b} = \begin{cases} \binom{z+a-1}{b-1} & \text{for } b > 0 \\ 0 & \text{for } b = 0 \end{cases}$$

and thus, for any $k \in \mathbb{N}$,

$$\nabla^k \binom{z+a}{b} = \begin{cases} \binom{z+a-k}{b-k} & \text{for } b \geq k \\ 0 & \text{for } b < k \end{cases}$$

Now apply ∇^k for $k = 1, \dots, n$ to the formula provided by lemma 5.12 and recall $a_{n+1} = q$:

$$(\nabla^k \mathrm{HP}_T)(z) = \binom{z - q + n - k}{n - k} - \sum_{i=k}^{n} \binom{z - a_i + i - 1 - k}{i - k} \tag{5.1}$$

Now extract the constant terms respectively evaluate at zero (just remember that the binomial coefficients represent polynomials in z). The constant term of

$$\binom{z+a}{b} = \frac{(z+a)\cdots(z+a-b+1)}{b \cdots 1}$$

is simply $\binom{a}{b}$ for $a \geq 0$, it is 0 for $0 \leq a < b$, but for $a < 0$ it is $(-1)^b \binom{b-a-1}{b}$. With $\binom{a}{b} = 0$ for $0 \leq a < b$, the constant term is $(-1)^b \binom{b-a-1}{b}$ for any $a < b$.

Since $a_i \geq q \geq 1$ for $i = 0, \dots, n$, collecting the constant terms of (5.1) yields

$$(\nabla^k \mathrm{HP}_T)(0) = (-1)^{n-k} \binom{q-1}{n-k} - \sum_{i=k}^{n} (-1)^{i-k} \binom{a_i}{i-k}.$$

Hence one can resolve for

$$a_{k+1} = (\nabla^k \mathrm{HP}_T)(0) - (-1)^{n-k} \binom{q-1}{n-k} + 1 + \sum_{i=k+2}^{n} (-1)^{i-k} \binom{a_i}{i-k}$$

and finally determine a_1 from the equation for $\mathrm{HP}_T(z)$ provided by lemma 5.12. □

Note that $q \geq 1$ is not essential for the proof of lemma 5.13. However it simplifies the technical reasoning and will not hurt later on.

As mentioned before, an arbitrary cone decomposition will be extended to the cone decomposition of a space whose Hilbert polynomial is known. Since complete intersections have nice Hilbert functions and capture the dimension of the ideal, they were chosen for this construction. Lemmas 5.13 and 2.77 combine to

Corollary 5.14. *Let J be an ideal in $\mathbb{K}[X]$ generated by a homogeneous regular sequence $g_1, \dots, g_t$ of degrees $d_1, \dots, d_t$ and fix an admissible monomial ordering. If P is a degree-compatible q-exact decomposition of a vector space $T \subseteq \mathbb{K}[X]$ with $\mathrm{HF}_T = \mathrm{HF}_{N_J}$ for any $q \geq 1$, its Macaulay constants $a_1, \dots, a_{n+1}$ only depend on q, n, t, and $d_1, \dots, d_t$.*

Note that a_0 is explicitly excluded from the above result. It will be shown later how to overcome this using the bounds on the other Macaulay constants.

A New Decomposition In order to bound the Macaulay constants of a homogeneous ideal $I = \langle f_1, \dots, f_s \rangle$, Dubé uses the direct decompositions

$$\mathbb{K}[X] = I \oplus N_I$$

and

$$I = \langle f_1 \rangle \oplus \bigoplus_{i=2}^{s} f_i \cdot N_{\langle f_1, \ldots, f_{i-1} \rangle : f_i}. \tag{5.2}$$

The Hilbert functions of $\mathbb{K}[X]$ and $\langle f_1 \rangle$ are easily determined, and for all other summands one can calculate exact cone decompositions using `Split` (algorithm 1). The drawback is that, in Dubé's construction, the Macaulay constants achieve their worst case bound in the zero-dimensional case. Therefore a different decomposition is necessary.

Looking back at Dubé's paper, the key to improvement can be found in [12], corollary 5.2. Instead of calculating a cone decomposition of I, he separates the cone $\mathbf{C}(f_1, X)$ from the cone decomposition as in (5.2) and thereby improves the final bound slightly. Dealing with arbitrary non-trivial ideals, this is the best that can be done. But restricting to ideals I of a certain dimension r, this decomposition can be improved using an embedded regular sequence $g_1, \ldots, g_{n-r}$ whose length equals the height of the ideal. The following is a generalization of [12], lemma 5.1.

Lemma 5.15. *Let I be an ideal in $\mathbb{K}[X]$ generated by homogeneous polynomials $g_1, \ldots, g_t, f_1, \ldots, f_s$, and let $J = \langle g_1, \ldots, g_t \rangle \subseteq I$. For a fixed admissible monomial ordering $\prec$,*

$$I = J \oplus \bigoplus_{i=1}^{s} f_i \cdot N_{J_{i-1} : f_i} \tag{5.3}$$

with $J_k = \langle g_1, \ldots, g_t, f_1, \ldots, f_k \rangle$ for $k = 0, \ldots, s$.

Proof. In order to prove this, use induction to show

$$J_k = J \oplus \bigoplus_{i=1}^{k} f_i \cdot N_{J_{i-1} : f_i} \qquad \text{for } k = 0, \ldots, s \tag{5.4}$$

Then the equality $I = J_s$ yields the stated result.

The "$\supseteq$"-inclusion of (5.4) is clear since $f_1, \ldots, f_s \in I$ and $J \subseteq I$. For the other inclusion, the case $k = 0$ is trivial. So assume $k > 0$ and prove

$$J_k = J_{k-1} \oplus \left(f_k \cdot N_{J_{k-1} : f_k} \right).$$

Let $f \in J_k$ and thus

$$f = h + a \cdot f_k \qquad \text{with } h \in J_{k-1}, a \in \mathbb{K}[X].$$

Rewriting

$$a = (a - \mathrm{nf}_{J_{k-1} : f_k}(a)) + \mathrm{nf}_{J_{k-1} : f_k}(a)$$

yields

$$a \cdot f_k \in f_k \cdot (J_{k-1} : f_k) + f_k \cdot N_{J_{k-1} : f_k}.$$

Since $f_k \cdot (J_{k-1} : f_k) \subseteq J_{k-1}$, one gets $f \in J_{k-1} + f_k \cdot N_{J_{k-1} : f_k}$. It remains to show that the sum is direct. For any $k = 0, \ldots, s$, assume $h \in J_{k-1} \cap f_k \cdot N_{J_{k-1} : f_k}$ and therefore $h = a \cdot f_k$ for some $a \in N_{J_{k-1} : f_k}$. However $h \in J_{k-1}$ implies $a \in J_{k-1} : f_k$ and thus $a = 0$ and $h = 0$. □

The decomposition (5.3) will be used for the construction of a cone decomposition complementing J starting from a cone decomposition of N_I. Since I is the ideal whose Gröbner basis shall be bounded, it will be important to make sure that the maximal degrees of cones do not decrease in order to be able to apply lemma 5.10 later.

Lemma 5.16. *Let I be an ideal in $\mathbb{K}[X]$ which is generated by homogeneous polynomials $g_1, \ldots, g_t$, $f_1, \ldots, f_s$ and fix an admissible monomial ordering. Furthermore let $J = \langle g_1, \ldots, g_t \rangle \subseteq I$ and $d = \max\{\deg(f_i) : i = 1, \ldots, s\}$. Then any homogeneous 0-standard cone decomposition Q of N_I may be completed to a homogeneous d-exact cone decomposition P of a vector space $T \subseteq \mathbb{K}[X]$ with $\mathrm{HF}_T = \mathrm{HF}_{N_J}$ such that $\deg(Q) \leq \deg(P)$.*

Proof. By lemma 2.50, one can construct a homogeneous 0-standard cone decomposition Q_k of $N_{J_{k-1}:f_k}$ with $J_k = \langle g_1, \ldots, g_t, f_1, \ldots, f_k \rangle$ for each $k = 1, \ldots, s$. Then $f_k \cdot Q_k$ is a homogeneous $\deg(f_k)$-standard cone decomposition of $f_k \cdot N_{J_{k-1}:f_k}$. By lemma 2.48, $Q, Q_1, \ldots, Q_s$ can be refined to homogeneous d-standard cone decompositions $\tilde{Q}, \tilde{Q}_1, \ldots,$ $\tilde{Q}_s$. Since

$$\mathbb{K}[X] = J \oplus \bigoplus_{i=1}^{s} f_i \cdot N_{J_{i-1}:f_i} \oplus N_I,$$

the union

$$Q' = \tilde{Q} \cup \tilde{Q}_1 \cup \ldots \cup \tilde{Q}_s$$

is a homogeneous d-standard cone decomposition of $T = \bigoplus_{i=1}^{s} f_i \cdot N_{J_{i-1}:f_i} \oplus N_I$ and $\mathrm{HP}_T = \mathrm{HP}_{N_J}$ is obvious since all polynomials are homogeneous. By lemma 2.53, Q' can be refined to a homogeneous d-exact cone decomposition P of T. None of the operations decreases the degree of the cone decomposition, so $\deg(Q) \leq \deg(P)$. □

By lemma 5.13, all Macaulay constants of a degree-compatible d-exact cone decomposition P of a vector space T complementing J except $a_0 = \deg(P) + 1$ are determined by the Hilbert polynomial. The actual purpose of this construction, however, is to bound $\deg(P)$ (see lemma 5.10). This can be realized using the regularity of the ideal (which is known for a homogeneous complete intersection) in order to bridge the gap between a_1 and a_0.

Lemma 5.17. *Let I be an ideal in $\mathbb{K}[X]$ and fix a graded admissible monomial ordering $\prec$. If P is a degree-compatible q-exact cone decomposition of a vector space $T \subseteq \mathbb{K}[X]$ with $\mathrm{HF}_T = \mathrm{HF}_{N_I}$ and corresponding Macaulay constants $a_0, \ldots, a_{n+1}$,*

$$a_0 \leq \max\{a_1, \mathrm{reg}(I)\}.$$

Proof. Since $\prec$ is graded, the Hilbert function of $\mathbb{K}[X] = I \oplus N_I$ can be computed as sum of the Hilbert functions of I and N_I. The latter can be expressed using the Hilbert functions of the cones of P since the cone decomposition is degree-compatible. Since $\mathrm{HF}_{\mathbb{K}[X]}(z) = \mathrm{HP}_{\mathbb{K}[X]}(z)$ for all $z \in \mathbb{Z}$ and, by definition of the regularity, $\mathrm{HF}_I(z) = \mathrm{HP}_I(z)$ for all $z \geq$

$\operatorname{reg}(I)$, using corollary 2.32 yields for $\max\{a_1, \operatorname{reg}(I)\} \leq z < a_0$

$$\begin{aligned}\#\{C \in P : \dim(C) = 0, \deg(C) = z\} = \mathrm{HF}_{N_I}(z) - \mathrm{HP}_{N_I}(z) = \\ = (\mathrm{HF}_{\mathbb{K}[X]}(z) - \mathrm{HF}_I(z)) - (\mathrm{HP}_{\mathbb{K}[X]}(z) - \mathrm{HP}_I(z)) = 0.\end{aligned}$$

Thus there are no cones with degree greater or equal $\max\{a_1, \operatorname{reg}(I)\}$ which implies the statement. □

Applying lemma 5.17 to a homogeneous complete intersection and using lemma 2.77, one obtains

Corollary 5.18. *Let J be an ideal in $\mathbb{K}[X]$ generated by a homogeneous regular sequence $(g_1, \ldots, g_t)$ with degrees $d_1, \ldots, d_t$ and fix an admissible monomial ordering. If P is a q-exact degree-compatible cone decomposition of a vector space $T \subseteq \mathbb{K}[X]$ with $\mathrm{HP}_T = \mathrm{HP}_{N_J}$ and corresponding Macaulay constants $a_0, \ldots, a_{n+1}$,*

$$a_0 \leq \max\{a_1, d_1 + \ldots + d_t - n + 1\}.$$

Actually, now everything is clear — at least for the homogeneous case. Let $I \subsetneq \mathbb{K}[X]$ be an ideal of dimension r generated by polynomials $f_1, \ldots, f_s$. Using lemma 2.81, one obtains a homogeneous regular sequence $(g_1, \ldots, g_{n-r})$ in I (with the same degrees). Let $J = \langle g_1, \ldots, g_{n-r} \rangle$ be the ideal generated by the regular sequence. With lemmas 5.10 and 5.16, one can compute an exact degree-compatible cone decomposition P of a vector space $T \subseteq \mathbb{K}[X]$ with $\mathrm{HF}_T = \mathrm{HP}_{N_J}$ such that $\deg(P) + 1$ is a bound of the Gröbner basis degree of I. By corollary 5.18, it suffices to determine the Macaulay constants $a_1, \ldots, a_{n+1}$ of P. This can be done — as Dubé originally did — by comparing the Hilbert polynomials of $\mathbb{K}[X]$ and $J \oplus N_J$. However, the calculations are somewhat cumbersome.

The clue for avoiding this trouble is the reduction to a special case. Remember corollary 5.14: the Macaulay constants of P only depend on a few constants. Thus it suffices to calculate them once (for each set of parameters) — for a special case with an easy structure.

Lemma 5.19. *Let $I \subsetneq \mathbb{K}[X]$ be an ideal of dimension r generated by homogeneous polynomials $g_1, \ldots, g_{n-r}, f_1, \ldots, f_s$ where $(g_1, \ldots, g_{n-r})$ is a regular sequence of degrees $d_1, \ldots, d_{n-r}$ and $d = \max\{\deg(f_i) : i = 1, \ldots, s\}$, and fix an admissible monomial ordering. If Q is a homogeneous 0-standard cone decomposition of N_I,*

$$\deg(Q) \leq \max\left\{\deg(P^+), d_1 + \ldots + d_{n-r} - n\right\}$$

where P is a degree-compatible d-exact cone decomposition of N_J and $J = \left\langle x_1^{d_1}, \ldots, x_{n-r}^{d_{n-r}} \right\rangle$.

Proof. Let $\tilde{I} = \langle g_1, \ldots, g_{n-r} \rangle$. By lemma 5.16, one can extend any homogeneous 0-standard cone decomposition Q of N_I to a homogeneous d-exact cone decomposition $\tilde{Q}$ of a vector space T with $\mathrm{HP}_T = \mathrm{HP}_{N_{\tilde{I}}}$ and degree $\deg(\tilde{Q}) \geq \deg(Q)$. Let $a_0, \ldots, a_{n+1}$ be the Macaulay constants of $\tilde{Q}$. By corollary 5.18, $\deg(\tilde{Q}) = a_0 - 1 \leq \max\{a_1 - 1, d_1 + \ldots + d_{n-r} - n\}$. However, the Macaulay constants $a_1, \ldots, a_{n+1}$ of $\tilde{Q}$ only depend on $d, n, n-r$, and the degrees $d_1, \ldots, d_{n-r}$ as proved in corollary 5.14. The ideal $J = \left\langle x_1^{d_1}, \ldots, x_{n-r}^{d_{n-r}} \right\rangle$ is obviously a r-dimensional ideal generated by a homogeneous regular sequence with the same degrees. Thus any degree-compatible d-exact cone decomposition P of N_J (which exists by lemmas 2.50, 2.48, 2.53) has the same Macaulay constants (except, possibly, a_0) and thus $\deg(Q^+) = \deg(P^+) = a_1 - 1$.

□

Example 5.20. *It is very surprising that the Macaulay constants are independent of the ideal, but only depend on the degrees of the generators and the dimension. For verification, consider the very simple ideal $J = \langle x^2 \rangle$ with dimension $\dim(I) = 2$ in the ring $\mathbb{K}[x, y, z]$. This ideal is a complete intersection of the form in lemma 5.19. Using the concepts of this section and the algorithms from section 2.5, one can obtain a 2-exact cone decomposition P of N_J (cf. example 2.54). Due to its size, only the cones of positive dimension are listed:*

$$\left\{\mathbf{C}(xz, \{y, z\}), \mathbf{C}(z^3, \{y, z\}), \mathbf{C}(y^2z^2, \{y\}), \mathbf{C}(xy^4, \{y\}), \mathbf{C}(y^6, \{y\}), \mathbf{C}(y^6z, \{y\})\right\}$$

Now let $I = \langle x^2 - xy, xy + xy \rangle$ which also is a homogeneous ideal of dimension $\dim(I) = 2$. One can embed the complete intersection $I' = \langle x^2 - xy \rangle$ into I and then compute a cone decomposition Q of a vector space T which complements I'. This cone decomposition extends a cone decomposition of N_I:

$$\begin{aligned} Q^+ = \big\{&\mathbf{C}(y^2, \{y, z\}), \mathbf{C}(xy^2 + xyz, \{y, z\}), \mathbf{C}(yz^3, \{z\}), \\ &\mathbf{C}(z^5, \{z\}), \mathbf{C}(xz^5, \{z\}), \mathbf{C}(xyz^5 + xz^6, \{z\})\big\} \end{aligned}$$

Both P and Q are 2-exact cone decompositions with the same parameters n, r, d and thus — as expected — have the same Macaulay constants:

$$a_1 = 8, a_2 = 4, a_3 = 2.$$

Macaulay Constants By lemma 5.19, it remains to bound the Macaulay constant a_1 of a d-exact cone decomposition of N_J for the ideal $J = \left\langle x_1^{d_1}, \ldots, x_{n-r}^{d_{n-r}} \right\rangle$ in $\mathbb{K}[X]$, which will be fixed for the remainder of this section. Note that this is a monomial ideal for which all monomial orderings are equivalent. Hence, the monomial ordering will not be mentioned in the following lemmas.

The special shape of this ideal allows to dramatically simplify the calculations compared to the proof in Dubé's paper which does not make any assumption on the ideal. Nevertheless, the obtained bound will apply to any ideal by the preceding considerations (lemma 5.19).

From $r = \dim(J) = \deg(\mathrm{HP}_J) + 1$, one immediately deduces:

Lemma 5.21. *Let $J = \left\langle x_1^{d_1}, \ldots, x_{n-r}^{d_{n-r}} \right\rangle$ be an ideal in $\mathbb{K}[X]$ and $a_0, \ldots, a_{n+1}$ the Macaulay constants of a degree-compatible d-exact cone decomposition P of N_J. Then*

$$a_n = \ldots = a_{r+1} = d.$$

In the following, the construction of a d-exact cone decomposition for J will be presented. Along the way, bounds for the remaining Macaulay constants will be derived. First it is necessary to determine N_J. The following observation is obvious.

Corollary 5.22. *Let $J = \left\langle x_1^{d_1}, \ldots, x_{n-r}^{d_{n-r}} \right\rangle$ be an ideal in $\mathbb{K}[X]$. Then the space of normal forms of J equals the direct product*

$$N_J = T_r \times \mathbb{K}[x_{n-r+1}, \ldots, x_n],$$

where the vector space T_r is given by

$$T_r = \operatorname{span}_{\mathbb{K}}\{x^\alpha \in \mathbb{K}[x_1, \ldots, x_{n-r}] : \alpha \in \mathbb{N}^n, \alpha_i < d_i \textit{ for } i = 1, \ldots, n-r\}. \tag{5.5}$$

The construction of the cone decomposition will be inductive. It will prove crucial that, in each step, the part of the normal forms which is not covered has a form similar to N_J — the direct product of a finite vector space T_k generated by monomials and a polynomial ring in less variables. Thus the (vector space) dimension of T_k determines the number of cones of the highest dimension.

Lemma 5.23. *Let $T_k \subseteq \mathbb{K}[x_1, \ldots, x_{n-k}]$ be a vector space generated by monomials and P_k a degree-compatible cone decomposition of $T_k \times \mathbb{K}[x_{n-k+1}, \ldots, x_n]$. Then P_k has exactly $\dim_{\mathbb{K}}(T_k)$ cones of dimension k.*

Proof. For $k = 0$, the statement is obvious. For $k \geq 1$, the key is to look at the Hilbert polynomials. Consider a monomial basis $\{b_1, \ldots, b_s\}$ of T_k. Thus

$$T_k \times \mathbb{K}[x_{n-k+1}, \ldots, x_n] = b_1\mathbb{K}[x_{n-k+1}, \ldots, x_n] \oplus \ldots \oplus b_s\mathbb{K}[x_{n-k+1}, \ldots, x_n]$$

and

$$\mathrm{HP}_{T_k \times \mathbb{K}[x_{n-k+1}, \ldots, x_n]}(z) = \sum_{i=1}^{s} \binom{z - \deg(b_i) + k - 1}{k-1}.$$

On the other hand, one can compute the Hilbert polynomial from the the cone decomposition P_k by corollary 2.43:

$$\mathrm{HP}_{T_k \times \mathbb{K}[x_{n-k+1}, \ldots, x_n]}(z) = \sum_{C \in P_k^+} \binom{z - \deg(C) + \dim(C) - 1}{\dim(C) - 1}.$$

Now compare the coefficients of z^{k-1} of both representations of the Hilbert polynomial. Since P_k^+ only contains cones of dimension at most k, this yields

$$\sum_{i=1}^{s} \frac{1}{(k-1)!} = \sum_{\substack{C \in P_k^+ \\ \dim(C) = k}} \frac{1}{(k-1)!}$$

and thus $\#\left\{C \in P_k^+ : \dim(C) = k\right\} = s = \dim_{\mathbb{K}}(T_k)$. □

Looking at the explicit formula (5.5) for T_r, one obtains $\dim(T_r) = d_1 \cdots d_{n-r}$ and thus

Corollary 5.24. *Let $J = \left\langle x_1^{d_1}, \ldots, x_{n-r}^{d_{n-r}} \right\rangle$ be an ideal in $\mathbb{K}[X]$ and $a_0, \ldots, a_{n+1}$ the Macaulay constants of a degree-compatible d-exact cone decomposition P of N_J. Then*

$$a_r = d_1 \cdots d_{n-r} + d.$$

Now turn to the actual construction of a d-exact cone decomposition of N_J. In each induction step, the number of cones can be determined by lemma 5.23. This also fixes $a_{k-1} - a_k$.

Lemma 5.25. *Let $J = \left\langle x_1^{d_1}, \ldots, x_{n-r}^{d_{n-r}} \right\rangle$ be an ideal in $\mathbb{K}[X]$. Then, for any $d \geq 2$, there exist d-exact cone decompositions P_k and finite-dimensional subspaces $T_k \subseteq N_J \cap \mathbb{K}[x_1, \ldots, x_{n-k}]$ with a monomial basis such that*

$$N_J = (T_k \times \mathbb{K}[x_{n-k+1}, \ldots, x_n]) \oplus \bigoplus_{C \in P_k} C \qquad \text{for } k = 0, \ldots, r.$$

Let $a_0, \ldots, a_{n+1}$ be the Macaulay constants of P_0. Then $a_{k-1} \leq \frac{1}{2} a_k^2$ for $k = 2, \ldots, r$.

Proof. The induction starts with $k = r$. Let $P_r = \emptyset$, $a_n = \ldots = a_{r+1} = d$ (which makes P_r d-exact), and define T_r as in (5.5), i.e. $\dim_{\mathbb{K}}(T_r) = d_1 \cdots d_{n-r} + d$. Then all requirements are fulfilled.

Now $P_{r-1}, \ldots, P_0$ and $T_{r-1}, \ldots, T_0$ will be constructed inductively such that all cones in $P_{k-1} \setminus P_k$ have dimension k for $k = 1, \ldots, r$. The claim $a_{k-1} \leq \frac{1}{2} a_k^2$, for $k = 2, \ldots, r$, follows from $a_k - a_{k+1} = \dim(T_k)$ and $\dim(T_{k-1}) + a_k \leq \frac{1}{2} a_k^2$, for $k = 1, \ldots, r$, which will be verified inductively.

Let $1 \leq k \leq r$. By induction, P_k and T_k exist such that

$$N_J = (T_k \times \mathbb{K}[x_{n-k+1}, \ldots, x_n]) \oplus \bigoplus_{C \in P_k} C.$$

In order to make the induction work, it is necessary to choose $T_{k-1} \subseteq T_k$ and $P_{k-1} \supseteq P_k$. Keep in mind that $P_{k-1} \setminus P_k$ will be the subset of a cone decomposition of $T_k \times \mathbb{K}[x_{n-k+1}, \ldots, x_n]$ containing all the cones of dimension k. Thus, by lemma 5.23, $P_{k-1} \setminus P_k$ must contain exactly $\dim_{\mathbb{K}}(T_k)$ cones of dimension k. $P_k \subseteq P_0$ is already constructed and contains all cones of dimension larger than k. Hence $a_n, \ldots, a_{k+1}$ are fixed. Since P_{k-1} shall be d-exact, the cones of dimension k must have the degrees $a_{k+1}, a_{k+1}+1, a_{k+1}+2, \ldots$. Let $\{b_1, \ldots, b_s\}$ be a monomial basis of T_k with $\deg(b_1) \leq \ldots \leq \deg(b_s)$ and choose

$$C_i = b_i x_{n-k+1}^{a_{k+1}+i-\deg(b_i)-1} \mathbb{K}[x_{n-k+1}, \ldots, x_n] \qquad \text{for } i = 1, \ldots, s.$$

It is easy to see that $C_i \subseteq T_k \times \mathbb{K}[x_{n-k+1}, \ldots, x_n]$, $\deg(C_i) = a_{k+1} + i - 1$, and $\dim(C_i) = k$. Thus $P_{k-1} = P_k \cup \{C_1, \ldots, C_s\}$ is a d-exact degree-compatible cone decomposition and, by construction, $a_k - a_{k+1} = \#\{C \in P_{k-1} : \dim(C) = k\} = \dim(T_k)$. Since $T_k \subseteq \mathbb{K}[x_1, \ldots, x_{n-k}]$, furthermore

$$T_k \times \mathbb{K}[x_{n-k+1}, \ldots, x_n] = C_1 \oplus \ldots \oplus C_s \oplus (T_{k-1} \times \mathbb{K}[x_{n-k+2}, \ldots, x_n])$$

where

$$T_{k-1} = \operatorname{span}_{\mathbb{K}}\{b_i x_{n-k+1}^e : i = 1, \ldots, s, e = 0, \ldots, a_{k+1} + i - \deg(b_i) - 2\} \\ \subseteq \mathbb{K}[x_1, \ldots, x_{n-k+1}].$$

The above formula also implies $\dim_{\mathbb{K}}(P_{k-1}) < \infty$. Moreover

$$N_J = (T_{k-1} \times \mathbb{K}[x_{n-k+2}, \ldots, x_n]) \oplus \bigoplus_{C \in P_{k-1}} C.$$

So it only remains to bound $\dim_{\mathbb{K}}(T_{k-1}) + a_k$.

$$\dim_{\mathbb{K}}(T_{k-1}) = \sum_{i=1}^{s} (a_{k+1} + i - \deg(b_i) - 1) \leq \sum_{i=1}^{s} (a_{k+1} + i - 1) = s a_{k+1} + \frac{1}{2} s(s-1)$$

With $s = \dim_{\mathbb{K}}(T_k) = a_k - a_{k+1}$, the induction hypothesis, and $a_{k+1} \geq d \geq 2$,

$$\begin{aligned} \dim_{\mathbb{K}}(T_{k-1}) + a_k &\leq (a_k - a_{k+1})a_{k+1} + \frac{1}{2}(a_k - a_{k+1})(a_k - a_{k+1} - 1) + a_k \\ &= \frac{1}{2}\left(a_k^2 - a_{k+1}^2 + a_k + a_{k+1}\right) \leq \frac{1}{2}\left(a_k^2 - a_{k+1}^2 + \frac{1}{2}a_{k+1}^2 + a_{k+1}\right) \leq \frac{1}{2}a_k^2. \end{aligned}$$

□

Lemma 5.25 yields a d-exact cone decomposition P_0 that represents N_J up to a finite-dimensional vector space T_0. Let $\{b_1, \ldots, b_s\}$ be a monomial basis of T_0. Then the union $P = P_0 \cup \{\mathbf{C}(b_i, \emptyset) : i = 1, \ldots, s\}$ is a d-exact cone decomposition of N_J with Macaulay constants which fulfill the bounds of corollary 5.24 and lemma 5.25.

Corollary 5.26. *Let $J = \left\langle x_1^{d_1}, \ldots, x_{n-r}^{d_{n-r}} \right\rangle$ be an ideal in $\mathbb{K}[X]$ and $a_0, \ldots, a_{n+1}$ the Macaulay constants of a degree-compatible d-exact cone decomposition P of N_J. Then*

$$a_k \leq 2\left[\frac{1}{2}(d_1 \cdots d_{n-r} + d)\right]^{2^{r-k}} \qquad \text{for } k = 1, \ldots, r.$$

From the construction, one can even verify that $a_0 = a_1$ as predicted by lemma 5.17. This concludes the proof for the homogeneous case as a_1 bounds the Gröbner basis degree.

Theorem 5.27. *Let $\mathbb{K}$ be an infinite field and $I \subsetneq \mathbb{K}[X]$ be an ideal of dimension $r > 0$ generated by homogeneous polynomials $F = \{f_1, \ldots, f_s\}$ of degrees $d_1 \geq \ldots \geq d_s$. Then the Gröbner basis degree is bounded by*

$$G(F) \leq 2\left[\frac{1}{2}(d_1 \cdots d_{n-r} + d_1)\right]^{2^{r-1}}.$$

Proof. W.l.o.g. one can assume $d_1 \geq 2$. Otherwise the Gröbner basis degree would be bounded by 1 trivially. Let Q be a degree-compatible 0-standard cone decomposition of N_I as in lemma 5.10. Then $G(F) \leq \deg(Q) + 1$. By lemma 2.81, one can embed a regular sequence $g_1, \ldots, g_{n-r}$ in I with degrees $d_{k_1}, \ldots, d_{k_{n-r}}$ for some $1 \leq k_1 < \ldots < k_{n-r} \leq s$. Then lemma 5.19 bounds $\deg(Q)$ by the Macaulay constant $a_1 - 1$ of a d_1-exact cone decomposition of $J = \left\langle x_1^{k_1}, \ldots, x_{n-r}^{k_{n-r}} \right\rangle$. Corollary 5.26, finally, gives the bound on a_1:

$$a_1 \leq 2\left[\frac{1}{2}\left(d_{k_1} \ldots d_{k_{n-r}} + d_{k_1}\right)\right]^{2^{r-1}} \leq 2\left[\frac{1}{2}\left(d_1 \cdots d_{n-r} + d_1\right)\right]^{2^{r-1}}$$

The second inequality holds since $k_i \geq i$ for $i = 1, \ldots, n-r$ and thus $d_{k_i} \leq d_i$. Since the above bound for a_1 is greater than $d_1 + \ldots + d_{n-r} - n + 1$, the stated bound holds. □

Note that theorem 5.27 also holds over finite fields $\mathbb{F}$. To see this, consider an infinite extension $\mathbb{K}$ of $\mathbb{F}$, e.g. the algebraic closure. First consider the ideal dimension of the embedding $I \cdot \mathbb{K}[X]$ of the ideal $I \subseteq \mathbb{F}[X]$. Since $(I \cdot \mathbb{K}[X]) \cup \mathbb{K}[U] = \emptyset$ iff $I \cdot \mathbb{F}[U] = \emptyset$, the definition of the dimension by independent sets implies that the ideal dimensions of the ideal and its embedding are the same. Now calculate the reduced Gröbner basis of the ideal over $\mathbb{K}$ using the Buchberger algorithm (most other Gröbner basis algorithms would suit here). On the one hand, no immediate step of the Buchberger algorithm would involve coefficients from $\mathbb{K} \setminus \mathbb{F}$ and thus the reduced Gröbner basis also has coefficients in $\mathbb{F}$. On the other hand, the reduced Gröbner basis is the basis with the smallest degrees for homogeneous ideals. Thus the degree bound also applies to the reduced Gröbner basis.

Thanks to Gregor Kemper for this remark.

The Inhomogeneous Case Unlike the claim in [34], the lifting to the inhomogeneous case is not quite trivial. Given an ideal I generated by polynomials $f_1, \ldots, f_s$, Dubé considers the homogeneous ideal $\tilde{I} = \left\langle {}^h f_1, \ldots, {}^h f_s \right\rangle$. By lemma 2.24, the dehomogenization of a Gröbner basis G of $\tilde{I}$ yields a Gröbner basis of I. Since the dehomogenization only might decrease the degrees, it suffices to bound $\deg(G)$.

This approach, however, does not transfer straight forward to the dimension-dependent bounds. As example 2.83 shows, $\dim(\tilde{I})$ might be much larger than $\dim(I)$ such that the benefit of the presented construction vanishes. A possibility to avoid this using polynomials from the Noether normal form will be presented in the following. Unfortunately, the resulting bound will be slightly weaker than in the homogeneous case.

Lemma 5.28. *Let $\mathbb{K}$ be an infinite field and $I \subsetneq \mathbb{K}[X]$ be an ideal of dimension r generated by polynomials $f_1, \ldots, f_s$ of degrees $d_1 \geq \ldots \geq d_s$. Then there are polynomials $g_1, \ldots, g_{n-r} \in I$ such that $\operatorname{ht}\left\langle {}^h g_1, \ldots, {}^h g_{n-r} \right\rangle = \operatorname{ht}(I)$ and $\deg(g_i) \leq (d_1 \cdots d_{n-r})^2$ for $i = 1, \ldots, n-r$.*

Proof. By theorem 4.8, there are an invertible linear change of variables

$$\sigma : \mathbb{K}[X] \longrightarrow \mathbb{K}[X], x_k \mapsto a_{k,1}x_1 + \ldots + a_{k,n}x_n \qquad \text{with } a_{i,j} \in \mathbb{K} \text{ for } i, j = 1, \ldots, n$$

and $h_i \in I \cap \mathbb{K}[x_1, \ldots, x_i]$ such that $0 < \deg(h_i) = \deg_{x_i}(h_i) \leq (d_1 \cdots d_{n-r})^2$ for $i = r+1, \ldots, n$. Consider ${}^h h_{r+1}, \ldots, {}^h h_n$. These polynomials form a regular sequence of length $n-r$ and thus generate an ideal of height $n-r$. Now apply σ^{-1} and let $g_i = \sigma^{-1}(h_{r+i})$ for $i = 1, \ldots, n-r$. Since the height of an ideal is invariant under changes of variables and ${}^h g_i = \sigma^{-1}({}^h h_{r+i})$, the ideal $\left\langle {}^h g_1, \ldots, {}^h g_{n-r} \right\rangle$ has height $n-r$, too. □

Instead of considering $\tilde{I} = \left\langle {}^h f_1, \ldots, {}^h f_s \right\rangle$, the polynomials ${}^h g_1, \ldots, {}^h g_{n-r}$ from lemma 5.28 will be adjoined yielding $K = \left\langle {}^h g_1, \ldots, {}^h g_{n-r}, {}^h f_1, \ldots, {}^h f_s \right\rangle$. Since ${}^h g_1, \ldots, {}^h g_{n-r} \in I$, lemma 2.24 still applies. By corollary 2.75, ${}^h g_1, \ldots, {}^h g_{n-r}$ is a regular sequence and therefore one can use lemma 5.19.

Theorem 5.29. *Let $\mathbb{K}$ be an infinite field and $I \subsetneq \mathbb{K}[X]$ be an ideal of dimension r generated by polynomials $F = \{f_1, \ldots, f_s\}$ of degrees $d_1 \geq \ldots \geq d_s$. Then the Gröbner basis degree is bounded by*

$$G(F) \leq 2 \left[\frac{1}{2} \left((d_1 \cdots d_{n-r})^{2(n-r)} + d_1 \right) \right]^{2^r} .$$

Proof. Let ${}^h g_1, \ldots, {}^h g_{n-r}$ be the polynomials from lemma 5.28 with degrees $\tilde{d}_i = \deg(g_i) \leq (d_1 \cdots d_{n-r})^2$ for $i = 1, \ldots, n-r$, and $K = \left\langle {}^h g_1, \ldots, {}^h g_{n-r}, {}^h f_1, \ldots, {}^h f_s \right\rangle$. Because of the inclusions $\left\langle {}^h g_1, \ldots, {}^h g_{n-r} \right\rangle \subseteq K \subseteq {}^h I$, $K \subseteq \mathbb{K}[X_0]$ is a $(r+1)$-dimensional ideal in $n+1$ variables. Let Q be a degree-compatible 0-standard cone decomposition of N_K as in lemma 5.10. Then $G(F) \leq \deg(Q) + 1$ by lemma 2.20. On the other hand, lemma 5.19 bounds $\deg(Q)$ by the Macaulay constant $a_1 - 1$ of a d_1-exact cone decomposition of $J = \left\langle x_1^{\tilde{d}_1}, \ldots, x_{(n+1)-(r+1)}^{\tilde{d}_{(n+1)-(r+1)}} \right\rangle$ in the ring $\mathbb{K}[X_0]$. Corollary 5.26, finally, gives a bound on a_1. Since this bound is greater than $\tilde{d}_1 + \ldots + \tilde{d}_{(n+1)-(r+1)} - (n+1) + 1$,

$$G(F) \leq 2 \left[\frac{1}{2} \left(\tilde{d}_1 \cdots \tilde{d}_{(n+1)-(r+1)} + d_1 \right) \right]^{2^r} \leq 2 \left[\frac{1}{2} \left(\left((d_1 \cdots d_{n-r})^2 \right)^{n-r} + d_1 \right) \right]^{2^r} .$$

□

Again, it would be nice to generalize this result to arbitrary fields. The reasoning following theorem 5.27, however, does not hold here since a reduced basis w.r.t. to an arbitrary ordering does not necessarily have minimal degree.

Consider a basis F of an ideal I of polynomials over a finite field $\mathbb{F}$ in variables X and choose an infinite field extension $\mathbb{K} \supseteq \mathbb{F}$. Since $\mathbb{K}$ is a vector space over $\mathbb{F}$, one may choose a $\mathbb{F}$-basis B of $\mathbb{K}$ with $1 \in B$ and let $\varphi : \mathbb{K} \longrightarrow \mathbb{F}$ be the projection onto the basis element 1 given by $\varphi\left(\sum_{b \in B} a_b \cdot b\right) = a_1 \cdot 1$ (with $a_b \in \mathbb{F}$).

As noted before, the $\dim(I) = \dim(I \cdot \mathbb{K}[X])$. So by theorem 5.27, there is a Gröbner basis $G \subseteq \mathbb{K}[X]$ of $I \cdot \mathbb{K}[X]$ with the desired degree bound. Dividing each element of G by its leading coefficient, one may assume that $\operatorname{lc}(g) = 1$ for all $g \in G$.

The claim is that $\varphi(G) \subseteq \mathbb{F}[X]$ is a Gröbner basis of I with the desired degree bound. First note that $\deg(f) \geq \deg(\varphi(f))$ for all $f \in \mathbb{K}[X]$, so the degree bound holds. Moreover, the leading coefficients of the elements of G are 1, so $\operatorname{lm}(g) = \operatorname{lm}(\varphi(g))$ for all $g \in G$. Hence $\operatorname{lm}(I) = \operatorname{lm}(I \cdot \mathbb{K}[X]) = \operatorname{lm}(G) = \operatorname{lm}(\varphi(G))$ which proves that G is a Gröbner basis and finishes the proof.

Once again thanks to Gregor Kemper for this remark.

One can simplify the bound to $G(F) \leq 2\left[\frac{1}{2}\left(d^{2(n-r)^2} + d\right)\right]^{2^r}$ for $d = \max\{d_1, \ldots, d_s\}$.

Lower Bound Remember the Mayr-Meyer construction respectively theorem 5.2. To the best of the authors' knowledge, there is little known about the dimension of these ideals. Only for the Mayr-Meyer ideals there is a lower bound for the dimension which is linear in the number of variables (cf. [35]). For the following statement, it would be more interesting to have an upper bound. Though the trivial bound given by the number of variables suffices if the constants are irrelevant. The trick for obtaining a lower bound for the Gröbner basis degree is a combination with the well-known construction for the zero-dimensional case.

Example 5.30. *Fix a graded admissible monomial ordering $\prec$ and consider the ideal I_r in the polynomial ring $\mathbb{K}[x_1, \ldots, x_r]$ constructed by Yap. By theorem 5.2, the degree of the Gröbner basis G_r of I_r is bounded by $\deg(G_r) \geq d^{2^{(1/2-\varepsilon)r}}$ for any $\varepsilon > 0$ and sufficiently large $d, r \in \mathbb{N}$.*

It is well-known that the set of leading monomials of an irredundant Gröbner basis equals the set of minimally reducible monomials, i.e. the w.r.t. the ideal reducible monomials whose divisors are irreducible. Since $\prec$ is graded, the minimally reducible monomials have degrees up to the degree of the Gröbner basis. By the pigeon hole principle, there is some $k \in \{1, \ldots, r\}$ such that there is a w.r.t. I_r minimally reducible monomial $x^\alpha \in \mathbb{K}[x_1, \ldots, x_r]$ with $\deg_{x_k}(x^\alpha) \geq \frac{1}{r} d^{2^{(1/2-\varepsilon)r}}$.

Now define the ideal

$$I_{r,n} = I_r + \left\langle x_k - x_{r+1}^d, x_{r+1} - x_{r+2}^d, \ldots, x_{n-1} - x_n^d \right\rangle \subseteq \mathbb{K}[X],$$

let $\pi : \mathbb{K}[X] \longrightarrow \mathbb{K}[x_1, \ldots, x_r]$ be the projection which sends $x_{r+1}, \ldots, x_n$ to 1, and $\pi' : \mathbb{K}[X] \longrightarrow \mathbb{K}[x_{r+1}, \ldots, x_n]$ analogously. Consider the block ordering $\prec'$ on $\mathbb{K}[X]$ defined by $x^\alpha \prec' x^\beta$ iff $\pi(x^\alpha) \prec \pi(x^\beta)$ or $\pi(x^\alpha) = \pi(x^\beta)$ and $\pi'(x^\alpha) \prec_{lex} \pi'(x_\beta)$ for all $x^\alpha, x^\beta \in \mathbb{K}[X]$. Here $\prec_{lex}$ denotes the lexicographic monomial ordering with $x_{r+1} \succ_{lex} \cdots \succ_{lex} x_n$.

Then $x^\alpha \in \mathbb{K}[x_1, \ldots, x_r]$ is minimally irreducible w.r.t. I_r iff $x^\alpha x_k^{-\alpha_k} x_n^{\alpha_k d^{n-r}}$ is minimally irreducible w.r.t. $I_{r,n}$. Hence, the degree of any Gröbner basis $G_{r,n}$ of $I_{r,n}$ w.r.t. $\prec'$ is bounded by $\deg(G_{r,n}) \geq \frac{1}{r} d^{2^{(1/2-\varepsilon)r}} d^{n-r}$. The factor $\frac{1}{r}$ of this bound can be hidden in the constant ε.

Finally note that $\dim(I_{r,n}) \leq \dim(I_{r,n}) \leq r$. This follows easily since any w.r.t. $I_{r,n}$ independent set can contain at most one of the variables $x_k, x_{r+1}, \ldots, x_n$.

Theorem 5.31. *There are a monomial ordering and a family of ideals $I_{r,n} \subseteq \mathbb{K}[X]$ of dimension at most r for $r, n \in \mathbb{N}$ with $r \leq n$ which are generated by $O(n)$ polynomials $F_{r,n}$ of degrees bounded by d such that each Gröbner basis $G_{r,n}$ has a maximal degree of at least*

$$\deg(G_{r,n}) \geq d^{(n-r)2^{(1/2-\varepsilon)r}} \textit{ for any } \varepsilon > 0 \textit{ and sufficiently large } d, r \in \mathbb{N}.$$

This result is weaker than the one by Yap since it only works for special monomial orderings. Most likely, this cannot be avoided since the degree bounds for Gröbner bases of zero-dimensional ideals depend on the monomial ordering (cf. [31]). For some monomial orderings, one will — most likely — not obtain the single exponential dependence on n.

Theorem 5.32. *There is a family of ideals $I_{r,n} \subseteq \mathbb{K}[X]$ of dimension at most r for $r \le n \in \mathbb{N}$, generated by $O(n)$ polynomials $F_{r,n}$ of degrees bounded by d such that each Gröbner basis (with respect to any admissible monomial ordering $\prec$) has a maximal degree of at least*

$$\deg(\mathrm{GB}(F_{r,n})) \ge d^{2^{(1/2-\varepsilon)r}} \textit{ for any } \varepsilon > 0 \textit{ and sufficiently large } d, r \in \mathbb{N}.$$

Proof. Let F_r be as defined in theorem 5.2 and $F_{r,n} = F_r \cup \{x_{r+1}, \dots, x_n\}$. Then $I_{r,n}$, the ideal generated by $F_{r,n}$ in $\mathbb{K}[X]$, has dimension $\dim(I_{r,n}) \le r$ and the degree bound is exactly as in theorem 5.2. □

5.4. Toric Ideals

Remember that toric ideals are prime binomial ideals. Although it is a proper restriction, it seems reasonable to consider toric ideals I which are generated by binomials $F = \left\{x^{\alpha_i} - x^{\beta_i} \in \mathbb{K}[X] : i = 1, \dots, s\right\}$. The objective is to study the degrees of the polynomials in a reduced Gröbner basis of I in the worst case, for any admissible monomial ordering.

Lower Bound A well-known example (c.f. [35], III.2) provides an exponential lower degree bound for Gröbner bases. The following variant of this example is a toric ideal.

Example 5.33. *For any $s < n \in \mathbb{N}$ and $d_1, \dots, d_s \in \mathbb{N}$, let*

$$I = \left\langle x_1^{d_1} - x_{s+1}\right\rangle + \left\langle x_{i-1} - x_i^{d_i} : i = 2, \dots, s\right\rangle$$

be an ideal in $\mathbb{K}[X]$ generated by polynomials of degrees $d_1, \dots, d_s$ and fix the lexicographic monomial ordering $\prec$ with $x_1 \succ \ldots \succ x_n$. An easy calculation yields $x_s^{d_1 \cdots d_s} - x_{s+1} \in I$, but no smaller power of x_s can be leading monomial of a polynomial in I. Thus the unique reduced Gröbner basis of I w.r.t. $\prec$ is

$$G = \left\{x_s^{d_1 \cdots d_s} - x_{s+1}, x_{i-1} - x_i^{d_i} : i = 2, \dots, s\right\}.$$

It remains to show that I is toric. In order to verify this, consider the homomorphism

$$\varphi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^{n-s}, \alpha \mapsto A \cdot \alpha \textit{ with } A = \begin{pmatrix} d_2 \cdots d_s & d_3 \cdots d_s & \cdots & 1 & d_1 \cdots d_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

The claim is $I = I_\varphi$. It is easy to see $x_{i-1} - x_i^{d_i} \in I_\varphi$, for $i = 2, \dots, s$, and $x_1^{d_1} - x_{s+1} \in I_\varphi$. Thus $I \subseteq I_\varphi$.

On the other hand, consider $x^{\alpha^+} - x^{\alpha^-} \in I_\varphi$, i.e. $\alpha \in \ker(\varphi)$. Then

$$x^{\alpha^+} - x^{\alpha^-} \equiv x_s^{a_1} x_{s+1}^{c_1} - x_s^{a_2} x_{s+1}^{c_2} \mod \left\langle x_{i-1} - x_i^{d_i} : i = 2, \ldots, s \right\rangle \subseteq I \subseteq I_\varphi$$

for some $a_1, c_1, a_2, c_2 \in \mathbb{N}$. Denote the k-th unit vector in $\mathbb{Z}^n$ by e_k. Lemma 2.106 yields $(a_1 - a_2)e_s - (c_1 - c_2)e_{s+1} \in \ker(\varphi)$. Thus $(a_1 - a_2) + d_1 \cdots d_s(c_1 - c_2) = 0$. Assume w.l.o.g. $c_1 \leq c_2$ and therefore $a_1 \geq a_2$. Then

$$I \ni x_s^{d_1 \cdots d_s} - x_{s+1} \mid x_s^{a_1 - a_2} - x_{s+1}^{c_2 - c_1} \mid x_s^{a_1} x_{s+1}^{c_1} - x_s^{a_2} x_{s+1}^{c_2}$$

implies $I_\varphi \subseteq I$ which proves that $I = I_\varphi$ is toric.

It is easy to see that homogenization of the example w.r.t. a new indeterminate preserves all properties. The matrix A defining φ becomes

$$A = \begin{pmatrix} 0 & d_2 \cdots d_s & d_3 \cdots d_s & \cdots & 1 & d_1 \cdots d_s & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \\ 1 & -1 & -1 & \cdots & -1 & -1 & -1 & \cdots & -1 \end{pmatrix}.$$

This yields the same lower bound for an ideal in $n + 1$ variables and a graded monomial ordering.

The previous example proves the following lower bound which is almost as strong as theorem 5.6.

Theorem 5.34. *For any $s \leq n \in \mathbb{N}$ and $d_1, \ldots, d_s \in \mathbb{N}$, there is a toric ideal $I \subsetneq \mathbb{K}[X]$ generated by polynomials $F = \{f_1, \ldots, f_s\}$ of degrees $d_1, \ldots, d_s$ such*

$$\deg(\mathrm{GB}(F)) \geq d_1 \cdots d_s.$$

Upper Bound In [42], §4, Sturmfels gives a single exponential upper degree bound for Gröbner bases in terms of the coefficients of a matrix A defining the toric ideal $I_{\ker_{\mathbb{Z}^n}(A)}$. In the following, his proof will be adapted to the situation of a toric ideal I_M given by a basis $B = \{\beta_1, \ldots, \beta_s\}$ of a saturated submodule M of $\mathbb{Z}^n$. The case in which the ideal is represented by a basis $F = \left\{x^{\alpha_i} - x^{\beta_i} : i = 1, \ldots, s\right\}$ of the ideal I_M can easily be reduced to the former case. Following the Sturmfels' strategy, it is possible to reuse a part of his proof. His idea was to consider module elements with small support.

Definition 5.35. *Let M be a saturated submodule of $\mathbb{Z}^n$. A vector $0 \neq \gamma \in M$ is called* circuit *of M iff its* support $\mathrm{supp}(\gamma) = \{k \in \{1, \ldots, n\} : \gamma_k \neq 0\}$ *is minimal w.r.t. inclusion among the elements of M and* $\gcd(\gamma_1, \ldots, \gamma_n) = 1$.

Definition 5.36. *Let I be a toric ideal in $\mathbb{K}[X]$. Then $x^{\alpha^+} - x^{\alpha^-} \in I$ is called* primitive *iff there is no other binomial $x^{\beta^+} - x^{\beta^-} \in I$ with $x^{\beta^+} \mid x^{\alpha^+}$ and $x^{\beta^-} \mid x^{\alpha^-}$.*

Definition 5.37. *Let $\alpha, \beta \in \mathbb{Z}^n$. Then α is* conformal *to β iff* $\operatorname{supp}(\alpha^+) \subseteq \operatorname{supp}(\beta^+)$ *and* $\operatorname{supp}(\alpha^-) \subseteq \operatorname{supp}(\beta^-)$.

Lemma 5.38 (Sturmfels 1996)**.** *Let M be an saturated module of $\mathbb{Z}^n$. Given a bound $|\gamma^+|, |\gamma^-| \leq d$ for the positive and negative parts of all circuits $\gamma \in M$, the degree of the reduced Gröbner basis G of $I_M \subseteq \mathbb{K}$ is bounded by* $\deg(G) \leq nd$.

Proof. (from [42], §4) Let G be the reduced Gröbner basis of I_M and consider $x^{\alpha^+} - x^{\alpha^-} \in G$ with $x^{\alpha^+} \succ x^{\alpha^-}$. Then x^{α^+} is minimally reducible w.r.t. I_M and $x^{\alpha^-} = \operatorname{nf}_{I_M}(x^{\alpha^+})$. If $x^{\beta^+} \mid x^{\alpha^+}$ and $x^{\beta^-} \mid x^{\alpha^-}$ for some $x^{\beta^+} - x^{\beta^-} \in I_M$, $x^{\beta^+} = x^{\alpha^+}$ since x^{α^+} is minimally reducible. Since $\operatorname{nf}_{I_M}(x^{\alpha^+})$ is minimal w.r.t. $\prec$ in $x^{\alpha^+} + I_M$, also $x^{\beta^-} = x^{\alpha^-}$. Thus $x^{\alpha^+} - x^{\alpha^-}$ is primitive. Thus is suffices to show that the exponent vector of each primitive binomial in I_M can be expressed by circuits in a controlled way.

Let $0 \neq \alpha \in \mathbb{Q}M$. Then there is a circuit $\gamma \in M$ with $\operatorname{supp}(\gamma) \subseteq \operatorname{supp}(\alpha)$. Assume w.l.o.g. that $\alpha_k\gamma_k > 0$ for some $k = 1, \ldots, n$ (otherwise replace γ by $-\gamma$). Let

$$c = \min\left\{\frac{\alpha_i}{\gamma_i} \in \mathbb{Q} : \alpha_i\gamma_i > 0, i = 1, \ldots, n\right\}.$$

By definition of c, $\alpha - c\gamma \in \mathbb{Q}M$ is conformal to α and has strictly smaller support. Thus, by induction, each $\alpha \in M$ is a non-negative rational linear combination of n circuits conformal to α.

Now consider a primitive binomial $x^{\alpha+} - x^{\alpha-} \in I_M$. The last paragraph yields

$$\alpha = \sum_{i=1}^{n} c_i\gamma_i \qquad \text{for some } c_i \in \mathbb{Q}_{\geq 0} \text{ and circuits } \gamma_i \in M \text{ conformal to } \alpha \text{ for } i = 1, \ldots, n.$$

Since $\gamma_1, \ldots, \gamma_n$ are conformal to α and $c_1, \ldots, c_n \geq 0$, $\alpha^+ = c_1\gamma_1^+ + \ldots + c_n\gamma_n^+$ and $\alpha^- = c_1\gamma_1^- + \ldots + c_n\gamma_n^-$. Furthermore, α is primitive and hence $c_1, \ldots, c_n < 1$ follows. Thus

$$\deg(x^{\alpha^+} - x^{\alpha^-}) = \max\left\{|\alpha^+|, |\alpha^-|\right\} \leq \max\left\{\sum_{i=1}^{n}|\gamma_i^+|, \sum_{i=1}^{n}|\gamma_i^-|\right\} \leq nd.$$

□

Lemma 5.39. *Let $I_M \subseteq \mathbb{K}[X]$ be a toric ideal given by a basis $\{\beta_1, \ldots, \beta_s\}$ of the module $M \subseteq \mathbb{Z}^n$ with 2-norms $d_i = \|\beta_i\|_2$ for $i = 1, \ldots, s$ such that $d_1 \geq \ldots \geq d_s$. Then the degree of the reduced Gröbner basis G of I_M is bounded by* $\deg(G) \leq \frac{1}{4}(n+1)^3 d_1 \cdot d_1 \cdots d_n$.

Proof. It is suitable to use matrix notation. Therefore let $B = (\beta_1, \ldots, \beta_s)$ and observe $M = B \cdot \mathbb{Z}^s$. Also remember the notation of definition 1.2 and write $B_J = B_{J,\{1,\ldots,s\}}$.

In order to examine circuits more closely, let $M_J = \{\alpha \in M : \alpha_i = 0 \text{ for all } i \in J\} = B \cdot \ker_{\mathbb{Z}^s}(B_J)$. This corresponds to a projection π onto a $(n - \#J)$-dimensional subspace, i.e.

$$\mathbb{Z}^s \xrightarrow{B} \mathbb{Z}^n \xrightarrow{\pi} \mathbb{Z}^{n-\#J} \times \{0\}^{\#J}.$$

Since $M_J = \pi(M)$, $\dim_{\mathbb{Q}}(M_J) = \dim_{\mathbb{Q}}(M) - \dim_{\mathbb{Q}}(\ker_M(\pi)) \geq \dim_{\mathbb{Q}}(M) - \#J$.

Let γ be a circuit and $J = \operatorname{supp}(\gamma)$. Then $\gamma \in M_J$ and $\dim_{\mathbb{Q}}(M_J) = 1$. Otherwise one could project out one more coordinate and obtain a non-zero element of M whose support is strictly contained in J which is a contradiction.

Therefore $\gamma = B \cdot c$ for some $c \in \mathbb{Z}^s$ and $0 = \gamma_J = B_J \cdot c$. Let $r = \operatorname{rank}(B_J)$ and assume $r < s$ (otherwise add a vector $\beta_{s+1} = 0$ to the module basis). Then $r = \dim_{\mathbb{Q}}(M) - \dim_{\mathbb{Q}}(M_J) \leq \#J$. One can choose a $r \times (r+1)$-submatrix $\tilde{B}$ of B_J with $\operatorname{rank}(\tilde{B}) = r$. Thus the kernel of $\tilde{B} = (\tilde{b}_1, \dots, \tilde{b}_{r+1})$ is one-dimensional and, by lemma 1.1, generated by

$$\tilde{c} = \sum_{i=1}^{r+1} (-1)^i \det(\tilde{b}_1, \dots, \tilde{b}_{i-1}, \tilde{b}_{i+1}, \dots, \tilde{b}_{r+1}) e_i.$$

This vector $\tilde{c} \in \mathbb{Z}^{r+1}$ extends to a solution $c' \in \mathbb{Z}^s$ of $B_J \cdot c' = 0$ by padding with zeros. Then $\gamma' = B \cdot c'$ is an element of M_J and, since $\dim(M_J) = 1$, a rational multiple of γ. From lemma 1.3 and $B \cdot \ker(B_J) = M_J \neq \{0\}$, one deduces that, for the right choice of $\tilde{B}$, one obtains $\gamma' = B \cdot c' \neq 0$. Since $\gamma \in \mathbb{Z}^n$ is a circuit, especially $\gcd(\gamma_1, \dots, \gamma_n) = 1$. On the other hand, $\beta_1, \dots, \beta_s$ and thus $\tilde{b}_1, \dots, \tilde{b}_{r+1}$ are integral vectors as well as c' and γ'. Together, $\gamma' = k\gamma$ for some $0 \neq k \in \mathbb{Z}$. Hence, $|\gamma| \leq |\gamma'| = |B \cdot c'|$. c' was chosen such that $\gamma_J = B_J \cdot c' = 0$. Thus at most $n - \#J \leq n - r$ non-zero coefficients of γ remain:

$$|\gamma| \leq (n-r) \max \left\{ \left| \sum_{i=1}^{s} (\beta_i)_k c'_i \right| : k = 1, \dots, n \right\}$$

Now c' is obtained from $\tilde{c}$ by padding with zeros. Hence it can only have $r+1$ non-zero entries:

$$|\gamma| \leq (n-r)(r+1) \max \left\{ |(\beta_i)_k c'_i| : i = 1, \dots, s, k = 1, \dots, n \right\}$$

Since $0 \leq r \leq \#J < n$, one obtains using Hadamard's determinant inequality

$$\begin{aligned} |\gamma| &\leq \frac{1}{4}(n+1)^2 \max \left\{ |(\beta_i)_k| : i = 1, \dots, s, k = 1, \dots, n \right\} \max \left\{ |c'_i| : i = 1, \dots, s \right\} \leq \\ &\leq \frac{1}{4}(n+1)^2 d_1 \prod_{i=1}^{r+1} \|\tilde{b}_i\|_2 \leq \frac{1}{4}(n+1)^2 d_1 d_1 \cdots d_{r+1}. \end{aligned}$$

With $|\gamma^+|, |\gamma^-| \leq |\gamma|$, this calculation and lemma 5.38 prove the claimed bound. □

Theorem 5.40. *Let I be a toric ideal in $\mathbb{K}[X]$ generated by binomials $F = \left\{ x^{\alpha_i} - x^{\beta_i} : i = 1, \dots, \right.$ $\left. s \right\}$ of degrees $d_1 \geq \ldots \geq d_s$. Then the Gröbner basis degree is bounded by*

$$G(F) \leq \sqrt{2}^{n-3} (n+1)^3 d_1 \cdot d_1 \cdots d_n.$$

Proof. If F is an ideal basis of the toric ideal $I = I_M$, $B = \{\alpha_1 - \beta_1, \ldots, \alpha_s - \beta_s\}$ is a basis of the module $M \subseteq \mathbb{Z}^n$. Since

$$\begin{aligned}\|\alpha_i - \beta_i\|_2 \leq & \sqrt{2} \max \left\{ \|(\alpha_i - \beta_i)^+\|_2, \|(\alpha_i - \beta_i)^-\|_2 \right\} \leq \\ \leq & \sqrt{2} \max \left\{ |(\alpha_i - \beta_i)^+|, |(\alpha_i - \beta_i)^-| \right\} \leq \\ \leq & \max \{ |\alpha_i|, |\beta_i| \} = \sqrt{2} \deg(x^{\alpha_i} - x^{\beta_i^-}) = \sqrt{2} d_i\end{aligned}$$

for $i = 1, \ldots, s$, lemma 5.39 concludes the proof. □

Part III.

Complexity Bounds

6. Gröbner Basis Computation without Degree Bounds

The following exposition extends the results by Kühnle and Mayr in [28]. The goal is to compute Gröbner bases on Turing machines with low space complexity. The algorithm by Kühnle and Mayr requires exponential space and is therefore asymptotically optimal. The matching lower bound was given by Mayr and Meyer in [33]. However, the algorithm's time and space complexity essentially depends only on the degree bounds by Hermann (theorem 4.1) and Dubé (theorem 5.1) which are used in order to turn a polynomial equation into a system of linear equations. Chapters 4 and 5 showed that there are many ideal classes for which the worst cases are much better. One could plug-in the derived bounds and obtain an algorithm which uses less space but only works correctly for the particular class of ideals. This is somewhat annoying since good theoretical bounds are necessary for an efficient algorithm.

This chapter will present an algorithm which works correctly for all ideals and whose complexity depends on the particular instance. Thus it will be much better for most cases and in the same magnitude for worst case examples like those constructed by Mayr and Meyer respectively Yap. The key idea is to implement a space-efficient S-polynomial criterion which allows to check whether a Gröbner basis is complete. Then it is possible to incrementally compute the Gröbner basis.

Note that — just like in [28] — the monomial ordering must be given as a rational weight matrix. This is a proper restriction since not all monomial orderings can be represented this way. However all common monomial orderings can be represented by a rational weight matrix. Moreover, one can approximate any monomial ordering up to an arbitrary degree with a rational weight matrix.

Reduction to Linear Algebra Kühnle and Mayr came up with a way to compute normal forms efficiently. This is central to the following and thus will be explained in detail. Let I be the ideal in $\mathbb{K}[X]$ whose Gröbner basis shall be computed and assume it is generated by polynomials $f_1, \dots, f_s$. Since $h - \mathrm{nf}_I(h) \in I$ for any polynomial $h \in \mathbb{K}[X]$, there exists a representation

$$h - \mathrm{nf}_I(h) = \sum_{i=1}^{s} a_i f_i \qquad \text{with } a_1, \dots, a_s \in \mathbb{K}[X]. \tag{6.1}$$

Their idea was to rewrite this equation as linear system and apply the result from corollary 3.26. First assume $\deg(a_i f_i) \leq D$ for $i = 1, \dots, s$ and worry about D later. Name the coefficients by

$$\begin{aligned} a_i &= \sum_{|\alpha|\le D-\deg(f_i)} \mathbf{a}_{i,\alpha} x^\alpha && \text{for } i=1,\dots,s \\ f_i &= \sum_{|\beta|\le \deg(f_i)} f_{i,\beta} x^\beta && \text{for } i=1,\dots,s \\ h &= \sum_{|\gamma|\le D} h_\gamma x^\gamma && \text{and} \\ \mathrm{nf}_I(h) &= \sum_{|\gamma|\le D} \mathbf{y}_\gamma x^\gamma. \end{aligned}$$

Then (6.1) is equivalent to

$$h_\gamma - \mathbf{y}_\gamma = \sum_{i=1}^{s} \sum_{\substack{|\alpha|\le D-\deg(f_i)\\ |\beta|\le\deg(f_i)\\ \alpha+\beta=\gamma}} \mathbf{a}_{i,\alpha} f_{i,\beta} \qquad \text{for all } \gamma\in\mathbb{N}^n, |\gamma|\le D. \tag{6.2}$$

Note that the unknowns of the system are printed in bold letters. Rewrite the system in matrix form

$$h - E\cdot\mathbf{y} = F\cdot\mathbf{a}$$

where $h=(h_\gamma)_{|\gamma|\le D}$, $\mathbf{y}=(\mathbf{y}_\gamma)_{|\gamma|\le D}$, $\mathbf{a}=(\mathbf{a}_{i,\alpha})_{\substack{i=1,\dots,s\\|\alpha|\le D-\deg(f_i)}}$, E is the identity matrix of size $\binom{D+n}{n}$ and F is the according coefficient matrix. If it is possible to compute the coefficients of F efficiently, one can apply corollary 3.26 to

$$\begin{pmatrix} F & E \end{pmatrix} \cdot \begin{pmatrix} \mathbf{a} \\ \mathbf{y} \end{pmatrix} = h \tag{6.3}$$

and thereby solve (6.1).

Definition 6.1. *Let I be an ideal in $\mathbb{K}[X]$ generated by polynomials $F=\{f_1,\dots,f_s\}$ and fix an admissible monomial ordering $\prec$. For any given $D\in\mathbb{N}$ and $h\in\mathbb{K}[X]$, the w.r.t. $\prec$ minimal polynomial $\tilde{h}=\sum_{|\alpha|\le D}\boldsymbol{y}_\alpha x^\alpha$ for which* (6.2) *is solvable is denoted by* $\mathrm{nf}_F(h,D)=\tilde{h}$. *If* $\mathrm{nf}_F(h,D)\ne h$, *h is called* D-reducible *w.r.t. F.*

Note that D-reducibility does not imply reducibility nor the other way round.

Lemma 6.2 (Kühnle, Mayr 1996). *Let I be an ideal in the polynomial ring $\mathbb{K}[X]$ over a well-endowed field $\mathbb{K}$, let I be generated by polynomials $F=\{f_1,\dots,f_s\}$, and fix an admissible monomial ordering $\prec$ represented by a rational weight matrix $W\in\mathbb{Q}^{n\times n}$. For any given $D\in\mathbb{N}$ and $h\in\mathbb{K}[X]$, it is possible to compute* $\mathrm{nf}_F(h,D)$. *If q bounds the bitsize of all numerators and denominators in W, F, and h, the algorithm is in SPACE*$(\log^2(sD^nq))$.

Proof. (from [28], §3 and §4) The idea is to find a special maximal minor of (6.2) respectively its matrix form (6.3) which corresponds to the w.r.t. $\prec$ minimal solution of the system, i.e. $\mathrm{nf}_F(h, D)$. The caveat, of course, is the space consumption. Storing the whole matrix is prohibitive, but even storing which of the $\binom{D+n}{n}$ rows respectively $O(sD^n)$ columns belong to the minor requires too much storage. Thus this has to be avoided in a clever way. It is also necessary to tackle the computation of the indices of F in (6.3).

For the first problem, the solution lies in the choice of a special minor. Fix an ordering in which one can enumerate the rows (respectively columns) with little space requirement (postpone the choice of the ordering for a moment). Then there is a canonical maximal minor for which the index set of rows respectively columns is lexicographically minimal. For this minor, one can "locally" compute whether a row (respectively column) belongs to the minor. It suffices to compare the rank of the minor of the first $k-1$ rows (respectively columns) and the minor of the first k rows (respectively columns) differ. The k-th row (respectively k-th column) belongs to the minor iff both ranks differ. Using corollary 3.26, one can determine both ranks in space $O(\log^2(sD^n q))$.

Next consider the order of the columns and rows. Remember that the columns correspond to the variables $\mathbf{a}_{i,\alpha}$ and $\mathbf{y}_\gamma$. The desired solution $\tilde{h} = \mathrm{nf}_F(h, D)$ is minimal w.r.t. $\prec$ which means that the coefficients $\mathbf{y}_\gamma$ corresponding to large monomials of $\tilde{h}$ are zero. Choosing columns for the minor corresponds to choosing the non-zero variables of the solution. By the greedy computation of the minor and the Steinitz exchange lemma, the variables which should be zero have to be in the last columns. Thus the columns will be ordered with the variables $\mathbf{a}_{i,\alpha}$ first (in arbitrary order) and the $\mathbf{y}_\alpha$ following in increasing order w.r.t. $\prec$. This guarantees that the solution $\tilde{h}$ which will be computed from the above minor is minimal w.r.t. $\prec$. It turns out that the order or the rows is arbitrary.

For the above construction, it is necessary to enumerate the all monomials up to degree D ordered by $\prec$ (this also can be used if an arbitrary order is required). Assume that the algorithm only stores the current monomial. The next term will be found in an exhaustive search which requires the storage of two more monomials, the enumeration monomial and the smallest monomial found during the enumeration which is greater than the current monomial. This needs space $O(n \log(D))$. By corollary 3.23 and since $\prec$ is represented by a matrix, the comparison of two monomials w.r.t. $\prec$ can be done in SPACE$(\log^2(nD))$.

Last but not least, consider the matrix F. Given a row index γ and a column index (i, α), the corresponding matrix coefficient is $f_{i,\beta}$ if $\beta = \gamma - \alpha \geq 0$ and 0 otherwise. So it suffices to write down α, β, γ, and i which can be done in space $O(n \log(D) + \log(s))$. Since the matrix dimensions of the linear system are $O(sD^n)$, corollary 3.26 and the intermediate space requirements yield the stated complexity. □

Degree Bounds The key for turning lemma 6.2 into an algorithm which computes a Gröbner basis is the structure lemma 2.13. It claims that the reduced Gröbner basis always has the form $\mathrm{GB}(I) = \{x^\alpha - \mathrm{nf}_I(x^\alpha) \in \mathbb{K}[X] : x^\alpha \text{ minimally reducible w.r.t. } I\}$. The remaining pieces of the jigsaw are a suitable degree bound and a way to enumerate the minimally reducible monomials.

Kühnle and Mayr bound the degree of the minimally reducible monomials by Dubé's degree bound. Then they represent the monomial ordering as single rational weight function (on the appearing monomials) and bound the degree of a normal form by estimating the length of the reduction w.r.t. the reduced Gröbner basis. This yields

Lemma 6.3 (Kühnle, Mayr 1996)**.** *Let I be an ideal in $\mathbb{K}[X]$ and fix an admissible monomial ordering $\prec$ represented by a non-negative rational weight matrix $W \in \mathbb{Q}^{n,n}$. Let B be a bound on all numerators and denominators of the entries of W and assume its Gröbner basis degree is bounded by $\deg(\mathrm{GB}(I)) \le G$. Then the degree of the normal form of a polynomial $h \in \mathbb{K}[X]$ w.r.t. I is bounded by*

$$\deg(\mathrm{nf}_I(h)) \le \deg(h)^n n^{n^2} B^{2n^2+2n} G^{n^2+1}.$$

Proof. See [28], section 2. □

While lemma 6.3 is necessary for the computation of arbitrary normal forms, it can be avoided for the computation of Gröbner bases. In this case, degree bounds like Dubé's or the dimension-dependent analogon, theorem 5.29, apply not only to the minimally reducible monomials but also to their normal forms. In the following theorem, the main result of [28] will be improved by applying the dimension-dependent bounds by Kratzer and the author of the thesis. Later, the degree bounds will be replaced by an incremental algorithm with a S-polynomial criterion.

Theorem 6.4. *Let $\mathbb{K}$ be a well-endowed field and $I \subsetneq \mathbb{K}[X]$ be an ideal of dimension r generated by polynomials $F = \{f_1, \ldots, f_s\}$ of degrees bounded by d, and fix an admissible monomial ordering $\prec$ represented by a rational weight matrix $W \in \mathbb{Q}^{n\times n}$. If q bounds the bitsize of all numerators and denominators in W and F, it is possible to compute the reduced Gröbner basis G of I w.r.t. $\prec$ in SPACE$(n^8 2^{4r} \log^2(sdq))$.*

Proof. (improving on [28], §5) By lemma 2.13, the leading monomials of the elements of a reduced Gröbner basis are minimally reducible, i.e. they are reducible but none of their divisors is. Then the Gröbner basis polynomials are obtained as difference of the leading monomial and its normal form w.r.t. I. Hence it suffices to enumerate all monomials $x^\alpha \in \mathbb{K}[X]$ up to the maximal Gröbner basis degree D_1 and check for each, whether it is D_2-reducible for a suitable D_2, but all the divisors $x_k^{-1}x^\alpha$ ($k = 1, \ldots, n$) are D_2-irreducible. This check is done using lemma 6.2.

In order to obtain the mentioned space bound, remember theorem 5.29. It states that

$$\deg(\mathrm{GB}(I)) \le 2\left[\frac{1}{2}\left(d^{2(n-r)^2} + d\right)\right]^{2^r} := D_1.$$

Furthermore, $x^\alpha - \mathrm{nf}_I(x^\alpha) \in \mathrm{GB}(I)$ yields $\deg(\mathrm{nf}_I(x^\alpha)) \le \deg(\mathrm{GB}(I))$. Now D_2 must be large enough to ensure $\mathrm{nf}_F(x^\alpha, D_2) = \mathrm{nf}_I(x^\alpha)$ for all monomials $x^\alpha \in \mathbb{K}[X]$ up to degree

D_1. The corresponding representation degree is bounded by Kratzer's theorem 4.9 (with $\mu = \min\{n, s\}$):

$$\begin{aligned} D_2 :=& D_1 + \left(d\left((n+1)\max\left\{D_1, (n+2)^2\left(d^\mu + 1\right)^{\mu+2}\right\} + 1\right)^{n-r}\right)^{2^r} = \\ =& D_1 + \left(d\left((n+1)D_1 + 1\right)^{n-r}\right)^{2^r} \end{aligned}$$

The complexity is dominated by the computation of normal forms and thus can be derived from lemma 6.2 as

$$\begin{aligned} \mathrm{SPACE}(\log^2(sD_2^n q)) = \mathrm{SPACE}(\log^2(sD_1^{n(n-r)2^r} q)) = \\ = \mathrm{SPACE}(\log^2(sd^{n(n-r)^3 2^{2r}} q)) = \mathrm{SPACE}(n^8 2^{4r} \log^2(sdq)). \end{aligned}$$

The bound for the gradings of the coefficients follows directly from lemma 6.2. □

The S-Polynomial Criterion The algorithm in theorem 6.4 always uses the worst case degree bounds. Thus the size of the linear system only depends on the degree signature of the input and the ideal dimension. In the worst case, this is optimal because the membership problem is exponential space complete (shown by Mayr, Meyer in [33]). Still, for most instances this complexity can be avoided as the improvement of the original result by Kühnle and Mayr indicates. In the following, this will be done blindly — i.e. without the knowledge of better degree bounds — by increasing D step by step. As soon as the Gröbner basis is complete, the calculation can be aborted. Unfortunately the result is not necessarily reduced. The contribution of the author of this thesis is to show how this can be done space-efficiently using S-polynomials.

Given an ideal I in $\mathbb{K}[X]$ generated by polynomials $F = \{f_1, \dots, f_s\}$, remember the structure lemma 2.13 for the reduced Gröbner basis of I. It claims that $x^\alpha - \mathrm{nf}_I(x^\alpha)$ is an element of the Gröbner iff x^α is minimally reducible w.r.t. I. The idea is to approximate this by

$$G = \{x^\alpha - \mathrm{nf}_I(x^\alpha, D) \in \mathbb{K}[X] : \alpha \in \mathbb{N}^n, x^\alpha \text{ is minimally } D\text{-reducible w.r.t. } F, |\alpha| \leq D\}$$

and check the Gröbner basis using lemma 2.15. With $g_\alpha = x^\alpha - \mathrm{nf}_I(x^\alpha, D)$ for all $\alpha \in \mathbb{N}^n$, this means to consider

$$\begin{aligned} \mathrm{S}(g_\alpha, g_\beta) &= \sum_{g_\gamma \in G} a_{\alpha,\beta,\gamma} g_\gamma & & g_\alpha, g_\beta \in G, \\ \mathrm{lm}(a_{\alpha,\beta,\gamma} g_\gamma) &\preceq \mathrm{lm}(S(g_\alpha, g_\beta)) & \text{for} \quad & i = 1, \dots, s, \text{ and} \\ f_i &= \sum_{g_\gamma \in G} b_{i,\gamma} g_\gamma & & a_{\alpha,\beta,\gamma}, b_{i,\gamma} \in \mathbb{K}[X]. \end{aligned} \tag{6.4}$$

Note the last set of equation which verifies that G generates I. As before, the space efficient linear algebra methods of corollary 3.26 can be applied if the degrees of $a_{\alpha,\beta,\gamma}$ and $b_{i,\gamma}$ are bounded by D. With

$$\begin{aligned}
\mathrm{S}(g_\alpha, g_\beta) = h_{\alpha,\beta} &= \sum_{|\varepsilon|\le 2D} h_{\alpha,\beta,\varepsilon} x^\varepsilon && \text{for } |\alpha|, |\beta| \le D, x^\alpha, x^\beta \text{ minimally } D\text{-reducible w.r.t. } F,\\
a_{\alpha,\beta,\gamma} &= \sum_{|\zeta|\le D} \mathbf{a}_{\alpha,\beta,\gamma,\zeta} x^\zeta && \text{for } |\alpha|, |\beta|, |\gamma| \le D,\\
g_\gamma &= \sum_{|\eta|\le D} g_{\gamma,\eta} x^\eta && \text{for } |\gamma| \le D,\\
f_i &= \sum_{|\varepsilon|\le 2D} f_{i,\varepsilon} x^\varepsilon && \text{for } i = 1, \dots, s, \text{ and}\\
b_{i,\gamma} &= \sum_{|\zeta|\le D} \mathbf{b}_{i,\gamma,\zeta} x^\zeta && \text{for } i = 1, \dots, s, |\gamma| \le D,
\end{aligned}$$

(6.4) yields a system of linear equations

$$\begin{aligned}
h_{\alpha,\beta,\varepsilon} &= \sum_{|\gamma|\le D} \sum_{\substack{|\zeta|\le D\\ |\eta|\le D\\ \zeta+\eta=\varepsilon}} \mathbf{a}_{\alpha,\beta,\gamma,\zeta} g_{\gamma,\eta} && \begin{array}{l} \forall |\alpha|, |\beta| \le D, |\varepsilon| \le 2D :\\ \quad x^\alpha, x^\beta \text{ minimally } D\text{-reducible w.r.t. } F \end{array}\\
\mathbf{a}_{\alpha,\beta,\gamma,\zeta} &= 0 && \begin{array}{l} \forall |\alpha|, |\beta|, |\gamma|, |\zeta| \le D : x^\gamma x^\zeta \succ \mathrm{lm}(h_{\alpha,\beta}),\\ \quad x^\alpha, x^\beta \text{ minimally } D\text{-reducible w.r.t. } F \end{array}\\
\mathbf{a}_{\alpha,\beta,\gamma,\zeta} &= 0 && \begin{array}{l} \forall |\alpha|, |\beta|, |\gamma|, |\zeta| \le D :\\ \quad x^\gamma \text{ not minimally } D\text{-reducible w.r.t. } F,\\ \quad x^\alpha, x^\beta \text{ minimally } D\text{-reducible w.r.t. } F \end{array}\\
f_{i,\varepsilon} &= \sum_{|\gamma|\le D} \sum_{\substack{|\zeta|\le D\\ |\eta|\le D\\ \zeta+\eta=\varepsilon}} \mathbf{b}_{i,\gamma,\zeta} g_{\gamma,\eta} && \forall i = 1, \dots, s, |\varepsilon| \le 2D\\
\mathbf{b}_{i,\gamma,\zeta} &= 0 && \begin{array}{l} \forall i = 1, \dots, s, |\gamma|, |\zeta| \le D :\\ \quad x^\gamma \text{ not minimally } D\text{-reducible w.r.t. } F \end{array}
\end{aligned} \tag{6.5}$$

With $S = \{\alpha \in \mathbb{N}^n : |\alpha| \le D, x^\alpha$ minimally D-reducible w.r.t. $F\}$, $h = (h_{\alpha,\beta,\varepsilon})_{\substack{|\alpha|,|\beta|\in S\\ |\varepsilon|\le 2D}}$, $\mathbf{a} = (\mathbf{a}_{\alpha,\beta,\gamma,\zeta})_{\substack{|\alpha|,|\beta|\in S\\ |\gamma|,|\zeta|\le D}}$, $f = (f_{i,\varepsilon})_{\substack{i=1,\dots,s,\\ |\varepsilon|\le 2D}}$, and $\mathbf{b} = (\mathbf{b}_{i,\gamma,\zeta})_{\substack{i=1,\dots,s\\ |\gamma|,|\zeta|\le D}}$, one can write (6.5) in matrix form

$$\begin{pmatrix} G & 0 \\ E_1 & 0 \\ E_2 & 0 \\ 0 & F \\ 0 & E_3 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{a} \\ \mathbf{b} \end{pmatrix} = \begin{pmatrix} h \\ 0 \\ 0 \\ f \\ 0 \end{pmatrix}. \tag{6.6}$$

It remains to show, how G, F, E_1, E_2, and E_3 can be computed efficiently.

Theorem 6.5. *Let I be an ideal in the polynomial ring $\mathbb{K}[X]$ over a well-endowed field $\mathbb{K}$, let I be generated by polynomials $F = \{f_1, \dots, f_s\}$, and fix an admissible monomial ordering $\prec$ represented by a rational weight matrix $W \in \mathbb{Q}^{n \times n}$. If q bounds the bitsize of all numerators and denominators in W and F, it is possible to compute a Gröbner basis G of I w.r.t. $\prec$ in SPACE$(\log^2(sD^n q))$ where D bounds the representation degrees of the Gröbner basis.*

Proof. The algorithm starts with $D = \max\{\deg(f_i) : i = 1, \dots, s\}$ and doubles D after each step. For each value of D, it solves (6.5) respectively (6.6) using corollary 3.26. If the system is solvable, then

$$G = \{x^\alpha - \mathrm{nf}_I(x^\alpha, D) \in \mathbb{K}[X] : \alpha \in \mathbb{N}^n, x^\alpha \text{ is minimally } D\text{-reducible w.r.t. } F, |\alpha| \le D\}$$

is a Gröbner basis of I. In this case, the algorithm terminates with computing these polynomials by solving the smaller system (6.2) and the enumeration technique of theorem 6.4. Thus the complexity is dominated by the part that solves (6.5) for the largest value of D.

It was already discussed how to check whether a monomial is minimally D-reducible and compare two monomials w.r.t. $\prec$. Thus one can enumerate the set S and it is legal to index the matrices by indices from S. First consider the matrices E_1, E_2, and E_3. One can choose all of them to be square matrices whose only non-zero entries are on the diagonal. The entry on the diagonal corresponding to a variable $\mathbf{a}_{\alpha,\beta,\gamma,\zeta}$ respectively $\mathbf{b}_{i,\gamma,\zeta}$ is 1 if the conditions of the respective line of (6.5) are fulfilled and 0 otherwise. Here the computation of $\mathrm{lm}(h_{\alpha,\beta})$ remains. It suffices to be able to compute the coefficients of the S-polynomial $h_{\alpha,\beta,\varepsilon}$. Then the leading monomial can be determined by enumerating all monomials and remembering the largest with non-zero coefficient. For the computation of $h_{\alpha,\beta,\varepsilon}$, observe $\mathrm{lm}(g_\alpha) = x^\alpha$ and $\mathrm{lm}(g_\beta) = x^\beta$ since x^α and x^β both are D-reducible w.r.t. F. So one can compute $x^\delta = \gcd(x^\alpha, x^\beta) = x^{\alpha \wedge \beta}$ and therefore

$$h_{\alpha,\beta} = \mathrm{S}(g_\alpha, g_\beta) = g_{\beta,\beta} x^{\beta-\delta} g_\alpha - g_{\alpha,\alpha} x^{\alpha-\delta} g_\beta = x^{\beta-\delta} g_\alpha - x^{\alpha-\delta} g_\beta.$$

The coefficients of F and G are $g_{\gamma,\eta}$ or zero. Which of both is the case can be determined analogously to lemma 6.2.

In total, there are $O(sD^{4n})$ variables and equations. Corollary 3.26 yields a complexity of $O(\log^2(sD^{4n}q))$ where the constant in the exponent can be dropped due to the logarithm and the O-notation. □

7. Membership Problem in Toric Ideals

Usually, the membership problem is solved by (at least implicitly) computing a representation of the polynomial w.r.t. the given basis. This is true for reductions w.r.t. a Gröbner basis as well as linear algebra approaches. In both cases a representation can be output without dramatic overhead once the membership of the polynomial was proved. Moreover, since the lower space bounds for the membership problem basically match the upper bounds for the representation problem, this situation is not very surprising.

For toric ideals, however, there might be a gap between the complexities of both problems. While the single exponential lower degree bound for the representation problem in toric ideals from section 4.6 suggests that this problem needs polynomial space in the input — as upper complexity bound, the PSPACE algorithm of Mayr for radical ideals in [32], corollary 8.2 applies —, the membership problem will be solved in polylogarithmic space in the following. The keys to this result are the representation of toric ideals by modules and the existence of cancellation-free representations.

Remember that toric ideals are assumed to be given by binomials, i.e. $I = \langle x^{\alpha_i} - x^{\beta_i} \in \mathbb{K}[X] : i = 1, \ldots, s\rangle$. Before analyzing the membership problem for arbitrary polynomials, restrict the problem to binomials $h = x^\gamma - x^\delta \in \mathbb{K}[X]$. By lemma 2.106, $h \in I$ is equivalent to $(\gamma - \delta) \in M = \mathbb{Z}(\alpha_1 - \beta_1) + \ldots + \mathbb{Z}(\alpha_s - \beta_s)$. Here M is a saturated submodule of $\mathbb{Z}^n$. This yields

$$\gamma - \delta = \sum_{i=1}^{s} c_i(\alpha_i - \beta_i) \qquad \text{with } c_i \in \mathbb{Z} \text{ for } i = 1, \ldots, s. \tag{7.1}$$

(7.1) is an inhomogeneous integral linear equation system, whose solvability over the integers has to be decided. This can be done in polynomial time, e.g. by computing the Hermite normal form, which is a kind of a triangular system, and then using back-substitution and divisibility tests. One can even compute an explicit solution, but this is only a module representation and does not easily yield an ideal representation.

Up to now, the fact that M is a *saturated* submodule of $\mathbb{Z}^n$ was not used. Remember this means $\varepsilon \in M$ iff $k\varepsilon \in M$ for any $0 \neq k \in \mathbb{Z}$ and $\varepsilon \in \mathbb{Z}^n$. Using this property, the system (7.1) can be relaxed to

$$\gamma - \delta = \sum_{i=1}^{s} y_i(\alpha_i - \beta_i) \qquad \text{with } y_i \in \mathbb{Q} \text{ for } i = 1, \ldots, s. \tag{7.2}$$

Obviously, any solution of (7.1) is also a solution of (7.2). On the other hand, given a solution $y_1, \dots, y_s$ of (7.2), let $0 \neq q \in \mathbb{Z}$ be the common denominator of $y_1, \dots, y_s$. Then

$$q(\gamma - \delta) = \sum_{i=1}^{s} (qy_i)(\alpha_i - \beta_i) \qquad \text{with } (qy_i) \in \mathbb{Z} \text{ for } i = 1, \dots, s.$$

So $q(\gamma - \delta) \in M$ and therefore $(\gamma - \delta) \in M$. All together, $h \in I$ if and only if (7.2) is solvable. Since the latter is a rational linear system, its solvability can be checked by two rank computations for the matrix of the homogeneous system and the extended coefficient matrix which can be done in polylogarthmic space (corollary 3.26).

Lemma 7.1. *Let I be a toric ideal in $\mathbb{K}[X]$ generated by binomials $F = \{x^{\alpha_i} - x^{\beta_i} \in \mathbb{K}[X] : i = 1, \dots, s\}$, let $h = x^{\gamma} - x^{\delta} \in \mathbb{K}[X]$ be a binomial, and let q bound the bitsize of all exponents $\beta_{i,j}$. Then the membership problem $h \overset{?}{\in} I$ can be solved in space $O(\log^2((n + s)q))$.*

Proof. (7.2) has n equations in s unknowns. Thus corollary 3.26 yields the stated complexity. □

This intermediate result will be used for solving the slightly more general case in which $h \in \mathbb{K}[X]$ is an arbitrary polynomial. The following complexity theorem uses lemma 2.107 and achieves a complexity similar to lemma 7.1.

Theorem 7.2. *Let I be a toric ideal in the polynomial ring $\mathbb{K}[X]$ over a well-endowed field $\mathbb{K}$ and let I be generated by binomials $F = \left\{x^{\alpha_i} - x^{\beta_i} \in \mathbb{K}[X] : i = 1, \dots, s\right\}$, let $h = \sum_{i=1}^{t} h_i x^{\gamma_i} \in \mathbb{K}[X]$ be any polynomial, and let q bound the bitsize of all numerators and denominators of the coefficients and the exponents. Then the membership problem $h \overset{?}{\in} I$ can be solved in space $O(\log^2((n+s+t)q))$.*

Proof. By lemma 7.1, one can check the membership of any binomial in space $O(\log^2((n + s)q))$. According to lemma 2.107, it suffices to consider representations of h by binomials in I whose monomials are in the support of h. This is formalized in

$$\sum_{i=1}^{t} h_i x^{\gamma_i} = \sum_{\substack{1 \le j < k \le t \\ x^{\gamma_j} - x^{\gamma_k} \in I}} c_{j,k}(x^{\gamma_j} - x^{\gamma_k}) \qquad \text{with } c_{j,k} \in \mathbb{K} \text{ for } j, k = 1, \dots, t. \tag{7.3}$$

This polynomial equation can be solved by considering the linear system of the coefficients

$$h_i = \sum_{\substack{1 \le j < i \\ x^{\gamma_j} - x^{\gamma_i} \in I}} (-c_{j,i}) + \sum_{\substack{i < k \le t \\ x^{\gamma_i} - x^{\gamma_k} \in I}} c_{i,k} \qquad \text{with } c_{j,k} \in \mathbb{K} \text{ for } i, j, k = 1, \dots, t$$

which has t equations and $O(t^2)$ unknowns. Using the space-efficient method for rank computations (corollary 3.26), again, the system can be solved in space $O(\log^2(tq))$.

When applying corollary 3.26, the matrix of the equation system has to be computed on the fly — storing it would require to much space. It is necessary to verify this can be done efficiently. First, it is necessary to determine the dimensions of the matrix. The number of rows (respectively equations) is simply t. The number of columns (respectively indeterminates) equals the number of pairs (j, k) with $j < k$ such that $x^{\gamma_j} - x^{\gamma_k} \in I$. This quantity can be determined by enumerating all pairs (j, k) with $j < k$ and counting how often the membership condition is fulfilled. The required space is $O(\log(t)+\log^2((n+s)q))$. The coefficients then can be computed from the row index i and a valid column index (j, k). If $i = j$, the coefficient is 1, if $i = k$, the coefficient is -1, and otherwise it is 0. □

8. Radical Computation in Low Dimensions

In chapter 6, the complexity of Gröbner basis computations was analyzed. Theorem 6.4 reached better bounds than Kühnle and Mayr in [28] due to the dimension-dependent degree bounds from sections 4.5 and 5.3. This chapter will demonstrate the application of these new results to a more complex algorithm. The computation of radicals by Laplagne [30] will be revisited in the following and its space complexity will be analyzed depending on the dimension.

Algorithm In the first part of the chapter, Laplagne's algorithm from [30] will be explained. The details will be given for the reader's convenience. The presentation will be restricted to fields of characteristic 0, although the results are slightly more general (infinite perfect fields should suffice).

Many algorithms for radical computation base on the Seidenberg lemma which allows the computation of radicals of zero-dimensional ideals.

Lemma 8.1 (Seidenberg Lemma [39]). *Let $\mathbb{K}$ be a field of characteristic 0 and $I \subsetneq \mathbb{K}[X]$ be a zero-dimensional ideal which contains square-free $0 \neq f_i \in I \cap \mathbb{K}[x_i]$ (i.e. $\gcd(f_i, f_i') = 1$) for each $i = 1, \ldots, n$. Then I is radical.*

Proof. (from [26], proposition 3.7.15) The proof is by induction on n. For $n = 1$, I is principal and contains the square-free polynomial f_1. Thus the generator $g \mid f_1$ of I is square-free and I is radical.

Now assume $n > 1$ and factorize $f_n = h_1 \cdots h_t$ into irreducible polynomials. Since f_n is square-free,

$$I = I + \langle f_n \rangle = I + \bigcap_{i=1}^{t} \langle h_i \rangle = \bigcap_{i=1}^{t} (I + \langle h_i \rangle).$$

Any intersection of radical ideals is radical itself, so it suffices to show that $J = I + \langle h_k \rangle$ is radical for each $k = 1, \ldots, t$. Since $0 \neq h_k \in \mathbb{K}[x_n]$ is irreducible, $\langle h_k \rangle \cap \mathbb{K}[x_n]$ is a maximal ideal and $\mathbb{L} = \mathbb{K}[x_n]/\langle h_k \rangle$ is a field. Consider the canonical homomorphism $\varphi : \mathbb{K}[x_1, \ldots, x_n] \longrightarrow \mathbb{L}[x_1, \ldots, x_{n-1}]$ which has the kernel $\ker(\varphi) = \langle h_k \rangle$. Observe $f_i = \varphi(f_i) \in \varphi(J) \cap \mathbb{L}[x_i]$ is square-free for each $i = 1, \ldots, n-1$. Furthermore $\ker(\varphi) \subseteq J$ which implies $\mathbb{K}[x_1, \ldots, x_n]/J \cong \mathbb{L}[x_1, \ldots, x_{n-1}]/\varphi(J)$ and hence $\dim(\varphi(J)) = 0$. Thus the induction hypotheses apply to $\varphi(I)$ and, since the ring $\mathbb{L}[x_1, \ldots, x_{n-1}]$ has less variables, $\varphi(J)$ is radical by induction. Now assume $f^e \in J$ for some $e \in \mathbb{N}$. Then $\varphi(f)^e = \varphi(f^e) \in \varphi(J)$ implies $\varphi(f) \in \varphi(J)$ since $\varphi(J)$ is radical. This means $f \in J + \ker(\varphi) = J$ and hence J is radical. □

Corollary 8.2. *Let $\mathbb{K}$ be a field of characteristic 0 and $I \subsetneq \mathbb{K}[X]$ be a zero-dimensional ideal and $f_i \in I \cap \mathbb{K}[x_i]$ for $i = 1, \ldots, n$. Let $g_i = \sqrt{f_i} = \frac{f_i}{\gcd(f_i, f_i')}$ be the square-free part of f_i. Then $\sqrt{I} = I + \langle g_1, \ldots, g_n \rangle$.*

Having the Seidenberg lemma at hand, the radical computation will be reduced to the zero-dimensional case. One of the standard techniques herefore is localization w.r.t. a maximal independent set.

Lemma 1.58 predicts which primary components disappear on localization. In order to get control over this set, Laplagne transforms the ideal to Noether normal form. Then all primary components of maximal dimension remain and the radical of their intersection can be computed using the Seidenberg lemma. The missing primary components can be isolated using the ideal quotient (lemma 1.31) and their radical will be computed recursively. The whole procedure is summarized in algorithm 3.

Algorithm 3: `Radical`(I)

```
Data: Ideal $I$ in $\mathbb{K}[X]$
Result: $\sqrt{I}$
Compute change of variables $\sigma$ such that $\sigma(I)$ is in Noether normal form.
Let $r = \dim(I)$ and $U = \{x_1, \ldots, x_r\}$.
if $r = 0$ then return $\sqrt{I}$.
Compute $J = \left(\sqrt{\sigma(I) \cdot \mathbb{K}(U)[X \setminus U]}\right) \cap \mathbb{K}[X]$.
return $\sigma^{-1}(J) \cap$ Radical$(I : \sigma^{-1}(J)^\infty)$.
```

Lemma 8.3. *Let $I \subsetneq \mathbb{K}[X]$ be a r-dimensional ideal in Noether normal form with primary decomposition $I = Q_1 \cap \ldots \cap Q_t$, and define $U = \{x_1, \ldots, x_r\}$ and $J' = (I \cdot \mathbb{K}(U)[X \setminus U]) \cap \mathbb{K}[X]$. Then $\sqrt{I} = \sqrt{J'} \cap \sqrt{I : J'^\infty}$ and*

$$I : J'^\infty \supseteq \bigcap_{\substack{i=1 \\ \dim(Q_i) < r}}^{t} Q_i.$$

Proof. By lemma 1.58,

$$J' = \bigcap_{\substack{i=1 \\ Q_i \cap \mathbb{K}[U] = \{0\}}}^{t} Q_i.$$

Since I is in Noether normal form, there is a polynomial $g_i \in I \cap \mathbb{K}[x_1, \ldots, x_i]$ with $\deg_{x_i}(g_i) = \deg(g_i) > 0$ for each $i = r+1, \ldots, n$. Assume $\dim(Q_k) = r$ for some $k = 1, \ldots, t$. By lemma 2.69, $\dim(\operatorname{lm}(Q_k)) = \dim(Q_k) = r$. Consider the lexicographic monomial ordering $\prec$ with $x_1 \prec \ldots \prec x_n$. Then $x_i^{e_i} = \operatorname{lm}(g_i) \in \operatorname{lm}(I) \subseteq \operatorname{lm}(Q_k)$ for some $e_i \in \mathbb{N}$ and each $i = r+1, \ldots, n$, so U must be independent w.r.t. $\operatorname{lm}(Q_k)$ and thus independent w.r.t. Q_k. Hence $J' \subseteq Q_k$ and the claimed inclusion for $I : J'^\infty$ follows from lemma 1.31.

It remains to show $\sqrt{I} = \sqrt{J'} \cap \sqrt{I : J'^\infty}$. The same lemmas as above imply

$$\sqrt{J'} \cap \sqrt{I : J'^\infty} = \bigcap_{\substack{i=1\\ Q_i \cap \mathbb{K}[U]=\{0\}}}^{t} \sqrt{Q_i} \cap \bigcap_{\substack{i=1\\ J' \not\subseteq \sqrt{Q_i}}}^{t} \sqrt{Q_i} = \sqrt{Q_1} \cap \ldots \cap \sqrt{Q_t} = \sqrt{I}.$$

□

Lemma 8.4. *Let $I \subsetneq \mathbb{K}[X]$ be an ideal. Then $\texttt{Radical}(I) = \sqrt{I}$ and the recursion depth is bounded by $\dim(I) + 1$.*

Proof. Let $J' = (\sigma(I) \cdot \mathbb{K}(U)[X \setminus U]) \cap \mathbb{K}[X]$. By lemma 8.3, $\sqrt{\sigma(I)} = \sqrt{J'} \cap \sqrt{\sigma(I) : J'^\infty}$. Since $\sqrt{J'} = \left(\sqrt{\sigma(I)\mathbb{K}(U)[X \setminus U]}\right) \cap \mathbb{K}[X] = J$ and $\sigma(I) : J'^\infty = \sigma(I) : \sqrt{J'}^\infty$, applying σ^{-1} yields the correctness of Radical. Finally, $\dim(I : \sigma^{-1}(J)^\infty) < \dim(I)$ by lemma 8.3 since it is the intersection of ideals of dimension less then $\dim(I)$ and thus the recursion depth is at most $\dim(I) + 1$. □

Complexity Now that the correctness of Radical is established, the complexity will be analyzed. As in previous chapters, the emphasis will be on space-efficient methods. The first step is the change of variables into Noether normal form which was previously analyzed by Dickenstein et al. in [11]. The underlying algorithm and the necessary degree bounds were already presented in theorem 4.8. The following lemma applies the technique of corollary 3.26 and derives complexity bounds. Contrary to the arithmetic circuits used by Dickenstein, Boolean circuits will be used in the following supposing a well-endowed field. Therefore also the growth of coefficients has to be considered — mostly using lemma 3.8).

Lemma 8.5 (Dickenstein et al. 1991)**.** *Let $\mathbb{K}$ be a well-endowed infinite field and I be an ideal in $\mathbb{K}[X]$ generated by polynomials $F = \{f_1, \ldots, f_s\}$ of degrees bounded by d. It is possible to compute $r = \dim(I)$ and a change of variables $\sigma : \mathbb{K}[X] \longrightarrow \mathbb{K}[X], f(x) \mapsto f(Ax)$ with $A^{n \times n} \in \mathbb{K}$ such that $\{x_1, \ldots, x_r\}$ is independent w.r.t. $\sigma(I)$ and, for each $i = r+1, \ldots, n$, a polynomial $h_i \in \sigma(I) \cap \mathbb{K}[x_1, \ldots, x_i]$ with $\deg_{x_i}(h_i) = \deg(h_i) > 0$ and $\deg(h_i) \leq (d_1 \cdots d_{n-r})^2$. If q bounds the bitsize of all numerators and denominators in F, the algorithm can be implemented in SPACE$(n^4 \log^2(sdq))$ and the coefficients of the matrix A have bitsize $O(n^2 \log(d))$.*

Proof. (from [11], §1) First it is necessary to determine $r = \dim(I)$. Herefore enumerate all subsets $U \subseteq X$ and test whether $I \cap \mathbb{K}[U] \neq \{0\}$. The cardinality of the maximal w.r.t. I independent set U is the dimension of I.

A degree bound for the independence test is needed. Opposed to theorem 4.8, embedding a complete intersection J does not work since there might be sets $U \subseteq X$ which are dependent w.r.t. I but independent w.r.t. J. Thus a degree bound computed for J might be to low yielding false positives.

However, if $I \cap \mathbb{K}[U] \neq \{0\}$ and $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$, one can employ a consequence of Bézout's theorem (lemma 2.95) in order to bound $\deg(\mathbf{V}_{\overline{\mathbb{K}}}(I)) \leq d^n$. As in theorem 4.8, the existence of $h \in \sqrt{I} \cap \mathbb{K}[U]$ with $\deg(h) \leq d^n$ follows. Since $h \in \sqrt{I}$ iff ${x_0}^h h \in \sqrt{\langle {}^h f_1, \dots, {}^h f_s \rangle}$ and the representation of ${x_0}^h h$ can be chosen homogeneous, theorem 4.3 bounds the degree of the representation $h^k = g = \sum_{i=1}^s a_i f_i$ with $a_1, \dots, a_s \in \mathbb{K}[X]$ by $k \leq d^n$ and $\deg(a_i f_i) \leq d^n \deg({x_0}^h h) \leq d^n(d^n + 1)$ for $i = 1, \dots, s$.

Since there are $O((d^n(d^n+1))^n) = O(d^{2n^2})$ monomials of degree up to $d^n(d^n+1)$, the equation $h = \sum_{i=1}^s a_i f_i$ can — for given $f_1, \dots, f_s$ — finally be transformed to a linear system of size $O(sd^{2n^2})$ which has a non-trivial solution h iff U is dependent w.r.t. I. By corollary 3.26, this can be decided in space $O(n^4 \log^2(sdq))$ by two rank computations.

The initial change of variables just permutes the variables such that $U = \{x_1, \dots, x_r\}$ is independent w.r.t. I and thus its coefficients have constant size.

The rest of the algorithm is by induction. Each step $k = r+1, \dots, n$ of theorem 4.8 begins with the search for a polynomial $h_k \in \sigma(I) \cap \mathbb{K}[x_1, \dots, x_r, x_k]$ with representation degree bounded by $\deg(h_k) \leq d^{n-r}(d^{n-r}+1)$. The complexity for the computation of this polynomial is dominated by the computation of the dimension. For the change of variables, it is necessary to find a point $(y_1, \dots, y_r) \in \mathbb{K}^r$ at which $\tilde{h}(y_1, \dots, y_r, 1) \neq 0$ for the homogeneous component $\tilde{h}$ of highest degree of h_k. By lemma 1.44, this is possible with coefficients of size $O(n^2 \log(d))$ each. Thus the computation uses space $O(n^3 \log(d))$ since n coefficients have to be stored at a time. The evaluation is polylogarithmic in the bitsize using techniques from section 3.3 and thus is negligible. Due to the special form of the functions, the composition of the (at most n) changes of variables computed adds only $\log(n)$ to the bitsize of the coefficients which hides in the O-notation. □

Lemma 8.6. *Let $\mathbb{K}$ be a well-endowed field and $I, J \subsetneq \mathbb{K}[X]$ be ideals of dimension at most r which are generated by polynomials $f_1, \dots, f_s$ respectively $g_1, \dots, g_t$ of degrees bounded by d. Then one can compute the following by a Gröbner basis computation:*

1. *A polynomial in $I \cap \mathbb{K}[U]$ (if existent) for any $U \subseteq X$.*
2. *A basis of $I : J^\infty$.*
3. *A basis of $I \cap J$.*

The degrees of the computed polynomials and the cardinalities of the computed bases are bounded by $d^{n^{O(1)}2^{O(r)}}$. If q bounds all the bitsize numerators and denominators in the input, the computation can be performed in space $n^{O(1)}2^{O(r)} \log^{O(1)}((s+t)dq)$.

Proof. 1. is reduced by the elimination theorem 2.16. 2. and 3. can be computed using 1. applied to the ideals constructed in lemma 1.51 and lemma 1.52 respectively lemma 1.50. Note that all ideals involved in the computations have dimension $O(r)$ (more exactly $\leq r+$ number of newly introduced indeterminates). The degree bound of the reduced Gröbner basis follows from theorem 5.29. For the cardinality of the reduced Gröbner basis, note that there are less than $(d^{n^{O(1)}2^{O(r)}})^n = d^{n^{O(1)}2^{O(r)}}$ monomials of degree up to $d^{n^{O(1)}2^{O(r)}}$ and the elements of the Gröbner basis have pairwise distinct leading monomials. The space complexity is proved in theorem 6.4. □

Lemma 8.7. *Let $\mathbb{K}$ be a well-endowed field of characteristic 0 and $I \subsetneq \mathbb{K}[X]$ be an ideal of dimension r in Noether normal form generated by polynomials $F = \{f_1, \dots, f_s\}$ of degrees bounded by d and let $U = \{x_1, \dots, x_r\}$. If q bounds the bitsize of all numerators and denominators in F, it is possible to compute a basis of $\sqrt{I \cdot \mathbb{K}(U)[X \setminus U]} \cap \mathbb{K}[X]$ with degrees bounded by $d^{n^{O(1)}2^{O(r)}}$ in space $n^{O(1)}2^{O(r)} \log^{O(1)}(sdq)$.*

Proof. The key to this lemma is the Seidenberg lemma respectively corollary 8.2. In lemma 8.5, it was shown that $h_i \in I \cap \mathbb{K}[x_1, \dots, x_r, x_i]$ with $\deg(h_i) \le d^{2n}$, for $i = r+1, \dots, n$, can be computed in space $O(n^4 \log^2(sdq))$. Their derivations h_i' are easily calculated on the fly.

Avoiding the GCD-calculation, the LCM will be computed using the equality $\langle h_i \rangle \cap \langle h_i' \rangle = \langle \mathrm{lcm}(h_i, h_i') \rangle$ and lemma 8.6. Both $\langle h_i \rangle$ and $\langle h_i' \rangle$ have dimension r in $\mathbb{K}[x_1, \dots, x_r, x_i]$ and the bitsize of the coefficients of h_i is trivially bounded by $2^{O(n^4 \log^2(sdq))}$ (lemma 3.8). Hence the computation needs space $n^{O(1)}2^{O(r)} \log^{O(1)}(sdq)$. However, from the context, $\deg(\mathrm{lcm}(h_i, h_i')) \le 2d^{2n}$ is clear.

The polynomial division $g_i = \frac{h_i}{\gcd(h_i, h_i')} = \frac{\mathrm{lcm}(h_i, h_i')}{h_i'}$ can be formulated as linear system of size $O(\deg(\mathrm{lcm}(h_i, h_i'))^n) = O(d^{2n^2})$ with coefficients of bitsize $2^{n^{O(1)}2^{O(r)} \log^{O(1)}(sdq)}$ and solved using corollary 3.26. This suffices in order to realize the polynomial division in $n^{O(1)}2^{O(r)} \log^{O(1)}(sdq)$.

Furthermore one can contract the basis $\langle f_1, \dots, f_s, g_{r+1}, \dots, g_n \rangle$ of $\sqrt{I \cdot \mathbb{K}(U)[X \setminus U]}$ to a basis of $(I \cdot \mathbb{K}(U)[X \setminus U]) \cap \mathbb{K}[X]$ using lemma 2.17. This requires two more Gröbner basis computations — the first in order to fulfill the prerequisites of the lemma and the second for the saturation. Since the ideals have dimension $O(r)$, the degrees remain bounded by $d^{n^{O(1)}2^{O(r)}}$ and the space requirement by $n^{O(1)}2^{O(r)} \log^{O(1)}(sdq)$. □

Theorem 8.8. *Let $\mathbb{K}$ be a well-endowed field of characteristic 0. Then* `Radical` *can be implemented such that it computes a basis G of the radical of any r-dimensional ideal $I \subsetneq \mathbb{K}[X]$ generated by polynomials $F = \{f_1, \dots, f_s\}$ of degrees bounded by d such that $\deg(G) = d^{n^{O(r)}2^{O(r^2)}}$ in space $n^{O(r)}2^{O(r^2)} \log^{O(r)}(sdq)$ where q bounds the bitsize of all numerators and denominators in F.*

Proof. In any iteration, there are a constant number of Gröbner basis computations and similar operations which were discussed in lemmas 8.6 and 8.7. On input of degree d, cardinality s, and bitsize q, they produce output of degree and cardinality $d^{n^{O(1)}2^{O(r)}}$ in space $n^{O(1)}2^{O(r)} \log^{O(1)}(sdq)$ which implies a bitsize of $2^{n^{O(1)}2^{O(r)} \log^{O(1)}(sdq)}$ by lemma 3.8. Feeding such an operation with the output of another such operation yields a result of degree and cardinality of $\left(d^{n^{O(1)}2^{O(r)}}\right)^{n^{O(1)}2^{O(r)}} = d^{n^{O(1)}2^{O(r)}}$. The space complexity of this concatenation is bounded by

$$
\begin{aligned}
&n^{O(1)}2^{O(r)}\log^{O(1)}\left[\left(d^{n^{O(1)}2^{O(r)}}\right)\left(d^{n^{O(1)}2^{O(r)}}\right)\left(2^{n^{O(1)}2^{O(r)}\log^{O(1)}(sdq)}\right)\right] = \\
&\qquad = n^{O(1)}2^{O(r)}\left(n^{O(1)}2^{O(r)}\log^{O(1)}(d) + n^{O(1)}2^{O(r)}\log^{O(1)}(sdq)\right) = \\
&\qquad\qquad = n^{O(1)}2^{O(r)}\log^{O(1)}(sdq).
\end{aligned}
$$

Thus any constant number of operation stays within the same magnitude. By lemma 8.4, the algorithm performs r recursions which implies the stated bounds. □

Conclusion

As mentioned in the introduction and throughout, the computation of Gröbner bases is inherently complex. The goal of this thesis was to analyze this complexity for special ideal classes. Now it is time to summarize the results and point out open problems. The structure of the thesis will be used as guidance.

Representation Degree The representation degree in arbitrary ideals was revisited in section 4.1. The lower and upper bounds by Hermann respectively Yap only differ in two points: a factor of 2 in the second exponent and the dependence on the number of ideal generators. While the first seems negligible, it would be nice to clarify to which amount the degree depends on the number of generators.

The radical membership treated in section 4.2 has been intensely studied such that lower and upper bounds match exactly for the most important parameters.

In section 4.3, the representation problem for zero-dimensional ideals was considered. While the author of this thesis found various upper bounds in literature, the best of which was stated in theorem 4.6, he is not aware of any interesting lower bounds for this case. Also the upper bound might leave room to improvement when comparing it with the situation of the Gröbner basis degrees.

The upper degree bound for complete intersections in section 4.4 is neat and could be sharp, although no lower bound is known. The search for lower bounds for complete intersections might also yield a tight lower bound for the zero-dimensional case.

In section 4.5, two results were treated. The first was a version of effective Noether normalization. The degree bound presented in this thesis is slightly sharper than the one by Dickenstein et al. in [11]. This was possible due to the sharp bound for the radical membership problem by Jeloneck and the use of regular sequences. Still, the author suggests that it can be further improved. One could try to make use of the theory of multiplicities (section 2.9) and therefore avoid the radical membership problem. This could save the square in the degree bound. However, it is not quite obvious since the theory of multiplicities is mostly designed for the homogeneous case. Lemma 2.99 could be part of the remedy, but it doesn't apply straight forward since generators of the homogenization of an ideal are not easily obtained. Also combining lemmas 2.23 and 1.31 with corollary 2.100 yields no trivial result since the dimension of the ideal might change on homogenization (see lemma 2.70

and example 2.76) and thus ″hidden″ (i.e. lower dimesional) primary components must be considered.

The second result was Kratzer's upper bound for the representation degree. This bound could be somewhat sharpened using the improved Noether normalization. The lower bound for the representation problem is rather trivial, but attacking it most likely requires tackling the zero-dimensional case first and then combining the techniques as in theorem 5.31.

The chapter about representation degrees closes with a completely new construction that provides a lower bound for toric ideals in section 4.6. There is no complementing upper bound. The situation is the same for prime and radical ideals, super-classes of toric ideals. This is surprising due to the celebrated bounds of the radical membership (cf. section 4.2).

This concludes the survey of the representation degree and yields way to the chapter about the Gröbner basis degree.

Gröbner Basis Degree In section 5.1, it was shown that, for arbitrary ideals, the situation is very well understood. The lower and upper bounds only differ by a constant factor 2.

For zero-dimensionals ideals, however, the bounds match perfectly as seen in section 5.2. The tight upper bound is a slight improvement of the result by Caniglia et al. [6] which the author of this thesis could not find in literature. As soon as homogeneous ideals or graded monomial orderings (although with some caveats) are considered, the bounds are smaller by a magnitude as proved by Lazard and a trivial example.

Section 5.3 contains a main contribution of the thesis. Both upper and lower bounds for the Gröbner basis degree are derived depending on the ideal dimension. They agree up to a factor of 2 in the second exponents. The upper bound for inhomogeneous ideals would be affected by an improvement by the Noether normalization. Also techniques by Sombra in [41], §1 might be helpful in order to construct a homogeneous sequence with increasing degrees (thus the first polynomials would have much lower degrees). Both techniques, however, would only improve the bound by a factor of 2 in the first exponent. Attacking the second exponent would, on the one hand, require to improve the bounds for arbitrary ideals. On the other hand, a direct method for inhomogeneous ideals could be useful.

Finally, toric ideals are considered in section 5.4. A proof technique by Sturmfels [42] is adapted to ideal given by a basis yielding an upper bound. A lower bound is derived from an example by Möller and Mora [35]. Both bound are single exponential but leave some room for improvement.

Complexity It is well known that the complexity of Gröbner basis computations depends on the degrees of the bases and representations in the worst case. Mayr and Meyer [33] constructed polynomials of high degree in order to show that the membership problem and thus (Gröbner basis computation) is exponential space hard. Then Kühnle and Mayr [28] came up with a reduction of normal form and Gröbner basis computations to linear systems which can be computed space-efficiently proving that the computation of Gröbner bases is exponential space complete.

In chapter 6, the algorithm from [28] is revisited. First, the dimension-dependent bounds from previous chapters are used to sharpen the complexity estimate. Further improvement comes from the avoidance of the degree bounds for normal forms in lemma 6.3. In the second part, the algorithm is stripped of all degree bounds and transformed into an incremental algorithm. The complexity of this algorithm depends on the degrees of the actual basis and their representation (actually S-polynomials of basis elements) in terms of the generators.

Chapter 7 gives a short but insightful analysis of the membership problem of toric ideals (generated by binomials). By the reduction to a module membership problem, it can be solved in polynomial time or polylogarithmic space for arbitrary polynomials. It would be interesting to settle the complexity of the representation problem for toric ideals since this problem is most likely harder. This is suggested by the lower degree bound in section 4.6. Moreover, the definition of toric ideals via modules seems incompatible with the ideal representation.

The thesis finishes with the analysis of the radical computation by Laplagne [30]. Chapter 8 combines most previous results and yields improvements of twofold kind. First, the complexity is analyzed depending on the dimension of the ideal, basically replacing the number of variables by the ideal dimension in the bound. Secondly, the analysis takes the growth of coefficients into account which is neglected in the arithmetic circuits considered by Laplagne and could possibly lead to further escalation of the complexity.

These considerations demonstrate the importance of the ideal dimension as a measure of the complexity of various ideal computations from the very basics up to involved algorithms which are long concatenations of basic operations.

Space-efficient algorithms as considered in this thesis recompute subtasks so often that they would not perform well in practice. Still, the idea of space-efficiency appears whenever fast memory is limited but plenty of output is feasible. This situation requires a delicate balance of recomputations and storage which is highly dependent on the amount of memory available.

Moreover, the worst-case analysis is not telling the whole story in the case of Gröbner bases. Polynomials with random coefficients most likely form a regular sequence (though the case is not settled in the overdetermined setting, yet). The hardest problems then arise with growing coefficients. But examples occurring in applications are usually not that easy. Sometimes they have low dimensions or are toric and can be treated with techniques presented in this thesis. For other beneficent characterizations there might be similar results. Two questions arise in this context. Are the algorithms used in practice aware of these complexity results, e.g. do they (provably) perform better for low-dimensional ideals? If this is not the case, is it possible to construct algorithms which are suitable for these ideals? The goal of this thesis was *not* to answer these questions, so they might be partially answered (e.g. there are efficient algorithms for the computation of Gröbner bases of zero-dimensional ideals and their radicals).

Bibliography

[1] D. A. Bayer. *The division algorithm and the Hilbert scheme*. PhD thesis, Harvard University Cambridge, MA, USA, 1982. 83

[2] K. Blackburn. An alternative approach to multiplicity theory. *Proceedings of the London Mathematical Society*, 3(1):115, 1964. 54

[3] A. Borodin. On relating time and space to size and depth. *SIAM Journal on Computing*, 6(4):733–744, 1977. 65

[4] A. Borodin, S. Cook, and N. Pippenger. Parallel computation for well-endowed rings and space-bounded probabilistic machines. *Information and Control*, 58(1-3):113–136, 1983. 65, 66, 67, 68

[5] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Universität Innsbruck, Austria, 1965. 31

[6] L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, 6:131–151, 1989. 2, 84, 126

[7] L. Caniglia, A. Galligo, and J. Heintz. Equations for the projective closure and effective Nullstellensatz. *Discrete Applied Mathematics*, 33(1-3):11–23, 1991. 52

[8] A. Y. Chiu. *Complexity of Parallel Arithmetic Using the Chinese Remainder Representation*. PhD thesis, The University of Wisconsin-Milwaukee, WI, USA, 1995. 67

[9] D. A. Cox, J. B. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer New York, 1992. 7, 16, 21, 31, 35, 51

[10] D. A. Cox, J. B. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer, 2005. 7

[11] A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Applied Mathematics*, 33(1-3):73–94, 1991. 2, 75, 84, 121, 125

[12] T. W. Dubé. The Structure of Polynomial Ideals and Gröbner Bases. *SIAM Journal on Computing*, 19(4):750–773, 1990. 2, 37, 39, 40, 41, 83, 86, 87, 88, 90

[13] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Springer, 1995. 7, 17, 19, 24, 25, 43, 46, 48, 54

[14] D. Eisenbud and B. Sturmfels. Finding Sparse Systems of Parameters. *Journal of Pure and Applied Algebra*, 94(2):143–157, 1994. 50

[15] D. Eisenbud and B. Sturmfels. Binomial ideals. *Duke Mathematical Journal*, 84(1):1–46, 1996. 58

[16] G. Ferro. Some upper bounds for the multiplicity of an autoreduced subset of N^m and their applications. *Algebraic Algorithms and Error-Correcting Codes*, 3:306–315, 1986. 45

[17] M. Giusti. Some effectivity problems in polynomial ideal theory. *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, 174:159–171, 1984. 83

[18] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24(3):239–277, 1983. 51, 52

[19] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Mathematische Annalen*, 95(1):736–788, 1926. 2, 73

[20] D. T. Huynh. A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems. *Information and Control*, 68(1-3):196–206, 1986. 84

[21] Z. Jelonek. On the effective Nullstellensatz. *Inventiones Mathematicae*, 162(1):1–17, 2005. 74

[22] D. Kirby. On Bêzout's theorem. *The Quarterly Journal of Mathematics*, 39(4):469, 1988. 54, 56

[23] J. Kollar. Sharp effective nullstellensatz. *Journal of the American Mathematical Society*, 1(4):963–975, 1988. 74

[24] M. Kratzer. Computing the dimension of a polynomial ideal and membership in low-dimensional ideals. Master's thesis, Technische Universität München, Germany, October 2008. 2, 76

[25] H. Kredel and L. Weispfenning. Computing dimension and independent sets for polynomial ideals. *Journal of Symbolic Computation*, 6(2-3):231–247, 1988. 44, 45

[26] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 1*. Springer, 2000. 7, 19, 47, 119

[27] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 2*. Springer, 2005. 7, 46, 47, 54

[28] K. Kühnle and E. W. Mayr. Exponential space computation of Gröbner bases. In *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*, pages 63–71. ACM New York, NY, USA, 1996. 2, 107, 109, 110, 119, 126, 127

[29] R. E. Ladner and M. J. Fischer. Parallel prefix computation. *Journal of the ACM*, 27(4):831–838, 1980. 67

[30] S. Laplagne. An algorithm for the computation of the radical of an ideal. *Proceedings of the 2006 international symposium on Symbolic and algebraic computation*, pages 191–195, 2006. 2, 21, 22, 119, 127

[31] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. *European Computer Algebra Conference London*, 162:146–156, 1983. 85, 100

[32] E. W. Mayr. On polynomial ideals, their complexity, and applications. *Proceedings of the 10th International Symposium on Fundamentals of Computation Theory*, pages 89–89, 1995. 2, 115

[33] E. W. Mayr and A. R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46(3):305–329, 1982. 2, 61, 62, 73, 77, 84, 107, 111, 126

[34] E. W. Mayr and S. Ritscher. Degree bounds for Gröbner bases of low-dimensional polynomial ideals. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 21–27. ACM, 2010. 86, 97

[35] H. M. Möller and F. Mora. Upper and Lower Bounds for the Degree of Groebner Bases. *International Symposium on Symbolic and Algebraic Computation*, 174:172–183, 1984. 83, 84, 85, 99, 100, 126

[36] D. G. Northcott. *Lessons on rings, modules and multiplicities*, volume 44. Cambridge University Press, 1968. 54

[37] J. G. Oxley. *Matroid theory*. Oxford University Press, USA, 2006. 25

[38] J. Schmid. On the affine Bezout inequality. *Manuscripta Mathematica*, 88(1):225–232, 1995. 49

[39] A. Seidenberg. Constructions in algebra. *Transactions of the American Mathematical Society*, 197:273–313, 1974. 119

[40] I. R. Shafarevich. *Basic Algebraic Geometry*. Springer-Verlag, 1994. 84

[41] M. Sombra. A Sparse Effective Nullstellensatz. *Advances in Applied Mathematics*, 22(2):271–295, 1999. 126

[42] B. Sturmfels. *Gröbner bases and convex polytopes*. Amer Mathematical Society, 1996. 2, 57, 101, 102, 126

[43] D. J. Wright. General multiplicity theory. *Proceedings of the London Mathematical Society*, 3(1):269, 1965. 54, 55

[44] C. K. Yap. A new lower bound construction for commutative Thue systems with applications. *Journal of Symbolic Computation*, 12(1):1–27, 1991. 2, 73, 84

[45] O. Zariski and P. Samuel. Commutative Algebra, Volume II. *Graduate Texts in Mathematics*, 29, 1960. 54