Gröbner theory of zero dimensional ideals
with a view toward combinatorics

PhD thesis

BÁLINT FELSZEGHY

Institute of Mathematics,
Budapest University of Technology and Economics

Supervisor:
Lajos Rónyai

2007

Ezen értekezés bírálatai és a védésről készült jegyzőkönyv a későbbiekben a Budapesti Műszaki és Gazdaságtudományi Egyetem Természettudományi Karának Dékáni Hivatalában elérhető.

Alulírott Felszeghy Bálint kijelentem, hogy ezt a doktori értekezést magam készítettem, és abban csak a megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

....
Felszeghy Bálint

Contents

Chapter 1

Introduction

1.1 History of Gröbner bases and combinatorial applications

Gröbner bases are special systems of generators of a polynomial ideal. Although similar concepts appeared in the earlier works of H. Hironaka and A. I. Shirshov, the precise definitions and the bases of the theory have been laid down by the Austrian mathematician Bruno Buchberger. He discovered the main properties of Gröbner bases (and an algorithm to compute them) 40 years ago in his Ph. D. thesis [10] and in the paper [11] published a few years later. He was motivated mainly by questions in commutative algebra, but since then, Gröbner bases—which have been named after Buchberger's supervisor—found their applications in various topics of mathematics.

While getting better and better known in the 70s, Gröbner bases have been applied in algebraic geometry, symbolic computations, coding theory, automated reasoning, partial differential equations and numerical analysis. The proceedings of the conference *33 years of Gröbner bases* [13] give a good overview of these, and contain the English translation of Buchberger's original work as well. The theory keeps on being researched: last spring a special semester on Gröbner bases in Linz took place, where beside the topics already mentioned, a one week workshop was dedicated to combinatorial applications, a relatively new area where Gröbner bases may be used.

From the combinatorial point of view, Gröbner theory of zero dimensional ideals are of special interest. The present thesis investigates this topic: we contribute with theoretical examination of Gröbner bases of zero dimensional ideals, while giving equal importance to the applications of the new results in (algebraic) combinatorics. I will often refer to papers of Lajos Rónyai and Gábor Hegedűs who founded the basis of this theory.

1.2 Introduction to the theory

To get a better overview of what is contained in this thesis, let us shortly (and sometimes informally) introduce the basic concepts.

Let $\mathbb{F}$ be a field, $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[\mathbf{x}]$ the ring of polynomials in n indeterminates and I be an ideal in $\mathbb{F}[\mathbf{x}]$. We say that I is zero dimensional if $\mathbb{F}[\mathbf{x}]/I$ is a finite dimensional $\mathbb{F}$-vector space. The simplest such ideals are the vanishing ideals $I(V)$ of finite subsets V of $\mathbb{F}^n$: they contain all polynomials, which vanish on V as functions. A more general example of a zero dimensional ideal is the vanishing ideal of a finite multiset, consisting of all polynomials which not only vanish on V, but also have a prescribed multiplicity at each point of V (where the definition of multiplicity can be rather complicated).

To define Gröbner bases, one first needs a term order—a complete ordering of the monomials of $\mathbb{F}[\mathbf{x}]$, with some additional properties. The greatest monomial of a polynomial is its leading monomial. In the univariate case, the leading monomial is simply the highest degree term of the polynomial. A finite subset G of an ideal I is a Gröbner basis of I, if the leading monomial of any $f \in I$ is divisible by the leading monomial of some $g \in G$. Then G also generates the ideal in a 'nice' manner. To get an impression of what 'nice' means, one may think of an ideal which is generated by a system of linear equations. A Gröbner basis of this ideal is an equivalent system of linear equations, but which is in upper diagonal form. Actually, the power of Gröbner bases lives in the fact that they provide a symbolic method to examine solutions of systems of multivariate polynomial equations, similarly to the linear case above.

As the title suggests, we are interested in Gröbner bases of zero dimensional ideals. But also, we include a further concept in the term Gröbner theory, which is of great importance in the applications. The set of standard monomials $\mathrm{Sm}(I)$ of an ideal I consists of those monomials which do not occur as the leading monomial of any polynomial in I. The standard monomials form a linear basis of $\mathbb{F}[\mathbf{x}]/I$, which for instance implies that for a finite $V \subseteq \mathbb{F}^n$, all functions $V \to \mathbb{F}$ can be represented uniquely as linear combinations of elements of $\mathrm{Sm}(I(V))$.

The latter observation comes from the easy fact that the linear space of functions $V \to \mathbb{F}$ is isomorphic to $\mathbb{F}[\mathbf{x}]/I(V)$, provided that V is finite. And this is the point where combinatorics comes into the picture. Several interesting properties of V can be formalized in terms of functions on V; the simplest such being the cardinality of V, which is the dimension of the vector space $\mathbb{F}[\mathbf{x}]/I(V)$ by the above.

Let us pick an example, which is probably the most complex one discussed in the thesis. Let $\mathcal{G}$ be a modulo q L-intersecting, L-avoiding family. We shall give the precise definition in Chapter 6, it is enough now that $\mathcal{G}$ is a subset of the power set of $\{1, 2, \ldots, n\}$, with some additional criteria. A problem from extremal combinatorics is to give an upper bound for the cardinality of $\mathcal{G}$. Define $V_{\mathcal{G}} \subseteq \{0, 1\}^n \subseteq \mathbb{F}^n$ as the set of characteristic vectors of members of $\mathcal{G}$. In particular $|V_{\mathcal{G}}| = |\mathcal{G}|$. Thus if we could compute the standard monomials of $I(V_{\mathcal{G}})$, we would immediately get the cardinality of $\mathcal{G}$. We shall see that it is not that simple, but still we will be able to give an upper bound for $|\mathcal{G}|$.

Buchberger's algorithm is a general method to get a Gröbner basis of an arbitrary ideal, but it is far from being efficient from a computational point of view. For zero dimensional vanishing ideals $I(V)$, the Buchberger–Möller algorithm [12] gives a fast way to obtain a Gröbner basis and the standard monomials at once. However, this algorithm is still not applicable for a parametric family of ideals, which would be needed in combinatorial applications. Think for example of the ideals $I(V_{n,d})$, where $V_{n,d} \subseteq \mathbb{F}^n$ consists of all 0-1 vectors of Hamming weight d in $\{0, 1\}^n$. We investigate in Gröbner theory of zero dimensional ideals, with the aim of being able to work with these kinds of ideals.

1.3 Main results and structure of the thesis

We tried to do our best to make the thesis self-contained. All the necessary concepts and theorems needed to understand the subsequent parts are collected in Chapter 2. In particular we give the definition of term orders, standard monomials, Gröbner bases, and prove the basic theorems of the subject. The interested reader may find more details in [1], [9] or [28]. Section 2.2 contains useful facts about zero dimensional ideals. After defining the general notion of multiplicity and vanishing ideals of finite multisets, we give the characterization of these ideals in terms of primary decomposition to relate them to general zero dimensional ideals.

Right away in Chapter 3, we present two applications, both of which use Gröbner bases of $I(V)$, where V is a direct product of finite subsets of $\mathbb{F}$. The first result is an easy proof of a theorem of Harima [30]. We shall give a formula for the Hilbert function of complementary sets of points in V, and show an interesting consequence in boolean complexity theory. The special case, when $V = \{0, 1\}^n$ have been investigated earlier by Pintér and Rónyai in [35]. Our proof is different from their approach, and applies for more general sets V.

The second application of the chapter is to the solvability of certain polynomial equations over finite fields. Rédei's Conjecture [37] suggests a sufficient condition on multivariate polynomials f for having a root over finite prime fields. The conjecture in general has been disproved recently [38], however for special classes of polynomials it is still open. Under a slightly stronger assumption, we are able to prove the conjecture for generalized diagonal polynomials. Here, we make use of Alon's Combinatorial Nullstellensatz [3], which we translate to (and prove in) the language of Gröbner bases.

We turn back to the theoretical line in Chapter 4, and introduce the Lex Game, which plays a central role in the remaining of the thesis.

In general, Gröbner bases and standard monomials depend on the term order we use on the monomials. We shall consider the lexicographic order in that chapter, and give an equivalent description of lexicographic standard monomials of some classes of zero dimensional ideals. In fact, we define the Lex Game played by two players Lea and Stan. A zero dimensional ideal and a monomial are the parameters of the game, which determines the player who have winning strategy. For a fixed ideal I, the set of monomials such that Stan can win is denoted by $\mathrm{Stan}\,(I)$. For a quite wide class of ideals, this set is the same as $\mathrm{Sm}\,(I)$, and thus the game yields a combinatorial description of the standard monomials for these ideals.

It is proven in Section 4.2, that for vanishing ideals I of finite multisets $\mathrm{Stan}\,(I) = \mathrm{Sm}\,(I)$.

The subsequent section is divided into two subsections. In the first one, we prove a theorem on the 'shape' of reduced Gröbner bases of some zero dimensional ideals of bivariate polynomial rings. This result—which we think is interesting also on its own right—will then be applied in the second subsection to obtain $\mathrm{Stan}\,(I) = \mathrm{Sm}\,(I)$ for ideals I, such that the points of I (common zeros of the polynomials in I over the algebraic closure of $\mathbb{F}$) can be differentiated by their last two coordinates. Note that this is a slightly weaker condition than expecting points in general position.

The shorter Section 4.4 shows that $\mathrm{Stan}\,(I) \neq \mathrm{Sm}\,(I)$ in general. We formulate a conjecture, which claims that (just like $\mathrm{Sm}\,(I)$) $\mathrm{Stan}\,(I)$ forms a monomial basis of the linear space of polynomials modulo I.

The last section of Chapter 4 contains an algorithm to obtain $\mathrm{Stan}\,(I)$ in general, that is $\mathrm{Sm}\,(I)$ in certain cases. The fastest known algorithm to compute the lexicographic standard monomials of multiset ideals is Cerlienco and Mureddu's method [15]. As for such ideals $\mathrm{Stan}\,(I) = \mathrm{Sm}\,(I)$, our algorithm does the same job, and performs it faster. For more general ideals, the known methods are variants of the above mentioned Buchberger–Möller algorithm, at which one has to pay a lot in running time for the generality. Therefore, when $\mathrm{Stan}\,(I) = \mathrm{Sm}\,(I)$, the algorithm presented in this thesis is the fastest known method to get $\mathrm{Sm}\,(I)$. We implemented the algorithm for vanishing ideals of finite sets in Singular. The code can be found in the Appendix.

We collected several applications in Chapter 5. Except for those of Section 5.1, the theorems presented there are already known ones. Using the Lex Game, we tried to give elegant and simpler proofs for these results.

In Section 5.1 we shall show the rather surprising fact that the reduced lexicographic Gröbner basis of a vanishing ideal of a finite multiset is independent from the base field, provided that the points of the multiset are all in $\{0,1\}^n$.

The following section contains a proof of a generalization of the fundamental theorem of symmetric polynomials obtained first by Garsia [27]. Actually, the proof is a simplified version of Hegedűs and Rónyai's [31], using the Lex Game.

In the remaining part of the thesis, we shall focus on vanishing ideals of finite sets $V_{\mathcal{F}}$, where $V_{\mathcal{F}}$ consists of the characteristic vectors of some family of sets $\mathcal{F}$. In Section 5.3 we include a well-known theorem which relates the Hilbert function and standard monomials of $I(V_{\mathcal{F}})$ with the rank of an inclusion matrix. A similar theorem is also shown, which is applied in the next section to prove a rank formula of the inclusion matrix of all d-subsets versus all m-subsets of $[n]$. The proof was originally found by Wilson [39]. Our argument is adopted from [26], but it gets remarkably simplified by the Lex Game.

The goal of the last chapter is to show two different applications to extremal combinatorics. The common basis of the proofs is the good understanding of the algebraic properties of $I(V_{\mathcal{F}})$, where $\mathcal{F}$ is a modulo q complete ℓ-wide family of sets. The first section is quite a long one, as a lot of work is needed to compute the standard monomials, a Gröbner basis and the Hilbert function of $I(V_{\mathcal{F}})$. But then we shall be able to prove our results concerning the maximal size of two interesting set families in the last two sections.

We examine modulo q L-avoiding L-intersecting set families $\mathcal{G}$ in Section 6.2. After giving a short insight to the known results of the topic, we prove that if q is a power of a prime, L is a modulo q interval, and $|L| \leq n-q+2$, then $|\mathcal{G}| \leq \sum_{k=|L|}^{q-1} \binom{n}{k}$. We note that the statement in the case $|L| = q-1$ is known as the Babai–Frankl Conjecture, recently proven by Hegedűs and Rónyai [32].

The last section of the thesis gives a sharp upper bound to the cardinality of modulo q ℓ-wide families $\mathcal{G}$, which do not shatter any set of size $m+1$, namely $|\mathcal{G}| \leq \sum_{i=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m-iq-k}$, if q is a prime power and $0 \leq m \leq \frac{n+\ell}{2}$. We connect this result to an open conjecture of Frankl.

The present thesis is based on our papers [18], [19], [20], [21] and [22]. However no one-to-one correspondence between these articles and the chapters of the thesis can be found (which respects the contents), as we tried to select topics in an order that is easier to understand. Some parts—at least in this generality—have not been published yet.

Chapter 2

Preliminaries

Let us introduce first some general notation.

Throughout the thesis, n will be a positive integer, and $[n]$ stands for the set $\{1, 2, \dots, n\}$. By $\mathbb{N}$ we mean the nonnegative integers, $\mathbb{Z}$ is the set of integers, $\mathbb{Q}$ is the field of rational numbers, and $\mathbb{F}_q$ is the field of q elements, where q is a prime power. If A is any set, then 2^A is the power set of A.

Let $\mathbb{F}$ be a field. As usual, we denote by $\mathbb{F}[x_1, \dots, x_n] = \mathbb{F}[\mathbf{x}]$ the ring of polynomials in the variables $x_1, \dots, x_n$ over $\mathbb{F}$. To shorten our notation, we write $f(\mathbf{x})$ for $f(x_1, \dots, x_n)$. Also in general, vectors of length n are denoted by boldface letters, for example $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}^n$. If $\mathbf{w} \in \mathbb{N}^n$, we write $\mathbf{x}^{\mathbf{w}}$ for the monomial $x_1^{w_1} \dots x_n^{w_n} \in \mathbb{F}[\mathbf{x}]$. If $\mathbf{y} \in \mathbb{F}^n$, then $(\mathbf{x} - \mathbf{y})^{\mathbf{w}}$ stands for the polynomial $(x_1 - y_1)^{w_1} \dots (x_n - y_n)^{w_n}$.

We will quite often meet vectors of length $n - 1$, and sometimes of length $n - 2$. For $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}^n$ we set $\overline{\mathbf{y}} = (y_1, \dots, y_{n-1})$ and $\widetilde{\mathbf{y}} = (y_1, \dots, y_{n-2})$. We shall also use $\overline{\mathbf{y}}$ (or $\widetilde{\mathbf{y}}$) for denoting a vector of length $n-1$ (or $n-2$ respectively), even if it is not a prefix of a vector of length n. Similarly we shall write sometimes $\overline{\mathbf{w}}$, $\widetilde{\mathbf{w}}$, $\mathbb{F}[\overline{\mathbf{x}}]$, or even $\overline{\mathbf{x}}^{\overline{\mathbf{w}}}$ and $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}}$ instead of $x_1^{w_1} \dots x_{n-1}^{w_{n-1}}$ and $x_1^{w_1} \dots x_{n-2}^{w_{n-2}}$.

If I is an ideal of the ring $\mathbb{F}[\mathbf{x}]$, we denote it by $I \trianglelefteq \mathbb{F}[\mathbf{x}]$. The ideal generated by some polynomials $f_1, \dots, f_m \in \mathbb{F}[\mathbf{x}]$ is $\langle f_1, \dots, f_m \rangle$.

2.1 Gröbner basics

2.1.1 Monomials and term orders

Monomials form a linear basis of $\mathbb{F}[\mathbf{x}]$ as an $\mathbb{F}$-vector space. We say that a polynomial f *contains the monomial* $\mathbf{x}^{\mathbf{w}}$ (or $\mathbf{x}^{\mathbf{w}}$ *is a monomial of* f, or $\mathbf{x}^{\mathbf{w}}$ *appears in* f), if the coefficient of $\mathbf{x}^{\mathbf{w}}$ is not zero when f is written as a linear combination of monomials.

Note that the set of all monomials in n indeterminates forms a semigroup S (with multiplication of monomials), which is isomorphic to $(\mathbb{Z}^n, +)$. Ideals of S are exactly its upwards closed subsets (with respect to division), that is if a monomial in a semigroup ideal I divides $\mathbf{x}^{\mathbf{w}}$, then also $\mathbf{x}^{\mathbf{w}} \in I$. It is easy to see that $S \cong \mathbb{Z}^n$ is a *Noetherian semigroup*, that is any strictly increasing chain of its ideals is finite. (It may be verified via the equivalent statement that all ideals of $\mathbb{Z}^n$ are finitely generated, but it follows as well from the fact that $\mathbb{F}[\mathbf{x}]$ is a Noetherian ring.) It shall be useful sometimes to think of the set of monomials as a semigroup.

A polynomial ideal $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ is a *monomial ideal* if it can be generated by a set of monomials. Monomial ideals and semigroup ideals of S are in one-to-one correspondence in the following sense.

Proposition 2.1.1. *If H is a set of monomials, $I = \langle H \rangle$, then the semigroup ideal generated by H is exactly the set of all monomials which appears as a monomial of some polynomial $f \in I$. In particular every monomial of an $f \in I$ is in I, and I has a finite set of generators consisting of monomials.*

Proof. As every element of the semigroup ideal generated by H is divisible with a member of H, it is also contained in I. For the other direction, let $f \in I = \langle H \rangle$. Then there are monomials $\mathbf{x}^{\mathbf{w_1}}, \dots, \mathbf{x}^{\mathbf{w_m}} \in H$ and polynomials $h_1, \dots h_m \in \mathbb{F}[\mathbf{x}]$, such that

$$f(\mathbf{x}) = \sum_{i=1}^{m} h_i(\mathbf{x})\mathbf{x}^{\mathbf{w_i}}.$$

Every monomial on the right hand side is divisible with some $\mathbf{x}^{\mathbf{w_i}}$, and so the same is true for monomials of f, that is they are contained in the semigroup ideal generated by H.

As the semigroup of monomials are Noetherian, H may be replaced with a finite set, which also generates I. □

Definition 2.1.2. A total order $\prec$ on the monomials of $\mathbb{F}[\mathbf{x}]$ is a *term order*, if 1 is the minimal element of $\prec$, and $\prec$ is compatible with multiplication by monomials, that is $\mathbf{x}^{\mathbf{u}} \prec \mathbf{x}^{\mathbf{v}}$ implies $\mathbf{x}^{\mathbf{u}} \cdot \mathbf{x}^{\mathbf{w}} \prec \mathbf{x}^{\mathbf{v}} \cdot \mathbf{x}^{\mathbf{w}}$ for all $\mathbf{x}^{\mathbf{w}}, \mathbf{x}^{\mathbf{u}}, \mathbf{x}^{\mathbf{v}} \in \mathbb{F}[\mathbf{x}]$.

Two important term orders are the *lexicographic* (*lex* for short) and the *degree compatible lexicographic* (*deglex*) orders. We have $\mathbf{x}^{\mathbf{w}} \prec_{\text{lex}} \mathbf{x}^{\mathbf{u}}$ if and only if $w_i < u_i$ holds for the smallest index i such that $w_i \neq u_i$. As for deglex, we have that a monomial of smaller degree is smaller in deglex, and among monomials of the same degree lex decides the order.

Also in general, $\prec$ is *degree compatible*, if $\deg(\mathbf{x}^{\mathbf{w}}) < \deg(\mathbf{x}^{\mathbf{u}})$ implies $\mathbf{x}^{\mathbf{w}} \prec \mathbf{x}^{\mathbf{u}}$.

Example 2.1.3. For $n = 3$, the ordering of the first few monomials with respect to lex is

$$1 \prec x_3 \prec x_3^2 \prec x_3^3 \prec \cdots \prec x_2 \prec x_2x_3 \prec x_2x_3^2 \prec \cdots \prec x_2^2 \prec x_2^2x_3 \prec x_2^2x_3^2 \prec \\ \cdots \prec x_1 \prec x_1x_3 \prec x_1x_3^2 \prec \ldots,$$

with respect to deglex:

$$1 \prec x_3 \prec x_2 \prec x_1 \prec x_3^2 \prec x_2x_3 \prec x_2^2 \prec x_1x_3 \prec x_1x_2 \prec x_1^2 \prec x_3^3 \prec \ldots$$

and here is a different degree compatible one (it is called degrevlex):

$$1 \prec x_3 \prec x_2 \prec x_1 \prec x_3^2 \prec x_2x_3 \prec x_1x_3 \prec x_2^2 \prec x_1x_2 \prec x_1^2 \prec x_3^3 \prec \ldots$$

We prove two fundamental properties of term orders. The one which claims that $\prec$ is a well founded order is known as Dickson's Lemma.

Proposition 2.1.4. *Any term order $\prec$ is a refinement of division of monomials (that is if $\mathbf{x^w} \mid \mathbf{x^u}$, then $\mathbf{x^w} \preceq \mathbf{x^u}$) and is a well founded order.*

Proof. For the first statement, assume that $\mathbf{x^w} \mid \mathbf{x^u}$. Then $\frac{\mathbf{x^u}}{\mathbf{x^w}}$ is also a monomial, therefore $1 \preceq \frac{\mathbf{x^u}}{\mathbf{x^w}}$ holds. If we multiply this inequality with $\mathbf{x^w}$, we immediately get the desired result.

Suppose now for contradiction that $\prec$ is not well founded, thus there exists an infinite chain of monomials

$$\mathbf{x^{w_1}} \succ \mathbf{x^{w_2}} \succ \mathbf{x^{w_3}} \succ \cdots \succ \mathbf{x^{w_i}} \succ \mathbf{x^{w_{i+1}}} \succ \ldots$$

Consider the ascending chain of semigroup ideals

$$\langle \mathbf{x^{w_1}} \rangle \subseteq \langle \mathbf{x^{w_1}}, \mathbf{x^{w_2}} \rangle \subseteq \langle \mathbf{x^{w_1}}, \mathbf{x^{w_2}}, \mathbf{x^{w_3}} \rangle \subseteq \ldots$$

which cannot be infinite, as the semigroup of monomials is Noetherian. In particular there exists an i, such that $\mathbf{x^{w_{i+1}}} \in \langle \mathbf{x^{w_1}}, \ldots, \mathbf{x^{w_i}} \rangle$. But then $\mathbf{x^{w_j}}$ divides $\mathbf{x^{w_{i+1}}}$ for some $j \leq i$, and so $\mathbf{x^{w_j}} \preceq \mathbf{x^{w_{i+1}}}$ by the first statement of the Proposition. This contradicts to $\mathbf{x^{w_j}} \succ \mathbf{x^{w_{i+1}}}$. □

2.1.2 Standard and leading monomials

Let us fix a term order $\prec$.

Definition 2.1.5. The *leading term* (or *monomial*) $\mathrm{lm}(f)$ of a nonzero polynomial $f \in \mathbb{F}[\mathbf{x}]$ is the largest monomial (with respect to $\prec$) which appears in f.

We denote the set of all leading monomials of polynomials of a given ideal $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ by $\mathrm{Lm}(I) = \{\mathrm{lm}(f) : f \in I\}$, and we simply call them the *leading monomials of I*.

As every term order is compatible with multiplication, it is easy to verify that the leading monomial of a product $f \cdot g$ of two nonzero polynomials is $\mathrm{lm}\,(f) \cdot \mathrm{lm}\,(g)$. It follows that $\mathrm{Lm}\,(I)$ is a semigroup ideal in the semigroup of monomials, or in other words a monomial divisible with a leading monomial is again in $\mathrm{Lm}\,(I)$.

Definition 2.1.6. A monomial is called a *standard monomial* of I, if it is not a leading monomial of any $f \in I$. Let $\mathrm{Sm}\,(I)$ denote the set of standard monomials of I.

Being the complement of a semigroup ideal, $\mathrm{Sm}\,(I)$ is a *dual ideal*, which in our case means that any divisor of a standard monomial is also a standard monomial.

If we use more orderings in parallel, or want to emphasise the dependence of these concepts from the term order, we may write for instance $\mathrm{Sm}_{\prec}\,(I)$, $\mathrm{Lm}_{\mathrm{lex}}\,(I)$, etc.

We shall occasionally use the notation $\mathrm{Sm}\,(F)$ and $\mathrm{Lm}\,(F)$ for arbitrary sets $F \subseteq \mathbb{F}\,[\mathbf{x}]$ of polynomials instead of ideals.

Definition 2.1.7.

$$\begin{aligned}\mathrm{Lm}\,(F) &= \{\mathbf{x}^{\mathbf{w}} \;:\; \exists\, f \in F \;\mathrm{lm}\,(f) \mid \mathbf{x}^{\mathbf{w}}\}\,,\\ \mathrm{Sm}\,(F) &= \{\mathbf{x}^{\mathbf{w}} \in \mathbb{F}\,[\mathbf{x}]\} \setminus \mathrm{Lm}\,(F)\,.\end{aligned}$$

Thus $\mathrm{Lm}\,(F)$ is the semigroup ideal generated by the leading monomials of elements of F. Of course, if F is a polynomial ideal, then the earlier definition formulated only for ideals coincide with this more general one.

It is important to note that in general $\mathrm{Lm}\,(F) \neq \mathrm{Lm}\,(\langle F \rangle)$. We shall shortly find that $\mathrm{Lm}\,(F) = \mathrm{Lm}\,(\langle F \rangle)$ is one of the properties which characterize Gröbner bases (provided that F is finite).

To simplify arguments (like the proof of Proposition 2.1.4), we will extend the term orderings from monomials to nonzero polynomials. By $f \prec g$, we mean $\mathrm{lm}\,(f) \prec \mathrm{lm}\,(g)$.

2.1.3 The existence of Gröbner bases

Definition 2.1.8. A finite subset $G \subseteq I$ is a *Gröbner basis* of I, if for every nonzero $f \in I$ there exists a $g \in G$, such that $\mathrm{lm}\,(g)$ divides $\mathrm{lm}\,(f)$. In other words, a Gröbner basis of I is a finite set $G \subseteq I$, with $\mathrm{Lm}\,(I) = \mathrm{Lm}\,(G)$, or equivalently $\mathrm{Sm}\,(I) = \mathrm{Sm}\,(G)$.

Note that being a Gröbner basis depends on the underlying term order.

It is not transparent from the above definition, but we shall prove that a Gröbner basis of I in fact generates I.

Example 2.1.9. Suppose that the characteristic of $\mathbb{F}$ is not 2. Then a Gröbner basis of the ideal $I = \langle x_1 - x_2, x_1 + x_2 \rangle$ is $G = \{x_1, x_2\}$ (with respect to any term order in this case). It is easy to see that $G \subseteq I$ (and therefore $\operatorname{Lm}(G) \subseteq \operatorname{Lm}(I)$), and also that $\operatorname{Lm}(I) \subseteq \operatorname{Lm}(G)$. But the set $G' = \{x_1 - x_2, x_1 + x_2\}$ is not a Gröbner basis of I, since if for example $x_2 \prec x_1$, then $x_2 \in I$ is not divisible by the leading monomial of any element in G'. We can also write $\operatorname{Sm}(G) = \{1\}$ and $\operatorname{Sm}(G') = \{1, x_2\}$ (if $x_2 \prec x_1$).

Theorem 2.1.10. *Every ideal I has a Gröbner basis.*

Proof. Since $\operatorname{Lm}(I)$ is a semigroup ideal in a Noetherian semigroup, there exists a finite set H of monomials, which (in the semigroup sense) generates $\operatorname{Lm}(I)$. Then by the definition $\operatorname{Lm}(H) = \operatorname{Lm}(I)$. For all monomials $\mathbf{x}^{\mathbf{w}} \in H$, let $g_{\mathbf{w}}$ be a polynomial in I, such that $\operatorname{lm}(g_{\mathbf{w}}) = \mathbf{x}^{\mathbf{w}}$. (Such a polynomial exists by $\mathbf{x}^{\mathbf{w}} \in \operatorname{Lm}(I)$.) It is clear that $G = \{g_{\mathbf{w}} : \mathbf{x}^{\mathbf{w}} \in H\}$ is a Gröbner basis of I. □

2.1.4 Reduction

The most important property of the Gröbner bases is that they generate the corresponding ideals in a nice way. We will now examine this.

The *leading coefficient* of a polynomial is the coefficient of its leading term. Suppose that $f \in \mathbb{F}[\mathbf{x}]$ contains a monomial $\mathbf{x}^{\mathbf{w}} \cdot \operatorname{lm}(g)$, where g is some other polynomial with leading coefficient c. Then we can *reduce f with g*, that is, we can replace $\mathbf{x}^{\mathbf{w}} \cdot \operatorname{lm}(g)$ in f with $\mathbf{x}^{\mathbf{w}} \cdot \left(\operatorname{lm}(g) - \frac{1}{c} g\right)$. In other words, we subtract $\frac{c_f \mathbf{x}^{\mathbf{w}}}{c} \cdot g$ from f, where c_f is the coefficient of the monomial $\mathbf{x}^{\mathbf{w}} \cdot \operatorname{lm}(g)$ in f. We will refer to this as a *reduction step.* For example, if $f = x_1^3 x_2 + x_3$, and $g = x_1^2 - x_1$, then the result of the reduction step will be $x_1^2 x_2 + x_3$.

Definition 2.1.11. We say that a polynomial f is *reduced* with respect to a finite set of polynomials G, if none of the monomials of f is divisible by $\operatorname{lm}(g)$ for any $g \in G$. This is exactly the case when no reduction steps on f can be carried out with any element of G.

Note that $\operatorname{lm}\left(\mathbf{x}^{\mathbf{w}} \cdot \left(\operatorname{lm}(g) - \frac{1}{c} g\right)\right) \prec \mathbf{x}^{\mathbf{w}} \cdot \operatorname{lm}(g)$. As $\prec$ is a well founded order, this guarantees that if we reduce f repeatedly using a finite set of polynomials G, then we end up with a reduced $\hat{f}$ in finitely many steps.

Moreover, we get a decomposition

$$f(\mathbf{x}) = \sum_{i=1}^{m} g_i(\mathbf{x})h_i(\mathbf{x}) + \hat{f}(\mathbf{x}) \tag{2.1}$$

of f, where $G = \{g_1, \ldots, g_m\}$, $h_1, \ldots, h_m \in \mathbb{F}[\mathbf{x}]$, $\hat{f}$ is reduced with respect to G, and $\operatorname{lm}(g_i h_i) \preceq \operatorname{lm}(f)$ holds.

Definition 2.1.12. A polynomial f *can be reduced to* $\hat{f}$, if there exists a decomposition of the form (2.1). We emphasise that it is not required that the decomposition is a result of reduction steps.

Example 2.1.13. Let $g_1(x_1, x_2) = x_1x_2 + x_1$, $g_2(x_1, x_2) = x_1x_2 + x_2$ be polynomials, $G = \{g_1, g_2\}$ and $f(x_1, x_2) = 2x_1x_2 + x_1 + x_2$. If we reduce f first with g_1, then we get $x_2 - x_1$, and when reducing f with g_2, then the result is $x_1 - x_2$. That is, f can be reduced to both polynomials. And also $f = g_1 + g_2$, thus f can be reduced to 0 as well, although 0 cannot be a result of subsequent reduction steps.

We shall see that this happens because G is not a Gröbner basis of the ideal $\langle G \rangle$. We are going to prove that the reduction of any polynomial with respect to a Gröbner basis is unique, and therefore can be obtained using reduction steps.

Here is our first theorem which can be proven with the aid of Gröbner bases.

Theorem 2.1.14. *If I is an ideal of $\mathbb{F}[\mathbf{x}]$, then the cosets of the elements of* $\operatorname{Sm}(I)$ *in the factor space $\mathbb{F}[\mathbf{x}]/I$ form a linear basis of the $\mathbb{F}$-vector space $\mathbb{F}[\mathbf{x}]/I$. It follows that*

$$\dim_{\mathbb{F}}(\mathbb{F}[\mathbf{x}]/I) = |\operatorname{Sm}(I)|,$$

in particular I is a zero dimensional ideal if and only if $|\operatorname{Sm}(I)| < \infty$.

Proof. The cosets of elements of $\operatorname{Sm}(I)$ are linearly independent in $\mathbb{F}[\mathbf{x}]/I$, since if

$$\sum_{i=1}^{m} a_i \left(\mathbf{x}^{\mathbf{w_i}} + I\right) = 0,$$

then

$$f(\mathbf{x}) = \sum_{i=1}^{m} a_i \mathbf{x}^{\mathbf{w_i}} \in I.$$

If $f \neq 0$, then $\mathrm{lm}(f) \in \mathrm{Lm}(I)$ which contradicts the fact that f is a linear combination of standard monomials.

We want to show that $\mathrm{Sm}(I)$ generates $\mathbb{F}[\mathbf{x}]$ modulo I. Let $f \in \mathbb{F}[\mathbf{x}]$ be a polynomial, G an arbitrary Gröbner basis of I, and $\hat{f}$ a reduction of f with respect to G. Then as $\sum_{i=1}^{m} g_i(\mathbf{x})h_i(\mathbf{x}) \in I$, f and $\hat{f}$ represent the same coset in $\mathbb{F}[\mathbf{x}]/I$. Since $\hat{f}$ is reduced with respect to G, its monomials cannot be in $\mathrm{Lm}(G) = \mathrm{Lm}(I)$, that is $\hat{f}$ is a linear combination of standard monomials of I. But this means that modulo I, f is also a linear combination of elements of $\mathrm{Sm}(I)$. □

Proposition 2.1.15. *If G is a Gröbner basis of the ideal I, then for every polynomial $f \in \mathbb{F}[\mathbf{x}]$, there exists a unique polynomial $\hat{f}$, such that f can be reduced to $\hat{f}$ with G, and $f \in I$ if and only if $\hat{f} = 0$. In particular $\langle G \rangle = I$.*

Proof. If f can be reduced to both $\hat{f}_1$ and $\hat{f}_2$ with G, then $\hat{f}_1 - \hat{f}_2 \in I$, while $\hat{f}_1 - \hat{f}_2$ is a linear combination of standard monomials, thus $\hat{f}_1 - \hat{f}_2 = 0$.

It is clear that f and $\hat{f}$ are the same modulo I, if f can be reduced to $\hat{f}$. But when $\hat{f}$ is reduced with respect to a Gröbner basis of I, then it is a linear combination of standard monomials of I, and so $\hat{f} \in I$ if and only if $\hat{f} = 0$. □

The previous statement explains the power of Gröbner bases. We say that a finite set of polynomials G is a *Gröbner basis* if it is a Gröbner basis of $\langle G \rangle$. Reduction steps can be used to calculate the reduction of a polynomial with respect to a Gröbner basis G, taking elements of G in an arbitrary order. This means for example that given a Gröbner basis of I, it can be decided easily whether a polynomial is in I. In general, a polynomial f represents the same coset in $\mathbb{F}[\mathbf{x}]/I$ as $\hat{f}$, and a system of representatives of the cosets of I are the linear combinations of standard monomials.

It worth noting that these properties actually characterize Gröbner bases. We thus have the following equivalent definitions of Gröbner bases.

Theorem 2.1.16. *The following are equivalent for a finite subset G of an ideal $I \trianglelefteq \mathbb{F}[\mathbf{x}]$.*

1. *For all $f \in I \setminus \{0\}$, there exists a $g \in G$, such that* $\mathrm{lm}(g) \mid \mathrm{lm}(f)$.
2. $\mathrm{Sm}(G) = \mathrm{Sm}(I)$
3. *Every $f \in I$ can be reduced to 0 with G.*
4. *$\langle G \rangle = I$ and the reduction of every $f \in \mathbb{F}[\mathbf{x}]$ with G is unique.*

In these cases G is a Gröbner basis of I. □

To complete the proof, one needs to show that claim 3 (or 4) implies claim 1 (or 2). The proof is not too complicated (see [1] for instance), but as we shall not use these facts later, we omit it here.

2.1.5 The reduced Gröbner basis

Gröbner bases of an ideal are not unique, for example if G is a Gröbner basis of I, then we get a different Gröbner basis by adding arbitrary, but finitely many polynomials from I to G. However there exist some reasonable conditions to make it unique.

Definition 2.1.17. If the leading coefficient of every polynomial g in a Gröbner basis G of I is 1, and g is reduced with respect to $G \setminus \{g\}$, then G is a *reduced Gröbner basis* of I.

In other words, a Gröbner basis G is reduced if and only if the leading coefficients are 1, and for all $g \in G$, the polynomial $g - \mathrm{lm}\,(g)$ is a linear combination of standard monomials (of G).

Theorem 2.1.18. *There exists a unique reduced Gröbner basis for every ideal.*

Proof. To show the existence, let G be any Gröbner basis of I, such that the leading coefficient of all $g \in G$ is 1. Let us modify G as follows. We throw away those polynomials $g \in G$ (working with them in a fixed order), for which $\mathrm{lm}\,(g)$ is divisible by the leading monomial of some other, previously not dropped polynomial. The set of polynomials G_1 obtained this way is still a Gröbner basis, as for all minimal elements $\mathbf{x}^{\mathbf{w}}$ of $\mathrm{Lm}\,(I)$ with respect to division, we kept exactly one $g \in G$, such that $\mathrm{lm}\,(g) = \mathbf{x}^{\mathbf{w}}$.

If $g \in G_1$, then put $\hat{g}$ for the reduction of $g - \mathrm{lm}\,(g)$ with G_1, and

$$G_2 = \{\mathrm{lm}\,(g) + \hat{g} \ : \ g \in G_1\}\,.$$

Then G_2 is again a Gröbner basis, since the leading monomials of elements of G_1 and of G_2 are the same, and $\mathrm{lm}\,(g) + \hat{g}$ equals to g modulo I, in particular $\mathrm{lm}\,(g) + \hat{g} \in I$. It is also clear that G_2 is reduced.

Suppose for the proof of uniqueness that both G and H are reduced Gröbner bases of I. Since the leading monomials can not divide each other in a reduced Gröbner basis, we get that $\{\mathrm{lm}\,(g) \ : \ g \in G\}$ (just like $\{\mathrm{lm}\,(h) \ : \ h \in H\}$) is the set of minimal elements (with respect to division) of $\mathrm{Lm}\,(I)$. Let $g \in G$ and $h \in H$, such that $\mathrm{lm}\,(g) = \mathrm{lm}\,(h)$. Then $g - h$ is a linear combination of standard monomials and $g - h \in I$, hence $g - h = 0$. We conclude that $G = H$. □

The set of leading monomials of the reduced Gröbner basis of I is called the minimal generators of $\mathrm{Lm}\,(I)$, since, as we have seen in the previous proof, these are exactly the minimal elements of $\mathrm{Lm}\,(I)$ with respect to division.

2.1.6 The Hilbert function

Finally, we write about the Hilbert function, an algebraic concept, which is related to Gröbner basis theory, and appears quite often in algebraic and combinatorial applications.

We write $\mathbb{F}\left[\mathbf{x}\right]_{\le m}$ for the vector space of polynomials over $\mathbb{F}$ with degree at most m. Similarly, if $I \trianglelefteq \mathbb{F}\left[\mathbf{x}\right]$ is an ideal then $I_{\le m} = I \cap \mathbb{F}\left[\mathbf{x}\right]_{\le m}$ stands for the linear subspace of polynomials in I with degree at most m.

Definition 2.1.19. The *Hilbert function* of the $\mathbb{F}$-algebra $\mathbb{F}\left[\mathbf{x}\right]/I$ is $H_I : \mathbb{N} \to \mathbb{N}$, where

$$H_I(m) = \dim_{\mathbb{F}}\left(\mathbb{F}\left[\mathbf{x}\right]_{\le m}/I_{\le m}\right).$$

The next proposition is a slight generalization of Theorem 2.1.14.

Proposition 2.1.20. *Let $\prec$ be a degree compatible ordering. The cosets of standard monomials of degree at most m form a linear basis of $\mathbb{F}\left[\mathbf{x}\right]_{\le m}/I_{\le m}$.*

Proof. As the standard monomials are linearly independent modulo I, and $I_{\le m} \subseteq I$, we have that they are linearly independent modulo $I_{\le m}$ as well. We shall show that they generate the linear space of polynomials of degree at most m modulo $I_{\le m}$.

Let $f \in \mathbb{F}\left[\mathbf{x}\right]_{\le m}$ and let $\hat{f}$ be the reduction of f with some Gröbner basis of I. Note that when reducing f, we can only use polynomials of degree at most m, since by the degree compatibility, the leading monomial of a polynomial of degree greater than m would be greater with respect to $\prec$ than any monomial of f. Therefore both $\hat{f}$ and $f - \hat{f}$ is of degree at most m. In particular $f - \hat{f} \in I_{\le m}$, so it is enough to generate $\hat{f}$ by standard monomials of degree at most m. As $\hat{f}$ is reduced, it is a linear combination of standard monomials, which by the bound on the degree of $\hat{f}$ have degree at most m. □

An immediate consequence is the following.

Corollary 2.1.21. *If $\prec$ is a degree compatible order, then $H_I(m)$ is the number of standard monomials of I of degree at most m.*

2.2 Zero dimensional ideals

Let V be a finite set of points $V \subseteq \mathbb{F}^n$. The *vanishing ideal* of V is the set of all polynomials from $\mathbb{F}[\mathbf{x}]$, which, as functions $\mathbb{F}^n \to \mathbb{F}$ vanish on V. That is

$$I(V) = \{f \in \mathbb{F}[\mathbf{x}] \,:\, f(\mathbf{y}) = 0 \text{ for all } \mathbf{y} \in \mathbb{F}^n\}.$$

To go further, we want to work with ideals of polynomials, which also have prescribed multiplicities at given points. We shall give the precise definition of multiplicity in Subsection 2.2.1, and also define the notion of a finite algebraic multiset, which encodes a finite set and multiplicities in each of its points.

We shall examine lexicographic standard monomials of zero dimensional ideals in Chapter 4. As a preparation, we investigate in the primary decomposition of zero dimensional ideals in this section, in particular give a characterization of vanishing ideals of finite algebraic multisets in terms of primary decomposition.

Although results of this section are derived by simple arguments from well-known facts, some of them may not be found in the literature.

Note that the factor space $\mathbb{F}[\mathbf{x}]/I(V)$ is isomorphic to the space of functions $V \to \mathbb{F}$, where the isomorphism maps a coset $f(\mathbf{x}) + I(V)$ to the function $\mathbf{v} \mapsto f(\mathbf{v})$, where $\mathbf{v} \in V$. To see this, one should check that by the finiteness of V, every function $V \to \mathbb{F}$ can be represented by a polynomial in $\mathbb{F}[\mathbf{x}]$. From this, and from Theorem 2.1.14, it follows that $|\mathrm{Sm}(I(V))| = |V|$, which is a special case of the upcoming Corollary 2.2.13.

2.2.1 Algebraic multisets

We say that $M \subseteq \mathbb{N}^n$ is a *downset* if $\mathbf{m} \in M$, $\mathbf{r} \in \mathbb{N}^n$ and $\forall\, i\ r_i \leq m_i$ implies $\mathbf{r} \in M$. Let $\mathbf{y} \in \mathbb{F}^n$ be a point, $M \subseteq \mathbb{N}^n$ a downset and $f \in \mathbb{F}[\mathbf{x}]$ a polynomial. Write f as a polynomial of the variables $\mathbf{x} - \mathbf{y} = (x_1 - y_1, \ldots, x_n - y_n)$ and let $c_{\mathbf{w}} \in \mathbb{F}$ be the coefficient of $(\mathbf{x} - \mathbf{y})^{\mathbf{w}}$, that is

$$f(\mathbf{x}) = \sum_{\mathbf{w} \in \mathbb{N}^n} c_{\mathbf{w}} (\mathbf{x} - \mathbf{y})^{\mathbf{w}}. \tag{2.2}$$

Definition 2.2.1. For a finite downset $M \subseteq \mathbb{N}^n$, we say that f *has multiplicity M in* $\mathbf{y}$, if $c_{\mathbf{w}} = 0$ whenever $\mathbf{w} \in M$.

This definition of multiplicity is slightly different from what is usual in the literature, but for us it shall be more convenient. Note that f has also multiplicity M' in $\mathbf{y}$ for each downset $M' \subseteq M$. In particular, every polynomial f has multiplicity $M = \emptyset$ at every point $\mathbf{y}$, while if f has multiplicity $M \neq \emptyset$ at $\mathbf{y}$, then $\mathbf{0} \in M$, and hence f vanishes at $\mathbf{y}$.

To work with this notion, we need to get the coefficients $c_{\mathbf{w}}$ in (2.2) easily. For this purpose, consider the linear map $P_{\mathbf{w}} \colon \mathbb{F}[\mathbf{x}] \to \mathbb{F}[\mathbf{x}]$, $P_{\mathbf{w}} \colon \mathbf{x}^{\mathbf{u}} \mapsto \binom{\mathbf{u}}{\mathbf{w}}\mathbf{x}^{\mathbf{u}-\mathbf{w}}$, where $\binom{\mathbf{u}}{\mathbf{w}} = \binom{u_1}{w_1} \dots \binom{u_n}{w_n}$. Note that in characteristic 0 we have $P_{\mathbf{w}} = \frac{1}{\mathbf{w}!} \cdot \frac{\partial^{\mathbf{w}}}{\partial \mathbf{x}^{\mathbf{w}}}$, where $\mathbf{w}! = w_1! \dots w_n!$. By slight abuse of notation, instead of $P_{\mathbf{w}}$ we shall use the latter—even if the characteristic is not zero and $\mathbf{w}! = 0$ in $\mathbb{F}$. Properties of $P_{\mathbf{w}}$ that are well known for differential operators (like the Leibniz rule) will be clearer this way.

From the Taylor series of f, we have that the value of the polynomial

$$\frac{1}{\mathbf{w}!} \cdot \frac{\partial^{\mathbf{w}}}{\partial \mathbf{x}^{\mathbf{w}}} f(\mathbf{x}) = \frac{1}{w_1! \dots w_n!} \cdot \frac{\partial^{w_1 + \dots + w_n}}{\partial x_1^{w_1} \dots \partial x_n^{w_n}} f(x_1, \dots, x_n)$$

in $\mathbf{y}$ is $c_{\mathbf{w}}$. We shall write $\frac{1}{\mathbf{w}!} \cdot \frac{\partial^{\mathbf{w}}}{\partial \mathbf{x}^{\mathbf{w}}} f(\mathbf{y})$ instead of the complicated expression $\frac{1}{\mathbf{w}!} \cdot \frac{\partial^{\mathbf{w}}}{\partial \mathbf{x}^{\mathbf{w}}} f(\mathbf{x})$ *taken in* $\mathbf{y}$.

Definition 2.2.2. A (finite) *algebraic multiset* is a function $\mathcal{V} \colon \mathbb{F}^n \to 2^{\mathbb{N}^n}$, such that $\mathcal{V}(\mathbf{y}) = \emptyset$ with only finitely many exceptions $\mathbf{y} \in \mathbb{F}^n$, and for all $\mathbf{y} \in \mathbb{F}^n$, the image $\mathcal{V}(\mathbf{y}) \subseteq \mathbb{N}^n$ is a finite downset. The set $V = \{\mathbf{y} : \mathcal{V}(\mathbf{y}) \neq \emptyset\}$ contains the *points of* $\mathcal{V}$.

Any $V \subseteq \mathbb{F}^n$ is also an algebraic multiset by setting $\mathcal{V}(\mathbf{y}) = \{\mathbf{0}\}$ if $\mathbf{y} \in V$ and $\mathcal{V}(\mathbf{y}) = \emptyset$ otherwise.

Definition 2.2.3. The *vanishing ideal of* $\mathcal{V}$ is

$$I(\mathcal{V}) = \{f \in \mathbb{F}[\mathbf{x}] \,:\, f \text{ has multiplicity } \mathcal{V}(\mathbf{y}) \text{ in } \mathbf{y} \text{ for all } \mathbf{y} \in \mathbb{F}^n\}.$$

If V is the set of points of some $\mathcal{V}$, then $I(\mathcal{V}) \subseteq I(V)$. Algebraic multisets appear naturally in interpolation problems involving constraints on higher derivatives.

2.2.2 Primary decomposition

By the Noether–Lasker theorem ([6] Chapter 4) every ideal $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ is a finite intersection of primary ideals, each corresponding to a different prime ideal. For zero dimensional ideals we can be more specific:

Proposition 2.2.4. *Let $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ be a zero dimensional ideal. Then there are uniquely determined primary ideals Q_j $(j = 1, \dots, k)$ such that $I = \prod_{j=1}^{k} Q_j$ and the radicals $\sqrt{Q_j} = M_j$ are pairwise different maximal ideals. The M_j are exactly those maximal ideals which contain I.*

Proof. The Noether–Lasker theorem gives that there exist primary ideals Q_j such that the $\sqrt{Q_j}$ are all different and $I = \bigcap_{j=1}^{k} Q_j$. As $I \subseteq Q_j \subseteq \sqrt{Q_j} = M_j$, the M_j have dimension zero as well, but a zero dimensional prime ideal is maximal. Now the second uniqueness theorem of primary decomposition gives immediately the uniqueness of the decomposition.

Since the M_j are pairwise different, the Q_j are relatively prime, so we have $\bigcap_{j=1}^{k} Q_j = \prod_{j=1}^{k} Q_j$.

Finally if $M \supseteq I$ is any maximal ideal then $M \supseteq \sqrt{I} = \bigcap_{j=1}^{k} \sqrt{Q_j} = \prod_{j=1}^{k} M_j$. As M is prime, there exists an $M_j \subseteq M$, but then $M_j = M$ by the maximality of M_j. □

Definition 2.2.5. We say that an ideal $Q \trianglelefteq \mathbb{F}[\mathbf{x}]$ corresponds to a point $\mathbf{y} \in \mathbb{F}^n$ if $\sqrt{Q} = \langle x_1 - y_1, \ldots, x_n - y_n \rangle$. Let I be a zero dimensional ideal with primary decomposition $I = \prod_{j=1}^{k} Q_j$. If every Q_j corresponds to some point $\mathbf{y_j}$, then we say that I is a *splitting ideal.*

For example the ideal $\langle x^2 + 1 \rangle$ in $\mathbb{Q}[x]$ is not a splitting ideal, although it is of dimension zero. Note that $\langle x^2 + 1 \rangle \trianglelefteq \mathbb{Q}(i)[x]$ is a splitting ideal (where $i^2 = -1$).

From now on, we will only work with splitting ideals. As we are mainly interested in the standard monomials of I, this is not a serious restriction. Indeed, if I is an arbitrary zero dimensional ideal, then we can pass to the algebraic closure $\overline{\mathbb{F}}$ and change I to $I_{\overline{\mathbb{F}}} = I \cdot \overline{\mathbb{F}}[\mathbf{x}]$. It is not hard to see that the standard monomials of $I_{\overline{\mathbb{F}}}$ and I are the same. Moreover, for every primary component Q of $I_{\overline{\mathbb{F}}}$, the radical $\sqrt{Q}$ is maximal, hence by Hilbert's Nullstellensatz it is of the form $\langle x_1 - y_1, \ldots, x_n - y_n \rangle$ for some $\mathbf{y} \in \overline{\mathbb{F}}^n$. In fact, for a fixed I it suffices to pass to a finite extension $\mathbb{F}'$ of $\mathbb{F}$ instead of the algebraic closure.

We shall simply write

$$I = \prod_{\mathbf{y} \in \mathbb{F}^n} Q_{\mathbf{y}} \tag{2.3}$$

as the primary decomposition of I, keeping in mind that if $Q_{\mathbf{y}} \neq \mathbb{F}[\mathbf{x}]$, then $Q_{\mathbf{y}}$ is $\langle x_1 - y_1, \ldots, x_n - y_n \rangle$-primary, but of course $Q_{\mathbf{y}} = \mathbb{F}[\mathbf{x}]$ with only finitely many exceptions.

Definition 2.2.6. We call $\mathbf{y} \in \mathbb{F}^n$ *a point of* I (or *a point associated to* I) if $Q_{\mathbf{y}} \neq \mathbb{F}[\mathbf{x}]$ in the primary decomposition of I.

Definition 2.2.7. Let $Q \trianglelefteq \mathbb{F}[\mathbf{x}]$ be an ideal and $\mathbf{y} \in \mathbb{F}^n$ be a point. We say that Q is $\mathbf{y}$-*monomial* if it can be generated by some polynomials of the form $(\mathbf{x}-\mathbf{y})^{\mathbf{w}}$. A $\mathbf{0}$-monomial ideal is a monomial ideal in the usual sense.

The next theorem claims that finite multiset ideals are exactly the zero dimensional ideals which locally look like monomial ideals.

Theorem 2.2.8. *Suppose that*

$$I = \prod_{\mathbf{y}\in\mathbb{F}^n} Q_{\mathbf{y}}$$

is the primary decomposition of a zero dimensional splitting ideal. Then there exists a finite multiset $\mathcal{V}$, such that $I = I(\mathcal{V})$ if and only if $Q_{\mathbf{y}}$ is $\mathbf{y}$-monomial for all $\mathbf{y}$ associated to I. In this case

$$\mathbf{w} \in \mathcal{V}(\mathbf{y}) \iff (\mathbf{x}-\mathbf{y})^{\mathbf{w}} \notin Q_{\mathbf{y}}.$$

Proof. Assume first that $I = I(\mathcal{V})$. Then we decompose $\mathcal{V}$ to the finite 'union' of its points. That is, let $\mathcal{V}^{\mathbf{y}}$ be the multiset which is $\emptyset$ on $\mathbb{F}^n \setminus \{\mathbf{y}\}$, and $\mathcal{V}^{\mathbf{y}}(\mathbf{y}) = \mathcal{V}(\mathbf{y})$. Then $I(\mathcal{V}) = \bigcap_{\mathbf{y}\in\mathbb{F}^n} I(\mathcal{V}^{\mathbf{y}})$. If $\mathbf{y}$ is a point of $\mathcal{V}$, then the radical $\sqrt{I(\mathcal{V}^{\mathbf{y}})} = \langle x_1 - y_1, \dots, x_n - y_n\rangle$ is a maximal ideal so the $I(\mathcal{V}^{\mathbf{y}})$ are relatively prime primary ideals thus $I(\mathcal{V}) = \prod_{\mathbf{y}\in\mathbb{F}^n} I(\mathcal{V}^{\mathbf{y}})$ is the primary decomposition of I. Uniqueness of primary decomposition implies that $Q_{\mathbf{y}}$ has to be equal to $I(\mathcal{V}^{\mathbf{y}})$.

It remains to verify that $I(\mathcal{V}^{\mathbf{y}})$ is $\mathbf{y}$-monomial. Suppose that $f(\mathbf{x}) = \sum_{\mathbf{w}\in\mathbb{N}^n} c_{\mathbf{w}}(\mathbf{x}-\mathbf{y})^{\mathbf{w}}$ is in $I(\mathcal{V}^{\mathbf{y}})$. If $c_{\mathbf{w}} \neq 0$ then $\mathbf{w} \notin \mathcal{V}^{\mathbf{y}}(\mathbf{y})$ and so $(\mathbf{x}-\mathbf{y})^{\mathbf{w}}$ is also in $I(\mathcal{V}^{\mathbf{y}})$, which proves the first part.

Conversely, suppose that all $Q_{\mathbf{y}}$ are $\mathbf{y}$-monomial. Define $\mathcal{V}$ by

$$\mathcal{V}(\mathbf{y}) = \{\mathbf{w} \,:\, (\mathbf{x}-\mathbf{y})^{\mathbf{w}} \notin Q_{\mathbf{y}}\} \tag{2.4}$$

for all points $\mathbf{y}$ of I. Using the above defined decomposition of $\mathcal{V}$ to multisets $\mathcal{V}^{\mathbf{y}}$, we obtain $(\mathbf{x}-\mathbf{y})^{\mathbf{w}} \in I(\mathcal{V}^{\mathbf{y}}) \iff \mathbf{w} \notin \mathcal{V}^{\mathbf{y}}(\mathbf{y}) \iff \mathbf{w} \notin \mathcal{V}(\mathbf{y}) \iff (\mathbf{x}-\mathbf{y})^{\mathbf{w}} \in Q_{\mathbf{y}}$. As $Q_{\mathbf{y}}$ is $\mathbf{y}$-monomial this yields $I(\mathcal{V}^{\mathbf{y}}) = Q_{\mathbf{y}}$, thus

$$I = \bigcap_{\mathbf{y}\in\mathbb{F}^n} Q_{\mathbf{y}} = \bigcap_{\mathbf{y}\in\mathbb{F}^n} I(\mathcal{V}^{\mathbf{y}}) = I(\mathcal{V}).$$

The equivalence is proved.

To show that the only right choice for $\mathcal{V}$ is the one given by (2.4), note that it follows from the first part of the proof that $I(\mathcal{V}) = I(\mathcal{V}')$ implies $\mathcal{V} = \mathcal{V}'$. □

Corollary 2.2.9. *Let $Q_{\mathbf{y}}$ be a $\mathbf{y}$-monomial primary component of $I(\mathcal{V})$. Then*

$$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(Q_{\mathbf{y}}) \iff \mathbf{w} \in \mathcal{V}(\mathbf{y}).$$

In particular $|\mathrm{Sm}\,(Q_{\mathbf{y}})| = |\mathcal{V}(\mathbf{y})|$.

Proof. The monomial $\mathbf{x}^{\mathbf{w}}$ is in $\mathrm{Lm}\,(Q_{\mathbf{y}})$ if and only if there exists an $f(\mathbf{x}) \in Q_{\mathbf{y}}$ with $\mathrm{lm}\,(f) = \mathbf{x}^{\mathbf{w}}$. Writing f as a polynomial in the variables $x_i - y_i$, we have that the coefficient of $(\mathbf{x}-\mathbf{y})^{\mathbf{w}}$ is not zero, and as $Q_{\mathbf{y}}$ is $\mathbf{y}$-monomial, $(\mathbf{x}-\mathbf{y})^{\mathbf{w}}$ itself is in $Q_{\mathbf{y}}$ (see Proposition 2.1.1). But $(\mathbf{x}-\mathbf{y})^{\mathbf{w}} \in Q_{\mathbf{y}}$ is equivalent to $\mathbf{w} \notin \mathcal{V}(\mathbf{y})$ by the last statement of Theorem 2.2.8. □

Example 2.2.10. The primary decomposition of the vanishing ideal $I(V)$ of a finite set $V \subseteq \mathbb{F}^n$ has the additional property that all primary components are maximal, that is $Q_{\mathbf{y}} = \langle x_1 - y_1, \ldots, x_n - y_n \rangle$.

Suppose now that $\mathcal{V}$ is such that for all $\mathbf{y}$ there exists some $m_{\mathbf{y}} \in \mathbb{N}$ with $\mathcal{V}(\mathbf{y}) = \{\mathbf{m} \in \mathbb{N}^n : \sum_{i=1}^{n} m_i < m_{\mathbf{y}}\}$. Then $I(\mathcal{V})$ contains those polynomials which have a root in $\mathbf{y}$ of multiplicity (in the usual sense) $m_{\mathbf{y}}$, and $Q_{\mathbf{y}} = \langle x_1 - y_1, \ldots, x_n - y_n \rangle^{m_{\mathbf{y}}}$ in the primary decomposition of $I(\mathcal{V})$.

Definition 2.2.11. The cardinality of a finite multiset $\mathcal{V}$ is

$$|\mathcal{V}| = \sum_{\mathbf{y} \in \mathbb{F}^n} |\mathcal{V}(\mathbf{y})|\,.$$

Lemma 2.2.12. *If* $I = \prod_{j=1}^{k} I_j$ *where the ideals* I_j *of* $\mathbb{F}[\mathbf{x}]$ *are relatively prime in pairs, then* $|\mathrm{Sm}\,(I)| = \sum_{j=1}^{k} |\mathrm{Sm}\,(I_j)|$.

Proof. By the Chinese Remainder Theorem,

$$\mathbb{F}[\mathbf{x}]/I \cong \bigoplus_{j=1}^{k} \mathbb{F}[\mathbf{x}]/I_j.$$

Theorem 2.1.14 implies that by taking dimensions of both sides, we get the required equality. □

The next corollary is extremely important, we shall use it several times in the thesis.

Corollary 2.2.13. *For every finite multiset* $\mathcal{V}$

$$|\mathrm{Sm}\,(I(\mathcal{V}))| = |\mathcal{V}|\,.$$

Proof. Put Lemma 2.2.12, Corollary 2.2.9 and Definition 2.2.11 together. □

We now prove an easy characterization of Gröbner bases of vanishing ideals of finite multisets.

Lemma 2.2.14. *If $\mathcal{V}$ is a finite multiset, $G \subseteq I(\mathcal{V})$ is finite, then G is a Gröbner basis of $I(\mathcal{V})$ if and only if $|\mathcal{V}| = |\mathrm{Sm}\,(G)|$.*

Proof. We know that G is a Gröbner basis of $I(\mathcal{V})$ if and only if $\mathrm{Sm}\,(I(\mathcal{V})) = \mathrm{Sm}\,(G)$. But $\mathrm{Sm}\,(I(\mathcal{V})) \subseteq \mathrm{Sm}\,(G)$ always holds when $G \subseteq I(\mathcal{V})$, so G is a Gröbner basis iff $|\mathrm{Sm}\,(I(\mathcal{V}))| = |\mathrm{Sm}\,(G)|$ (using also that $|\mathrm{Sm}\,(I(\mathcal{V}))|$ is finite). Corollary 2.2.13 tells us that this last equality holds if and only if $|\mathcal{V}| = |\mathrm{Sm}\,(G)|$, and this is what we wanted to show. □

Chapter 3

Gröbner bases of boxes

Having learned the basics of Gröbner theory, we have arrived at a place where our first combinatorial and algebraic applications can be shown. The easiest, yet interesting case is that of a vanishing ideal of a set of points which is a direct product of finite subsets of $\mathbb{F}$. The two topics included in this chapter are based on such calculations. We reprove a theorem of Harima in a special case and Alon's Combinatorial Nullstellensatz using Gröbner bases. We present applications of both theorems.

For more complicated sets of points, further investigation in the theory of Gröbner bases of vanishing ideals will be needed, which will be carried out in Chapter 4.

Results of Section 3.1 appeared in a less general form in our paper [22]. The application of Alon's theorem is published in [18], together with other results on the topic which are not included in the thesis.

3.1 Harima's theorem for finite sets of points

Here we prove an important special case of a theorem by T. Harima. It establishes a connection among the Hilbert functions of $I(V)$ and $I(V^c)$, where V is a finite set of points and V^c is the complement of V in some box $B \supseteq V$. The precise definitions follow.

Definition 3.1.1. Let $V \subseteq \mathbb{F}^n$, and suppose that $V \subseteq B_1 \times B_2 \times \cdots \times B_n = B$ for some finite nonempty sets $B_1, \ldots, B_n \subseteq \mathbb{F}$. Such a set B is called a *box.* The *complement of* V *(in* B*)* is $V^c = B \setminus V$.

Throughout this section, we suppose that $B_1, \ldots, B_n \subseteq \mathbb{F}$ are finite sets, and that $V \subseteq B_1 \times B_2 \times \cdots \times B_n = B$, as in the previous definition. Set $k_i = |B_i|$, $\mathbf{k} = (k_1, \ldots, k_n)$ and $k = \deg\left(\mathbf{x}^{\mathbf{k}}\right) = \sum\limits_{i \in [n]} k_i$.

The main result of this section is the following.

Theorem 3.1.2. *For the Hilbert functions of $I(V)$ and $I(V^c)$, we have*

$$H_{I(B)}(m) - |V| = H_{I(V^c)}(m) - H_{I(V)}(k - n - m - 1).$$

for every $m = 0, 1, \dots, k - n$.

In formula (3.1.5) of [30], Tadahito Harima presents a similar formula for more general point sets, namely for two disjoint finite point sets $\mathbb{X}, \mathbb{Y} \subset \mathbf{P}^n(\mathbb{F})$ in the projective n-space over $\mathbb{F}$, instead of V and V^c, such that $\mathbb{X} \cup \mathbb{Y}$ is a complete intersection. The formula was used in his characterization of the Hilbert functions of Artinian Gorenstein algebras with the weak Stanley property.

Here we focus on disjoint point sets (V and V^c), such that their union is a box. Our approach is based on direct computations with polynomial functions.

The important special case, when the box B is $\{0,1\}^n$, has already been treated in our survey paper [22]. A different proof for that case had been given earlier by Pintér and Rónyai [35]. An advantage of their method is that it works for more general coefficient rings, rather than fields (which include the rings $\mathbb{Z}_d = \mathbb{Z}/d\mathbb{Z}$, where d is a positive integer). An application to the (modular weak degree) complexity of Boolean functions is also given in [35].

The proof of Theorem 3.1.2 is obtained through a proposition, which establishes a one-to-one correspondence between standard monomials of $I(V)$ and a certain subset of leading monomials of $I(V^c)$. But first, let us show a simple lemma, describing the reduced Gröbner bases of boxes, which is needed for the proof of the proposition.

Lemma 3.1.3. *The reduced Gröbner basis of $I(B)$ is*

$$G = \left\{ \prod_{b \in B_i} (x_i - b) \ : \ i \in [n] \right\}$$

with respect to any term order. In particular, the minimal leading monomials of $I(B)$ are $x_i^{k_i}$ ($i \in [n]$), and $\mathrm{Sm}\,(I(B)) = \{\mathbf{x}^{\mathbf{w}} \ : \ \forall\, i \in [n] \ w_i < k_i\}$.

Proof. Since $G \subseteq I(B)$, and $|\mathrm{Sm}\,(G)| = \prod_{i \in [n]} k_i = |B|$, by Lemma 2.2.14 G is indeed a Gröbner basis. It is obvious then that G is also reduced. □

Proposition 3.1.4. *Let $\mathbf{x}^{\mathbf{w}}$ be a monomial such that $w_i < k_i$ for all $i \in [n]$. Then*

$$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V)) \iff \mathbf{x}^{\mathbf{k}-\mathbf{w}-\mathbf{1}} \in \mathrm{Lm}\,(I(V^c))\,,$$

where $\mathbf{x}^{\mathbf{k}-\mathbf{w}-\mathbf{1}} = x_1^{k_1 - w_1 - 1} \dots x_n^{k_n - w_n - 1}$.

Proof. Suppose that $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$ and also $\mathbf{x}^{\mathbf{k}-\mathbf{w}-\mathbf{1}} \in \mathrm{Lm}\,(I(V^c))$. If $f \in I(V)$ with leading monomial $\mathbf{x}^{\mathbf{w}}$, and $g \in I(V^c)$ with $\mathrm{lm}\,(g) = \mathbf{x}^{\mathbf{k}-\mathbf{w}-\mathbf{1}}$, then clearly $f \cdot g \in I(B)$, and $\mathrm{lm}\,(f \cdot g) = \prod\limits_{i \in [n]} x_i^{k_i - 1} = \mathbf{x}^{\mathbf{k}-\mathbf{1}}$. That is $\mathbf{x}^{\mathbf{k}-\mathbf{1}} \in \mathrm{Lm}\,(I(B))$, a contradiction to Lemma 3.1.3.

Therefore, $\mathbf{x}^{\mathbf{k}-\mathbf{w}-\mathbf{1}} \in \mathrm{Lm}\,(I(V^c))$ implies $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$. For the other direction, consider the map $\sigma : \mathrm{Sm}\,(I(B)) \to \mathrm{Sm}\,(I(B))$, $\mathbf{x}^{\mathbf{w}} \mapsto \mathbf{x}^{\mathbf{k}-\mathbf{w}-\mathbf{1}}$. It is an involution, and so what we have just proven is that σ maps $\mathrm{Lm}\,(I(V^c)) \cap \mathrm{Sm}\,(I(B))$ to $\mathrm{Sm}\,(I(V))$. To complete the proof, it remains to see that σ is a one-to-one correspondence between $\mathrm{Lm}\,(I(V^c)) \cap \mathrm{Sm}\,(I(B))$ and $\mathrm{Sm}\,(I(V))$, for which it is enough to show that $|\mathrm{Lm}\,(I(V^c)) \cap \mathrm{Sm}\,(I(B))| = |\mathrm{Sm}\,(I(V))|$.

By $V^c \subseteq B$, we have $\mathrm{Sm}\,(I(V^c)) \subseteq \mathrm{Sm}\,(I(B))$, thus

$$\begin{aligned} &|\mathrm{Lm}\,(I(V^c)) \cap \mathrm{Sm}\,(I(B))| = |\mathrm{Sm}\,(I(B)) \setminus \mathrm{Sm}\,(I(V^c))| = \\ &\qquad = |\mathrm{Sm}\,(I(B))| - |\mathrm{Sm}\,(I(V^c))| = |B| - |V^c| = |V| = |\mathrm{Sm}\,(I(V))|\,. \end{aligned}$$

□

Proof of Theorem 3.1.2. Let $\prec$ be a degree compatible term order. The number of monomials in $\mathrm{Lm}\,(I(V^c)) \cap \mathrm{Sm}\,(I(B)) = \mathrm{Sm}\,(I(B)) \setminus \mathrm{Sm}\,(I(V^c))$ of degree d is $H_{I(B)}(d) - H_{I(B)}(d-1) - \big(H_{I(V^c)}(d) - H_{I(V^c)}(d-1)\big)$. By Proposition 3.1.4, this is the same as $H_{I(V)}(k-d-n) - H_{I(V)}(k-d-n-1)$, the number of standard monomials of degree $k-d-n$ for $I(V)$. We have

$$\begin{aligned} &H_{I(B)}(d) - H_{I(B)}(d-1) = \\ &\quad = H_{I(V^c)}(d) - H_{I(V^c)}(d-1) + H_{I(V)}(k-d-n) - H_{I(V)}(k-d-n-1) \end{aligned}$$

for every $0 \le d \le k-n$ (we use the convention $H_I(-1) = 0$). By adding these up for $d = 0, \dots, m$, we obtain

$$H_{I(B)}(m) = H_{I(V^c)}(m) + H_{I(V)}(k-n) - H_{I(V)}(k-n-m-1).$$

Since every standard monomial of $I(V)$ has degree at most $k-n$ (as they are divisors of $x_1^{k_1-1} \dots x_n^{k_n-1}$), we have $H_{I(V)}(k-n) = |V|$, and the theorem follows. □

Theorem 3.1.2 allows us to formulate an interesting minimax relation among two metrics known from boolean complexity theory. For $V \subsetneq B$, let $a(V)$ stand for the smallest degree of a polynomial with monomials only from $\mathrm{Sm}\,(I(B))$, which vanishes on V. We have $0 \le a(V) \le k-n$.

Also, when $V \subseteq B$ is nonempty, we define $b(V)$ to be the smallest integer d such that $H_{I(V)}(d) = |V|$. In other words, $b(V)$ is the smallest degree d

such that every function from V to $\mathbb{F}$ can be represented by a polynomial from $\mathbb{F}[\mathbf{x}]$ of degree at most d. Then $0 \le b(V) \le k-n$ holds. One may observe that $b(V)$ is the Castelnuovo–Mumford regularity of $I(V)$.

Corollary 3.1.5. *Assume that $V \subseteq B$ is nonempty. Then we have*

$$a(V^c) + b(V) = k - n.$$

Proof. Let us show first that $a(V^c) + b(V) \ge k - n$. If $\mathbf{v} \in B$, then denote by $\chi_{\mathbf{v}}$ the function on B, which vanish on $B \setminus \{\mathbf{v}\}$, and $\chi_{\mathbf{v}}(\mathbf{v}) = 1$. Lagrange interpolation yields a polynomial representation h of $\chi_{\mathbf{v}}$, which consists only of monomials from $\mathrm{Sm}\,(I(B))$ and whose leading monomial is $x_1^{k_1-1} \dots x_n^{k_n-1}$. In particular, $\deg(h) = k - n$. As h is a linear combination of standard monomials, $\chi_{\mathbf{v}}$ cannot be represented by a polynomial of smaller leading monomial, thus neither by a polynomial of smaller degree.

Suppose that $f \in I(V^c)$ is a linear combination of elements of $\mathrm{Sm}\,(I(B))$, such that $\deg(f) = a(V^c)$. Clearly f cannot vanish on B; assume that $f(\mathbf{v}) \ne 0$, $\mathbf{v} \in V$. Let g be a polynomial function on V, such that $g(\mathbf{v}) = \frac{1}{f(\mathbf{v})}$, g is zero on every other point of V, and $\deg(g) \le b(V)$. Then $f \cdot g$ is of degree at most $a(V^c)+b(V)$, it represents the function $\chi_{\mathbf{v}}$, thus $a(V^c)+b(V) \ge k-n$.

The other inequality is easy when $V = B$, so we may suppose that $V \subsetneq B$, and so that $a(V^c) > 0$. We apply Theorem 3.1.2 with $m = a(V^c) - 1$. Note first, that $H_{I(V^c)}(m) = H_{I(B)}(m)$, because monomials from $\mathrm{Sm}\,(I(B))$ of degree $\le m$ are linearly independent over $\mathbb{F}$, as functions on V^c. Theorem 3.1.2 gives now that $H_{I(V)}(k-n-m-1) = |V|$, hence $b(V) \le k-n-m-1 = k - n - a(V^c)$. This proves the assertion. □

3.2 Alon's Combinatorial Nullstellensatz and a conjecture of Rédei

The famous paper [3] of Noga Alon is one of the most important milestones of applications of polynomial techniques in combinatorics and algebra. Although in his paper he does not explicitly mention Gröbner bases, Lemma 3.1.3 can be considered as a reformulation of Alon's Combinatorial Nullstellensatz. This is applied in lots of other papers through the 'non-vanishing theorem' ([3, Theorem 1.2]) which will be placed in our context and proved in this section.

To illustrate the applicability of Alon's statement, we present a theorem, which claims that a generalized diagonal polynomial over a finite prime field has at least one root, provided that some condition on the number of variables and the degree of the polynomial is fulfilled. We connect this result, which appeared originally in [18], to a conjecture of Rédei.

Theorem 3.2.1 (Alon's non-vanishing theorem). *Let $B_i \subseteq \mathbb{F}$ be finite nonempty sets with $|B_i| = k_i$ for $i \in [n]$, and let $f \in \mathbb{F}[\mathbf{x}]$ be a polynomial, such that* $\deg(f) = \sum_{i=1}^{n}(k_i - 1)$ *and that the coefficient of* $\mathbf{x}^{\mathbf{k-1}} = \prod_{i=1}^{n} x_i^{k_i-1}$ *is not 0. Then f does not vanish on the box $B = B_1 \times \cdots \times B_n$, that is $f \notin I(B)$.*

Proof. Let us reduce f with the reduced Gröbner basis of $I(B)$, and denote the result with $\hat{f}$. Note that $\mathbf{x}^{\mathbf{k-1}}$ is a standard monomial of $I(B)$. By the special form of the above Gröbner basis (see Lemma 3.1.3), every reduction step replaces a monomial with other monomials of smaller degree. These imply that the coefficient of $\mathbf{x}^{\mathbf{k-1}}$ in f and $\hat{f}$ are the same. (Actually, $\mathrm{lm}\left(\hat{f}\right) = \mathbf{x}^{\mathbf{k-1}}$.) In particular $\hat{f} \neq 0$. Being a linear combination of standard monomials, this implies $\hat{f} \notin I(B)$ and thus that $f \notin I(B)$. □

We now turn to an application of the previous result.

In 1946 László Rédei formulated a conjecture (see [37]) about the solvability of polynomial equations over finite fields. Although Rónyai [38] showed that there are counterexamples, for polynomials of certain special forms the conjecture holds. A description of some cases when the conjecture is true, together with Rónyai's counterexamples can be found in [18].

Let p be a prime, and $f \in \mathbb{F}_p[\mathbf{x}]$ be a polynomial. Suppose that the degree of f in x_i ($\deg_{x_i}(f)$ for short) is at most $p-1$ for all $i \in [n]$, that is the polynomial is reduced with respect to the Gröbner basis of $I(\mathbb{F}_p^n)$.

The *rank* of f is defined to be the least positive integer r for which there exists an invertible homogeneous linear change of variables which carries f into a polynomial with r variables. We then write $\mathrm{rank}(f) = r$. One may think of the rank as the effective number of variables of the polynomial. While this definition captures well the intuitive meaning of the rank, the following equivalent definition is easier to use for computations.

Let us denote the linear subspace of $\mathbb{F}_p[\mathbf{x}]$ spanned by the partial derivatives of f by F, that is

$$F = \mathrm{Lin}_{\mathbb{F}_p}\left\{\frac{\partial f(\mathbf{x})}{\partial x_i} \;:\; i \in [n]\right\}.$$

It can be shown (see [38]) that $\mathrm{rank}(f) = \dim_{\mathbb{F}_p}(F)$.

We can now state Rédei's conjecture.

Conjecture 3.2.2 (Rédei). *If $f \in \mathbb{F}_p[\mathbf{x}]$ is not constant, $\deg_{x_i}(f) \leq p-1$ $(i \in [n])$, and $\deg(f) \leq \operatorname{rank}(f)$ then f has a root in $\mathbb{F}_p^n$.*

We shall examine a family of polynomials for which the conjecture is still open. Assuming a slightly stronger condition than Rédei's, we are able to prove the existence of a root of any member of the family.

Definition 3.2.3. Let p be a prime. A polynomial of the form

$$f(\mathbf{x}) = \sum_{i=1}^{n} a_i x_i^d + g(\mathbf{x}) \in \mathbb{F}_p[\mathbf{x}]$$

is a *generalized diagonal polynomial*, whenever $1 \leq d \leq p-1$, $a_1 \dots a_n \neq 0$ and $\deg g < d$.

Theorem 3.2.4. *Suppose that $\left\lceil \frac{p-1}{\lfloor \frac{p-1}{d} \rfloor} \right\rceil \leq n$. Then the generalized diagonal polynomial $f = \sum\limits_{i=1}^{n} a_i x_i^d + g$ has a root in $\mathbb{F}_p^n$.*

Proof. We can assume that $\left\lceil \frac{p-1}{\lfloor \frac{p-1}{d} \rfloor} \right\rceil = n$, for otherwise we may get a similar polynomial in $\left\lceil \frac{p-1}{\lfloor \frac{p-1}{k} \rfloor} \right\rceil$ variables by substituting zeros in the place of some x_i. Let $h = 1 - f^{p-1}$. We intend to show that h does not vanish on $\mathbb{F}_p^n$. Since the value of f^{p-1} at any point of $\mathbb{F}_p^n$ can only be either 0 or 1, this will imply that there exists a root of f. Let

$$\begin{aligned} k_i &= \left\lfloor \frac{p-1}{d} \right\rfloor d + 1 \qquad \text{for } i \in [n-1] \text{ and} \\ k_n &= (p-1)\,d - (n-1) \left\lfloor \frac{p-1}{d} \right\rfloor d + 1. \end{aligned}$$

It is obvious that $1 \leq k_i \leq p$ for $i \in [n-1]$ and $\sum\limits_{i=1}^{n} (k_i - 1) = (p-1)d = \deg(h)$. The following simple calculation

$$\begin{aligned} k_n &= (p-1)\,d - \left(\left\lceil \frac{p-1}{\lfloor \frac{p-1}{d} \rfloor} \right\rceil - 1 \right) \left\lfloor \frac{p-1}{d} \right\rfloor d + 1 \\ &\leq (p-1)\,d - \left(\frac{p-1}{\lfloor \frac{p-1}{d} \rfloor} - 1 \right) \left\lfloor \frac{p-1}{d} \right\rfloor d + 1 = \left\lfloor \frac{p-1}{d} \right\rfloor d + 1 \leq p \qquad \text{and} \\ k_n &> (p-1)\,d - \frac{p-1}{\lfloor \frac{p-1}{d} \rfloor} \left\lfloor \frac{p-1}{d} \right\rfloor d + 1 = 1 \end{aligned}$$

gives that also $1 \leq k_n \leq p$.

In h, there is a monomial $\mathbf{x}^{\mathbf{k-1}}$ contributed by $\left(\sum\limits_{i=1}^{d} a_i x_i^d\right)^{p-1}$, since $x_i^{k_i-1} = \left(x_i^d\right)^{\left\lfloor \frac{p-1}{d} \right\rfloor}$ (for $i \in [n-1]$), and $x_n^{k_n-1} = \left(x_n^d\right)^{p-1-(n-1)\left\lfloor \frac{p-1}{d} \right\rfloor}$. The coefficient of $\mathbf{x}^{\mathbf{k-1}}$ is therefore

$$-\frac{(p-1)!}{\prod\limits_{i=1}^{n} \frac{k_i-1}{d}!} \prod_{i=1}^{n} a_i^{\frac{k_i-1}{d}} \neq 0.$$

By choosing arbitrary subsets $B_i \subseteq \mathbb{F}_p$ with $|B_i| = k_i$, the conditions of the non-vanishing theorem hold, therefore h does not vanish on $B \subseteq \mathbb{F}_p^n$. This proves the claim. □

If $d \mid p-1$ then the statement is also true in an arbitrary finite field. We shall obtain this result by a slight modification of the previous proof. Actually, this claim has already been proved by Carlitz [14], in a way different from ours.

Theorem 3.2.5. *Assume that $q = p^r$ is a prime power. If d divides $p-1$, $d \leq n$ and $f = \sum\limits_{i=1}^{n} a_i x_i^d + g \in \mathbb{F}_q[\mathbf{x}]$ (with $\deg(g) < d$), then f has a root in $\mathbb{F}_q^n$.*

Proof. We may suppose that $d = n$. We apply Alon's non-vanishing theorem for the polynomial $h = 1 - f^{q-1}$ with all $k_i = q$ and $B = \mathbb{F}_q^n$. The coefficient of $\mathbf{x}^{\mathbf{k-1}}$ is

$$-\frac{(q-1)!}{\left(\frac{q-1}{d}!\right)^d} \prod_{i=1}^{d} a_i^{\frac{q-1}{d}}.$$

(Here we used that d divides $q-1$, which follows from the fact that $p^r - 1$ is divisible with $p-1$.) To see that this coefficient is not zero in $\mathbb{F}_q$, it is enough to show that p does not divide $\frac{(q-1)!}{((q-1)/d)!^d}$. The largest power of p which divides the numerator is

$$\sum_{i=1}^{\infty} \left\lfloor \frac{p^r-1}{p^i} \right\rfloor = \sum_{i=1}^{r-1} \left\lfloor p^{r-i} - \frac{1}{p^i} \right\rfloor = \sum_{i=1}^{r-1} \left(p^{r-i} - 1\right) .$$

This is the same for the denominator. Indeed

$$d \sum_{i=1}^{\infty} \left\lfloor \frac{\frac{p^r-1}{d}}{p^i} \right\rfloor = d \sum_{i=1}^{r-1} \left\lfloor \frac{p^{r-i}-1}{d} + \frac{p^i-1}{p^i d} \right\rfloor =$$

$$d\sum_{i=1}^{r-1}\frac{p^{r-i}-1}{d}=\sum_{i=1}^{r-1}\left(p^{r-i}-1\right).$$

The second to the last equality holds since $0<\frac{p^i-1}{p^i d}<1$ and $d \mid p-1$ implies that $\frac{p^{r-i}-1}{d}$ is an integer. □

To compare Theorem 3.2.4 with Rédei's conjecture, we observe that for a generalized diagonal polynomial f, if $d=1$ then $\mathrm{rank}(f)=1$, otherwise we have $\mathrm{rank}(f)=n$. Indeed, put

$$f_i(\mathbf{x})=\frac{\partial f}{\partial x_i}(\mathbf{x})=da_ix_i^{d-1}+\frac{\partial g}{\partial x_i}(\mathbf{x}).$$

Suppose that there exist some α_i such that $\sum_{i=1}^{n}\alpha_i f_i=0$ holds. As $\deg\left(\frac{\partial g}{\partial x_i}\right)<d-1$, the coefficient of x_i^{d-1} is $\alpha_i d a_i$, hence $\alpha_i=0$ for each i, which means that the f_i are linearly independent, and $\mathrm{rank}(f)=n$.

We conclude that Rédei's conjecture predicts that there is a root of f in $\mathbb{F}_p^n$, in case $d\le n$. Unless $d|p-1$, this is a slightly weaker condition than $\left\lceil\frac{p-1}{\left\lfloor\frac{p-1}{d}\right\rfloor}\right\rceil\le n$, the one we used to prove Theorem 3.2.4.

Chapter 4

The Lex Game

In this chapter we introduce the Lex Game. This is our main tool which can be applied to compute the lexicographic standard monomials of ideals of combinatorial interest. Such applications are treated in the next chapters, for which one has to know the lex standard monomials of vanishing ideals $I(V)$ of finite sets of points V. However, the game can be used to compute lex standard monomials for more general zero dimensional ideals.

For a fixed ideal, we somehow obtain a set of monomials $\mathrm{Stan}\,(I)$ as a result of the game. We shall show in Section 4.2, that if $I = I(\mathcal{V})$ for some algebraic multiset $\mathcal{V}$, then $\mathrm{Stan}\,(I) = \mathrm{Sm}_{\mathrm{lex}}\,(I)$. The subsequent section proves the same for a different class of zero dimensional ideals. In fact, there we also reveal interesting properties of the structure of lexicographic Gröbner bases. We shall see that $\mathrm{Stan}\,(I) \neq \mathrm{Sm}_{\mathrm{lex}}\,(I)$ in general; we formulate a conjecture about $\mathrm{Stan}\,(I)$ instead. The last section of this chapter provides an algorithm that computes $\mathrm{Stan}\,(I)$, and hence $\mathrm{Sm}_{\mathrm{lex}}\,(I)$ in certain cases.

The Game was first introduced in [20], and the general form appeared in [21], where the proof of the multiset case can also be found. The results in Section 4.3 have not yet been published. The algorithm in the case $I = I(V)$ is in [20], the general one is a simple modification of that treatment.

Throughout the chapter, we use the lexicographic ordering, so—even if it is not stated explicitly—$\mathrm{Sm}\,(I)$ and $\mathrm{Lm}\,(I)$ are defined with respect to lex.

4.1 Rules of the Lex Game

Let I be a zero dimensional splitting ideal with primary decomposition of the form (2.3) and let $\mathbf{w} \in \mathbb{N}^n$ be an n dimensional vector of natural numbers. With these data fixed, we define the Lex Game $\mathrm{Lex}\,(I; \mathbf{w})$, which is played by two people Lea and Stan.

Both Lea and Stan know I and $\mathbf{w}$.

1 Lea chooses w_n (not necessarily different) elements of $\mathbb{F}$.

Stan (knowing Lea's choices) picks a value $y_n \in \mathbb{F}$.

They set r_n to be the multiplicity of y_n among Lea's guesses.

2 Lea now chooses w_{n-1} (not necessarily different) elements of $\mathbb{F}$.

Stan (knowing Lea's choices) picks a $y_{n-1} \in \mathbb{F}$.

They record the result r_{n-1}, the number of y_{n-1} among Lea's choices.

... (The game goes on in the same fashion.)

n Lea chooses w_1 (not necessarily different) elements of $\mathbb{F}$.

Stan (knowing Lea's choices) finally picks a $y_1 \in \mathbb{F}$.

They put the number of correct guesses in r_1.

Suppose that the *result vector* of the game is $\mathbf{r} = (r_1, \dots, r_n) \in \mathbb{N}^n$. The winner is Lea precisely if $\mathbf{x}^{\mathbf{r}} \in \operatorname{Lm}(Q_{\mathbf{y}})$.

When $I = I(\mathcal{V})$ or $I = I(V)$ we may also write $\operatorname{Lex}(\mathcal{V}; \mathbf{w})$ or $\operatorname{Lex}(V; \mathbf{w})$ respectively.

From the combinatorial point of view, the most interesting case is that of $I = I(V)$ for a finite subset $V \subseteq \mathbb{F}^n$. Then the primary decomposition consists of maximal ideals $\langle x_1 - y_1, \dots, x_n - y_n \rangle$ corresponding to the points $\mathbf{y} \in V$, and so $\operatorname{Sm}(Q_{\mathbf{y}}) = \{1\}$ for all $\mathbf{y} \in V$. If Stan picks the y_i such that $\mathbf{y} \notin V$ then $Q_{\mathbf{y}} = \mathbb{F}[\mathbf{x}]$, $\operatorname{Sm}(Q_{\mathbf{y}}) = \emptyset$, so Lea wins the game even without any successful guess ($\mathbf{r} = \mathbf{0}$). But when Stan chooses a $\mathbf{y}$ in V then $\mathbf{x}^{\mathbf{r}} \in \operatorname{Lm}(Q_{\mathbf{y}})$ if and only if there exists an $r_i \geq 1$. That is, Lea's goal in $\operatorname{Lex}(V; \mathbf{w})$ is to find out at least one coordinate of $\mathbf{y}$, and Stan will pick the y_i to prevent Lea from this, while paying attention to have $\mathbf{y} \in V$.

Example 4.1.1. Let $n = 5$, and $\alpha, \beta \in \mathbb{F}$ be different elements. Let V be the set of all α-β sequences in $\mathbb{F}^5$ in which the number of the α coordinates is 1, 2 or 3. We claim that Lea can win in the game $\operatorname{Lex}(V; \mathbf{w})$ if $\mathbf{w} = (11100)$, but if $\mathbf{w} = (01110)$, then Stan has a winning strategy.

Indeed, let $\mathbf{w} = (11100)$. To have $\mathbf{y} \in V$, Stan is forced to select values from $\{\alpha, \beta\}$. If Stan gives only β for the last 2 coordinates, then Lea will choose α in the first three, therefore either $\mathbf{y}$ does not contain any α coordinates, or one of Lea's guesses are correct. However if Stan gives at least one

α for the last 2 coordinates, then Lea, by keeping on choosing β, can prevent $\mathbf{y}$ to have at least two β coordinates.

In the case $\mathbf{w} = (01110)$ Stan's winning strategy is to pick $y_5 = \beta$, and choose the complement of Lea's guess from $\{\alpha, \beta\}$ (for the 4th, 3rd and 2nd coordinates). One can easily check that y_1 then can always be taken such that $\mathbf{y} \in V$.

Another special case, which contains the previous one, is when I is the vanishing ideal of a finite algebraic multiset $\mathcal{V}$ of $\mathbb{F}^n$. By Theorem 2.2.8 we know that in this case each primary component $Q_{\mathbf{y}}$ is $\mathbf{y}$-monomial so Corollary 2.2.9 applies: Lea wins the game if and only if the result vector $\mathbf{r}$ is not in $\mathcal{V}(\mathbf{y})$.

Our goal is to determine the winner of the game. As the Lex Game is a finite and deterministic game, depending on I and $\mathbf{w}$, either of the two players always has a winning strategy. From now on, we say that Lea (Stan) wins the game if she (he) has a winning strategy.

Definition 4.1.2. For I fixed, the set

$$\mathrm{Stan}\,(I) = \{\mathbf{x}^{\mathbf{w}} \ : \ \text{Stan wins } \mathrm{Lex}\,(I; \mathbf{w})\}$$

is the set of *Stan monomials.*

We investigate $\mathrm{Stan}\,(I)$. In particular we show that for any finite algebraic multiset $\mathrm{Stan}\,(I(\mathcal{V})) = \mathrm{Sm}\,(I(\mathcal{V}))$. We will also see that $\mathrm{Stan}\,(I) = \mathrm{Sm}\,(I)$ holds when every two points associated with I can be distinguished by looking only at their last two coordinates, in particular when $n \leq 2$.

Before going on, we take a look at the quite easy case $n = 1$.

Proposition 4.1.3. *If $n = 1$, then for every splitting ideal I we have* $\mathrm{Sm}\,(I) = \mathrm{Stan}\,(I)$.

Proof. Let $w \geq 0$ be an integer. Then $x^w \in \mathrm{Sm}\,(I)$ if and only if $w < |\mathrm{Sm}\,(I)| = \sum_{y \in \mathbb{F}} |\mathrm{Sm}\,(Q_y)|$ by the fact that $\mathrm{Sm}\,(I)$ is a downset with respect to division and Lemma 2.2.12. But this means precisely that no matter how Lea is trying, there has to be a $y \in \mathbb{F}$ which is at most $|\mathrm{Sm}\,(Q_y)| - 1$ times among her guesses, thus Stan wins the game as $x^{|\mathrm{Sm}(Q_y)|-1} \in \mathrm{Sm}\,(Q_y)$. □

4.2 The multiset case

We show in this section that the Lex Game gives a combinatorial description of the standard monomials of $I(\mathcal{V})$. We remind the reader that in this case the condition that determines the winner is $\mathbf{r} \in \mathcal{V}(\mathbf{y})$.

Theorem 4.2.1. *Let $\mathcal{V}$ be a finite algebraic multiset. Then* $\operatorname{Sm}(I(\mathcal{V})) = \operatorname{Stan}(I(\mathcal{V}))$. *In other words: Lea wins* $\operatorname{Lex}(\mathcal{V}; \mathbf{w})$ *iff* $\mathbf{x}^{\mathbf{w}} \in \operatorname{Lm}(I(\mathcal{V}))$.

Before the proof, we introduce some notation. If $y \in \mathbb{F}$ and $m \geq 0$ is an integer, then let $\mathcal{V}_{y,m}$ be the finite multiset of $\mathbb{F}^{n-1}$ for which

$$\mathcal{V}_{y,m}(\overline{\mathbf{y}}) = \left\{ \overline{\mathbf{m}} \in \mathbb{N}^{n-1} \ : \ (\overline{\mathbf{m}}, m) \in \mathcal{V}(\overline{\mathbf{y}}, y) \right\}$$

holds for all $\overline{\mathbf{y}} \in \mathbb{F}^{n-1}$.

This somewhat cumbersome piece of notation intends to capture a simple aspect of the game: suppose that at the first step of a $\operatorname{Lex}(\mathcal{V}; \mathbf{w})$ game Lea guessed y precisely m times and Stan revealed that $y_n = y$. Then they continue as if they have just started a $\operatorname{Lex}(\mathcal{V}_{y,m}; \overline{\mathbf{w}})$ game. Indeed, $(\overline{\mathbf{r}}, m) \in \mathcal{V}(\overline{\mathbf{y}}, y)$ if and only if $\overline{\mathbf{r}} \in \mathcal{V}_{y,m}(\overline{\mathbf{y}})$, which means that Lea wins the original game with exactly $m = r_n$ correct guesses for $y = y_n$ given in the first round if and only if she wins $\operatorname{Lex}(\mathcal{V}_{y,m}; \overline{\mathbf{w}})$.

Recall from Subsection 2.2.1 that the coefficient of $(\mathbf{x}-\mathbf{y})^{\mathbf{w}}$ in $f(\mathbf{x})$, when written as a polynomial in the variables $\mathbf{x} - \mathbf{y}$ is

$$\frac{1}{\mathbf{w}!} \cdot \frac{\partial^{\mathbf{w}}}{\partial \mathbf{x}^{\mathbf{w}}} f(\mathbf{y}) = \frac{1}{w_1! \dots w_n!} \cdot \frac{\partial^{w_1 + \dots + w_n}}{\partial x_1^{w_1} \dots \partial x_n^{w_n}} f(\mathbf{x}) \text{ at } \mathbf{x} = \mathbf{y}.$$

We will need the following lemma.

Lemma 4.2.2. *Suppose that $f(\mathbf{x}) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} g(x_n) + h(\mathbf{x}) \in I(\mathcal{V})$, $h(\mathbf{x}) \prec \overline{\mathbf{x}}^{\overline{\mathbf{w}}}$. Let m be a nonnegative integer and $y \in \mathbb{F}$ such that the polynomial $(x_n - y)^{m+1}$ does not divide $g(x_n)$ in $\mathbb{F}[x_n]$. Then $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \operatorname{Lm}(I(\mathcal{V}_{y,m}))$.*

Proof. If $m' < m$ then $I(\mathcal{V}_{y,m'}) \subseteq I(\mathcal{V}_{y,m})$ holds and also $\operatorname{Lm}(I(\mathcal{V}_{y,m'})) \subseteq \operatorname{Lm}(I(\mathcal{V}_{y,m}))$, hence we may assume without loss of generality that $g(x_n) = (x_n - y)^m \hat{g}(x_n)$, with some $\hat{g}$ not vanishing at y. Set

$$\hat{f}(\overline{\mathbf{x}}) = \frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} f(\overline{\mathbf{x}}, y).$$

As $f(\mathbf{x}) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} (x_n - y)^m \hat{g}(x_n) + h(\mathbf{x})$, the Leibniz rule gives that

$$\hat{f}(\overline{\mathbf{x}}) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} \hat{g}(y) + \frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} h(\overline{\mathbf{x}}, y).$$

Every monomial of $h(\mathbf{x})$ is less than $\overline{\mathbf{x}}^{\overline{\mathbf{w}}}$, hence the same is true for every monomial of $\frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} h(\overline{\mathbf{x}}, y)$. Thus $\operatorname{lm}\left(\hat{f}\right) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}}$, using also that $\hat{g}(y) \neq 0$. We shall be done, once we show that $\hat{f}(\overline{\mathbf{x}}) \in I\left(\mathcal{V}_{y,m}\right)$.

Let $\overline{\mathbf{y}} \in \mathbb{F}^{n-1}$ and $\overline{\mathbf{m}} \in \mathcal{V}_{y,m}(\overline{\mathbf{y}})$ be arbitrary. We need to prove that

$$\frac{1}{\overline{\mathbf{m}}!} \cdot \frac{\partial^{\overline{\mathbf{m}}}}{\partial \overline{\mathbf{x}}^{\overline{\mathbf{m}}}} \hat{f}(\overline{\mathbf{y}}) = 0.$$

By the definitions, $(\overline{\mathbf{m}}, m) \in \mathcal{V}(\overline{\mathbf{y}}, y)$. Using that $f(\mathbf{x}) \in I(\mathcal{V})$ we have

$$0 = \frac{1}{(\overline{\mathbf{m}}, m)!} \cdot \frac{\partial^{(\overline{\mathbf{m}}, m)}}{\partial \overline{\mathbf{x}}^{\overline{\mathbf{m}}} x_n^m} f(\overline{\mathbf{y}}, y) = \left. \frac{\partial^{\overline{\mathbf{m}}} \left(\frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} f(\overline{\mathbf{x}}, y) \right)}{\overline{\mathbf{m}}! \cdot \partial \overline{\mathbf{x}}^{\overline{\mathbf{m}}}} \right|_{\overline{\mathbf{x}} = \overline{\mathbf{y}}} = \frac{1}{\overline{\mathbf{m}}!} \cdot \frac{\partial^{\overline{\mathbf{m}}}}{\partial \overline{\mathbf{x}}^{\overline{\mathbf{m}}}} \hat{f}(\overline{\mathbf{y}})$$

as we stated. □

Proof of Theorem 4.2.1. We prove the statement by induction on n, the case $n = 1$ already being covered in Proposition 4.1.3. Suppose that $n > 1$ and that the theorem is true for $n - 1$. Set

$$Z = \left\{ (y, m) \in \mathbb{F} \times \mathbb{N} : \overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \operatorname{Sm}\left(I(\mathcal{V}_{y,m}) \right) \right\}.$$

The inductive hypothesis yields that Stan wins $\operatorname{Lex}(\mathcal{V}_{y,m}; \overline{\mathbf{w}})$ if and only if $(y, m) \in Z$. From what we said about the connection between the games $\operatorname{Lex}(\mathcal{V}; \mathbf{w})$ and $\operatorname{Lex}(\mathcal{V}_{y,m}; \overline{\mathbf{w}})$ it follows that Stan wins $\operatorname{Lex}(\mathcal{V}; \mathbf{w})$ if and only if $w_n < |Z|$. Therefore it is enough to show that

$$\mathbf{x}^{\mathbf{w}} \in \operatorname{Sm}\left(I(\mathcal{V}) \right) \iff w_n < \left| \left\{ (y, m) \in \mathbb{F} \times \mathbb{N} : \overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \operatorname{Sm}\left(I(\mathcal{V}_{y,m}) \right) \right\} \right|. \tag{4.1}$$

Suppose first that $\mathbf{x}^{\mathbf{w}} \in \operatorname{Lm}\left(I(\mathcal{V}) \right)$, and let $f(\mathbf{x}) \in I(\mathcal{V})$ be a witness of this fact, that is $\operatorname{lm}(f) = \mathbf{x}^{\mathbf{w}}$. By collecting the terms of the form $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^i$ ($i \in \mathbb{N}$) we get a decomposition $f(\mathbf{x}) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} g(x_n) + h(\mathbf{x})$, where $h(\mathbf{x}) \prec \overline{\mathbf{x}}^{\overline{\mathbf{w}}}$ and $\deg(g) = w_n$.

If for some $(y, m) \in \mathbb{F} \times \mathbb{N}$ the polynomial $(x_n - y)^{m+1}$ does not divide $g(x_n)$, then by Lemma 4.2.2 we have $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \operatorname{Lm}\left(I\left(\mathcal{V}_{y,m} \right) \right)$ and so $(y, m) \notin Z$. But there are at most $\deg(g)$ pairs $(y, m) \in \mathbb{F} \times \mathbb{N}$ such that $(x_n - y)^{m+1}$ divides g as $\mathbb{F}[x_n]$ is a unique factorization domain. This means that $|Z| \leq \deg(g) = w_n$.

For the other direction, assume that $\mathbf{x}^{\mathbf{w}} \in \operatorname{Sm}\left(I(\mathcal{V}) \right)$. It suffices to show that $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{|Z|} \in \operatorname{Lm}\left(I(\mathcal{V}) \right)$, since in this case $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{|Z|}$ cannot be a divisor of $\mathbf{x}^{\mathbf{w}}$, that is $w_n < |Z|$.

Put $m_y = \min\{m \in \mathbb{N} : (y,m) \notin Z\}$ for all $y \in \mathbb{F}$. On the one hand, $(y, m_y) \notin Z$ implies the existence of a polynomial $f_y(\overline{\mathbf{x}})$ such that $f(\overline{\mathbf{x}}) \prec \overline{\mathbf{x}}^{\overline{\mathbf{w}}}$ and $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} + f_y(\overline{\mathbf{x}}) \in I(\mathcal{V}_{y,m_y})$. On the other hand, by the minimality of m_y we know that $(y,0)$, $(y,1)$, $\ldots$, $(y, m_y - 1) \in Z$, from which we get

$$|Z| = \sum_{y \in \mathbb{F}} m_y. \tag{4.2}$$

Set $F = \{y \in \mathbb{F} : \exists \overline{\mathbf{y}} \in \mathbb{F}^{n-1} \text{such that } \mathcal{V}(\overline{\mathbf{y}}, y) \neq \emptyset\}$. As F is the set of the last coordinates of points of $\mathcal{V}$, F is finite. For every $y \in F$ let $M_y = \max\{m : \exists \overline{\mathbf{y}} \in \mathbb{F}^{n-1} : \mathcal{V}_{y,m}(\overline{\mathbf{y}}) \neq \emptyset\}$ and $\chi_y(x_n)$ be a polynomial such that for $0 \le m \le M_y$ and $y' \in F$

$$\frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} \chi_y(y') = \begin{cases} 1, & \text{if } m = 0 \text{ and } y' = y \\ 0 & \text{otherwise} \end{cases}. \tag{4.3}$$

Since F is finite, we have finitely many conditions on χ_y which can be satisfied by a polynomial.

And eventually let

$$s(\mathbf{x}) = \left(\overline{\mathbf{x}}^{\overline{\mathbf{w}}} + \sum_{y \in F} \chi_y(x_n) f_y(\overline{\mathbf{x}}) \right) \cdot \prod_{y \in F} (x_n - y)^{m_y}.$$

By the properties of the lexicographic order, the leading monomial of $\left(\overline{\mathbf{x}}^{\overline{\mathbf{w}}} + \sum\limits_{y \in F} \chi_y(x_n) f_y(\overline{\mathbf{x}}) \right)$ is $\overline{\mathbf{x}}^{\overline{\mathbf{w}}}$, and so (4.2) implies that $\operatorname{lm}(s(\mathbf{x})) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{|Z|}$. It remains to verify $s(\mathbf{x}) \in I(\mathcal{V})$.

Let $(\overline{\mathbf{y}}, y) \in \mathbb{F}^n$ and $(\overline{\mathbf{m}}, m) \in \mathcal{V}(\overline{\mathbf{y}}, y)$ be arbitrary. (The existence of such an $(\overline{\mathbf{m}}, m)$ implies $y \in F$.) We want to show that $\frac{1}{(\overline{\mathbf{m}},m)!} \cdot \frac{\partial^{(\overline{\mathbf{m}},m)}}{\partial \overline{\mathbf{x}}^{\overline{\mathbf{m}}} x_n^m} s(\overline{\mathbf{y}}, y) = 0$. Property (4.3) of the polynomials $\chi_{y'}(x_n)$ gives

$$\frac{1}{i!} \cdot \frac{\partial^i}{\partial x_n^i} \left(\overline{\mathbf{x}}^{\overline{\mathbf{w}}} + \sum_{y' \in F} \chi_{y'}(y) f_{y'}(\overline{\mathbf{x}}) \right) = \begin{cases} \overline{\mathbf{x}}^{\overline{\mathbf{w}}} + f_y(\overline{\mathbf{x}}) & \text{if } i = 0 \\ 0 & \text{if } 0 < i \le m \end{cases}$$

using also that $m \le M_y$. This yields

$$\frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} s(\overline{\mathbf{x}}, y) = \left(\overline{\mathbf{x}}^{\overline{\mathbf{w}}} + f_y(\overline{\mathbf{x}}) \right) \cdot \frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} \prod_{y' \in F} (y - y')^{m_{y'}}.$$

If $m < m_y$ then we are done, as every term of $\frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} \prod\limits_{y' \in F} (x_n - y')^{m_{y'}}$ is divisible by $(x_n - y)$, and hence it vanishes at y. Assume therefore that

$m \geq m_y$. As $(\overline{\mathbf{m}}, m)$ is in the downset $\mathcal{V}(\overline{\mathbf{y}}, y)$ we also have $(\overline{\mathbf{m}}, m_y) \in \mathcal{V}(\overline{\mathbf{y}}, y)$ or equivalently $\overline{\mathbf{m}} \in \mathcal{V}_{y,m_y}(\overline{\mathbf{y}})$. Since $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} + f_y(\overline{\mathbf{x}}) \in I(\mathcal{V}_{y,m_y})$, we have

$$\frac{1}{\overline{\mathbf{m}}!} \cdot \frac{\partial^{\overline{\mathbf{m}}}}{\partial \overline{\mathbf{x}}^{\overline{\mathbf{m}}}} \left(\overline{\mathbf{y}}^{\overline{\mathbf{w}}} + f_y(\overline{\mathbf{y}})\right) = 0,$$

and so

$$\frac{1}{(\overline{\mathbf{m}}, m)!} \cdot \frac{\partial^{(\overline{\mathbf{m}}, m)}}{\partial \overline{\mathbf{x}}^{\overline{\mathbf{m}}} x_n^m} s(\overline{\mathbf{y}}, y) = \frac{1}{\overline{\mathbf{m}}!} \cdot \frac{\partial^{\overline{\mathbf{m}}}}{\partial \overline{\mathbf{x}}^{\overline{\mathbf{m}}}} \left(\frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} s(\overline{\mathbf{y}}, y) \right) =$$
$$\frac{1}{\overline{\mathbf{m}}!} \cdot \frac{\partial^{\overline{\mathbf{m}}}}{\partial \overline{\mathbf{x}}^{\overline{\mathbf{m}}}} \left(\left(\overline{\mathbf{y}}^{\overline{\mathbf{w}}} + f_y(\overline{\mathbf{y}})\right) \cdot \frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} \prod_{y' \in F} (y - y')^{m_{y'}} \right) =$$
$$\left(\frac{1}{\overline{\mathbf{m}}!} \cdot \frac{\partial^{\overline{\mathbf{m}}}}{\partial \overline{\mathbf{x}}^{\overline{\mathbf{m}}}} \left(\overline{\mathbf{y}}^{\overline{\mathbf{w}}} + f_y(\overline{\mathbf{y}})\right) \right) \cdot \left(\frac{1}{m!} \cdot \frac{\partial^m}{\partial x_n^m} \prod_{y' \in F} (y - y')^{m_{y'}} \right) = 0.$$

This completes the proof. □

As it is clear from the above proof, the 'essence' of Theorem 4.2.1 can be formulated without the game. (Although it might be a bit harder to interpret this result.)

Theorem 4.2.3. *If $\mathcal{V}$ is a finite algebraic multiset, $n \geq 2$, and $\mathbf{w} \in \mathbb{N}^n$ then*

$$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\left(I(\mathcal{V})\right) \iff w_n < \left| \left\{ (y, m) \in \mathbb{F} \times \mathbb{N} \;:\; \overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \mathrm{Sm}\left(I(\mathcal{V}_{y,m})\right) \right\} \right|.$$

It worth to mention the following, which is actually proven here without the game.

Proposition 4.2.4.

$$|\mathrm{Sm}\left(I(\mathcal{V})\right)| = \sum_{(y,m) \in \mathbb{F} \times \mathbb{N}} |\mathrm{Sm}\left(I(\mathcal{V}_{y,m})\right)|$$

Proof. A simple calculation shows that $|\mathcal{V}| = \sum_{(y,m) \in \mathbb{F} \times \mathbb{N}} |\mathcal{V}_{y,m}|$, so the claim follows from Corollary 2.2.13. □

4.3 Points in almost general position

We now consider zero dimensional splitting ideals I such that every point of I can be recognised by its last two coordinates, that is if $\mathbf{y}$ and $\mathbf{y}'$ are points of I, $y_n = y'_n$ and $y_{n-1} = y'_{n-1}$ then $\mathbf{y} = \mathbf{y}'$. Our goal in this section to prove that for such an I the standard and the Stan monomials are the same.

As a preparation we examine the lex Gröbner bases of ideals of $\mathbb{F}[s,t]$.

4.3.1 Vanishing ideals of the plane

We shall characterize the reduced lex Gröbner bases of ideals $I \trianglelefteq \mathbb{F}[s,t]$, such that $t \in \sqrt{I}$ and $t \prec s$. One could easily generalize our results to the case when $t - y \in \sqrt{I}$ (instead of $t \in \sqrt{I}$), where $y \in \mathbb{F}$.

By $\deg_s(h)$—as we did before—we mean the degree of the multivariate polynomial h in s. To slightly shorten our statements, we shall write $\deg_s(h) < w$, even when h does not depend on s, in particular if $h = 0$.

Lemma 4.3.1. *Let $I \trianglelefteq \mathbb{F}[s,t]$ be an ideal such that $t \in \sqrt{I}$. Suppose that $s^w p(t) + h(s,t) \in I$, $p \neq 0$ and $\deg_s(h) < w$. Then there is an $\hat{h}(s,t) \in \mathbb{F}[s,t]$ such that $\deg_s(\hat{h}) < w$ and $s^w t^\ell + \hat{h}(s,t) \in I$, where $\ell = \max\{\ell' : t^{\ell'}$ divides $p(t)\}$.*

The Lemma claims that for example $s(t^2+1) \in I$ implies that $s + c \in I$ for some $c \in \mathbb{F}$, provided that $t \in \sqrt{I}$.

Proof. Assume that $t^{\ell_0} \in I$. We may suppose that $\ell < \ell_0$ because otherwise the statement is trivial. Thus t^ℓ is the greatest common divisor of $p(t)$ and t^{ℓ_0}, and so there exist polynomials $g_1(t), g_2(t)$ such that $p(t)g_1(t) + t^{\ell_0}g_2(t) = t^\ell$. Now $s^w p(t) + h(s,t) \in I$ and $t^{\ell_0} \in I$ so

$$(s^w p(t) + h(s,t))\, g_1(t) + s^w t^{\ell_0} g_2(t) = s^w t^\ell + h(s,t) g_1(t)$$

is also in I, that is choosing $\hat{h}(s,t) = h(s,t)g_1(t)$ will do. □

The 'shape' of the lex reduced Gröbner basis of our ideals can now be formulated as follows.

Theorem 4.3.2. *Let $I \trianglelefteq \mathbb{F}[s,t]$ be an ideal such that $t \in \sqrt{I}$. Put $\ell_w = \min\{\ell : s^w t^\ell \in \mathrm{Lm}(I)\}$ for ($w = 0, 1, \dots$), where $\mathrm{Lm}(I)$ is understood with respect to the lex order induced by $t \prec s$. If $g(s,t) \in I$ and $\mathrm{lm}(g) = s^w t^{\ell_w}$ then $g(s,t) = c \cdot s^w t^{\ell_w} + h(s,t)$ for some $c \in \mathbb{F}$, $h(s,t) \in \mathbb{F}[s,t]$ such that $\deg_s(h) < w$ and t^{ℓ_w} divides $h(s,t)$.*

Proof. It is clear that $\ell_0 \geq \ell_1 \geq \dots$ so—since I contains a power of t—all ℓ_w is finite.

Let $g \in I$ be a polynomial with $\operatorname{lm}(g) = s^w t^{\ell_w}$. Collecting together in $s^w p(t)$ the terms divisible with s^w we get $g(s,t) = s^w p(t) + h(s,t)$ to which one can apply Theorem 4.3.1. By the minimality of ℓ_w, we have that $p(t)$ is $c \cdot t^{\ell_w}$ for some $c \in \mathbb{F}$, thus $g(s,t) = c \cdot s^w t^{\ell_w} + h(s,t)$, and $\deg_s(h) < w$.

We shall show that t^{ℓ_w} divides $h(s,t)$ by induction on w. If $w = 0$ then h can only be 0. Suppose that the statement is true for $w' < w$ and suppose for contradiction that h is not divisible with t^{ℓ_w}. Let $v \in \mathbb{N}$ be maximal such that $s^v t^\ell$ is a monomial of h and $\ell < \ell_w$. We know that $v \leq \deg_s(h) < w$, so $\ell_v \geq \ell_w$. Let g_v be in I and $\operatorname{lm}(g_v) = s^v t^{\ell_v}$, so by the induction hypothesis we know that t^{ℓ_v} divides g_v.

Consider the polynomial $g(s,t) \cdot t^{\ell_v - \ell_w} \in I$ and reduce it with g_v to get the polynomial $\hat{g}$. There is a monomial $s^v t^{\ell + \ell_v - \ell_w}$ in $g_w(s,t) \cdot t^{\ell_v - \ell_w}$, which cannot be cancelled in the reduction, since $\ell + \ell_v - \ell_w < \ell_v$ but every monomial of g_v is divisible with t^{ℓ_v}. Thus $\hat{g} \neq 0$ and if $\operatorname{lm}(\hat{g}) = s^{v'} t^{\ell'}$ then $v' \geq v$. But this gives $\ell' < \ell_v$ since otherwise $s^{v'} t^{\ell'}$ could have been reduced with g_v, which also means that $s^{v'} t^{\ell'}$ is a monomial of $g(s,t) \cdot t^{\ell_v - \ell_w}$. Thus by the maximality of v we have $v = v'$ and so $s^v t^{\ell'} \in \operatorname{Lm}(I)$ a contradiction to the definition of ℓ_v as $\ell' < \ell_v$. □

We benefit from this statement in the n variable case as follows. Recall that $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} = x_1^{w_1} \dots x_{n-2}^{w_{n-2}}$.

Corollary 4.3.3. *Assume that $n \geq 2$, $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $x_n \in \sqrt{I}$ and that*

$$\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p(x_{n-1}, x_n) - h(\widetilde{\mathbf{x}}, x_{n-1}, x_n) \in I$$

with $h(\mathbf{x}) \prec \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}}$. Then there are polynomials $\hat{h}(\mathbf{x}), \hat{p}(x_{n-1}, x_n)$ such that

$$\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} \hat{p}(x_{n-1}, x_n) x_n^{w_n} - \hat{h}(\widetilde{\mathbf{x}}, x_{n-1}, x_n) \in I,$$

$\hat{h}(\mathbf{x}) \prec \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}}$ and $\operatorname{lm}(\hat{p}) = x_{n-1}^{w_{n-1}}$, where $\operatorname{lm}(p) = x_{n-1}^{w_{n-1}} x_n^{w_n}$.

Proof. Set

$$I_{\widetilde{\mathbf{w}}} = \left\{ g \in \mathbb{F}[x_{n-1}, x_n] \ : \ \exists \hat{h} \in \mathbb{F}[\mathbf{x}] \text{ such that } \hat{h} \prec \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} \text{ and } \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} g - \hat{h} \in I \right\}.$$

Obviously $I_{\widetilde{\mathbf{w}}}$ is an ideal in $\mathbb{F}[x_{n-1}, x_n]$ and $x_n^\ell \in I_{\widetilde{\mathbf{w}}}$ if $x_n^\ell \in I$. Since $p \in I_{\widetilde{\mathbf{w}}}$, there is a $g \in I_{\widetilde{\mathbf{w}}}$, whose leading monomial divides $\operatorname{lm}(p)$, say $\operatorname{lm}(g) \cdot x_{n-1}^{u_{n-1}} x_n^{u_n} = x_{n-1}^{w_{n-1}} x_n^{w_n}$ and which is in the reduced Gröbner basis of $I_{\widetilde{\mathbf{w}}}$. Theorem 4.3.2 applies to $I_{\widetilde{\mathbf{w}}}$ so $g(x_{n-1}, x_n) \cdot x_{n-1}^{u_{n-1}} x_n^{u_n}$ is divisible with $x_n^{w_n}$. Set $\hat{p} = \frac{g \cdot x_{n-1}^{u_{n-1}} x_n^{u_n}}{x_n^{w_n}}$. Then $\operatorname{lm}(\hat{p}) = x_{n-1}^{w_{n-1}}$, and $\hat{p} \cdot x_n^{w_n} \in I_{\widetilde{\mathbf{w}}}$, which guarantees the required properties of $\hat{p}$. □

4.3.2 The game for almost general points

Without forgetting the ultimate goal of this section (to prove $\operatorname{Stan}(I) = \operatorname{Sm}(I)$ for certain ideals) we show two statements about leading monomials of some product ideals, which actually will be crucial in the proof of the main theorem.

Proposition 4.3.4. *Suppose that I_1 and I_2 are zero dimensional splitting ideals such that their points can be distinguished by their last coordinate (that is if $\mathbf{y}$ is a point of I_1 and $\mathbf{z}$ is a point of I_2 then $y_n \neq z_n$).*
If $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{m_1} \in \operatorname{Lm}(I_1)$ and $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{m_2} \in \operatorname{Lm}(I_2)$ then $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{m_1+m_2} \in \operatorname{Lm}(I_1 I_2)$.

Proof. For every $\mathbf{y} \in \mathbb{F}^n$ associated to I_1, the primary component of I_1 corresponding to $\mathbf{y}$ is $\langle x_1 - y_1, \ldots, x_n - y_n \rangle$-primary and thus contains a polynomial $(x_n - y_n)^{c_{\mathbf{y}}}$ for some $c_{\mathbf{y}} \in \mathbb{N}$. Multiplying these together, we get a polynomial $f_1(x_n) \in I_1$. Similarly we have $f_2(x_n) \in I_2$. As the irreducible components of $f_1(x_n)$ are of the form $x_n - y_n$, where y_n is a possible last coordinate of a point of I_1, it follows that f_1 and f_2 are relatively prime polynomials. Therefore there exist $g_1(x_n), g_2(x_n) \in \mathbb{F}[x_n]$ such that

$$1 - f_1(x_n) g_1(x_n) - f_2(x_n) g_2(x_n) = 0. \tag{4.4}$$

We also have two polynomials $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} p_j(x_n) - h_j(\mathbf{x}) \in I_j$ $(j = 1, 2)$ such that $\deg(p_j) = m_j$ and $h_j(\mathbf{x}) \prec \overline{\mathbf{x}}^{\overline{\mathbf{w}}}$. Such polynomials do exist since $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{m_j} \in \operatorname{Lm}(I_j)$, hence in any polynomial showing this fact we can collect together the terms divisible with $\overline{\mathbf{x}}^{\overline{\mathbf{w}}}$ in a polynomial $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} p(x_n)$, and put every other term in $-h(\mathbf{x})$.

Multiplying (4.4) with $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} p_1(x_n) p_2(x_n)$ we get

$$\begin{aligned} \overline{\mathbf{x}}^{\overline{\mathbf{w}}} p_1(x_n) p_2(x_n) - \overline{\mathbf{x}}^{\overline{\mathbf{w}}} p_2(x_n) f_1(x_n) p_1(x_n) g_1(x_n) - \\ \overline{\mathbf{x}}^{\overline{\mathbf{w}}} p_1(x_n) f_2(x_n) p_2(x_n) g_2(x_n) = 0 \end{aligned}$$

Note that $\left(\overline{\mathbf{x}}^{\overline{\mathbf{w}}} p_2(x_n) - h_2(\mathbf{x})\right) f_1(x_n) \in I_1 I_2$ and $\left(\overline{\mathbf{x}}^{\overline{\mathbf{w}}} p_1(x_n) - h_1(\mathbf{x})\right) f_2(x_n) \in I_1 I_2$, and so

$$f(\mathbf{x}) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} p_1(x_n) p_2(x_n) - h_2(\mathbf{x}) f_1(x_n) p_1(x_n) g_1(x_n) - h_1(\mathbf{x}) f_2(x_n) p_2(x_n) g_2(x_n)$$

is in $I_1 I_2$. The leading monomial of f is $\operatorname{lm}(f) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{\deg(p_1 p_2)} = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{m_1+m_2}$ using that $h_1(\mathbf{x}) \prec \overline{\mathbf{x}}^{\overline{\mathbf{w}}}$ (and $h_2(\mathbf{x}) \prec \overline{\mathbf{x}}^{\overline{\mathbf{w}}}$), so the same is true for $h_1 f_2 p_2 g_2$ (and $h_2 f_1 p_1 g_1$) by the properties of the lexicographic order. This proves the statement. □

The next proposition (and its proof as well) looks similar, except that we have to apply Corollary 4.3.3 in the proof, which was not at all trivial to verify. In fact, the reason why Stan monomials are in general not equal to standard monomials is that the straightforward generalization of these propositions is not true (see Example 4.4.1).

Proposition 4.3.5. *Suppose that I_1 and I_2 are zero dimensional splitting ideals such that their points have all the same last coordinates but they can be distinguished by their second to the last coordinate (that is if $\mathbf{y}$ is a point of I_1 and $\mathbf{z}$ is a point of I_2 then $y_n = z_n$ and $y_{n-1} \neq z_{n-1}$).*
If $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m_1} x_n^{w_n} \in \mathrm{Lm}\,(I_1)$ and $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m_2} x_n^{w_n} \in \mathrm{Lm}\,(I_2)$ then $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m_1+m_2} x_n^{w_n} \in \mathrm{Lm}\,(I_1 I_2)$.

Proof. Without loss of generality, we may suppose that the common last coordinate of the points of I_1 and I_2 is 0, since a change of variables $x'_n = x_n - y_n$ does not affect the standard monomials.

The ideal I_1 has dimension zero, thus a power of x_n is in I_1, that is it satisfies the conditions of Corollary 4.3.3. Applying our usual trick, any polynomial which shows $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m_1} x_n^{w_n} \in \mathrm{Lm}\,(I_1)$ can be written in the form $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p(x_{n-1}, x_n) - h(\mathbf{x})$ from which by Corollary 4.3.3 we get that there exist polynomials such that $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p_1(x_{n-1}, x_n) x_n^{w_n} - h_1(\mathbf{x}) \in I_1$, $\mathrm{lm}\,(p_1) = x_{n-1}^{m_1}$ and $h_1 \prec \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}}$. Similarly we have $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p_2(x_{n-1}, x_n) x_n^{w_n} - h_2(\mathbf{x}) \in I_2$, $\mathrm{lm}\,(p_2) = x_{n-1}^{m_2}$ and $h_2 \prec \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}}$.

Exactly as in the proof of Proposition 4.3.4, there are relatively prime polynomials $f_1(x_{n-1}) \in I_1$ and $f_2(x_{n-1}) \in I_2$ and $g_1(x_{n-1}), g_1(x_{n-1}) \in \mathbb{F}[x_{n-1}]$ such that

$$1 - f_1(x_{n-1}) g_1(x_{n-1}) - f_2(x_{n-1}) g_2(x_{n-1}) = 0$$

Multiplying this with $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p_1(x_{n-1}) p_2(x_{n-1}) x_n^{w_n}$ we get

$$\begin{gathered} \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p_1(x_{n-1}, x_n) p_2(x_{n-1}, x_n) x_n^{w_n} - \\ \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p_2(x_{n-1}, x_n) x_n^{w_n} f_1(x_{n-1}) p_1(x_{n-1}, x_n) g_1(x_{n-1}) - \\ \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p_1(x_{n-1}, x_n) x_n^{w_n} f_2(x_{n-1}) p_2(x_{n-1}, x_n) g_2(x_{n-1}) = 0. \end{gathered}$$

As we see that the polynomials $\left(\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p_2(x_{n-1}, x_n) x_n^{w_n} - h_2(\mathbf{x})\right) f_1(x_{n-1})$ and $\left(\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p_1(x_{n-1}, x_n) x_n^{w_n} - h_1(\mathbf{x})\right) f_2(x_{n-1})$ are both in $I_1 I_2$, we have that

$$\begin{gathered} f(\mathbf{x}) := \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} p_1(x_{n-1}, x_n) p_2(x_{n-1}, x_n) x_n^{w_n} - \\ h_2(\mathbf{x}) f_1(x_{n-1}) p_1(x_{n-1}, x_n) g_1(x_{n-1}) - h_1(\mathbf{x}) f_2(x_{n-1}) p_2(x_{n-1}, x_n) g_2(x_{n-1}) \end{gathered}$$

is in $I_1 I_2$. The leading monomial of f is $\mathrm{lm}\,(f) = \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} \cdot \mathrm{lm}\,(p_1 p_2) \cdot x_n^{w_n} = \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m_1+m_2} x_n^{w_n}$ since by $h_1(\mathbf{x}) \prec \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}}$ (and $h_2(\mathbf{x}) \prec \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}}$) we have $h_1 f_2 p_2 g_2 \prec \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}}$ (and $h_2 f_1 p_1 g_1 \prec \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}}$). The proposition follows. □

Theorem 4.3.6. *If I is a zero dimensional splitting ideal, and for all different points $\mathbf{y}, \mathbf{z}$ of I either $y_n \neq z_n$ or $y_{n-1} \neq z_{n-1}$ then*

$$\operatorname{Stan}(I) = \operatorname{Sm}(I).$$

In particular if $n = 2$, then the standard and the Stan monomials are the same for every zero dimensional splitting ideal.

Proof. Suppose that $n \geq 2$. Let the primary decomposition be $I = \prod_{\mathbf{y} \in \mathbb{F}^n} Q_{\mathbf{y}}$ and for $y, y' \in \mathbb{F}$ put

$$I_y = \prod_{\substack{\mathbf{y} \in \mathbb{F}^n \\ y_n = y}} Q_{\mathbf{y}} \text{ and } I_{y,y'} = \prod_{\substack{\mathbf{y} \in \mathbb{F}^n \\ y_n = y, y_{n-1} = y'}} Q_{\mathbf{y}}.$$

In fact, the assumption on I implies that $I_{y,y'}$ is either $\mathbb{F}[\mathbf{x}]$ or a primary component of I.

A game $\operatorname{Lex}(I_{y,y'}; \mathbf{w})$ is quite simple. If $I_{y,y'}$ is primary, then there is only one point $\mathbf{y}$ of $I_{y,y'}$, so if Lea guesses for the coordinates of $\mathbf{y}$ in each round respectively, then the result vector $\mathbf{r}$ is either $\mathbf{w}$ (if Stan's point was $\mathbf{y}$) or $\mathbf{0}$ (if it was any other). But in the latter case Lea wins the game as $\mathbf{x}^{\mathbf{0}} = 1 \in \operatorname{Lm}(\mathbb{F}[\mathbf{x}])$. Therefore we see that $\operatorname{Stan}(I_{y,y'}) = \operatorname{Sm}(I_{y,y'})$ (and obviously $\operatorname{Stan}(\mathbb{F}[\mathbf{x}]) = \emptyset = \operatorname{Sm}(\mathbb{F}[\mathbf{x}])$).

We now prove that $\operatorname{Stan}(I_y) = \operatorname{Sm}(I_y)$. As $|\operatorname{Stan}(I_y)| = |\operatorname{Sm}(I_y)|$ (see Proposition 4.4.2 in the next section), it is enough to show that the left hand side contains the right.

Fix a $\mathbf{w} \in \mathbb{N}^n$ such that Lea can win the game $\operatorname{Lex}(I_y; \mathbf{w})$. We have to see that $\mathbf{x}^{\mathbf{w}} \in \operatorname{Lm}(I_y)$. Set

$$m_{y,y'} = \min\left\{m \in \mathbb{N} \,:\, \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m} x_n^{w_n} \in \operatorname{Lm}(I_{y,y'})\right\}.$$

In the first round Lea guesses y as this is the only possible last coordinate of the points of I_y. If $w_{n-1} < \sum_{y' \in \mathbb{F}} m_{y,y'}$, then in the next round there exists a y' for which Lea can guess only $m < m_{y,y'}$ times. We claim that if Stan picks such a point of I_y then Lea cannot win the game. This contradiction will yield $w_{n-1} \geq \sum_{y' \in \mathbb{F}} m_{y,y'}$. The result vector is now $(*, \ldots, *, m, w_n)$, which means that Lea can win this game if and only if she can win $\operatorname{Lex}(I_{y,y'}; (\widetilde{\mathbf{w}}, m, w_n))$ We have just seen that this latter is equivalent to $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m} x_n^{w_n} \in \operatorname{Lm}(I_{y,y'})$, which is not the case as $m < m_{y,y'}$.

Therefore we have $w_{n-1} \geq \sum\limits_{y' \in \mathbb{F}} m_{y,y'}$. We now apply Proposition 4.3.5 to get from $\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{m_{y,y'}} x_n^{w_n} \in \operatorname{Lm}(I_{y,y'})$ that

$$\widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{\sum_{y' \in \mathbb{F}} m_{y,y'}} x_n^{w_n} \in \operatorname{Lm}\left(\prod_{y' \in \mathbb{F}} I_{y,y'}\right) = \operatorname{Lm}(I_y).$$

Therefore also $\mathbf{x}^{\mathbf{w}} = \widetilde{\mathbf{x}}^{\widetilde{\mathbf{w}}} x_{n-1}^{w_{n-1}} x_n^{w_n} \in \operatorname{Lm}(I_y)$. This proves $\operatorname{Stan}(I_y) = \operatorname{Sm}(I_y)$.

To show $\operatorname{Stan}(I) = \operatorname{Sm}(I)$ we will do essentially the same thing. Again fix a $\mathbf{w} \in \mathbb{N}^n$ such that Lea wins $\operatorname{Lex}(I; \mathbf{w})$. Put

$$m_y = \min\left\{m \in \mathbb{N} \,:\, \overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^m \in \operatorname{Lm}(I_y)\right\}.$$

If $w_n < \sum\limits_{y \in \mathbb{F}} m_y$ then there has to be a y that is guessed by Lea in the first round only $m < m_y$ times. Lea can still win the game, thus she can win $\operatorname{Lex}(I_y; (\overline{\mathbf{w}}, m))$ as well which implies $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^m \in \operatorname{Lm}(I_y)$, a contradiction to the minimality of m_y.

Using Proposition 4.3.4 we have

$$\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{\sum_{y \in \mathbb{F}} m_y} \in \operatorname{Lm}\left(\prod_{y \in \mathbb{F}} I_y\right) = \operatorname{Lm}(I)$$

and by $w_n \geq \sum\limits_{y \in \mathbb{F}} m_y$ also $\mathbf{x}^{\mathbf{w}} = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{w_n} \in \operatorname{Lm}(I)$.

We conclude that $\operatorname{Stan}(I) \supseteq \operatorname{Sm}(I)$ which yields our statement. □

4.4 The general case

The standard monomials and Stan monomials are not the same in general.

Example 4.4.1. Let $I \trianglelefteq \mathbb{F}[x_1, x_2, x_3]$ be the product of the primary ideals $Q_{(0,0,0)} = (x_1^3, x_2^2, x_3^3, x_1x_2 + x_3^2)$, $Q_{(1,0,0)} = ((x_1-1)^3, x_2^2, x_3^3, (x_1-1)x_2 + x_3^2)$. It can be checked that $x_1^2x_2$ is a standard monomial, but not a Stan monomial, while $x_1^4x_3^2$ is a Stan monomial and a leading monomial at the same time. (To see this, it may be useful that $\{x_1^3, x_2^2, x_3^3, x_1x_2 + x_3^2, x_2x_3^2, x_1^2x_3^2\}$ is the reduced Gröbner basis of $Q_{(0,0,0)}$, and we get that of $Q_{(1,0,0)}$ if we replace x_1 with $x_1 - 1$.)

Suppose that $I = \prod_{\mathbf{y}\in\mathbb{F}^n} Q_{\mathbf{y}}$ with $Q_{\mathbf{y}}$ being a primary ideal corresponding to $\mathbf{y}$. For each $\mathbf{y} \in \mathbb{F}^n$ set

$$Q'_{\mathbf{y}} = \{(\mathbf{x}-\mathbf{y})^{\mathbf{w}} \ : \ \mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(Q_{\mathbf{y}})\}$$

and let $I' = \prod_{\mathbf{y}\in\mathbb{F}^n} Q'_{\mathbf{y}}$. Clearly $Q'_{\mathbf{y}}$ is a $\mathbf{y}$-monomial primary ideal, thus I' is the vanishing ideal of a finite multiset.

An immediate consequence of the definition is that the games $\mathrm{Lex}\,(I;\mathbf{w})$ and $\mathrm{Lex}\,(I';\mathbf{w})$ are the same, more precisely $\mathrm{Stan}\,(I) = \mathrm{Stan}\,(I')$, as the standard monomials of $Q_{\mathbf{y}}$ and $Q'_{\mathbf{y}}$ coincide.

By Theorem 4.2.1 we have $\mathrm{Stan}\,(I') = \mathrm{Sm}\,(I')$, thus

$$\mathrm{Stan}\,(I) = \mathrm{Sm}\,(I')$$

for every splitting ideal I.

We conjecture that just like $\mathrm{Sm}\,(I)$, also $\mathrm{Stan}\,(I) = \mathrm{Sm}\,(I')$ is a linear basis of the vector space $\mathbb{F}[\mathbf{x}]/I$. At least we have the following simple observation.

Proposition 4.4.2. *Let I be an arbitrary zero dimensional splitting ideal. Then*

$$|\mathrm{Stan}\,(I)| = \dim_{\mathbb{F}}(\mathbb{F}[\mathbf{x}]/I).$$

Proof. Using Lemma 2.2.12 we get

$$|\mathrm{Stan}\,(I)| = |\mathrm{Sm}\,(I')| = \sum_{\mathbf{y}\in\mathbb{F}^n} \left|\mathrm{Sm}\left(Q'_{\mathbf{y}}\right)\right| = \sum_{\mathbf{y}\in\mathbb{F}^n} |\mathrm{Sm}\,(Q_{\mathbf{y}})| = |\mathrm{Sm}\,(I)|,$$

which, by Theorem 2.1.14, yields the desired equality. □

One could think that $\mathrm{Sm}\,(I)$ may be a linear basis of $\mathbb{F}[\mathbf{x}]/I'$, but it is not true. On the contrary, computational experiments suggest that, as a subset of the linear space $\mathbb{F}[\mathbf{x}]/I'$, the set $\mathrm{Sm}\,(I)$ has as low rank as it can have, namely $\mathrm{Sm}\,(I)$ and $\mathrm{Sm}\,(I) \cap \mathrm{Sm}\,(I')$ generate the same linear subspace of $\mathbb{F}[\mathbf{x}]/I'$.

4.5 Computing the Stan monomials

Here we introduce a fast combinatorial algorithm to compute the Stan monomials of any zero dimensional splitting ideal, provided that the primary decomposition

$$I = \prod_{\mathbf{y}\in\mathbb{F}^n} Q_{\mathbf{y}}$$

and $\mathrm{Sm}\,(Q_{\mathbf{y}})$ for all $\mathbf{y} \in \mathbb{F}^n$ is known. Actually, we will only make use of the list of the points of I, and $\mathrm{Sm}\,(Q_{\mathbf{y}})$ for all point $\mathbf{y}$ of I.

We have seen that the Stan monomials of $I(\mathcal{V})$ and I are the same, if $\mathcal{V}$ is defined by $\mathcal{V}(\mathbf{y}) = \{\mathbf{w} : \mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(Q_{\mathbf{y}})\}$. From now on, we suppose that $I = I(\mathcal{V})$. Note that in this case, $\mathrm{Sm}\,(Q_{\mathbf{y}}) = \{\mathbf{x}^{\mathbf{w}} : \mathbf{w} \in \mathcal{V}(\mathbf{y})\}$, therefore knowing all $\mathrm{Sm}\,(Q_{\mathbf{y}})$ and $\mathcal{V}$ is equivalent.

The importance of our algorithm is that by Theorem 4.2.1 in fact we get $\mathrm{Sm}\,(I(\mathcal{V}))$. Such an algorithm was first given by Cerlienco and Mureddu [15]. Here we present a computationally more efficient variant. The method in [15] is combinatorial in the sense that algebraic operations in $\mathbb{F}$ are not needed. Algorithm MB in [15] determines $\mathrm{Sm}\,(I(\mathcal{V}))$ in an incremental fashion by adding new points and multiplicities to a given multiset and modifying the set of standard monomials accordingly. Implementation details and complexity are not discussed there. It appears that the best implementation of MB takes at least $c\,|\mathcal{V}|^2\,n^2$ steps for some fixed positive c. (See Definition 2.2.11 for the meaning of $|\mathcal{V}|$.)

Here we take a somewhat different approach. First we carry out some preprocessing of $\mathcal{V}$ by building a trie (see below for the definitions or Subsection 6.3 in [33] for more detailed discussion). This way, we organize the relevant information about $\mathcal{V}$ in a data structure which allows afterwards a very fast computation.

The algorithm for the case of vanishing ideals of sets has been implemented in Singular [29], the code is included in the Appendix, and may be downloaded from
`http://www.math.bme.hu/~fbalint/publ/singular.html`

4.5.1 Standard monomials of a trie

First we remind the reader of the definitions related to the data structure trie.

A *trie* is a tree in the graph theoretical sense, with a special vertex called root. We say that a vertex v is on the ith level of the trie if the distance between v and the root is i. In particular, the root is on the 0th level. The children of a vertex v of the ith level are all those vertices on the $(i+1)$st level which are connected to v. As one would expect, if u is a child of v, then v is the parent of u. Vertices which have no child are called leaves. The root has no parent. Here we shall suppose that the leaves of a trie are all on the same level. By the depth of a trie we mean the level of the leaves. If v is a vertex different from the root and u is on the path from v to the root, then v is a *descendant* of u. The subtrie of a trie corresponding to a vertex v contains all descendants of v, and the root of this subtrie is v.

We shall speak about the standard monomials $\mathrm{Sm}\,(T)$ of a trie T in the following sense.

Definition 4.5.1. Suppose that T is a trie of depth n. If T consists of a single root ($n = 0$), then $\mathrm{Sm}\,(T) = \{1\}$. Otherwise, when the depth is $n \geq 1$, we say that a monomial $\mathbf{x}^{\mathbf{w}}$ is in $\mathrm{Sm}\,(T)$ if and only if there exist more than w_n children of the root for which $\overline{\mathbf{x}}^{\overline{\mathbf{w}}}$ is a standard monomial of the corresponding subtrie.

We define the trie $T(\mathcal{V})$ recursively. If $n = 1$ then the root of $T(\mathcal{V})$ has $|\mathcal{V}|$ children, which are all leaves of the trie. If $n > 1$ then $T(\mathcal{V})$ consists of a root whose children are the roots of the tries $T(\mathcal{V}_{y,m})$ for each pair $(y, m) \in \mathbb{F} \times \mathbb{N}$ such that the multiset $\mathcal{V}_{y,m}$ is not empty (that is $\mathcal{V}_{y,m}$ is not constant $\emptyset$ on $\mathbb{F}^{n-1}$).

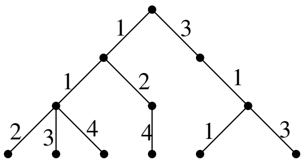


Figure 4.1: The trie $T(V)$ of $V = \{(2, 1, 1), (3, 1, 1), (4, 1, 1), (4, 2, 1), (1, 1, 3), (3, 1, 3)\}$ (where V is understood as a multiset in the straightforward way).

Recall that Theorem 4.2.3 claims that

$$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(\mathcal{V})) \iff w_n < \left|\left\{(y, m) \in \mathbb{F} \times \mathbb{N} \,:\, \overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \mathrm{Sm}\,(I(\mathcal{V}_{y,m}))\right\}\right|.$$

Corollary 4.5.2. *For any nonempty algebraic multiset $\mathcal{V}$, we have*

$$\mathrm{Sm}\,(I(\mathcal{V})) = \mathrm{Sm}\,(T(\mathcal{V})).$$

We will therefore concentrate on computing the standard monomials of tries.

A simple consequence of Corollary 4.5.2, and Proposition 4.2.4 is that

$$\sum_{j=1}^{r} |\mathrm{Sm}\,(T_j)| = |\mathrm{Sm}\,(T)|\,, \tag{4.5}$$

where $T_1, \ldots, T_r$ are the subtries of T corresponding to the children of the root of T. And from this, by easy induction we infer that

$$|\mathrm{Sm}\,(T)| = |\{\text{leaves of } T\}|\,. \tag{4.6}$$

4.5.2 The naive approach

The recursive definition of $\mathrm{Sm}\,(T)$ yields a straightforward recursive algorithm. We shall compute the standard monomials of T' for all subtries T' of T.

For a leaf of T—considering it as a trie T' of depth 0— we set $\mathrm{Sm}\,(T') = \{1\}$. Suppose now that T' is subtrie of T, such that the root of T' is on the $n-i$th level of T. Denote by $T_1, \ldots, T_r$ the subtries of T, corresponding to the children of the root of T'. Assume that $\mathrm{Sm}\,(T_j) \subseteq \mathbb{F}[x_1, \ldots, x_{i-1}]$ is already computed ($j \in [r]$). Consider the following procedure.

```
$S := \emptyset$;
For all $j \in [r]$ and $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} \in \mathrm{Sm}\,(T_j)$ do
        $w := 1 + \max\left(\{\ell \geq 0 \,:\, x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^{\ell} \in S\} \cup \{-1\}\right)$;
        $S := S \cup \{x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^{w}\}$;
endfor;
```

Note that when $i = 1$, then the empty product $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}}$ is defined to be 1.

We claim that the result S is precisely $\mathrm{Sm}\,(T')$. When $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^{w}$ is put in S, then we know that $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^{w-1}$ is already in S (if $w > 0$) implying that there were w occurrences of the monomial $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}}$ in $\mathrm{Sm}\,(T_1), \ldots, \mathrm{Sm}\,(T_{j-1})$. Thus, together with $\mathrm{Sm}\,(T_j)$ there are $w+1$ of those, hence $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^{w}$ is indeed a standard monomial of $\mathrm{Sm}\,(T')$. On the other hand,

$$|S| = \sum_{j=1}^{r} |\mathrm{Sm}\,(T_j)| = |\mathrm{Sm}\,(T')|$$

using equation (4.5), which justifies the claim.

To make this algorithm efficient we have to compute quickly the quantities $\max\{\ell \geq 0 \,:\, x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^{\ell} \in S\}$. In the remainder of this section we will show how one can do this. This will substantially change the outlook of the algorithm as well. The idea to use another trie for this purpose was suggested by Balázs Rácz.

4.5.3 Another try

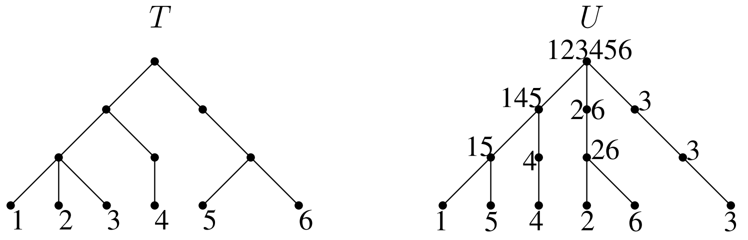
We intend to build a second trie U for the exponent vectors of $\mathrm{Sm}\,(T)$ in the following sense. The children of any vertex are labelled with $0, 1, \ldots$ in turn. Thus a leaf l of U is associated with a vector $\mathbf{w} \in \mathbb{N}^n$, where w_i is the ith label on the path from the root to l. Our goal is to construct U, such that the set of vectors corresponding to leaves of U is the set of the exponent vectors of $\mathrm{Sm}\,(T)$.

We build U level by level. This way, the vertices on the ith level of U will correspond to monomials in variables $x_1, \ldots, x_i$ (or equivalently to vectors from $\mathbb{N}^i$).

Furthermore, the algorithm gives a one-to-one correspondence between leaves of T and U. This is the key point of the algorithm, which can be summarized in an informal way as follows. We put every leaf of T in the root of U at the beginning. Then they will walk down in the trie, each of them to a separate leaf. Actually, they will help us to construct the lower levels of U by showing in which direction they want to go further. And they have a strange nature: if the paths in T from two leaves l_1 and l_2 meets in the $(n - i)$th level, then they want to be in different vertices of U from the ith level, but otherwise they prefer to go to the vertex with the smallest possible number. (Recall that the vertices of U are numbered.) In the following pseudo code of the algorithm we record the current place (vertex) of the leaves of T in an array A.

```
Let $U$ be a tree consisting of a single root $r$;
For $l \in \{$leaves of $T\}$ do $A[l] := r$; endfor;
For $i = 1, \ldots, n$ do
   //We now build the $i$th level of $U$
   For $v \in \{$vertices on the $(n-i)$th level of $T\}$ do
      For $l \in \{$leaves of $T$ which are descendants of $v\}$ do
         $b[A[l]] := 0$;
      endfor;
      For $l \in \{$leaves of $T$ which are descendants of $v\}$ do
         $A[l] :=$ (the child of $A[l]$ with number $b[A[l]]$);
         //If such a child does not exist, we create a new one
         $b[A[l]] := b[A[l]] + 1$;
      endfor;
   endfor;
endfor;
```

The following example gives the result of the algorithm applied to $T = T(V)$ of the set V of Figure 4.1. We numbered the leaves of T to make the assignment and their path from the root visible. However we left out the labels of the vertices of U, as they can be reconstructed easily: number the vertices having the same parent with $0, 1, \ldots$ from left to right.



As we will soon prove, the trie U that we finally get by the algorithm is the trie of the exponent vectors of $\mathrm{Sm}\,(T(V))$. Thus the figure shows that $\mathrm{Sm}\,(T(V)) = \{1, x_3, x_2, x_1, x_1x_3, x_1^2\}$. The monomials are listed in the left-to-right order of the leaves of U.

To prove the correctness of the algorithm, we have to verify three basic properties of the paths of the leaves of T in U. To be more precise, by the trace of l, we mean the set of those vertices of U in which l sometimes have been (that is, the different values of $A[l]$) during the algorithm.

Lemma 4.5.3. *The path of l forms a path from the root to a leaf of U.*

Proof. This is trivial as at first we assigned l to the root and in every phase l moved to a child of its current place. □

Lemma 4.5.4. *If two leaves l_1 and l_2 of T have been in the same vertex on the ith level of U, then the ancestors of l_1 and l_2 on the $(n-i)$th level of T are different.*

Proof. Suppose by contradiction that l_1 and l_2 have a common ancestor v on the $(n-i)$th level of T and that l_1 and l_2 have been in the same vertex on the ith level of U. By Lemma 4.5.3 we know that l_1 and l_2 have been in the same vertex on the $(i-1)$th level of U as well. That is, when building the ith level of U and working in the

`For` $v \in \{$`vertices on the` $(n-i)$ `level of` $T\}$ `do`

loop with the common ancestor v, then we have $A[l_1] = A[l_2]$, hence the counter b should have separated them on the ith level of U. □

Lemma 4.5.5. *Let l be a leaf of T and for some $0 \leq i \leq n$ let v be the ancestor of l on the $(n-i)$th level of T. Suppose that the trace of l in U from the root to the ith level leads through vertices labelled with $w_1, \ldots, w_i$ respectively. Then*

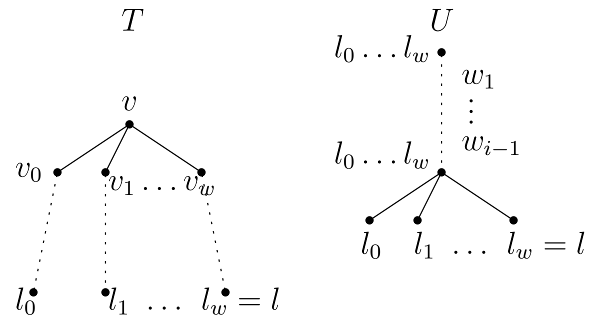
$$x_1^{w_1} \ldots x_i^{w_i} \in \mathrm{Sm}\,(T_v)\,,$$

where T_v is the subtrie of T corresponding to v.

Proof. We use induction on i. If $i = 0$ then the statement is immediate.

Suppose that the claim is true for the $(i-1)$st level of U, and let $w_1 \dots w_{i-1} w$ be the labels of the path in U of a leaf l of T.

By the algorithm, there exist leaves $l_0, l_1, \dots, l_{w-1}, l_w = l$ of T, such that they all have been to the vertex $w_1 \dots w_{i-1}$ of U (the place of l in the $(i-1)$th level), and their common ancestor on the $(n-i)$th level of T is v. Denote the ancestor of l_j on the $(n-i+1)$st level of T by v_j. By Lemma 4.5.4, the v_j are pairwise different. The induction hypothesis gives that $x_1^{w_1} \dots x_{i-1}^{w_{i-1}} \in \operatorname{Sm}(T_{v_j})$ for $j = 0, \dots, w$, hence $x_1^{w_1} \dots x_{i-1}^{w_{i-1}} x_i^w \in \operatorname{Sm}(T_v)$ by the definition of $\operatorname{Sm}(T_v)$.



□

We now have everything to prove the correctness of the algorithm.

Theorem 4.5.6. *The trie U given by the above algorithm is the trie of the exponent vectors of* $\operatorname{Sm}(T)$.

Proof. On the one hand, we apply Lemma 4.5.5 with $i = n$: This implies that every monomial corresponding to a leaf of U is in $\operatorname{Sm}(T)$.

On the other hand, since the root of T is a common ancestor for every leaf of T, Lemma 4.5.4 yields that every leaf of U contains exactly one leaf l of T. This gives that the number of leaves of U and T is the same, and by equation (4.6), this also equals to $|\operatorname{Sm}(T)|$, proving our claim. □

4.5.4 Running time

To sum up, the algorithm that computes $\operatorname{Sm}(I(\mathcal{V}))$ consists of two major stages. We first construct the trie $T(\mathcal{V})$, and then use the above algorithm to compute $\operatorname{Sm}(T(\mathcal{V})) = \operatorname{Sm}(I(\mathcal{V}))$.

Throughout we use the *uniform cost* measure (Section 1.3 in [2]) to discuss bounds on the running time of the algorithms. In this setting the cost of an elementary instruction is 1. We assume that reading or writing an element of $\mathbb{F}$ and testing the equality of two elements of $\mathbb{F}$ are elementary operations and hence have unit costs. We need no arithmetic operations in $\mathbb{F}$.

Proposition 4.5.7. *Let m be the number of leaves of T. When T is given, the above algorithm computes $\mathrm{Sm}\,(T)$ in $O(nm)$ time.*

Proof. Consider the two `For` loops

```
For $v \in$ {vertices on the $(n-i)$th level of $T$} do
    For $l \in$ {leaves of $T$ which are descendants of $v$} do.
```

As every leaf l of T has exactly one ancestor v on the $(n-i)$th level of T, we work with every l only once, and so building of the ith level of U requires $O(m)$ steps. □

We have not treated yet the algorithm to build the trie $T(\mathcal{V})$ of $\mathcal{V}$. This can be done in an incremental fashion. We start with an empty trie and insert points and multiplicities of $\mathcal{V}$ in turn. We can add either a new point $\mathbf{y}$ with a single multiplicity set $\{\mathbf{0}\}$, or an already existing point $\mathbf{y}$, with a new multiplicity $\mathbf{m}$, such that $\{\mathbf{m}\} \cup \mathcal{V}(\mathbf{y})$ is still a downset. Adding the new element $(\mathbf{y}, \mathbf{m})$ to the structure implies the creation of a new root-to-leaf path in $T(\mathcal{V})$. It is an easy exercise to prove that such a step can be done in $O(nr)$ time, where r is the maximum number of children a vertex of $T(\mathcal{V})$ has. It follows that constructing $T(\mathcal{V})$ requires $O\left(|\mathcal{V}|\, nr\right)$ elementary steps. We have therefore proven

Theorem 4.5.8. *Let r be the maximal number of children of the vertices of $T(\mathcal{V})$. Then the algorithm presented in this section computes $\mathrm{Sm}\,(I(\mathcal{V}))$ in $O\left(|\mathcal{V}|\, nr\right)$ time. A rough upper bound is $O\left(|\mathcal{V}|^2\, n\right)$.*

Chapter 5

Applications of the Game – a warm up

The Lex Game is a powerful tool in the Gröbner theory of zero dimensional ideals. We shall illustrate this through several examples in the remaining of the thesis. While Chapter 6 is devoted to a single subject—extremal combinatorics—, this present chapter contains three different topics: applications to the theory of Gröbner bases, to a different field of algebra, and to algebraic combinatorics.

We shall examine first the dependence of the lex standard monomials and Gröbner bases of vanishing ideals of finite multisets from the base field. Corollary 5.1.1 in a less general form appeared in our paper [20] on the Lex Game, while Corollary 5.1.2 is not yet published.

Section 5.2 deals with a generalization of the fundamental theorem of symmetric polynomials. The approach is a simplified version (with the aid of the Lex Game, of course) of that of Hegedűs, Nagy and Rónyai [31].

We then start to investigate ideals associated to set families and include a well-known theorem which establishes a connection between Hilbert functions and inclusion matrices. A similar theorem is used in Section 5.4, where we compute the rank of a certain inclusion matrix modulo p. The original method of [26] to obtain this rank is again simplified by the Lex Game. This, as well as the application to symmetric polynomials is taken from our survey paper [22].

In the last three sections, we shall work with ideals of finite sets of points. Recall that if $V \subseteq \mathbb{F}^n$ is finite, then the primary components of $I(V)$ are maximal ideals, which in terms of the game means that it is enough for Lea to find out only one coordinate of $\mathbf{y}$ if $\mathbf{y} \in V$, and Lea is the winner also if $\mathbf{y} \notin V$.

5.1 Properties of lex Gröbner bases

Here we shall examine some immediate consequences of the Lex Game for vanishing ideals of finite multisets $\mathcal{V}$.

It follows from Theorem 4.2.1 that the standard monomials are largely independent of the base field $\mathbb{F}$, and of the precise embedding of $\mathcal{V}$ into $\mathbb{F}^n$. As we consider more than one field here, let us temporarily put $I_{\mathbb{F}}(\mathcal{V})$ for the ideal $I(\mathcal{V})$ in $\mathbb{F}[\mathbf{x}]$.

Corollary 5.1.1. *Let $\mathcal{V}$ be a finite multiset in $\mathbb{F}^n$ and assume that $B_i \subseteq \mathbb{F}$ ($i \in [n]$) are finite sets, such that $B = B_1 \times \cdots \times B_n$ contains all points of $\mathcal{V}$. Let $\hat{\mathbb{F}}$ be any field and suppose that $\varphi_i\colon B_i \to \hat{\mathbb{F}}$ are injective maps for $i \in [n]$. For $\mathbf{y} \in B$, put $\boldsymbol{\varphi}(\mathbf{y}) = (\varphi_1(y_1), \ldots, \varphi_n(y_n))$. The image of $\mathcal{V}$ is then $\hat{\mathcal{V}}$, where $\hat{\mathcal{V}}(\boldsymbol{\varphi}(\mathbf{y})) = \mathcal{V}(\mathbf{y})$, and if $\hat{\mathbf{y}} \in \hat{\mathbb{F}}^n$ is not in the image of $\boldsymbol{\varphi}$, then $\hat{\mathcal{V}}(\hat{\mathbf{y}}) = \emptyset$. Then*

$$\mathrm{Sm}_{\mathrm{lex}}\left(I_{\mathbb{F}}(\mathcal{V})\right) = \mathrm{Sm}_{\mathrm{lex}}\left(I_{\hat{\mathbb{F}}}\left(\hat{\mathcal{V}}\right)\right).$$

In particular, if all points of $\mathcal{V}$ are in $\{0,1\}^n$, then $\mathrm{Sm}_{\mathrm{lex}}\left(I_{\mathbb{F}}(\mathcal{V})\right)$ is independent of the base field $\mathbb{F}$.

Proof. The standard monomials of the primary components of the two corresponding ideals are the same by

$$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\left(Q_{\mathbf{y}}\right) \iff \mathbf{w} \in \mathcal{V}(\mathbf{y}) \iff \mathbf{w} \in \hat{\mathcal{V}}(\boldsymbol{\varphi}(\mathbf{y})) \iff \mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\left(Q_{\boldsymbol{\varphi}(\mathbf{y})}\right),$$

using Corollary 2.2.9. Therefore the $\mathrm{Lex}\left(\mathcal{V};\mathbf{w}\right)$ game is essentially the same as the $\mathrm{Lex}\left(\hat{\mathcal{V}};\mathbf{w}\right)$ game, since we have changed only the names of the coordinates to guess (bijectively).

The second part follows from the first, because $0 \neq 1$ in any field $\mathbb{F}$. □

The second part of the corollary concerning (not multi-) sets $V \subseteq \{0,1\}^n$ has been proven in [5] by a different method.

We now show that the reduced lexicographic Gröbner basis of $I_{\mathbb{F}}(\mathcal{V})$ for a multiset with points from $\{0,1\}^n$ is essentially the same over any field. We remark that this can be generalized with some restrictions to finite multisets with more than two integer coordinate values.

If $f \in \mathbb{Z}[\mathbf{x}]$, then for all fields $\mathbb{F}$ of characteristic 0 we clearly have $f \in \mathbb{F}[\mathbf{x}]$, but also if the characteristic of $\mathbb{F}$ is $p > 0$, we can still consider f as an element of $\mathbb{F}[\mathbf{x}]$ by reducing its integer coefficients modulo p.

Corollary 5.1.2. *If the points of $\mathcal{V}$ are in $\{0,1\}^n$, then the reduced lex Gröbner basis G of $I_{\mathbb{Q}}(\mathcal{V})$ has integer coefficients. For an arbitrary field $\mathbb{F}$, the set in $\mathbb{F}[\mathbf{x}]$ corresponding to G is the reduced lex Gröbner basis of the ideal $I_{\mathbb{F}}(\mathcal{V})$.*

Proof. Let $\mathbf{x}^{\mathbf{w}} + g(\mathbf{x})$ be an element of the reduced lex Gröbner basis of $I_{\mathbb{Q}}(\mathcal{V})$, where $g \in \mathbb{Q}[\mathbf{x}]$, and every monomial of g is contained in $\mathrm{Sm}\,(I_{\mathbb{Q}}(V))$. Suppose by contradiction that $g \notin \mathbb{Z}[\mathbf{x}]$.

Let z be a minimal positive integer, such that $zg(\mathbf{x})$ has integer coefficients. If a prime p divides z, then the minimality of z implies that not all coefficients of $zg(\mathbf{x})$ are divisible with p. Reduce $zg \in \mathbb{Z}[\mathbf{x}]$ modulo p to get a nonzero polynomial over $\mathbb{F}_p$, which (modulo p) vanishes on $\mathcal{V}$, as $z\mathbf{x}^{\mathbf{w}} + zg(\mathbf{x})$ vanishes on $\mathcal{V}$ and $p \mid z$. Thus the leading monomial of $zg(\mathbf{x})$ is in $\mathrm{Lm}\left(I_{\mathbb{F}_p}(\mathcal{V})\right) = \mathrm{Lm}\,(I_{\mathbb{Q}}(\mathcal{V}))$, by Corollary 5.1.1. That is a contradiction.

For the second statement, let $\mathbb{F}$ be an arbitrary field and let us think of G as a subset of $\mathbb{F}\,[\mathbf{x}]$. Obviously $G \subseteq I_{\mathbb{F}}(\mathcal{V})$ is still true and the leading monomials of G remain the same. By $\mathrm{Sm}\,(I_{\mathbb{F}}(\mathcal{V})) = \mathrm{Sm}\,(I_{\mathbb{Q}}(\mathcal{V})) = \mathrm{Sm}\,(G)$, we have that G is a Gröbner basis of $I_{\mathbb{F}}(\mathcal{V})$. As the elements of G, except for their leading monomials, are linear combinations of standard monomials, G is also reduced. □

5.2 Generalization of the fundamental theorem of symmetric polynomials

We present an easy proof of a theorem by Garsia [27], which is a generalization of the fundamental theorem of symmetric polynomials. The original source of this proof is [31], where the authors used a different way to compute the lex standard monomials of the ideal in question. The reason why we chose to include this topic is that we think that the proof by the Lex Game is easier than the original one, and also since it is a good practice for the reader to get familiar with the game in a nice algebraic application. This approach has appeared in [22].

The *ith elementary symmetric polynomial* is

$$\sigma_i(\mathbf{x}) = \sum_{\substack{\mathbf{w}\in\{0,1\}^n \\ \deg(\mathbf{x}^{\mathbf{w}})=i}} \mathbf{x}^{\mathbf{w}},$$

provided that $0 \leq i \leq n$. Later we will also use the *complete symmetric polynomial of degree* $i \geq 0$, which is

$$h_i(\mathbf{x}) = \sum_{\substack{\mathbf{w}\in\mathbb{N}^n \\ \deg(\mathbf{x}^{\mathbf{w}})=i}} \mathbf{x}^{\mathbf{w}}.$$

The fundamental theorem of symmetric polynomials claims that if $f(\mathbf{x})$

is a symmetric polynomial, then it can be written uniquely as a finite sum

$$f(\mathbf{x}) = \sum_{\mathbf{u}\in\mathbb{N}^n} \alpha_{\mathbf{u}} \boldsymbol{\sigma}(\mathbf{x})^{\mathbf{u}},$$

where $\alpha_{\mathbf{u}} \in \mathbb{F}$, and $\boldsymbol{\sigma}(\mathbf{x})^{\mathbf{u}}$ stands for $\prod_{i\in[n]} \sigma_i(\mathbf{x})^{u_i}$.

We intend to prove the following generalization, which was obtained by A. Garsia [27].

Theorem 5.2.1. *Any polynomial $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ can be written uniquely as a finite sum*

$$f(\mathbf{x}) = \sum_{\substack{\mathbf{w}\in\mathbb{N}^n \\ \mathbf{w}\le\mathbf{v}}} \sum_{\mathbf{u}\in\mathbb{N}^n} \alpha_{\mathbf{w},\mathbf{u}} \mathbf{x}^{\mathbf{w}} \boldsymbol{\sigma}(\mathbf{x})^{\mathbf{u}},$$

where $\mathbf{v} = (0, 1, \dots, n-1)$, $\mathbf{w} \le \mathbf{v}$ is understood coordinatewise, and $\alpha_{\mathbf{w},\mathbf{u}} \in \mathbb{F}$.

We need some preparations before the proof. Let $z_1, \dots, z_n$ be different elements of a field and set

$$V = \{(z_{\pi(1)}, \dots, z_{\pi(n)}) \ : \ \pi \in S_n\}$$

the set of all permutations of the sequence $z_1, \dots, z_n$.

We first show that the lexicographic standard monomials of $I(V)$ are exactly the divisors of $x_2 x_3^2 \dots x_n^{n-1}$. In other words, the minimal lex leading monomials are of the form x_i^i for $i \in [n]$.

Proposition 5.2.2. *For the set of points V defined above, we have that $\mathbf{x}^{\mathbf{w}}$ is a lexicographic standard monomial of $I(V)$ if and only if $\mathbf{w} \le (0, 1, \dots, n-1)$.*

Proof. One can get the lexicographic standard monomials of V using the Lex Game. Suppose that $\mathbf{w} \le (0, 1, \dots, n-1)$. Then Stan's strategy will be to pick in the $(n-i+1)$th step (for y_i) any element from the set $\{z_1, \dots, z_n\} \setminus \{y_n, \dots, y_{i+1}\}$. This set has exactly i elements, so $w_i < i$ guarantees that Lea cannot choose all of them, that is there will always be a proper choice for Stan.

On the other hand, if for example $w_i \ge i$, then in the $(n-i+1)$th step Lea can choose all the elements of $\{z_1, \dots, z_n\} \setminus \{y_n, \dots, y_{i+1}\}$. If Stan wants to pick a value for y_i which is different from Lea's guesses, then y_i will either be the same as a previously selected y_j (and then $\mathbf{y} \notin V$) or an element different from all z_j (again $\mathbf{y} \notin V$). It means that Stan loses the game either ways. □

We use the following easy fact without proof (see for example [16]) which holds for all $i \in [n]$:

$$\sum_{j=0}^{i}(-1)^j h_{i-j}(x_i,\dots,x_n)\sigma_j(\mathbf{x}) = 0. \tag{5.1}$$

Let $i \in [n]$ and set

$$f_i(\mathbf{x}) = \sum_{j=0}^{i}(-1)^j h_{i-j}(x_i,\dots,x_n)\sigma_j(\mathbf{z}).$$

Proposition 5.2.3. *The set of polynomials $\{f_i : i \in [n]\}$ is the reduced Gröbner basis of V for all term orders, such that the order of the variables is $x_1 \succ x_2 \succ \cdots \succ x_n$.*

Proof. Clearly, if $x_1 \succ x_2 \succ \cdots \succ x_n$ holds for a term order, then $\mathrm{lm}\,(f_i) = x_i^i$, and the leading coefficient of f_i is 1. It is also obvious by Proposition 5.2.2 that every monomial of $f_i(\mathbf{x}) - x_i^i$ is a lex standard monomial. Equation (5.1) implies that f_i vanishes on V. As the minimal lex leading monomials (again by Proposition 5.2.2) are $\{x_i^i : i \in [n]\}$, we have that $\{f_i : i \in [n]\}$ is indeed a reduced lex Gröbner basis. But the leading monomials of the f_i for all term orders $\prec$ considered in the statement are the same, thus $\mathrm{Sm}_{\mathrm{lex}}\,(I(V)) \supseteq \mathrm{Sm}_{\prec}\,(I(V))$. Due to the equality of the cardinalities of the two sides, we have that the standard monomials are the same for all term orders considered. We conclude that $\{f_i : i \in [n]\}$ is a reduced Gröbner basis also with respect to $\prec$. □

Proof of Theorem 5.2.1. We had a good reason for not choosing base field for V until now. Let $\mathbb{F}(\mathbf{z})$ be the function field over $\mathbb{F}$ in n variables $z_1,\dots,z_n$ and let $V \subseteq \mathbb{F}(\mathbf{z})$ be the set of all permutations of these variables, as before.

Let $f(\mathbf{x}) \in \mathbb{F}\,[\mathbf{x}] \subseteq \mathbb{F}(\mathbf{z})[\mathbf{x}]$ be any polynomial, and reduce $f(\mathbf{x})$ by the Gröbner basis $\{f_i(\mathbf{x}) \in \mathbb{F}(\mathbf{z})[\mathbf{x}] : i \in [n]\}$ of V. The result is an $\mathbb{F}(\mathbf{z})$-linear combination of monomials $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$. Furthermore, since actually $f_i \in \mathbb{F}\,[\mathbf{z}]\,[\mathbf{x}]$, and f_i is symmetric in the variables $z_1,\dots,z_n$, the coefficients of the $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$ in this $\mathbb{F}(\mathbf{z})$-linear combination are symmetric polynomials from $\mathbb{F}[\mathbf{z}]$. (Note that as the leading coefficients of members of a reduced Gröbner basis are 1, there is no need of any division during the reduction.) Thus as functions on V, we have an equality

$$f(\mathbf{x}) = \sum_{\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \mathbf{x}^{\mathbf{w}} g_{\mathbf{w}}(\mathbf{z}),$$

where $g_{\mathbf{w}}(\mathbf{z}) \in \mathbb{F}[\mathbf{z}]$ is a symmetric polynomial. Therefore putting $\mathbf{z}$ in the place of $\mathbf{x}$ (since $\mathbf{z} \in V$) we get the equation

$$f(\mathbf{z}) = \sum_{\mathbf{z}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \mathbf{z}^{\mathbf{w}} g_{\mathbf{w}}(\mathbf{z})$$

of elements of $\mathbb{F}(\mathbf{z})$. An application of the fundamental theorem of symmetric polynomials, together with $\mathrm{Sm}\,(I(V)) = \{\mathbf{x}^{\mathbf{w}} \,:\, \mathbf{w} \leq (0,1,\ldots,n-1)\}$ yields the existence of the required form for f.

Uniqueness now follows: suppose that

$$f(\mathbf{x}) = \sum_{\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \sum_{\mathbf{u} \in \mathbb{N}^n} \alpha_{\mathbf{w},\mathbf{u}} \mathbf{x}^{\mathbf{w}} \boldsymbol{\sigma}(\mathbf{x})^{\mathbf{u}}.$$

Then as functions on V we have

$$f(\mathbf{x}) = \sum_{\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \sum_{\mathbf{u} \in \mathbb{N}^n} \alpha_{\mathbf{w},\mathbf{u}} \mathbf{x}^{\mathbf{w}} \boldsymbol{\sigma}(\mathbf{z})^{\mathbf{u}} = \sum_{\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))} \mathbf{x}^{\mathbf{w}} \tilde{g}_{\mathbf{w}}(\mathbf{z}),$$

for some polynomials $\tilde{g}_{\mathbf{w}}(\mathbf{z}) \in \mathbb{F}[\mathbf{z}]$. We have expressed $f(\mathbf{x})$ as an $\mathbb{F}(\mathbf{z})$-linear combination of standard monomials. However this is unique, hence $\tilde{g}_{\mathbf{w}}(\mathbf{z}) = g_{\mathbf{w}}(\mathbf{z})$, and so (using the uniqueness part of the fundamental theorem of symmetric polynomials) the claim follows. □

5.3 Hilbert function and inclusion matrices

This section can be considered as a preparation for the combinatorial applications of the theory. We introduce the notation to be used in the remaining of the thesis. We also prove a well-known connection between Hilbert functions and inclusion matrices.

Definition 5.3.1. A *set family* or *set system* is a subset of $2^{[n]}$.

For example $\binom{[n]}{m}$ denotes the family of all *m-subsets* of $[n]$ (subsets which have cardinality m), and $\binom{[n]}{\leq m}$ is the family of those subsets that have at most m elements.

The *characteristic vector* $\mathbf{v}_F$ of a set $F \subseteq [n]$ is an element of $\{0,1\}^n$, such that its ith coordinate is 1 if and only if $i \in F$. The set of characteristic vectors of a family of sets $\mathcal{F}$ is denoted by $V_{\mathcal{F}}$. We shall simplify our notation by writing

$$I(\mathcal{F}) = \{f \in \mathbb{F}\,[\mathbf{x}] \,:\, f(\mathbf{v}_F) = 0 \text{ for all } F \in \mathcal{F}\}$$

instead of $I(V_{\mathcal{F}})$ for the vanishing ideal of $V_{\mathcal{F}}$. In what follows, we shall always work with vanishing ideals of this kind. Note that $V_{\mathcal{F}} \subseteq \{0,1\}^n$, and therefore, when playing Lex $(V_{\mathcal{F}}; \mathbf{w})$, we shall assume that Stan always picks y_i from $\{0,1\}$ even if both numbers were among Lea's guesses and so Stan loses the game by such a choice. But this is reasonable, since if $y_i \notin \{0,1\}$, then $\mathbf{y} \notin V$, that is, Stan would lose the game anyway.

When $\mathcal{F}$ is a system of sets, we call $H_{I(\mathcal{F})}(m)$ the *Hilbert function of* $\mathcal{F}$ and denote it simply by $H_{\mathcal{F}}(m)$. In the combinatorial literature $H_{\mathcal{F}}(m)$ is usually given in terms of inclusion matrices.

Definition 5.3.2. For two families $\mathcal{F}, \mathcal{G} \subseteq 2^{[n]}$ the *inclusion matrix* $I(\mathcal{F}, \mathcal{G})$ is a matrix of size $|\mathcal{F}| \times |\mathcal{G}|$, whose rows and columns are indexed by the elements of $\mathcal{F}$ and $\mathcal{G}$, respectively. The entry at position (F, G) is 1 if $G \subseteq F$ and 0 otherwise $(F \in \mathcal{F}, G \in \mathcal{G})$.

Definition 5.3.3. For a subset $M \subseteq [n]$, the monomial x_M is defined to be $\prod\limits_{i \in M} x_i$ (and $x_\emptyset = 1$). We say that a polynomial is *multilinear* or *squarefree* if it is a linear combination of some x_M $(M \subseteq [n])$.

Proposition 5.3.4.

$$H_{\mathcal{F}}(m) = \dim_{\mathbb{F}} \left(\mathbb{F}\left[\mathbf{x}\right]_{\leq m} / I(\mathcal{F})_{\leq m} \right) = \operatorname{rank}_{\mathbb{F}} I\left(\mathcal{F}, \binom{[n]}{\leq m} \right).$$

Proof. Since for all $i \in [n]$ we have $x_i^2 - x_i \in I_{\mathcal{F}}$, we see that all standard monomials of $I(\mathcal{F})$ are squarefree.

Proposition 2.1.20 implies that among all multilinear monomials of degree at most m, the maximum number of modulo $I(\mathcal{F})$ linearly independent monomials is the same as the number of standard monomials of $I(\mathcal{F})$ of degree at most m, that is $H_{\mathcal{F}}(m)$. Therefore

$$H_{\mathcal{F}}(m) = \operatorname{rank}_{\mathbb{F}} \left\{ x_M + I(\mathcal{F}) \,:\, |M| \leq m \right\}, \tag{5.2}$$

where the rank of a set is the maximum number of linearly independent elements it contains.

As $\mathbb{F}\left[\mathbf{x}\right] / I(V_{\mathcal{F}})$ is isomorphic to the space of functions on $V_{\mathcal{F}}$, it is also isomorphic to $\mathbb{F}^{|\mathcal{F}|}$. The isomorphism maps a function $f(\mathbf{x})$ to a vector $\mathbf{f}$, such that the coordinate of $\mathbf{f}$ corresponding to a set $F \in \mathcal{F}$ is $f(\mathbf{v}_F)$. Rewriting equation (5.2) in line with this isomorphism we obtain

$$H_{\mathcal{F}}(m) = \operatorname{rank}_{\mathbb{F}} \left\{ \left(x_M(\mathbf{v}_F) \right)_{F \in \mathcal{F}} \,:\, M \in \binom{[n]}{\leq m} \right\}.$$

To finish the proof, note that $x_M(\mathbf{v}_F)$ equals to 1 if and only if $M \subseteq F$, and it is zero otherwise. It means that $(x_M(\mathbf{v}_F))_{F\in\mathcal{F}}$ is exactly the column of the inclusion matrix in question corresponding to $M \in \binom{[n]}{\le m}$. □

We will benefit from a similar statement in Section 5.4.

Proposition 5.3.5. *Let $\mathcal{P}_{\mathcal{F},m}$ be the linear space of functions from $V_{\mathcal{F}}$ to $\mathbb{F}$ which can be represented as homogeneous multilinear polynomials of degree m. (With a slight abuse of notation we could write $\mathcal{P}_{\mathcal{F},m} = \mathbb{F}\left[\mathbf{x}\right]_{=m} / I(\mathcal{F})_{=m}$.) Then*

$$\dim_{\mathbb{F}}\left(\mathcal{P}_{\mathcal{F},m}\right) = \operatorname{rank}_{\mathbb{F}} I\left(\mathcal{F}, \binom{[n]}{m}\right).$$

Proof. The proof is very much similar to that of Proposition 5.3.4. Here, the monomials of degree m generate $\mathcal{P}_{\mathcal{F},m}$, and columns of the inclusion matrix $I\left(\mathcal{F}, \binom{[n]}{m}\right)$ correspond exactly to these monomial functions. □

Incidence matrices and their ranks are important in the study of finite geometries as well. Standard monomials and Hilbert functions are also useful in that setting. The reader is referred to Moorhouse [34] for an account on applications of this type.

5.4 Wilson's rank formula

Consider the inclusion matrix $A = I\left(\binom{[n]}{d}, \binom{[n]}{m}\right)$, where $m \le d \le n - m$.

A famous theorem of Richard M. Wilson [39, Theorem 2] describes a diagonal form of A over $\mathbb{Z}$, that is A is shown to be row-column equivalent over $\mathbb{Z}$ to a diagonal matrix with diagonal entries $\binom{d-i}{m-i}$ with multiplicity $\binom{n}{i} - \binom{n}{i-1}$ for $0 \le i \le m$. As a corollary, the following rank formula holds:

Theorem 5.4.1. *Let p be a prime. Then*

$$\operatorname{rank}_{\mathbb{F}_p}(A) = \sum_{\substack{0\le i\le m \\ p\nmid\binom{d-i}{m-i}}} \binom{n}{i} - \binom{n}{i-1}.$$

We shall outline a proof which uses polynomial functions, and notions related to Gröbner bases. The idea follows that of [26], however the proof is notably simplified by the Lex Game. Compared to our paper [22], where we originally published the result, we have implemented only slight modifications.

We note first that the rank of A is exactly the dimension of the linear space $\mathcal{P}_{d,m}$ over $\mathbb{F}_p$ of the functions from $V_{\binom{[n]}{d}}$ to $\mathbb{F}_p$ which are spanned by the monomials x_M with $|M| = m$ (see Proposition 5.3.5).

Let P_m denote the subspace of homogeneous multilinear polynomials in $\mathbb{F}_p[\mathbf{x}]$ of degree m. Suppose that $m \leq \frac{n}{2}$, and for a set $M \subseteq [n]$, $|M| \leq m$ we define the squarefree polynomial

$$y_M = \sum_{\substack{M' \supseteq M \\ |M'|=m}} x_{M'} \in P_m.$$

To simplify our notation, we write I for the vanishing ideal $I\left(\binom{[n]}{m}\right)$ of $\binom{[n]}{m}$.

Lemma 5.4.2. *The collection of polynomials y_M, where $x_M \in \mathrm{Sm}(I)$, is a linear basis of P_m over $\mathbb{F}_p$.*

Proof. Since $\{x_M + I \,:\, x_M \in \mathrm{Sm}(I)\}$ is a linear basis of $\mathbb{F}_p[\mathbf{x}]/I$, and $x_M + I = y_M + I$ (they represent the same function on $V_{\binom{[n]}{m}}$), we obtain that $\{y_M + I \,:\, x_M \in \mathrm{Sm}(I)\}$ is a basis of $\mathbb{F}_p[\mathbf{x}]/I$. As $y_M \in P_m$, it is also clear that $P_m + I = \mathbb{F}_p[\mathbf{x}]$. From the fact that $P_m \cap I = \{0\}$, we have a natural isomorphism $P_m \longrightarrow \mathbb{F}_p[\mathbf{x}]/I$ which sends y_M to $y_M + I$. We conclude that $\{y_M \,:\, x_M \in \mathrm{Sm}(I)\}$ is indeed a basis of P_m. □

We can state Wilson's rank formula in this setting as follows.

Theorem 5.4.3. *Let p be a prime, suppose that $m \leq d \leq n - m$ and put $I = I\left(\binom{[n]}{m}\right)$. A basis of the space $\mathcal{P}_{d,m}$ of $\mathbb{F}_p$-valued functions on $V_{\binom{[n]}{d}}$, which are $\mathbb{F}_p$-linear combinations of monomials x_M, $|M| = m$ is*

$$B = \left\{ y_M \,:\, x_M \in \mathrm{Sm}(I),\, p \nmid \binom{d - |M|}{m - |M|} \right\}.$$

In particular,

$$\dim_{\mathbb{F}_p}(\mathcal{P}_{d,m}) = |B| = \sum_{\substack{0 \leq i \leq m \\ p \nmid \binom{d-i}{m-i}}} \binom{n}{i} - \binom{n}{i-1}.$$

Proof. Let $\mathbf{v}_F$ be the characteristic vector of a d-subset of $[n]$. It is immediate that

$$y_M(\mathbf{v}_F) = \binom{d - |M|}{m - |M|} \cdot x_M(\mathbf{v}_F). \tag{5.3}$$

We obtain that, as a function on $V_{\binom{[n]}{d}}$, y_M is a scalar multiple of x_M. This, together with the linear independence of the x_M gives that B is an independent set. Also, B spans $\mathcal{P}_{d,m}$, because P_m spans $\mathcal{P}_{d,m}$ by definition, and the y_M span P_m by Lemma 5.4.2. To conclude, it remains to verify that for $0 \leq i \leq m$ there are exactly $\binom{n}{i} - \binom{n}{i-1}$ monomials of degree i in $\mathrm{Sm}\,(I)$. This will be proven in Lemma 5.4.4. □

We say that a vector $\mathbf{w} \in \{0,1\}^n$ is a *ballot sequence* if in every prefix of $\mathbf{w}$ there are at least as many 0, as 1 coordinates. In the proof of the next lemma, we shall see that $\mathbf{x}^{\mathbf{w}}$ is a lex standard monomial of $I\left(\binom{[n]}{m}\right)$ iff $\deg(\mathbf{x}^{\mathbf{w}}) \leq m$ and $\mathbf{w}$ is a ballot sequence.

Lemma 5.4.4. *For an arbitrary term order and any integers $0 \leq i \leq m \leq \frac{n}{2}$, there are exactly $\binom{n}{i} - \binom{n}{i-1}$ monomials of degree i in $\mathrm{Sm}\left(I\left(\binom{[n]}{m}\right)\right)$.*

Proof. We will restrict ourselves to the lex order. Note that this is enough for completing the proof of Theorem 5.4.3. In fact, this lemma is a consequence of a more general theorem (Theorem 6.1.22) we shall prove in Chapter 6.

We claim that $\mathbf{x}^{\mathbf{w}}$ is a lex standard monomial of $I = I\left(\binom{[n]}{m}\right)$ if and only if $\deg(\mathbf{x}^{\mathbf{w}}) \leq m$ and $\mathbf{w}$ is a ballot sequence. We can use the Lex Game $\mathrm{Lex}\left(V_{\binom{[n]}{m}}; \mathbf{w}\right)$ to prove this.

First of all, if $\mathbf{w} \notin \{0,1\}^n$, then say $w_i \geq 2$. Lea may guess for both 0 and 1 in the ith step of the game, and so one of her guesses shall be correct.

If the number of 1 coordinates in $\mathbf{w}$ is more than m, then Lea will choose 0 at each of her guesses. This way, Stan has to put $y_i = 1$ for more than m times, therefore $\mathbf{y} \notin V_{\binom{[n]}{m}}$ at the end, and Lea wins. That is, if $\deg(\mathbf{x}^{\mathbf{w}}) > m$, then $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I)$.

Suppose now that $\deg(\mathbf{x}^{\mathbf{w}}) \leq m$ and $\mathbf{w} \in \{0,1\}^n$ is not a ballot sequence. Let $i \in [n]$ be such that $(w_1, \ldots, w_i)$ is the shortest prefix of $\mathbf{w}$ that violates the ballot condition. It is easy to see that i is odd, and there are exactly $\frac{i+1}{2}$ coordinates equal to 1. Assume that when in the game Stan picks y_{i+1}, then there are $m-k$ ones among $y_n, \ldots, y_{i+1}$. Stan would win only if he could pick the remaining $y_i, \ldots, y_1$, such that k of them was 1, $i-k$ of them was 0. But if $k \leq \frac{i-1}{2}$, then Lea always chooses 0, thus there will be at least $\frac{i+1}{2} > k$ ones among $y_i, \ldots, y_1$. And when $k > \frac{i-1}{2}$, then $i - k \leq \frac{i-1}{2}$, so if Lea keeps on choosing 1, then Stan has to claim at least $\frac{i+1}{2} > i - k$ zero coordinates, and hence he loses the game.

Next we show how Stan can win if $\mathbf{w}$ is a ballot sequence with at most m ones. Set $J = \{j \in [n] \,:\, w_j = 1\}$. For all $j \in J$ let us pick an $\ell(j) \in [n]$, such that $w_{\ell(j)} = 0$, $\ell(j) < j$, and $\ell : J \to [n]$ is injective. (This can be done if $\mathbf{w}$

is a ballot sequence.) Let us put $L = \{\ell(j) : j \in J\}$, and $K = [n] \setminus (J \cup L)$. Stan's strategy to choose y_i is the following. If $i \in J$, then Lea will guess something, so he just claims the opposite (in $\{0, 1\}$). If $i \in L$, say $i = \ell(j)$, then he picks $y_{\ell(j)}$, such that $\{y_j, y_{\ell(j)}\} = \{0, 1\}$. (Note that when choosing the $\ell(j)$th coordinate, he already fixed y_j by $\ell(j) < j$.) This way, Stan will have exactly $|J|$ ones in $(y_i : i \in J \cup L)$. Therefore he picks $m - |J|$ ones from the y_k $(k \in K)$, and wins.

Now it follows immediately, that the lex standard monomials of $I\left(\binom{[n]}{m}\right)$ of degree at most i are the same as the lex standard monomials of $I\left(\binom{[n]}{i}\right)$. In particular, there are $\binom{n}{i}$ of them, and then there are $\binom{n}{i} - \binom{n}{i-1}$ standard monomials of degree i. This proves the lemma. □

The approach given here allows a considerable generalization of the rank formula. We mention without proof a result of this type (for details, see [26]). Suppose that $0 \leq m_1 < m_2 \cdots < m_r \leq d \leq n - m_r$ and let p be a prime. Consider the set family $\mathcal{F} = \binom{[n]}{m_1} \cup \binom{[n]}{m_2} \cup \cdots \cup \binom{[n]}{m_r}$. Then

$$\operatorname{rank}_{\mathbb{F}_p}\left(I\left(\binom{[n]}{d}, \mathcal{F}\right)\right) = \sum_{\substack{0 \leq i \leq m_r \\ p \nmid n_i}} \binom{n}{i} - \binom{n}{i-1},$$

where $n_i = \gcd\left(\binom{d-i}{m_1-i}, \binom{d-i}{m_2-i}, \ldots, \binom{d-i}{m_r-i}\right)$.

Chapter 6

Applications to extremal combinatorics

The focus now will be on a certain family of subsets $\mathcal{F}$ of $[n]$. We shall work really hard in Section 6.1 to get familiar with the vanishing ideal $I(\mathcal{F})$ of $V_{\mathcal{F}}$: we compute its standard monomials, Hilbert function and one of its Gröbner bases. Then, with this information given, the two applications in the following two sections will be relatively easy; they use the formula for the Hilbert function of $I(\mathcal{F})$.

The first part of Section 6.1 concerning the lex standard monomial calculations has been included in [20], the same paper where the Lex Game has been published. Further results, particularly the formula for the Hilbert function, and the two applications to extremal combinatorics have appeared in [19].

6.1 Calculations with modulo q complete ℓ-wide families

The final goal of this section is to compute the Hilbert function of the ideal $I(\mathcal{F})$ over $\mathbb{F}_p$, where $\mathcal{F}$ is a modulo q complete ℓ-wide family, and q is a power of p.

Definition 6.1.1. Let q, d, ℓ be integers such that $1 \leq \ell < q$. Then the *modulo q complete ℓ-wide family* is

$$\mathcal{F} = \{F \subseteq [n] \, : \, \exists\, f \in \mathbb{Z} \text{ such that } d \leq f < d + \ell \text{ and } |F| \equiv f \pmod{q}\}.$$

Subfamilies of this $\mathcal{F}$ are called *modulo q ℓ-wide families.*

As substituting d' for d where $d \equiv d' \pmod{q}$ does not affect $\mathcal{F}$, from now on, we may suppose that also

$$\frac{n-q-\ell}{2} < d \leq \frac{n+q-\ell}{2}$$

holds.

In other words, $\mathcal{F}$ contains all subsets of $[n]$ which have cardinality modulo q in the interval $[d, d+\ell-1]$ (of length ℓ). The restrictions on the parameters ℓ and q tell us exactly that if $|F| \equiv d+\ell \pmod{q}$, then $F \notin \mathcal{F}$ (that is, $\mathcal{F}$ is in fact ℓ-wide).

An example, which we already know from the previous chapter is $\binom{[n]}{m}$, a modulo q complete 1-wide family, with $d = m$ and any $q > n$.

The computation of $H_{\mathcal{F}}(m)$ is done in three major stages: we determine the set of lexicographic standard monomials of $I(\mathcal{F})$, then compute a lex Gröbner basis, and verifying that it is also a deglex Gröbner basis, we count the deglex standard monomials of any given degree to get the Hilbert function.

6.1.1 Lexicographic standard monomials

We start the description of lex standard monomials for a more general class of ideals. Proposition 6.1.3 is valid for all ideals of the form $I(\mathcal{F})$, where $\mathcal{F}$ is any family such that for all $f \in \mathbb{Z}$ either $\binom{[n]}{f} \subseteq \mathcal{F}$ or $\binom{[n]}{f} \cap \mathcal{F} = \emptyset$. Let us introduce a convenient notation for these families of sets.

If $D \subseteq \mathbb{Z}$, then we write

$$\mathcal{F}_{D,n} = \{F \subseteq [n] \,:\, |F| \in D\}.$$

For $t \in \mathbb{Z}$ and $A \subseteq \mathbb{Z}$ we put

$$A - t = \{a - t \,:\, a \in A\}.$$

For any $A \subseteq \mathbb{Z}$, we set

$$A^{(0)} = A \cup (A-1) \qquad \text{and} \qquad A^{(1)} = A \cap (A-1).$$

If $\mathbf{w} = (w_1, \ldots, w_n) \in \{0,1\}^n$ then

$$D^{(\mathbf{w})} = \left(\ldots\left(\left(D^{(w_1)}\right)^{(w_2)}\right)^{\cdots}\right)^{(w_n)}.$$

We shall see shortly that $D^{(\mathbf{w})}$ is a convenient tool to decide whether $\mathbf{x}^{\mathbf{w}}$ is a lex standard monomial of $I(\mathcal{F}_{D,n})$: we prove that $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}_{\mathrm{lex}}\left(I(\mathcal{F}_{D,n})\right)$ if and only if $0 \in D^{(\mathbf{w})}$. We illustrate this by taking another look at our old Example 4.1.1 from Chapter 4.

Example 6.1.2. Set $D = \{1, 2, 3\}$ and $I = I(\mathcal{F}_{D,5})$. We have already seen that with $\mathbf{w} = (11100)$ the monomial $\mathbf{x}^{\mathbf{w}}$ is in $\mathrm{Lm}\,(I)$ while if $\mathbf{w} = (01110)$ then $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I)$. Computing $D^{(\mathbf{w})}$ gives $D^{(1)} = \{1, 2\}$, $D^{(1,1)} = \{1\}$, $D^{(1,1,1)} = \emptyset$, thus $D^{(1,1,1,0)} = D^{(1,1,1,0,0)} = \emptyset$, indeed $0 \notin D^{(\mathbf{w})}$ in the first case. If $\mathbf{w} = (01110)$ then one can check that $D^{(\mathbf{w})} = \{-1, 0\}$ which agrees with $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I)$.

Proposition 6.1.3.

$$\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}_{\mathrm{lex}}\,(I(\mathcal{F}_{D,n})) \iff \mathbf{w} \in \{0,1\}^n \textit{ and } 0 \in D^{(\mathbf{w})}.$$

Proof. We shall show that Stan wins Lex $\left(V_{\mathcal{F}_{D,n}}; \mathbf{w}\right)$ if and only if $\mathbf{w} \in \{0,1\}^n$ and $0 \in D^{(\mathbf{w})}$, which implies the claim.

We have $V_{\mathcal{F}_{D,n}} \subseteq \{0,1\}^n$, hence if $w_i \geq 2$ for some i, then Lea wins. Thus, for the rest of the proof we assume that $\mathbf{w} \in \{0,1\}^n$.

We prove by induction on n that

$$A := \left\{t \in \mathbb{Z} \,:\, \text{Stan wins Lex}\left(V_{\mathcal{F}_{D-t,n}}; \mathbf{w}\right)\right\} = D^{(\mathbf{w})}. \tag{6.1}$$

This will be sufficient, because by definition $0 \in A$ if and only if Stan wins Lex $\left(V_{\mathcal{F}_{D,n}}; \mathbf{w}\right)$.

To prove (6.1), first we consider the case $n = 1$. If $w = 0$ then Stan wins Lex $\left(V_{\mathcal{F}_{D-t,1}}; w\right)$ if and only if $\mathcal{F}_{D-t,1} \neq \emptyset$, since Lea is not allowed to guess anything. This means $(D - t) \cap \{0, 1\} \neq \emptyset$, so $t \in D \cup (D - 1) = D^{(w)}$. If $w = 1$ then Stan wins if and only if $|\mathcal{F}_{D-t,1}| = 2$, since Lea can check only one of the two possibilities. Thus $\{0, 1\} \subseteq (D - t)$ hence $t \in D \cap (D - 1) = D^{(w)}$.

Suppose that the statement is true for $n - 1$, that is with

$$C = \left\{t \in \mathbb{Z} \,:\, \text{Stan wins Lex}\left(V_{\mathcal{F}_{D-t,n-1}}; \overline{\mathbf{w}}\right)\right\},$$

we have $C = D^{(\overline{\mathbf{w}})}$. We have to prove that $C^{(w_n)} = A$.

When Stan and Lea play a Lex $\left(V_{\mathcal{F}_{D-t,n}}; \mathbf{w}\right)$ game, and Stan reveals the last coordinate y_n, then they keep on playing either a Lex $\left(V_{\mathcal{F}_{D-t,n-1}}; \overline{\mathbf{w}}\right)$ game (if $y_n = 0$) or a Lex $\left(V_{\mathcal{F}_{D-t-1,n-1}}; \overline{\mathbf{w}}\right)$ game (if $y_n = 1$).

If $w_n = 0$ then Stan wins Lex $\left(V_{\mathcal{F}_{D-t,n}}; \mathbf{w}\right)$ if and only if he wins either Lex $\left(V_{\mathcal{F}_{D-t,n-1}}; \overline{\mathbf{w}}\right)$ or Lex $\left(V_{\mathcal{F}_{D-t-1,n-1}}; \overline{\mathbf{w}}\right)$, since he can choose y_n accordingly.

If $w_n = 1$ then Stan wins Lex $\left(V_{\mathcal{F}_{D-t,n}}; \mathbf{w}\right)$ if and only if he wins both of the games Lex $\left(V_{\mathcal{F}_{D-t,n-1}}; \overline{\mathbf{w}}\right)$ and Lex $\left(V_{\mathcal{F}_{D-t-1,n-1}}; \overline{\mathbf{w}}\right)$, since in this case Lea can force either of the above alternatives by a suitable guess for y_n.

We conclude that $C^{(w_n)} = A$, hence $A = D^{(\mathbf{w})}$ and the proof is complete. □

We now focus on sets D, such that $\mathcal{F}_{D,n}$ is a modulo q complete ℓ-wide family, that is when d, q and ℓ are integers with $1 \leq \ell < q$, and

$$D = \{f \in \mathbb{Z} \,:\, \exists f' \in \mathbb{Z} \text{ such that } d \leq f' \leq d + \ell - 1 \text{ and } f' \equiv f \pmod{q}\}\,.$$

We still assume that $\frac{n-q-\ell}{2} < d \leq \frac{n+q-\ell}{2}$.

The notion of a lattice path is essential for going further. A *lattice path* is a polygon in a square grid in the X,Y-plane with the following properties. It starts at the origin $(0, 0)$ and proceeds in finitely many unit length steps. We allow two kinds of steps: it can either be horizontal (X direction), going from a point (i, j) to $(i + 1, j)$, or vertical (Y direction), moving from (i, j) to $(i, j + 1)$. Thus for example a step from $(i + 1, j)$ to (i, j) is forbidden. A lattice path always ends at a point (n_X, n_Y) with $n_X, n_Y \in \mathbb{N}$.

There is an easy one-to-one correspondence between lattice paths of length n and elements of $\{0, 1\}^n$. If $\mathbf{w} \in \{0, 1\}^n$, then the corresponding lattice path $\hat{\mathbf{w}}$ is such that the ith step of $\hat{\mathbf{w}}$ is horizontal if and only if $w_i = 1$ (and vertical otherwise).

Denote the line $Y = X - \ell + q$ by L^+ and the line $Y = X - \ell$ by L^-. Now the description of the lexicographic standard monomials of a modulo q complete ℓ-wide family is the following.

Theorem 6.1.4. *Let $\mathcal{F}$ be a modulo q complete ℓ-wide family. We have $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}_{\mathrm{lex}}(I(\mathcal{F}))$ if and only if*

1. $\mathbf{w} \in \{0, 1\}^n$,
2. *$\hat{\mathbf{w}}$ does not touch the line L^- before touching the line L^+, and*
3. *if $\hat{\mathbf{w}}$ does not reach any of these two lines, then the X coordinate of its endpoint n_X (which is in fact the degree of $\mathbf{x}^{\mathbf{w}}$) satisfies $n_X \leq \min\{d + \ell - 1, n - d\}$.*

It is instructive to visualize the above theorem.

Every $\hat{\mathbf{w}}$ corresponding to a $\mathbf{w} \in \{0, 1\}^n$ intersects one of the thick lines of Figure 6.1. Theorem 6.1.4 states that if $\hat{\mathbf{w}}$ reaches the thicker line first then $\mathbf{x}^{\mathbf{w}}$ is a leading monomial, otherwise $\mathbf{x}^{\mathbf{w}}$ is a standard monomial.

Proof of Theorem 6.1.4. By Proposition 6.1.3, it is enough to show that the lattice path criteria of the theorem hold if and only if $0 \in D^{(\mathbf{w})}$. We may suppose that $\mathbf{w} \in \{0, 1\}^n$.

The sketch of the proof is the following. A bit long, but completely elementary argument will show that $D^{(\mathbf{w})} = \emptyset$ iff $\hat{\mathbf{w}}$ touches L^- before reaching L^+, and $D^{(\mathbf{w})} = \mathbb{Z}$ iff $\hat{\mathbf{w}}$ touches L^+ before reaching L^-. Once we will be

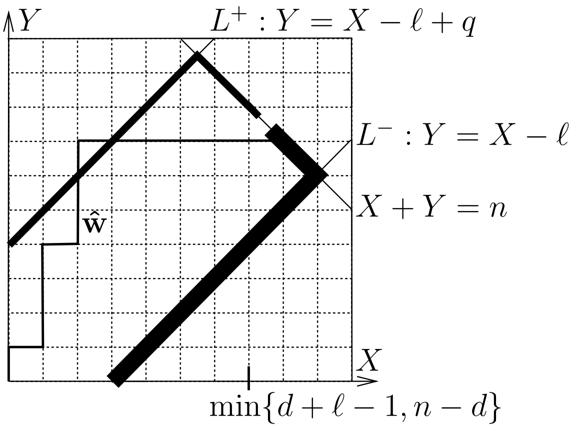


Figure 6.1: $n = 15$, $q = 7$, $\ell = 3$ and $d = 5$ or $d = 8$. We see that $x_2x_6x_{10}x_{11}x_{12}x_{13}x_{14}x_{15}$ is a lex standard monomial.

ready with these, we shall consider the case, when $\hat{\mathbf{w}}$ does not touch any of the two above lines.

Let a, b be integers. We define the interval $[a,b]$ as

$$[a,b] := \{c \in \mathbb{Z} \,:\, a \le c \le b\}\,,$$

in particular if $a > b$ then $[a,b] = \emptyset$. If $[a,b] \neq \emptyset$ then $[a,b]^{(0)} = [a-1,b]$ and $[a,b]^{(1)} = [a,b-1]$. More generally suppose that in $\mathbf{w} \in \{0,1\}^n$ there are n_X one and $n - n_X = n_Y$ zero coordinates, and for every proper prefix $\mathbf{w}'$ of $\mathbf{w}$ we have $[a,b]^{(\mathbf{w}')} \neq \emptyset$. Then

$$[a,b]^{(\mathbf{w})} = [a - n_Y, b - n_X]. \tag{6.2}$$

Here $[a - n_Y, b - n_X]$ is empty if and only if $a - n_Y > b - n_X$, that is, the length $b - a + 1$ of the interval $[a,b]$ is at most $n_X - n_Y$. From $[a,b]^{(\overline{\mathbf{w}})} \neq \emptyset$ and $[a,b]^{(\mathbf{w})} = \emptyset$ it follows that $w_n = 1$ and $a - n_Y \le b - (n_X - 1)$. Therefore if $\mathbf{w}$ is as above, then $[a - n_Y, b - n_X] = \emptyset$ if and only if $b - a + 1 = n_X - n_Y$. One may generalize easily these observations as follows: if $\mathbf{w}^*$ is the shortest prefix of $\mathbf{w} \in \{0,1\}^n$ for which $[a,b]^{(\mathbf{w}^*)} = \emptyset$ then $\mathbf{w}^*$ has exactly $b - a + 1$ more one coordinates than zeros.

Suppose now that $A \subseteq \mathbb{Z}$ is a union of intervals $A = \bigcup\limits_{i \in \Gamma} [a_i, b_i]$, which are separated in the sense that for $i, j \in \Gamma$ the set $[a_i, b_i] \cup [a_j, b_j]$ is not an interval unless $i = j$. Then clearly we have

$$A^{(w)} = \bigcup_{i \in \Gamma} [a_i, b_i]^{(w)} \quad \text{for } w \in \{0,1\}. \tag{6.3}$$

If $A \subseteq \mathbb{Z}$, $q \in \mathbb{Z}$ and $\mathbf{w} \in \{0,1\}^n$ then

$$(A-q)^{(\mathbf{w})} = A^{(\mathbf{w})} - q. \tag{6.4}$$

In our case we have $D = \bigcup_{i\in\mathbb{Z}} (A - iq)$, with $A = [d, d+\ell-1]$. By the assumption $\ell < q$ one can see that the intervals $A - iq = [d-iq, d+\ell-1-iq]$ are separated. From (6.3) and (6.4) easy induction on n gives that

$$D^{(\mathbf{w})} = \bigcup_{i\in\mathbb{Z}} \left(A^{(\mathbf{w})} - iq\right), \tag{6.5}$$

provided that $\left|A^{(\mathbf{w}')}\right| < q$ for every prefix $\mathbf{w}'$ of $\mathbf{w}$. If there exists a prefix $\mathbf{w}'$ for which $\left|A^{(\mathbf{w}')}\right| = q$, then the intervals of D merge in $D^{(\mathbf{w}')}$, that is $D^{(\mathbf{w}')} = \mathbb{Z}$. Since $\mathbb{Z}^{(0)} = \mathbb{Z}^{(1)} = \mathbb{Z}$, in this case $D^{(\mathbf{w})} = \mathbb{Z}$ as well.

Thus (6.5) allows us to reduce the calculation of $D^{(\mathbf{w})}$ to that of the interval $A^{(\mathbf{w})}$. In particular $D^{(\mathbf{w})} = \emptyset$ if and only if $A^{(\mathbf{w})} = \emptyset$ and there is no prefix $\mathbf{w}'$ of $\mathbf{w}$ such that $\left|A^{(\mathbf{w}')}\right| = q$. Let $\mathbf{w}^*$ be the shortest prefix of the above $\mathbf{w}$ for which $A^{(\mathbf{w}^*)} = \emptyset$. We have seen that $\mathbf{w}^*$ has ℓ more 1 coordinates than zeros, that is, the path $\hat{\mathbf{w}}^*$ reaches the line L^- ($Y = X - \ell$) at its endpoint. The condition $\left|A^{(\mathbf{w}')}\right| < q$ for every prefix $\mathbf{w}'$ of $\mathbf{w}^*$ together with the condition on $\mathbf{w}^*$ is equivalent to that $\mathbf{w}'$ has less than $q-\ell$ more zeros than ones, or equivalently, the path $\hat{\mathbf{w}}'$ stays under the line L^+ ($Y = X + q - \ell$).

To sum up, $D^{(\mathbf{w})}$ is empty if $\hat{\mathbf{w}}$ touches the line L^- before reaching L^+. In particular we have $0 \notin D^{(\mathbf{w})}$ in this case. If $\hat{\mathbf{w}}$ reaches L^+ first, then $D^{(\mathbf{w})} = \mathbb{Z}$, hence $0 \in D^{(\mathbf{w})}$.

It remains to consider the case when $\hat{\mathbf{w}}$ stays between the two lines. Let the endpoint of $\hat{\mathbf{w}}$ be (n_X, n_Y). Here $D^{(\mathbf{w})}$ can be calculated according to (6.5). By (6.2) we have

$$A^{(\mathbf{w})} = [d, d+\ell-1]^{(\mathbf{w})} = [d - n_Y, d+\ell-1-n_X],$$

hence we obtain that

$$D^{(\mathbf{w})} = \bigcup_{i\in\mathbb{Z}} [d + iq - n_Y, d + iq + \ell - 1 - n_X]. \tag{6.6}$$

The intersection of L^+ and $X + Y = n$ is the point $\left(\frac{n-q+\ell}{2}, \frac{n+q-\ell}{2}\right)$. Since (n_X, n_Y) is on $X + Y = n$, and below L^+, it follows that

$$n_Y \leq \frac{n+q-\ell}{2} \quad \text{and} \tag{6.7}$$

$$n_X \geq \frac{n-q+\ell}{2} \quad . \tag{6.8}$$

By (6.6) we have $0 \in D^{(\mathbf{w})}$ if and only if there exists an $i \in \mathbb{Z}$ such that $d + iq - n_Y \leq 0 \leq d + \ell - 1 + iq - n_X$. From this, we infer

$$d + iq \leq n_Y \leq \frac{n + q - \ell}{2}$$

by (6.7) and

$$d + iq \geq n_X - \ell + 1 \geq \frac{n - q + \ell}{2} - \ell + 1 > \frac{n - q - \ell}{2}$$

follows from (6.8). We obtained that $0 \in D^{(\mathbf{w})}$ implies $\frac{n-q-\ell}{2} < d+iq \leq \frac{n+q-\ell}{2}$, which holds only for $i = 0$. Therefore $0 \in D^{(\mathbf{w})}$ if and only if $d - n_Y \leq 0 \leq d + \ell - 1 - n_X$ which is precisely the condition $n_X \leq \min\{n - d, d + \ell - 1\}$ by $n_Y = n - n_X$. □

From now on, it will be much more convenient to write x_M for a multilinear polynomial instead of $\mathbf{x}^{\mathbf{w}}$. (Actually, the reason why we have not switched to this before is that explaining $D^{(M)}$ would have been quite cumbersome.) We also replace our notation for the lattice path $\hat{\mathbf{w}}$ to $\hat{M}$, if $\mathbf{x}^{\mathbf{w}} = x_M$. That is, the ith step of the lattice path $\hat{M}$ is vertical exactly when $i \in M$.

The next goal is to determine the minimal lex leading monomials of $I(\mathcal{F})$.

Corollary 6.1.5. *A multilinear monomial x_M is a minimal element with respect to divisibility of* $\mathrm{Lm}_{\mathrm{lex}}(I(\mathcal{F}))$ *if and only if*

1. *$\hat{M}$ reaches any of the two lines L^- and $X = \min\{d + \ell - 1, n - d\} + 1$, say in the ith step for the first time,*

2. *before the ith step $\hat{M}$ does not touch the line L^+, and*

3. *after the ith step it proceeds only upwards.*

The corollary claims that x_M is a minimal element of $\mathrm{Lm}_{\mathrm{lex}}(I(\mathcal{F}))$ if $\hat{M}$ touches the thicker line of Figure 6.2 before reaching the thiner one and proceeds upwards from that point.

Proof of Corollary 6.1.5. By Theorem 6.1.4 it is clear that every multilinear leading monomial x_M satisfies conditions (1) and (2) of the corollary. Suppose that $\hat{M}$ touches L^- or $X = \min\{d+\ell-1, n-d\}+1$ in the ith step for the first time. The third condition follows from minimality: if $N := \{j \in M \; : \; j \leq i\}$ then the same theorem implies that x_N is a leading monomial. Since x_N divides x_M, we have that $x_M = x_N$ which in terms of lattice paths means that after the ith step $\hat{M}$ proceeds only upwards.

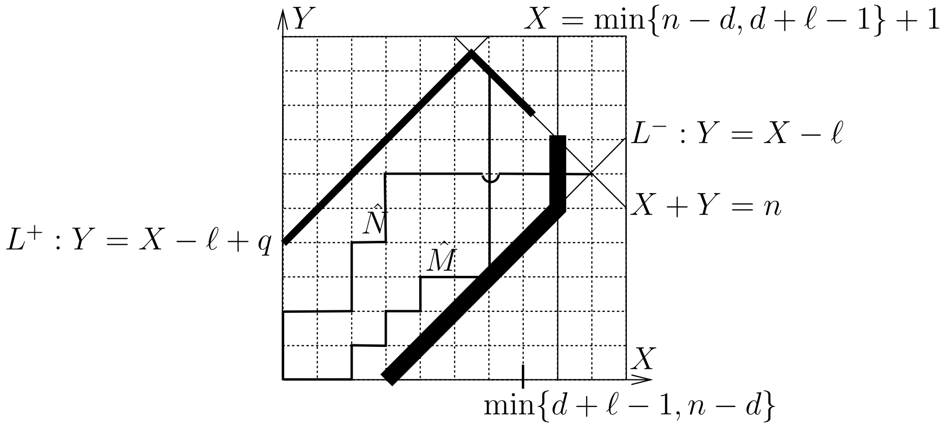


Figure 6.2: We have $n = 15$, $q = 7$, $\ell = 3$ and $d = 5$ or $d = 8$. From Corollary 6.1.5 we learn that $x_M = x_1x_2x_4x_6x_8x_9$ is a minimal leading monomial, while $x_N = x_3x_4x_7x_{10}x_{11}x_{12}x_{13}x_{14}x_{15}$ is a leading monomial which is not minimal. Indeed, leaving out one of the variables x_{11}, x_{12}, x_{13}, x_{14}, x_{15} from x_N we get a (minimal) leading monomial.

Conversely, assume that the three conditions of the corollary hold for x_M. We will show that if $\hat{M}$ touches $X = \min\{d+\ell-1, n-d\}+1$, then it cannot reach later L^+, or in other words: the last point of the thicker line of Figure 6.2 is below L^+. If this holds then the conditions (1) and (2) of the corollary together with Theorem 6.1.4 imply that x_M is a leading monomial. Using that $\frac{n-\ell-q+1}{2} \le d \le \frac{n-\ell+q}{2}$ we get

$$\begin{aligned}\min\{d+\ell-1, n-d\}+1 &\ge \min\left\{\frac{n+\ell-q-1}{2}, \frac{n+\ell-q}{2}\right\}+1 = \\ &= \frac{n+\ell-q+1}{2} \qquad (6.9)\end{aligned}$$

The X coordinate of the intersection of L^+ and $X+Y=n$ is $\frac{n+\ell-q}{2}$, therefore equation (6.9) gives the desired result.

It remains to verify the minimality of x_M. If x_N is a proper divisor of x_M, then the degree of x_N is at most $\min\{d+\ell-1, n-d\}$, so, to be a leading monomial, $\hat{N}$ has to reach the line L^- according to Theorem 6.1.4. But it cannot, as $\hat{N}$ is to the left of $\hat{M}$ while L^- is to the right. □

We are left with collecting the non-squarefree minimal elements of the set $\mathrm{Lm}_{\mathrm{lex}}(I(\mathcal{F}))$. Obviously $x_i^2 - x_i \in I(\mathcal{F})$ for all $i \in [n]$, thus we only have to check if the x_i^2 are minimal generators of the initial ideal. The next corollary claims that in the non-degenerate cases $x_2^2, \dots, x_n^2$ are minimal leading monomials; and also x_1^2, as long as $\ell \ge 2$.

Corollary 6.1.6. *The non-multilinear minimal generators of the initial ideal* $\langle \mathrm{Lm}_{\mathrm{lex}}\,(I(\mathcal{F}))\rangle$ *are characterized as follows.*

- *If* $\mathcal{F} = \{\emptyset\}$ *or* $\mathcal{F} = \{[n]\}$*, then all the minimal elements of* $\mathrm{Lm}_{\mathrm{lex}}\,(I(\mathcal{F}))$ *are squarefree.*
- *If* $\mathcal{F} = \{\emptyset, [n]\}$*, then the only non-squarefree minimal leading monomial is* x_n^2*.*
- *In every remaining case,* $x_2^2, \ldots, x_n^2$ *are among the minimal generators of the initial ideal, and if* $\ell \geq 2$ *then so is* x_1^2*.*

Proof. We have to look for those $i \in [n]$ such that x_i is a standard monomial. The first case is trivial as $|\mathrm{Sm}_{\mathrm{lex}}\,(I(\mathcal{F}))| = |\mathcal{F}| = 1$, so $\mathrm{Sm}_{\mathrm{lex}}\,(I(\mathcal{F})) = \{1\}$.

In the second case note that setting $\ell = 1$, $q = n$ and $d = 0$ gives $\mathcal{F}$ as a modulo q complete ℓ-wide family. Thus Theorem 6.1.4 yields $\mathrm{Sm}_{\mathrm{lex}}\,(I(\mathcal{F})) = \{1, x_n\}$, hence we are done.

Again from the theorem, we have that if $\min\{d + \ell - 1, n - d\} > 0$, then $x_2, \ldots, x_n$ are standard monomials, and if $\ell > 1$ then $x_1 \in \mathrm{Sm}_{\mathrm{lex}}\,(I(\mathcal{F}))$ too. Therefore, to prove the last statement, it suffices to show that $\min\{d + \ell - 1, n - d\} \leq 0$ implies $\mathcal{F} = \{\emptyset\}$, $\mathcal{F} = \{[n]\}$ or $\mathcal{F} = \{\emptyset, [n]\}$.

In the proof of Corollary 6.1.5 we have seen that the intersection of the lines $X + Y = n$ and $X = \min\{d + \ell - 1, n - d\} + 1$ is below L^+, thus if $\min\{d + \ell - 1, n - d\} \leq 0$ then by Theorem 6.1.4 the only possible standard monomials of $I(\mathcal{F})$ are 1 and x_n, in particular $|\mathcal{F}| \leq 2$. But when $n > 2$, then $|\mathcal{F}| > 2$, as $\mathcal{F}$ contains all $\binom{n}{f}$ subsets of $[n]$ of some given cardinalities f, and for $0 < f < n$ we have $\binom{n}{f} > 2$. It may happen that $n = 2$ and $\mathcal{F} = \{\{1\}, \{2\}\}$, but then $\min\{d + \ell - 1, n - d\} = 1$. We conclude that one of the first two cases occurs here. □

Let $M = \{m_1, \ldots, m_k\} \subseteq [n]$ be a set with $m_1 < \cdots < m_k$. Using Corollary 6.1.5, we will formulate now in terms of the m_i that x_M is a minimal element of $\mathrm{Lm}_{\mathrm{lex}}\,(I(\mathcal{F}))$.

To decide whether $\hat{M}$ intersects L^- until a certain point along the lattice path, it suffices to check those points (n_X, n_Y) of $\hat{M}$, for which the previous point of $\hat{M}$ is $(n_X - 1, n_Y)$. The ith such point is $(i, m_i - i)$, as the ith horizontal step occurs in the m_ith step of $\hat{M}$. Clearly $(i, m_i - i)$ is above $Y = X - \ell$ if and only if $m_i - i > i - \ell$. Therefore a lattice path $\hat{M}$ stays strictly above L^- before its m_kth step, where it touches L^- if and only if $2i - \ell < m_i$ for all $1 \leq i \leq k - 1$ and $m_k = 2k - \ell$.

On the other hand, $\hat{M}$ stays below L^+ if and only if the points $(i-1, m_i-i)$ are below L^+. This is equivalent to $m_i - i < (i - 1) - \ell + q$, that is to $m_i < 2i - \ell + q - 1$.

Definition 6.1.7. Let $M = \{m_1, \dots, m_k\} \subseteq [n]$ be such that $m_1 < \cdots < m_k$.

The set M is in $\mathcal{L}_1$ if and only if $1 \le k \le \min\{d + \ell - 1, n - d\} + 1$, $2i - \ell < m_i < 2i - \ell + q - 1$ for all $1 \le i \le k - 1$ and $m_k = 2k - \ell$.

Hence $\mathcal{L}_1$ contains those sets M corresponding to minimal elements of $\mathrm{Lm}_{\mathrm{lex}}(I(\mathcal{F}))$ for which $\hat{M}$ touches the line L^-.

The set M is in $\mathcal{L}_2$ if and only if $k = \min\{d + \ell - 1, n - d\} + 1$, $2i - \ell < m_i < 2i - \ell + q - 1$ for all $1 \le i \le k$.

Thus, $\mathcal{L}_2$ contains those sets M corresponding to minimal leading monomials for which $\hat{M}$ touches the line $X = \min\{d + \ell - 1, n - d\} + 1$ but not at its intersection with L^-.

Finally, we introduce a similar notation for the non-squarefree minimal generators of $\langle \mathrm{Lm}_{\mathrm{lex}}(I(\mathcal{F}))\rangle$.

Set

$$L_3 = \begin{cases} \emptyset, & \text{if } \mathcal{F} = \{\emptyset\} \text{ or } \mathcal{F} = \{[n]\}; \\ \{n\}, & \text{if } \mathcal{F} = \{\emptyset, [n]\}; \\ \{2, \dots, n\}, & \text{otherwise, when } \ell = 1; \\ \{1, 2, \dots, n\}, & \text{otherwise (when } \ell > 1). \end{cases}$$

To summarize the results of this subsection we have

Theorem 6.1.8. *The minimal generating set of the lex initial ideal of $I(\mathcal{F})$ is*

$$\{x_M \ : \ M \in \mathcal{L}_1 \cup \mathcal{L}_2\} \cup \{x_j^2 \ : \ j \in L_3\}.$$

6.1.2 A Gröbner basis

From now on we suppose that p is a prime, q is a power of p and that $\mathbb{F}$ is a field of characteristic p. The ideal $I(\mathcal{F})$ of $\mathcal{F}$ will be understood in $\mathbb{F}[\mathbf{x}]$ accordingly. We will construct polynomials $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ for all $M \in \mathcal{L}_1 \cup \mathcal{L}_2$ such that $f \in I(\mathcal{F})$ and $\mathrm{lm}(f) = x_M$. Theorem 6.1.8 and the fact that $x_i^2 - x_i \in I(\mathcal{F})$ will then imply that we have a lex Gröbner basis of $I(\mathcal{F}) \trianglelefteq \mathbb{F}[\mathbf{x}]$. We show that it is a Gröbner basis for other orderings as well.

Let $M \in \mathcal{L}_1$, $M = \{m_1, \dots, m_k\}$ and $m_1 < \cdots < m_k$. Put $m_{k+i} = m_k + i$ for $0 \le i \le n - m_k = n - 2k + \ell$ and set

$$M' = \{m_1, \dots, m_{n-k+\ell}\} = \{m_1, \dots, m_k, m_k + 1, m_k + 2, \dots, n\}.$$

The complement $U = [n] \setminus M'$ then has $k - \ell$ elements, say $u_0 > u_1 > \cdots > u_{k-\ell-1}$.

Let $t = (k - q + 1)^+$ (where $a^+ = a$ if $a \ge 0$ and 0 otherwise), and define

$$s_M(\mathbf{x}) = \sum_{i=t+1}^{n-k+\ell} x_{m_i}.$$

Let us first define g_M as a polynomial with rational coefficients. We will shortly see that in fact $g_M \in \mathbb{Z}[\mathbf{x}]$, thus we may consider g_M as a polynomial with coefficients in $\mathbb{F}$ as well.

$$g_M(\mathbf{x}) = \left(\prod_{i=1}^{t} \left(x_{m_i} - x_{u_{t-i}}\right) \binom{s_M(\mathbf{x}) - d - \ell + k}{k-t} \right) \text{ reduced by } x_j^2 - x_j.$$

Reduction here simply means that we replace x_j^w by x_j for all $j \in [n]$ and $w \geq 2$. As a result g_M is multilinear. If $t = 0$ then the empty product is defined to be 1. The definition of g_M makes sense, as if $1 \leq i \leq t$, then $0 \leq t - i \leq t - 1 = k - q < k - \ell$ gives that $u_{t-i} \in U$ is defined.

The next lemma assures that $g_M \in \mathbb{Z}[\mathbf{x}]$.

Lemma 6.1.9. *Let $g(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ be a polynomial and suppose that $g(\mathbf{v}) \in \mathbb{Z}$ for all $\mathbf{v} \in \{0,1\}^n$. Reduce $g(\mathbf{x})$ by $x_j^2 - x_j$ for all $j \in [n]$ to get $\hat{g}(\mathbf{x})$. Then $\hat{g}(\mathbf{x})$ has integer coefficients.*

Proof. Clearly $\hat{g}(\mathbf{x})$ is squarefree, thus it is the linear combination of monomials of the form x_F ($F \subseteq [n]$). Suppose by contradiction that for some $F \subseteq [n]$, the coefficient of x_F is not an integer. Assume furthermore that F is a minimal such set. The value of g on any $\mathbf{v} \in \{0,1\}^n$ is not changed by the reduction, since $x_j^2 - x_j$ vanishes on all such $\mathbf{v}$, that is $\hat{g}(\mathbf{v}) \in \mathbb{Z}$. On the other hand, $\hat{g}(\mathbf{v}_F)$ is exactly the sum of the coefficients of the monomials $x_{F'}$ in $\hat{g}(\mathbf{x})$ for all $F' \subseteq F$. By the minimality of F, these are all integers, except the coefficient of x_F. This is a contradiction, therefore $\hat{g} \in \mathbb{Z}[\mathbf{x}]$ holds. □

Now suppose that $\min\{d+\ell-1, n-d\} = d+\ell-1$, that is $d \leq \frac{n-\ell+1}{2}$. Let $M = \{m_1, \ldots, m_{d+\ell}\}$ be an element of $\mathcal{L}_2$ with $m_1 < \cdots < m_{d+\ell}$. Set $U = [n] \setminus M = \{u_0, u_1, \ldots, u_{n-d-\ell-1}\}$ and assume that $u_0 > u_1 > \cdots > u_{n-d-\ell-1}$. Finally set $t = (n-d-q+1)^+$. The polynomial in $I(\mathcal{F})$ with leading term x_M will be

$$h_M(\mathbf{x}) = \prod_{i=1}^{t} \left(x_{m_i} - x_{u_{t-i}}\right) \prod_{i=t+1}^{d+\ell} x_{m_i}.$$

We see that if $1 \leq i \leq t$ then $0 \leq t - i \leq t - 1 = n - d - q < n - d - \ell$. This means that $u_{t-i} \in U$ as we anticipated.

In the other case, where $\min\{d + \ell - 1, n - d\} = n - d$ we have $M = \{m_1, \ldots, m_{n-d+1}\} \in \mathcal{L}_2$, $m_1 < \cdots < m_{n-d+1}$, and the complement $U = [n] \setminus M = \{u_0, u_1, \ldots, u_{d-2}\}$ with $u_0 > u_1 > \cdots > u_{d-2}$. The right choice here is $t = (d + \ell - q)^+$ and

$$h_M(\mathbf{x}) = \prod_{i=1}^{t} \left(x_{m_i} - x_{u_{t-i}}\right) \prod_{i=t+1}^{n-d+1} (x_{m_i} - 1).$$

Again, $\ell < q$ gives that $t-i$ is in the appropriate range.

We shall prove that our polynomials form a Gröbner basis of $I(\mathcal{F})$ through some lemmas.

Lemma 6.1.10. *If* $f \equiv f' \pmod q$ *and* $0 \le m < q$ *is an integer then* $\binom{f}{m} \equiv \binom{f'}{m} \pmod p$.

Proof. It is enough to show that $\binom{q+f}{m} \equiv \binom{f}{m} \pmod p$. This holds since

$$\binom{q+f}{m} = \sum_{j=0}^{m} \binom{q}{j} \cdot \binom{f}{m-j} \equiv \binom{f}{m} \pmod p,$$

where we used the fact that $\binom{q}{j} \equiv 0 \pmod p$ if $0 < j < q$. □

Lemma 6.1.11. *If* $M \in \mathcal{L}_1$, *then* $g_M \in I(\mathcal{F})$.

Proof. We show that if $\mathbf{v}_F$ is the characteristic vector of an $F \in \mathcal{F}$ then $g_M(\mathbf{v}_F)$ (as an integer) is divisible with p. We shall use again that the value of g_M on any $\mathbf{v} \in \{0,1\}^n$ is not changed by the reduction modulo $x_j^2 - x_j$.

Because of the definition of t, we need to consider the cases $t = 0$ and $t \ge 1$ separately. Suppose first that $t = 0$, that is $k \le q-1$. Then $s_M(\mathbf{v}_F) = |F \cap M'|$, and hence

$$g_M(\mathbf{v}_F) = \binom{|F \cap M'| - d - \ell + k}{k}.$$

Let $z \in \mathbb{Z}$ such that $qz+d \le |F| < qz+d+\ell$. Now $|F \cap M'| \le |F| < qz+d+\ell$ and $|F \cap M'| = |F \setminus U| \ge |F| - |U| \ge qz+d+\ell-k$ gives

$$0 \le |F \cap M'| - d - \ell + k - qz < k < q.$$

By Lemma 6.1.10 we have $\binom{|F\cap M'|-d-\ell+k}{k} \equiv \binom{|F\cap M'|-d-\ell+k-qz}{k} = 0 \pmod p$ showing that $g_M(\mathbf{v}_F)$ vanishes modulo p.

Suppose that $t \ge 1$. If $s_M(\mathbf{v}_F) = |F \cap \{m_{t+1}, \dots, m_{n-k+\ell}\}| \not\equiv d+\ell-k-1 \pmod q$, then $s_M(\mathbf{v}_F) - d - \ell + k$ is congruent to an integer f between 0 and $q-2$, so by Lemma 6.1.10

$$\binom{s_M(\mathbf{v}_F) - d - \ell + k}{k-t} = \binom{s_M(\mathbf{v}_F) - d - \ell + k}{q-1} \equiv \binom{f}{q-1} = 0 \pmod p.$$

We may therefore assume that $|F \cap \{m_{t+1}, \dots, m_{n-k+\ell}\}| \equiv d+\ell-k-1 \pmod q$.

We claim then that $\prod_{i=1}^{t}\left(x_{m_i}-x_{u_{t-i}}\right)$ vanishes on $\mathbf{v}_F$. If it does not, then $|F\cap\{m_i,u_{t-i}\}|=1$ for all $1\le i\le t$, thus $|F\cap\{m_1,\ldots,m_t,u_0,\ldots,u_{t-1}\}|=t$. To sum up

$$|F|=|F\cap\{m_1,\ldots,m_t,u_0,\ldots,u_{t-1}\}|+|F\cap\{m_{t+1},\ldots,m_{n-k+\ell}\}|+ \\ |F\cap\{u_t,\ldots,u_{k-\ell-1}\}|\equiv t+d+\ell-k-1+|F\cap\{u_t,\ldots,u_{k-\ell-1}\}|\equiv \\ d+\ell+|F\cap\{u_t,\ldots,u_{k-\ell-1}\}|\pmod q,$$

that is,

$$|F|\equiv d+\ell+|F\cap\{u_t,\ldots,u_{k-\ell-1}\}|\pmod q.$$

This is a contradiction since $0\le|F\cap\{u_t,\ldots,u_{k-\ell-1}\}|\le k-\ell-t=q-1-\ell$ shows that $|F|$ is congruent to an integer in the interval $[d+\ell,d+q-1]$. □

Lemma 6.1.12. *If $M\in\mathcal{L}_2$, then $h_M\in I(\mathcal{F})$.*

Proof. We will verify the stronger statement that (as an integer) $h_M(\mathbf{v}_F)=0$ for all $F\in\mathcal{F}$. The proof is quite similar to that of the previous lemma.

Let us assume first that $\min\{d+\ell-1,n-d\}=d+\ell-1$. Suppose by contradiction that $M=\{m_1,\ldots,m_{d+\ell}\}\in\mathcal{L}_2$ and $F\in\mathcal{F}$ such that $h_M(\mathbf{v}_F)\neq0$. By the nonvanishing of the product $\prod_{i=1}^{t}\left(x_{m_i}-x_{u_{t-i}}\right)$ we have $|F\cap\{m_1,\ldots,m_t,u_0,\ldots,u_{t-1}\}|=t$ and from the other factor of h_M we infer that $\{m_{t+1},\ldots,m_{d+\ell}\}\subseteq F$. Thus

$$|F|=|F\cap\{m_1,\ldots,m_t,u_0,\ldots,u_{t-1}\}|+|F\cap\{m_{t+1},\ldots,m_{d+\ell}\}|+ \\ |F\cap\{u_t,\ldots,u_{n-d-\ell-1}\}|=t+(d+\ell-t)+|F\cap\{u_t,\ldots,u_{n-d-\ell-1}\}|, \tag{6.10}$$

which means

$$d+\ell\le|F|\le d+\ell+(n-d-\ell-t)=n-t\le n-(n-d-q+1)=d+q-1,$$

which is in contradiction to the definition of $\mathcal{F}$.

If $\min\{d+\ell-1,n-d\}=n-d$ is the case with $M=\{m_1,\ldots,m_{n-d+1}\}\in\mathcal{L}_2$, and $F\in\mathcal{F}$ was the counterexample for the statement, then again $|F\cap\{m_1,\ldots,m_t,u_0,\ldots,u_{t-1}\}|=t$. From the product $\prod_{i=t+1}^{n-d+1}(x_{m_i}-1)$ we get $|F\cap\{m_{t+1},\ldots,m_{n-d+1}\}|=0$. Similarly to the disjoint decomposition (6.10) we obtain

$$|F|=t+|F\cap\{u_t,\ldots,u_{d-2}\}|$$

and hence

$$d + \ell - q \le t \le |F| \le t + (d - 1 - t) = d - 1,$$

which contradicts the fact that $F \in \mathcal{F}$. $\square$

Lemma 6.1.13. *If $M \in \mathcal{L}_1$, and $\prec$ is a term order such that $x_n \prec \cdots \prec x_1$, then $\operatorname{lm}(g_M) = x_M$.*

Proof. Observe that in the definition of $\mathcal{L}_1$ we saw that $m_k = 2k - \ell$, from which we obtain $k = m_k - k + \ell \le n - k + \ell$. It follows that $s_M(\mathbf{x})$ contains the variables $x_{m_{t+1}}, \dots, x_{m_k}$, therefore the monomial $x_{m_{t+1}} \dots x_{m_k}$ appears in

$$\binom{s_M(\mathbf{x}) - d - \ell + k}{k - t} = \frac{1}{(k-t)!} \prod_{i=-d-\ell+t+1}^{-d-\ell+k} (s_M(\mathbf{x}) + i)$$

and its coefficient is 1. Obviously, this is the greatest multilinear monomial of the above product.

We claim that $x_{m_{t+1}} \dots x_{m_k}$ is also the leading term of

$$\binom{s_M(\mathbf{x}) - d - \ell + k}{k - t} \text{ reduced by } x_j^2 - x_j.$$

Indeed, any other monomial of the reduced polynomial is of the form x_N for some $N \subseteq \{m_{t+1}, \dots, m_{n-k+\ell}\}$, $|N| \le k - t$. Then clearly for the ith greatest element n_i of N it holds that $m_{t+i} \le n_i$, thus $x_{m_{t+i}} \succeq x_{n_i}$ which implies $x_{m_{t+1}} \dots x_{m_k} \succeq x_N$. On the other hand, the coefficient of $x_{m_{t+1}} \dots x_{m_k}$ remains 1, as the reduction of a monomial by some polynomial $x_j^2 - x_j$ reduces its degree.

We turn now to the leading term of $\prod_{i=1}^{t} \left(x_{m_i} - x_{u_{t-i}}\right)$. The set of variables of this part and of the one we have already considered are disjoint, hence we will need no more reduction by $x_j^2 - x_j$. Therefore we can use the fact that the greatest term of a product is the product of the leading monomials, and so it is enough to show, that the leading term of $\prod_{i=1}^{t} \left(x_{m_i} - x_{u_{t-i}}\right)$ is $x_{m_1} \dots x_{m_t}$. Applying again the rule for the leading monomials of products it suffices to verify that $m_i < u_{t-i}$.

Suppose for contradiction that $m_i \ge u_{t-i}$ (in fact this means that $m_i > u_{t-i}$ since M and U are disjoint), and that $i \ge 1$ is minimal satisfying this property. Note that the existence of such a $1 \le i \le t$ implies that $1 \le t$, that is $t = k - q + 1$. Consider the set

$$N = \{m_1, m_2 \dots, m_{i-1}, u_{t-i}, u_{t-i+1}, \dots, u_{k-\ell-1}\}.$$

By the minimality of i we have $m_{i-1} < u_{t-(i-1)} < u_{t-i} < m_i$, thus intersecting the equality $[n] = U \cup M$ with $[u_{t-i}]$ we get $[u_{t-i}] = N$. (This is also true if $i = 1$, one may check it directly.) We conclude that $m_i > u_{t-i} = |N| = i - 1 + (k - \ell - t + i) = 2i - \ell + q - 2$ a contradiction to $m_i < 2i - \ell + q - 1$ in the definition of $\mathcal{L}_1$. □

Lemma 6.1.14. *If $M \in \mathcal{L}_2$, and $\prec$ is a term order such that $x_n \prec \cdots \prec x_1$, then* $\operatorname{lm}(h_M) = x_M$.

Proof. The argument is very much similar to the previous one. In the first case, where $\min\{d + \ell - 1, n - d\} = d + \ell - 1$, it is clearly enough to show that $m_i < u_{t-i}$. If there was a counterexample, then let i be the minimal one, such that $m_i > u_{t-i}$. Then

$$\{m_1, m_2 \dots, m_{i-1}, u_{t-i}, u_{t-i+1} \dots, u_{n-d-\ell-1}\} = \{1, 2, \dots, u_{t-i}\},$$

thus $m_i > u_{t-i} = i - 1 + (n - d - \ell - t + i) = 2i - \ell + q - 2$. Every set in $\mathcal{L}_2$ has the property that $m_i < 2i - \ell + q - 1$, hence the above inequality is impossible.

If $\min\{d + \ell - 1, n - d\} = n - d$, then the minimal counterexample would yield

$$\{m_1, m_2, \dots, m_{i-1}, u_{t-i}, u_{t-i+1} \dots, u_{d-2}\} = \{1, 2, \dots, u_{t-i}\},$$

and so $m_i > u_{t-i} = i-1+(d-1-t+i) = 2i-\ell+q-2$ again a contradiction. In this case we also have to note that the leading monomial of $\prod_{i=t+1}^{n-d+1} (x_{m_i} - 1)$ is the product of the leading terms of the $x_{m_i} - 1$, that is $x_{m_{t+1}} \dots x_{m_{n-d+1}}$. □

We have almost proven the main theorem of the present subsection.

Theorem 6.1.15. *Let $\mathcal{L}_1$, $\mathcal{L}_2$ and L_3 be as in Definition 6.1.7, g_M, h_M the above defined polynomials. Suppose that $\prec$ is a term order such that $x_n \prec \cdots \prec x_1$, $\mathbb{F}$ is a field of characteristic p and q is a power of p. Then*

$$G = \{g_M \ : \ M \in \mathcal{L}_1\} \cup \{h_M \ : \ M \in \mathcal{L}_2\} \cup \{x_j^2 - x_j \ : \ j \in L_3\}$$

is a Gröbner basis with respect to $\prec$ of the ideal $I(\mathcal{F}) \trianglelefteq \mathbb{F}[\mathbf{x}]$. In particular $\operatorname{Sm}_\prec(I(\mathcal{F})) = \operatorname{Sm}_{\text{lex}}(I(\mathcal{F}))$.

Proof. We first suppose that we work with the lex order.

By Theorem 6.1.8, Lemma 6.1.13 and Lemma 6.1.14 we have that

$$\{\operatorname{lm}(g_M) \ : \ M \in \mathcal{L}_1\} \cup \{\operatorname{lm}(h_M) \ : \ M \in \mathcal{L}_2\} \cup \left\{\operatorname{lm}\left(x_j^2 - x_j\right) \ : \ j \in L_3\right\}$$

is the set of the minimal elements of $\mathrm{Lm}_{\mathrm{lex}}(I(\mathcal{F}))$. Lemmas 6.1.11 and 6.1.12 imply that $G \subseteq I(\mathcal{F})$. These together yield that G is a lex Gröbner basis.

Assume now that $\prec$ is an arbitrary term order, which, when restricted to the variables, coincides with lex. In Lemmas 6.1.13 and 6.1.14 we proved that the leading monomials of g_M and h_M with respect to $\prec$ are the same as for the lexicographic ordering, hence we have that $\mathrm{Sm}_{\prec}(I(\mathcal{F})) \subseteq \mathrm{Sm}_{\mathrm{lex}}(I(\mathcal{F}))$. But $|\mathrm{Sm}_{\prec}(I(\mathcal{F}))| = |\mathcal{F}| = |\mathrm{Sm}_{\mathrm{lex}}(I(\mathcal{F}))|$, thus $\mathrm{Sm}_{\prec}(I(\mathcal{F})) = \mathrm{Sm}_{\mathrm{lex}}(I(\mathcal{F})) = \mathrm{Sm}_{\mathrm{lex}}(G) = \mathrm{Sm}_{\prec}(G)$. □

Remark 6.1.16. An explicit form of g_M can be given by a formula involving elementary symmetric polynomials $\sigma_{N,i}(\mathbf{x}) = \sum\limits_{\substack{N' \subseteq N \\ |N'|=i}} x_{N'}$ as follows.

$$\left(\binom{s_M(\mathbf{x})+c}{m} \text{ reduced by } x_j^2 - x_j\right) = \sum_{i=0}^{m} (-1)^i \binom{i-c-1}{i} \sigma_{M',m-i}(\mathbf{x})$$

is valid for every $c \in \mathbb{Z}$ and $m \in \mathbb{N}$.

Proof. By a well-known identity of binomial coefficients we have

$$\binom{s_M(\mathbf{x})+c}{m} = \sum_{i=0}^{m} (-1)^i \binom{i-c-1}{i} \binom{s_M(\mathbf{x})}{m-i}.$$

The multilinear monomials form an $\mathbb{F}$-linear basis of the space of functions from $\{0,1\}^n$ to $\mathbb{F}$. In our case $\binom{s_M(\mathbf{v})}{m-i} = \sigma_{M',m-i}(\mathbf{v})$ for all $\mathbf{v} \in \{0,1\}^n$, and both polynomials $\left(\binom{s_M(\mathbf{x})}{m-i} \text{ reduced by } x_j^2 - x_j\right)$ and $\sigma_{M',m-i}(\mathbf{x})$ contain only squarefree monomials. They must be equal. □

One might ask how far G is from the unique reduced Gröbner basis of $I(\mathcal{F})$. Concerning this, we claim the following.

Remark 6.1.17. The leading coefficients of g_M, h_M and $x_j^2 - x_j$ are 1.
The leading monomials of G minimally generate the initial ideal of $I(\mathcal{F})$.
If $x_N \notin \mathrm{Sm}_{\prec}(I(\mathcal{F}))$ is a monomial of $g_M - \mathrm{lm}(g_M)$ or of $h_M - \mathrm{lm}(h_M)$ with nonzero coefficient, then x_N is a minimal leading monomial of the same degree as x_M, that is $N \in \mathcal{L}_1 \cup \mathcal{L}_2$ and $|N| = |M|$.

Proof. The first statement is immediate from the definitions. The second was verified in the proof of Theorem 6.1.15

For the last one, we intend to show that the lattice path $\hat{M}$ separates the lines L^- and $X = \min\{d+\ell-1, n-d\}$ from $\hat{N}$ in a 'week' sense, that is $\hat{N}$ cannot cross $\hat{M}$. It would yield that $\hat{N}$ can reach the lines L^- and

$X = \min\{d+\ell-1, n-d\}$ only at those points where $\hat{M}$ does, which proves our claim.

To this end, we show that $\hat{N}$ goes above and left of $\hat{M}$, or—to make it more precise—we show that the X coordinate of the intersection of $\hat{N}$ and $X+Y=j$ is less than or equal to the X coordinate of the intersection of $\hat{M}$ and $X+Y=j$ for all $j \in [n]$. In other words we need $|N \cap [j]| \le |M \cap [j]|$.

To prove this, let us fix a $j \in [n]$ and let i be maximal such that $m_i \le j$. If $m_{|M|} \le j$ (that is $i \ge |M|$), then

$$|N \cap [j]| \le |N| \le |M| = |M \cap [j]| \,.$$

Here we used that the leading monomial x_M has the highest degree in our polynomials.

Hence we may suppose that $j < m_{|M|}$, that is $i < |M|$. Therefore $|M \cap [j]| = |\{m_1, \dots, m_i\}| = i$. By the definition of g_M and h_M we have

$$N \subseteq \{m_1, \dots, m_t, u_0, \dots, u_{t-1}\} \cup \{m_{t+1}, m_{t+2}, \dots\}$$

and $|N \cap \{m_{i'}, u_{t-i'}\}| = 1$ for $i' = 1, \dots, t$. If $i \ge t$, then these imply

$$|N \cap [j]| \le |N \cap \{m_1, \dots, m_t, u_0, \dots, u_{t-1}\}| + |N \cap \{m_{t+1}, \dots, m_i\}| \le i,$$

and we are done. Otherwise, if $i < t$, then applying $m_{i+1} < u_{t-(i+1)}$, that we have learned from the proof of Lemma 6.1.13 and Lemma 6.1.14, we have

$$N \cap [j] \subseteq \{m_1, \dots, m_i, u_{t-i}, \dots, u_{t-1}\},$$

and so $|N \cap [j]| \le i$ by $|N \cap \{m_{i'}, u_{t-i'}\}| = 1$. □

The following example shows that in general G is not the reduced Gröbner basis.

Example 6.1.18. Put $p = q = 5$, $\ell = 1$, $d = 5$, $n = 10$ and $M = \{2, 4, 6, 8, 9\}$. Then $M \in \mathcal{L}_1$, $s_M(\mathbf{x}) = x_4 + x_6 + x_8 + x_9 + x_{10}$, and

$$g_M(\mathbf{x}) = \left((x_2 - x_7) \binom{s_M(\mathbf{x}) - 1}{4} \right) \text{ reduced by } x_j^2 - x_j.$$

As the coefficient of $x_4x_6x_8x_9$ in $\binom{s_M(\mathbf{x})-1}{4}$ is 1, we have that $x_4x_6x_7x_8x_9$ appears in g_M with coefficient -1. But $x_4x_6x_7x_8x_9$ is a leading monomial of $I(\mathcal{F})$. Let N be the corresponding set $\{4, 6, 7, 8, 9\} \in \mathcal{L}_1$. One can easily check (the proof of our previous remark helps), that $g_N - \mathrm{lm}\,(g_N)$ is a linear combination of standard monomials. Then it is not hard to see that $g_M + g_N$ is in the reduced Gröbner basis as well.

6.1.3 The Hilbert function

To compute the Hilbert function of $\mathcal{F}$, applying Corollary 2.1.21, we will count the number of standard monomials of a given degree with respect to a degree compatible ordering. Theorem 6.1.15 tells us that we can use the description of the standard monomials by lattice paths given in Theorem 6.1.4. Thus we proceed by counting cardinalities of certain sets of lattice paths.

Number of lattice paths between two lines

Let $s, t > 0$ be integers. We temporarily replace our previous notation L^+ and L^- to make the statements clearer. We will have two boundary lines $L^+\colon Y = X + s$ and $L^-\colon Y = X - t$. Let us fix a point $P = (n_X, n_Y)$ as the endpoint of our lattice paths. We assume that $n_X, n_Y \geq 0$ and $n = n_X + n_Y$.

Denote by A_1 the set of lattice paths that end in P and reach the line L^+. Let A_2 be the set of paths that end in P, reach L^+ and later sometimes touch L^-. In general let us denote by A_i the set of paths reaching L^+, L^-, L^+, $\ldots$ (i times) in this specified order and ending in P. The definition of A_i does not exclude those paths which have even more intersections with the given lines. In particular A_0 stands for all the lattice paths from the origin to the point P. Note that $A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots$.

Similarly, let B_i be the set of paths reaching L^-, L^+, L^-, $\ldots$ (i times) in this specified order, $B_0 = A_0$.

We can obtain the cardinality of A_i and B_i by applying the reflection principle i times as follows.

Lemma 6.1.19. *If $n_Y \geq n_X - t$ (that is if the origin and P are on the same side of L^-), then*

$$|A_{2i}| = \binom{n}{n_X - i(t+s)}, \quad and \quad |B_{2i+1}| = \binom{n}{n_X - i(t+s) - t}.$$

If $n_Y \leq n_X + s$ (that is if the origin and P are on the same side of L^+), then

$$|A_{2i+1}| = \binom{n}{n_X + i(t+s) + s}, \quad and \quad |B_{2i}| = \binom{n}{n_X + i(t+s)}.$$

Proof. For the proof we indicate the dependence of A_i from (n_X, n_Y) by writing $A_i(n_X, n_Y)$.

We prove the claim by induction on the subscript of A. Clearly we have $|A_0(n_X, n_Y)| = \binom{n}{n_X}$. Suppose that $i \geq 0$ and the statement is true for $2i$. Let $\hat{M} \in A_{2i+1}(n_X, n_Y)$ be a lattice path and suppose that its last intersection with L^+ is (v_1, v_2). Reflecting the section of $\hat{M}$ from (v_1, v_2) to (n_X, n_Y) with respect to the line L^+, we get an element of $A_{2i}(n_Y - s, n_X + s)$. Since $(n_Y - s, n_X + s)$ and the origin are on different sides of L^+, it is easy to see that this is a one-to-one correspondence between $A_{2i+1}(n_X, n_Y)$ and $A_{2i}(n_Y - s, n_X + s)$. We also have $n_X + s \geq n_Y \geq (n_Y - s) - t$, therefore the induction hypothesis applies: $|A_{2i+1}(n_X, n_Y)| = |A_{2i}(n_Y - s, n_X + s)| = \binom{n}{n_Y - s - i(t+s)} = \binom{n}{n_X + i(t+s) + s}$.

If $i \geq 1$ and the statement is true for $2i - 1$, then a similar reflection over L^- gives a one-to-one correspondence between $A_{2i}(n_X, n_Y)$ and $A_{2i-1}(n_Y + t, n_X - t)$, hence $|A_{2i}(n_X, n_Y)| = |A_{2i-1}(n_Y + t, n_X - t)| = \binom{n}{n_Y + t + (i-1)(t+s) + s}$.

Note that we implicitly gave a one-to-one correspondence between A_{2i} (respectively A_{2i+1}) and the lattice paths from the origin to $(n_X - i(s + t), n_Y + i(s + t))$ (respectively $(n_Y - i(s + t) - s, n_X + i(s + t) + s)$).

Finally, to verify the formulae for $|B_i|$ we can simply switch the role of s and t and reflect every lattice path over the line $Y = X$. □

We denote by C the set of those lattice paths, which join the origin with the point P without reaching any of the two lines L^+ and L^-.

Proposition 6.1.20. *If $n_X - t \leq n_Y \leq n_X + s$ (P is between L^+ and L^-), then*

$$|C| = \sum_{i=-\infty}^{\infty} \left(\binom{n}{n_X - i(t+s)} - \binom{n}{n_X - i(t+s) - t} \right).$$

Proof. Note that $C = A_0 \setminus (A_1 \cup B_1)$. It is easy to see that $A_i \cap B_i = A_{i+1} \cup B_{i+1}$, thus $|A_i \cup B_i| = |A_i| + |B_i| - |A_{i+1} \cup B_{i+1}|$. Applying this repeatedly we get

$$|C| = |A_0| - |A_1 \cup B_1| = |A_0| + \sum_{i=1}^{\infty} (-1)^i (|A_i| + |B_i|).$$

Here we used also that $A_i = B_i = \emptyset$ for i large enough.

Substituting the binomial coefficients from Lemma 6.1.19, we have

$$|C| = \binom{n}{n_X} - \binom{n}{n_X + s} - \binom{n}{n_X - t} + \sum_{i=1}^{\infty} \left(\binom{n}{n_X - i(t+s)} + \binom{n}{n_X + i(t+s)} - \binom{n}{n_X + i(t+s) + s} - \binom{n}{n_X - i(t+s) - t} \right) =$$
$$\sum_{i=-\infty}^{\infty} \left(\binom{n}{n_X - i(t+s)} - \binom{n}{n_X - i(t+s) - t} \right) + \sum_{i=1}^{\infty} \binom{n}{n_X + i(t+s) - t} - \sum_{i=0}^{\infty} \binom{n}{n_X + i(t+s) + s} =$$
$$\sum_{i=-\infty}^{\infty} \left(\binom{n}{n_X - i(t+s)} - \binom{n}{n_X - i(t+s) - t} \right).$$

□

Our last set of lattice paths D to examine consists of all the paths from the origin to P which do not reach L^- before reaching L^+ (it may reach neither).

Proposition 6.1.21. *If $n_Y \geq n_X - t$ (P is above L^-), then*

$$|D| = \sum_{i=0}^{\infty} \left(\binom{n}{n_X - i(t+s)} - \binom{n}{n_X - i(t+s) - t} \right).$$

If $n_Y \leq n_X - t$ (P is below L^-), then

$$|D| = \sum_{i=1}^{\infty} \left(\binom{n}{n_X + i(t+s) - t} - \binom{n}{n_X + i(t+s)} \right).$$

Proof. We have a disjoint union decomposition $D = \bigcup_{i=0}^{\infty} (A_{2i} \setminus B_{2i+1})$. Indeed, $A_{2i} \setminus B_{2i+1}$ contains a lattice path $\hat{M}$ if and only if the maximal sequence of intersections of $\hat{M}$ with L^+ and L^- which alternates is either L^+, L^-, …, L^+, L^- ($2i$ lines) or L^+, L^-, …, L^+, L^-, L^+ ($2i+1$ lines). The union of these give D.

Since $A_{2i} \supseteq B_{2i+1}$, Lemma 6.1.19 immediately proves the first statement.

Note that if P is below L^-, then by definitions $A_0 = B_1$, $A_{2i} = A_{2i-1}$ (for $i \geq 1$) and $B_{2i+1} = B_{2i}$ (for $i \geq 0$). The origin and P are on the same side of L^+, and so Lemma 6.1.19 yields formulae for A_{2i-1} and B_{2i}. Therefore

$$|D| = \sum_{i=0}^{\infty} (|A_{2i}| - |B_{2i+1}|) = \sum_{i=1}^{\infty} (|A_{2i-1}| - |B_{2i}|) =$$
$$\sum_{i=1}^{\infty} \left(\binom{n}{n_X + i(t+s) - t} - \binom{n}{n_X + i(t+s)} \right).$$

□

The Hilbert function of $\mathcal{F}$

To obtain the Hilbert function $H_{\mathcal{F}}(m)$, it remains to put together what we know about lattice paths and standard monomials of $I(\mathcal{F})$, where $\mathcal{F}$ is a modulo q complete ℓ-wide family of sets.

Theorem 6.1.22. *Let $r = \min\{d + \ell - 1, n - d\}$, suppose that the base field $\mathbb{F}$ is of characteristic p and q is a power of p.*
If $0 \le m \le r$, then

$$H_{\mathcal{F}}(m) = \sum_{i=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m - iq - k},$$

if $m > r$, then

$$H_{\mathcal{F}}(m) = \sum_{i=-\infty}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{r + iq - k} - \sum_{i=1}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m + iq - k}.$$

Proof. Instead of writing merely C and D, in this proof we again indicate their dependence on the endpoint (n_X, n_Y) of the lattice paths, while we leave $\mathcal{F}$ from the subscript of $H_{\mathcal{F}}$. We intend to apply the computations of the previous subsection with $s = q - \ell$ and $t = \ell$. By Theorem 6.1.15 and Corollary 2.1.21 we know that $H(m)$ is the number of elements of $\mathrm{Sm}_{\mathrm{lex}}(I(\mathcal{F}))$ of degree at most m, thus we can use the description of the lex standard monomials of Theorem 6.1.4.

Hence if $m \le r$ then the set of lattice paths corresponding to standard monomials of degree at most m is

$$\bigcup_{n_X=0}^{m} D(n_X, n - n_X).$$

Its cardinality is then given by the first case of Proposition 6.1.21:

$$H(m) = \sum_{n_X=0}^{m}\sum_{i=0}^{\infty}\left(\binom{n}{n_X - iq} - \binom{n}{n_X - iq - \ell}\right) = \sum_{i=0}^{\infty}\sum_{k=0}^{\ell-1}\binom{n}{m - iq - k}, \tag{6.11}$$

as we claimed.

Suppose now that $r < m < \frac{n+\ell}{2}$. The second inequality means exactly that the point $(m, n-m)$ is above L^-. In this case, the set of lattice paths we need is

$$\left(\bigcup_{n_X=0}^{r} D(n_X, n-n_X)\right) \cup \left(\bigcup_{n_X=r+1}^{m} (D(n_X, n-n_X) \setminus C(n_X, n-n_X))\right)$$

according to Theorem 6.1.4. We use Propositions 6.1.20 and 6.1.21 to get

$$H(m) = H(r) + \sum_{n_X=r+1}^{m}\left(\sum_{i=0}^{\infty}\left(\binom{n}{n_X - iq} - \binom{n}{n_X - iq - \ell}\right) - \sum_{i=-\infty}^{\infty}\left(\binom{n}{n_X - iq} - \binom{n}{n_X - iq - \ell}\right)\right) = H(r) - \sum_{i=1}^{\infty}\sum_{n_X=r+1}^{m}\left(\binom{n}{n_X + iq} - \binom{n}{n_X + iq - \ell}\right) = H(r) - \sum_{i=1}^{\infty}\sum_{k=0}^{\ell-1}\left(\binom{n}{m + iq - k} - \binom{n}{r + iq - k}\right).$$

Applying the formula for $H(r)$ we have already obtained, we have

$$\begin{aligned} H(m) &= \sum_{i=0}^{\infty}\sum_{k=0}^{\ell-1}\binom{n}{r - iq - k} + \sum_{i=1}^{\infty}\sum_{k=0}^{\ell-1}\left(\binom{n}{r + iq - k} - \binom{n}{m + iq - k}\right) \\ &= \sum_{i=-\infty}^{\infty}\sum_{k=0}^{\ell-1}\binom{n}{r + iq - k} - \sum_{i=1}^{\infty}\sum_{k=0}^{\ell-1}\binom{n}{m + iq - k}, \end{aligned}$$

which was to be proved.

Finally, if $\frac{n+\ell}{2} \leq m$, then let $r' = \left\lfloor \frac{n+\ell-1}{2} \right\rfloor$. The number of standard monomials of degree n_X between $r'+1$ and m are given by the lattice paths in

$$\bigcup_{n_X=r'+1}^{m} D(n_X, n-n_X).$$

Therefore by the second part of Proposition 6.1.21

$$H(m) = H(r') + \sum_{n_X=r'+1}^{m} \sum_{i=1}^{\infty} \left(\binom{n}{n_X + iq - \ell} - \binom{n}{n_X + iq} \right) = H(r') +$$
$$\sum_{i=1}^{\infty} \sum_{k=0}^{\ell-1} \left(\binom{n}{r' + iq - k} - \binom{n}{m + iq - k} \right) = \sum_{i=-\infty}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{r + iq - k} -$$
$$\sum_{i=1}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{r' + iq - k} + \sum_{i=1}^{\infty} \sum_{k=0}^{\ell-1} \left(\binom{n}{r' + iq - k} - \binom{n}{m + iq - k} \right) =$$
$$\sum_{i=-\infty}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{r + iq - k} - \sum_{i=1}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m + iq - k},$$

where we also used the just computed formula for $H(r')$. □

It is easy to see that in the case $m > r$, the first sum is precisely the cardinality of $\mathcal{F}$. Note that the second sum is 0 when $m > n + \ell - q - 1$. Therefore for such an m, $H_{\mathcal{F}}(m) = |\mathcal{F}|$.

In the combinatorial applications, we benefit from the next corollary.

Corollary 6.1.23. *If* $0 \le m \le \frac{n+\ell}{2}$, *then*

$$H_{\mathcal{F}}(m) \le \sum_{i=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m - iq - k}.$$

Proof. If $m \le r = \min\{d + \ell - 1, n - d\}$ then we are done by Theorem 6.1.22. Otherwise, suppose that $r < m \le \frac{n+\ell}{2}$. We have to show that

$$\sum_{i=-\infty}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{r + iq - k} - \sum_{i=1}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m + iq - k} \le \sum_{i=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m - iq - k}.$$

Instead of a direct calculation, let us recall a few details from the proof of Theorem 6.1.22.

The left hand side is the number of standard monomials of $I(\mathcal{F})$ of degree at most m. The corresponding lattice paths have the property, that they do not reach L^- before touching L^+ and that they end in $(n_X, n - n_X)$ for some $n_X \le m$, that is they all belong to the set

$$\bigcup_{n_X=0}^{m} D(n_X, n - n_X).$$

In the proof (equation (6.11)), we have seen that the right hand side is exactly the number of such lattice paths. (Note that the condition $m \le \frac{n+\ell}{2}$ means that the point $(m, n - m)$ is above L^-.) □

6.2 Maximal cardinality of L-avoiding L-intersecting families

Definition 6.2.1. Let L be a subset of integers and $\mathcal{G}$ be a system of sets. Then $\mathcal{G}$ is *modulo q L-avoiding* if $G \in \mathcal{G}$ and $f \in L$ implies $|G| \not\equiv f \pmod{q}$. We call $\mathcal{G}$ *L-intersecting* if for any two distinct sets $G_1, G_2 \in \mathcal{G}$ the congruence $|G_1 \cap G_2| \equiv f \pmod{q}$ holds for some $f \in L$.

The maximum number of sets a modulo q L-avoiding set family can contain has been studied extensively. Frankl and Wilson [24] proved that if $q = p$ a prime and $\mathcal{G}$ is a modulo p L-intersecting uniform (all sets have the same size) set system, then $|\mathcal{G}| \leq \binom{n}{|L|}$. If we replace the uniformity hypothesis to modulo p uniformity, such that $\mathcal{F}$ is L-avoiding, then we have $|\mathcal{G}| \leq \sum\limits_{k=0}^{|L|} \binom{n}{k}$, as it was proven by Deza, Frankl and Singhi [17].

Ten years later Alon, Babai and Suzuki [4] could prove that the uniformity hypothesis is not needed: if $\mathcal{F}$ is modulo p L-intersecting and L-avoiding, then $|\mathcal{G}| \leq \sum\limits_{k=2|L|-p+1}^{|L|} \binom{n}{k}$, provided that some condition on L holds. Also Qian and Ray-Chaudhuri [36] established the same upper bound under different assumptions on L.

These bounds are no longer true for composite numbers in the place of p. The interested reader may find results in this direction in the paper [8], which is also a good survey of the topic.

Babai and Frankl posed the question [7, p. 115] if in the case $|L| = q - 1$ the binomial coefficient $\binom{n}{q-1}$ was an upper bound of the size of a modulo q L-intersecting L-avoiding family. Recently Hegedűs and Rónyai [32] proved the affirmative answer. Our result generalizes this bound to a much greater class of sets L.

Definition 6.2.2. We call a set $L \subseteq \{0, \ldots, q-1\}$ a *modulo q interval* if it is either an interval of integers or a union of two intervals L_1 and L_2, such that $0 \in L_1$ and $q - 1 \in L_2$.

Theorem 6.2.3. *Let q be a power of a prime, L be a modulo q interval and $\mathcal{G} \subseteq 2^{[n]}$ be a modulo q L-avoiding, L-intersecting family of sets. If $|L| \leq n - q + 2$, then*

$$|\mathcal{G}| \leq \sum_{k=|L|}^{q-1} \binom{n}{k}.$$

Proof. Put $\ell = q - |L|$. If L is an interval of integers, then set $d = \max L + 1$, otherwise, when L is the union of two (separated) intervals L_1, L_2 and $0 \in L_1$, set $d = \max L_1 + 1$. Denote by $\mathcal{F}$ the modulo q complete ℓ-wide family with this parameter d. Then by the definitions $\mathcal{G} \subseteq \mathcal{F}$.

For any $G \in \mathcal{G}$ we define the polynomial $\hat{f}_G(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ to be

$$\hat{f}_G(\mathbf{x}) = \left(\sum_{\substack{k=0 \\ k \notin L}}^{q-1} \binom{\mathbf{x} \cdot \mathbf{v}_G - k - 1}{q-1} \right) \text{ reduced by } x_j^2 - x_j,$$

where $\mathbf{x} \cdot \mathbf{v} = \sum_{j=1}^{n} x_j v_j$ is the scalar product. We see from Lemma 6.1.9 that $\hat{f}_G \in \mathbb{Z}[\mathbf{x}]$.

Let $G' \in \mathcal{G}$ be a set from the set system. Then

$$\hat{f}_G(\mathbf{v}_{G'}) = \sum_{\substack{k=0 \\ k \notin L}}^{q-1} \binom{|G' \cap G| - k - 1}{q-1}. \tag{6.12}$$

If $G' \neq G$, then, as $\mathcal{G}$ is modulo q L-intersecting, $|G' \cap G| - k$ cannot be congruent to 0 modulo q for $k \notin L$. Note that it follows from Lemma 6.1.10 that

$$\binom{f-1}{q-1} \equiv \begin{cases} 0 \pmod{p}, \text{ if } f \not\equiv 0 \pmod{q} \\ 1 \pmod{p}, \text{ if } f \equiv 0 \pmod{q}. \end{cases}$$

That is, if $G' \neq G$, then all terms of the sum in (6.12) are zero modulo p. If $G' = G$, then using that $\mathcal{G}$ is modulo q L-avoiding we have exactly one nonzero term modulo p, which is actually congruent to 1.

Let $\mathbb{F}_p$ denote the field of p elements, where q is a power of p. Then we write f_G for the polynomial in $\mathbb{F}_p[\mathbf{x}]$ we obtain from $\hat{f}_G$ by reducing its integer coefficients modulo p. The above argument yields

$$f_G(\mathbf{v}_{G'}) = \begin{cases} 0 \text{ if } G \neq G' \\ 1 \text{ if } G = G'. \end{cases}$$

Since the degree of $\hat{f}_G$ is at most $q-1$, the same is true for f_G as well. Using our earlier notation, it means that $f_G \in \mathbb{F}_p[\mathbf{x}]_{\leq q-1}$. We claim that the cosets $f_G + I(\mathcal{F})_{\leq q-1}$ in the quotient space $\mathbb{F}_p[\mathbf{x}]_{\leq q-1} / I(\mathcal{F})_{\leq q-1}$ are linearly independent over $\mathbb{F}_p$. Indeed, suppose that

$$\sum_{G \in \mathcal{G}} \alpha_G f_G \in I(\mathcal{F})_{\leq q-1} \tag{6.13}$$

for some $\alpha_G \in \mathbb{F}_p$. Substitution of a characteristic vector $\mathbf{v}_G$ of a set $G \in \mathcal{G} \subseteq \mathcal{F}$ to (6.13) gives $\alpha_G = 0$ immediately.

To conclude, note that the number of the f_G is bounded by the dimension of $\mathbb{F}_p\left[\mathbf{x}\right]_{\leq q-1} / I(\mathcal{F})_{\leq q-1}$, that is

$$|\mathcal{G}| \leq \dim\left(\mathbb{F}_p\left[\mathbf{x}\right]_{\leq q-1} / I(\mathcal{F})_{\leq q-1}\right) = H_{\mathcal{F}}(q-1) \leq \sum_{i=0}^{\infty}\sum_{k=0}^{\ell-1}\binom{n}{q-1-iq-k} = \sum_{k=|L|}^{q-1}\binom{n}{k}.$$

by Corollary 6.1.23 (which we are allowed to use as $|L| \leq n-q+2$ implies the assumption $q-1 \leq \frac{n+\ell}{2}$ of the corollary). □

6.3 Families that do not shatter large sets

Definition 6.3.1. Consider a family $\mathcal{G}$ of subsets of $[n]$. We say that $\mathcal{G}$ *shatters* $M \subseteq [n]$ if

$$\{G \cap M \,:\, G \in \mathcal{G}\} = 2^M.$$

Definition 6.3.2. The system of sets $\mathcal{G}$ is an *ℓ-antichain* if it does not contain $\ell+1$ distinct sets $G_0, \dots, G_n$, such that $G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_\ell$.

Frankl [23] conjectured that if an ℓ-antichain $\mathcal{G}$ shatters no set of size $m+1$ for some integer $0 \leq m \leq \frac{n+\ell}{2}-1$, then $|\mathcal{G}| \leq \sum_{k=0}^{\ell-1}\binom{n}{m-k}$ must hold.

An ℓ-wide family (which of course can be understood as a modulo q ℓ-wide family for some q large enough) is an ℓ-antichain. In their manuscript [25], Friedl, Hegedűs and Rónyai showed that the upper bound is valid for ℓ-wide families. Our theorem is a generalization of that result, the special case follows by choosing $q > n$.

Theorem 6.3.3. *Let $\mathcal{G} \subseteq 2^{[n]}$ be a modulo q ℓ-wide family of sets, where q is a prime power. If $\mathcal{G}$ shatters no set of size $m+1$ for some integer $0 \leq m \leq \frac{n+\ell}{2}$, then*

$$|\mathcal{G}| \leq \sum_{i=0}^{\infty}\sum_{k=0}^{\ell-1}\binom{n}{m-iq-k}.$$

Proof. We first prove that if x_M is a standard monomial of any set system $\mathcal{G}$, then $\mathcal{G}$ shatters M. Suppose that $N \subseteq M$, but $N \notin \{G \cap M \,:\, G \in \mathcal{G}\}$. Let $\mathbf{v} = \mathbf{v}_N$ be the characteristic vector of N. Then the polynomial

$$\prod_{i \in M} (x_i + v_i - 1)$$

vanishes on $V_{\mathcal{G}}$ and its leading monomial is x_M, thus $x_M \in \mathrm{Lm}\,(I(\mathcal{G}))$. We conclude that $x_M \in \mathrm{Sm}\,(I(\mathcal{G}))$ implies $|M| \leq m$ for a family $\mathcal{G}$ which does not shatter any set of size $m+1$.

Recall that $\mathcal{G} \subseteq \mathcal{F}$, where $\mathcal{F}$ is a modulo q complete ℓ-wide family. This gives $\mathrm{Sm}\,(I(\mathcal{G})) \subseteq \mathrm{Sm}\,(I(\mathcal{F}))$, and so we can bound the cardinality of the standard monomials of $\mathcal{G}$ with the number of standard monomials of $\mathcal{F}$ of degree at most m. This latter is exactly $H_{\mathcal{F}}(m)$.

Therefore

$$|\mathcal{G}| = |\mathrm{Sm}\,(I(\mathcal{G}))| \leq H_{\mathcal{F}}(m),$$

and hence Corollary 6.1.23 gives the desired bound. □

The inequality in Theorem 6.3.3 is sharp. Choose $d = m - \ell + 1$ for a modulo q complete ℓ-wide family $\mathcal{F}$, and put $\mathcal{G} = \mathcal{F} \cap \binom{[n]}{\leq m}$. Then the fact that $\mathcal{G}$ does not contain any set of size $m+1$ implies that it cannot shatter any set of size $m+1$. The size of $\mathcal{G}$ is precisely $\sum\limits_{i=0}^{\infty} \sum\limits_{k=0}^{\ell-1} \binom{n}{m-iq-k}$.

Acknowledgement

First of all I would like to thank my supervisor, Lajos Rónyai, for initiating me into the topic of Gröbner bases, giving stimulating suggestions, guiding in the research, and providing a new mathematical problem every time I asked for it.

I gratefully acknowledge the comments and suggestions of Gábor Ivanyos and Alex Küronya who read through the whole thesis.

I am also grateful to Gábor Hegedűs, Balázs Rácz, Balázs Ráth and Dömötör Pintér for useful discussions on the subject.

Appendix A

Singular code of the algorithm

```
///////////////////////////////////////////////////////////////////////////////
version="$Id: lexsm.lib,v 1.1 2005/11/11 Singular Exp $";
category="Miscellaneous";
info="
LIBRARY:     lexsm.lib Computes the lexicographic standard monomials
AUTHOR:          B. Felszeghy, e-mail: fbalint@math.bme.hu
KEYWORDS:        standard monomials, vanishing ideal
PROCEDURES:
 LexSm(V)        standard monomials of a finite set of points V
 BuildTrie(V)        builds the reverse trie T of a set of points V
 BuildSmTrie(T)        from T builds the trie U encoding the standard monomials of V
 SmListFromTrie(U)     the list of standard monomials from the trie U
 InsertToTrie        inserts a point to a trie
";
///////////////////////////////////////////////////////////////////////////////

proc LexSm(list V)
"PURPOSE: Given V a finite set of points (ie integer vectors of the same length)
  it computes the lexicographic standard monomials of the vanishing
  ideal I(V).
USAGE:    LexSm(V); V list
THEORY:   See the paper at http://www.math.bme.hu/~fbalint/pub.html/lexgame.pdf
ASSUME:   V is a list of intvecs of the same length. This length has to be the
  same as the number of variables in the active ring.
NOTE:   Although the function works under the above assumptions, the result
  is not understood in general in the active ring.
  It does give the right answer if the active ring
  is a field F and if for any two points V[i] is not equal to V[j] then
  they are also different considered as elements of an affine space over F.
  The ordering of the active ring does not play a role.
RETURN:   The list of standard monomials.
EXAMPLE:  example LexSm; shows an example
SEE ALSO: BuildTrie, BuildSmTrie, SmListFromTrie"
{
  return(SmListFromTrie(BuildSmTrie(BuildTrie(V))));
};
example{
  "EXAMPLE:"; echo = 2;
  intvec po(1) = 1,1,3;
  intvec po(2) = 4,1,1;
  intvec po(3) = 3,1,3;
  intvec po(4) = 2,1,1;
  intvec po(5) = 4,2,1;
  intvec po(6) = 3,1,1;
  list V = po(1..6);
  ring R = 0,x(1..3),lp;
  LexSm(V);
};
///////////////////////////////////////////////////////////////////////////////

static proc InitLibrary
"PURPOSE: Sets up constants used by all procedures in this library.
USAGE:   if(!defined(Parent)){InitLibrary();};"
{
  int Parent = 1; export(Parent);
  int Children = 2; export(Children);
  int Value = 3; export(Value);
  int Nextnode = 4; export(Nextnode);
  int Firstleaf = 5; export(Firstleaf);
  int Lastleaf = 6; export(Lastleaf);
  int Depth = 1; export(Depth);
  int Root = 2; export(Root);
  int Null = -1; export(Null);
};



static proc Node(int parent, list children, int value, int nextnode,
 int firstleaf, int lastleaf)
"PURPOSE: Constructor function of a node object.
USAGE:    Node(parent, children, value, nextnode); parent int, children list,
  value int, nextnode int, firstleaf int, lastleaf int
RETURN:   A node object with the respective members.
NOTE:   A node is a vertex of a trie. A node can have a pointer to its parent,
  a list of pointers to its children, a value (that is the integer on
  the edge between the node and its parent), a pointer to a node on the
  same level of the trie, and pointers to two of the leafs which are
  descendants of the node. For a node node one can get them by
  node[Parent], node[Children], node[Value], node[Nextnode], node[Firstleaf]
  and node[Lastleaf] respectively.
SEE ALSO: SmNode"
{
  list newnode;
  newnode[Parent] = parent;
  newnode[Children] = children;
  newnode[Value] = value;
  newnode[Nextnode] = nextnode;
  newnode[Firstleaf] = firstleaf;
  newnode[Lastleaf] = lastleaf;
  return(newnode);
};
///////////////////////////////////////////////////////////////////////////////



static proc SmNode(int parent)
"PURPOSE: Another constructor function of a node object.
USAGE:    Node(parent); parent int
RETURN:   A node object with parent parent and an empty list of children.
SEE ALSO: Node"
{
  list newnode;
  newnode[Parent] = parent;
  newnode[Children] = list();
  return(newnode);
};
///////////////////////////////////////////////////////////////////////////////

static proc InitTrie(intvec point)
"PURPOSE: Initializes a trie consisting of a single path. The values on
  the edges are the integers from intvec point, the first element
  of point belongs to the only leaf, the last is below the root.
USAGE:    InitTrie(point); point intvec
RETURN:   The reverse trie of point."
{
  if(!defined(Parent)){InitLibrary();};
  list newtrie;
  int n = size(point);
  newtrie[Depth] = n;
  list children = Root+1;
  newtrie[Root] = Node(Null,children,Null,Null,Root+n,Root+n);
  for(int i=1; i<n; i++){
    children = Root+i+1;
    newtrie[Root+i] = Node(Root+i-1,children,point[n+1-i],Null,
   Root+n,Root+n);
  };
  newtrie[Root+n] = Node(Root+n-1,list(),point[1],Null,Root+n,Root+n);
  return(newtrie);
};
///////////////////////////////////////////////////////////////////////////////



proc InsertToTrie(intvec point, list trie)
"PURPOSE: Inserts a new point to the trie.
USAGE:    InsertToTrie(point, trie); point intvec trie list
ASSUME:   trie is a nonempty trie of points of the same length. Also point is of
  this length.
RETURN:   A trie with the new point inserted.
EXAMPLE:  example InsertToTrie; shows an example
SEE ALSO: BuildTrie"
{
  int n = trie[Depth];
  if( size(point) != n){
    ERROR("size(point_to_insert) not equals to trie[Depth]");
  };
  int current_node_index = Root;
  int new, childrensize,i;
  list children;
  for (int level=0;level<=n;level++){
    new = 1;
    children = trie[current_node_index][Children];
    childrensize = size(children);
    for (i=1;i<=childrensize;i++){
      if (trie[children[i]][Value]==point[n-level]){
        new = 0;
break;
      };
    };
    if(!new){
      current_node_index=children[i];
    }else{
      break;
    };
  };
  if(level != n){
    int branching_level = level;
    int branching_node_index = current_node_index;
    int triesize = size(trie);
    int last_new_node_index = triesize+n-branching_level;
    int last_node_index = children[childrensize];
    trie[branching_node_index][Children][childrensize+1] = triesize+1;
    children = list();
    for (level=branching_level+1;level<n;level++){
      triesize++;
      children = triesize+1;
      trie[triesize] = Node(current_node_index,children,point[n-level+1],
    trie[last_node_index][Nextnode],
    last_new_node_index,last_new_node_index);
      trie[last_node_index][Nextnode] = triesize;
      children = trie[last_node_index][Children];
      last_node_index = children[size(children)];
      current_node_index=triesize;
    };
    trie[last_new_node_index] = Node(current_node_index,list(),point[1],
trie[last_node_index][Nextnode],
last_new_node_index,last_new_node_index);
    trie[last_node_index][Nextnode] = last_new_node_index;

    current_node_index = branching_node_index;
    while(trie[current_node_index][Lastleaf] == last_node_index){
      trie[current_node_index][Lastleaf] = last_new_node_index;
      current_node_index = trie[current_node_index][Parent];
      if (current_node_index == Null){break;};
    };
  };
  return(trie);
};
example{
  "EXAMPLE:"; echo = 2;
  intvec po(1) = 0,0,0;
  intvec po(2) = 0,0,0;
  list tree = BuildTrie(po(1));
  InsertToTrie(po(2),tree);
};
//////////////////////////////////////////////////////////////////////////////

proc BuildTrie(list points)
"PURPOSE: Creates the reverse trie of the points listed in points. A point
  can only have integer coordinates. It also builds the pointers
  needed for the standard monomial computation, that is for any node
  pointers to its first and last leaf and a pointer to its right
  neighbour node on the same level.
USAGE:    BuildTrie(points); points list
ASSUME:   points is a list of intvecs, each of the same length.
RETURN:   The reverse trie of points.
NOTE:   This function works by calling InsertToTrie subsequently.
EXAMPLE:  example BuildTrie; shows an example
SEE ALSO: InsertToTrie"
{
  dbprint(1,"Starting BuildTrie...");
  list trie = InitTrie(points[1]);
  int m = size(points);
  for(int i=2;i<=m;i++){
    trie = InsertToTrie(points[i],trie);
  };
  dbprint(1,"BuildTrie is ready.");
  return(trie);
```

```
};
example{
  "EXAMPLE:";
  echo = 2;
  intvec po(1) = 2,1,1;
  intvec po(2) = 3,1,1;
  intvec po(3) = 4,1,3;
  intvec po(4) = 4,2,1;
  intvec po(5) = 1,1,3;
  intvec po(6) = 3,1,3;
  list V = po(1..6);
  BuildTrie(V);
};
///////////////////////////////////////////////////////////////////////////

proc BuildSmTrie(list trie)
"PURPOSE: Creates the trie encoding the lexicographic standard monomials
  of the points which belong to the argument trie.
USAGE:    BuildSmTrie(points); points list
ASSUME:   trie is a reverse trie, that is it was created by BuildTrie (or
  at least looks as if it was created that way).
RETURN:   The trie of standard monomials.
EXAMPLE:  example BuildSmTrie; shows an example
SEE ALSO: BuildTrie, SmListFromTrie, LexSm"
{
  dbprint(1,"Starting BuildSmTrie...");
  if(!defined(Parent)){InitLibrary();};
  list smtrie,A,b,newnode;
  int n = trie[Depth];
  smtrie[Depth] = n;
  smtrie[Root] = SmNode(Null);
  int current_leaf_index = trie[Root][Firstleaf];
  while(current_leaf_index != Null){
    A[current_leaf_index] = Root;
    current_leaf_index = trie[current_leaf_index][Nextnode];
  };
  int current_node_index,current_sm_node_index;
  int childrensize,smtriesize,last_leaf_index;
  for(int i=1;i<=n;i++){
    if(i==n){current_node_index = Root;}
    else{current_node_index = Root+n-i;};
    while(current_node_index != Null){
      current_leaf_index = trie[current_node_index][Firstleaf];
      last_leaf_index = trie[current_node_index][Lastleaf];
      while(1){
        b[A[current_leaf_index]]=0;
if(current_leaf_index == last_leaf_index){break;}
else{current_leaf_index = trie[current_leaf_index][Nextnode];};
      };
      current_leaf_index = trie[current_node_index][Firstleaf];
      while(1){
        current_sm_node_index = A[current_leaf_index];
        b[current_sm_node_index]=b[current_sm_node_index]+1;
        childrensize = size(smtrie[current_sm_node_index][Children]);
        if(childrensize < b[current_sm_node_index]){
          newnode = SmNode(current_sm_node_index);
          smtriesize = size(smtrie);
          smtrie[smtriesize+1] = newnode;
          smtrie[current_sm_node_index][Children][childrensize+1] = smtriesize+1;
        };
        A[current_leaf_index] =
smtrie[current_sm_node_index][Children][b[current_sm_node_index]];
if(current_leaf_index == last_leaf_index){break;}
else{current_leaf_index = trie[current_leaf_index][Nextnode];};
      };
      current_node_index = trie[current_node_index][Nextnode];
    };
  };
  dbprint(1,"BuildSmTrie is ready.");
  return(smtrie);
};
example{
  "EXAMPLE:"; echo = 2;
  intvec po(1) = 1,1,3;
  intvec po(2) = 4,1,1;
  intvec po(3) = 3,1,3;
  intvec po(4) = 2,1,1;
  intvec po(5) = 4,2,1;
  intvec po(6) = 3,1,1;
  list V = po(1..6);
  list tree = BuildTrie(V);
  BuildSmTrie(tree);
};
//////////////////////////////////////////////////////////////////////////////

proc SmListFromTrie(list smtrie)
"PURPOSE: Creates the list of standard monomials from the trie
  of standard monomials.
USAGE:    SmListFromTrie(smtrie); smtrie list
ASSUME:   smtrie is a rooted tree, and looks like a trie returned by
          BuildSmTrie.
RETURN:   The list of standard monomials.
EXAMPLE:  example SmListFromTrie; shows an example
SEE ALSO: BuildSmTrie, LexSm"
{
  dbprint(1,"Starting SmListFromTrie...");
  if(!defined(Parent)){InitLibrary();};
  int n = smtrie[Depth];
  if(!defined(basering)){
    string error_msg = "Set an active ring by typeing 'ring R = 0,(x(1..";
    error_msg = error_msg+string(n);
    error_msg = error_msg+")),lp;'";
    ERROR(error_msg);
  };
  if(nvars(basering)!=n){
    ERROR("The number of variables in ring is not equal to smtrie[Depth].");
  };
  if(!defined(exported_smtrie)){
    list exported_smtrie;
    export(exported_smtrie);
  };
  exported_smtrie = smtrie;
  list smlist = SmListFromTrieRec(1,Root,1);
  dbprint(1,"SmListFromTrie is Ready.");
  return(smlist);
};
example{
  "EXAMPLE:"; echo = 2;
  intvec po(1) = 1,1,3;
  intvec po(2) = 4,1,1;
  intvec po(3) = 3,1,3;
  intvec po(4) = 2,1,1;
  intvec po(5) = 4,2,1;
  intvec po(6) = 3,1,1;
  list V = po(1..6);
  ring R = 0,x(1..3),lp;
  list smtree = BuildSmTrie(BuildTrie(V));
  SmListFromTrie(smtree);
};
///////////////////////////////////////////////////////////////////////////////

static proc SmListFromTrieRec(poly product,int node_index, int depth){
  list mons;
  int current_node_index;
  list children = exported_smtrie[node_index][Children];
  int childrensize = size(children);
  if(childrensize == 0){
    mons = product;
  } else {
    for(int i=0;i<childrensize;i++){
      current_node_index = children[i+1];
      mons = mons+SmListFromTrieRec(var(depth)^i*product,current_node_index,depth+1);
    };
  };
  return(mons);
};
///////////////////////////////////////////////////////////////////////////////
```

Bibliography

[1] W. W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, *American Mathematical Society*, 1994.

[2] A. V. Aho, J. E. Hopcroft, J. D. Ullman, The design and analysis of computer algorithms, *Addison-Wesley*, Reading, Massachusetts, 1978.

[3] N. Alon, Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing* **8** **(1-2)** (1999), 7–29.

[4] N. Alon, L. Babai, H. Suzuki, Multilinear polynomials and Frankl–Ray-Chaudhuri–Wilson type intersection theorems, *J. Combin. Theory Ser. A* **58** (1991), 165–180.

[5] R. P. Anstee, L. Rónyai, A. Sali, Shattering news, *Graphs and Combinatorics* **18** (2002), 59–73.

[6] M. F. Atiyah, I. G. MacDonald, Introduction to Commutative Algebra, *Addison-Wesley*, Reading, 1969.

[7] L. Babai, P. Frankl, Linear Algebra Methods in Combinatorics, *Preliminary Version 2*, September 1992.

[8] L. Babai, P. Frankl, S. Kutin, D. Štefankovič, Set systems with restricted intersections modulo prime powers, *J. Combin. Theory Ser. A* **95** (2001), 39–73.

[9] T. Becker, V. Weispfenning, Gröbner bases – a computational approach to commutative algebra, *Springer-Verlag*, Berlin, Heidelberg, 1993.

[10] B. Buchberger Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, *PhD Thesis, Univ. of Innsbruck, Austria*, 1965.

[11] B. Buchberger, Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleischungssystem, *Aequationes Mathematicae*, **4** (1970), 374–383.

[12] B. Buchberger, H. M. Möller, The construction of multivariate polynomials with preassigned zeros, *Proc EUROCAM '82, Lecture Notes In Computer Science* **144** (1982), 24–31.

[13] B. Buchberger, F. Winkler (editors), Gröbner Bases and Applications, *London Mathematical Society Series*, Volume 251 (1998), Proc of the international conference "33 Years of Gröbner Bases"

[14] L. Carlitz, Solvabillity of certain equations in a finite field, *Quart. J. Math. (2)* **7** (1956), 3–4.

[15] L. Cerlienco, M. Mureddu, From algebraic sets to monomial linear bases by means of combinatorial algorithms, Formal power series and algebraic combinatorics, (Montreal, PQ, 1992) *Discrete Mathematics* **139** (1995), no. 1–3, 73–87.

[16] D. Cox, J. Little, D. O'Shea, *Ideals, varieties, and algorithms*, Springer-Verlag, Berlin, Heidelberg, 1992.

[17] M. Deza, P. Frankl, N. M. Singhi, On functions of strength t, *Combinatorica* **3** (1981), 331–339.

[18] B. Felszeghy On the solvability of some special equations over finite fields *Publ. Math. Debrecen* **68** (2006), 15–23.

[19] B. Felszeghy, G. Hegedűs, L. Rónyai, Algebraic properties of modulo q complete ℓ-wide families, *manuscript*, 2006.

[20] B. Felszeghy, B. Ráth, L. Rónyai, The lex game and some applications, *J. Symbolic Computation* **41** (2006), 663–681.

[21] B. Felszeghy, L. Rónyai, On the lexicographic standard monomials of zero dimensional ideals, *Proc. 10th Rhine Workshop on Computer Algebra (RWCA)* (2006), 95–105.

[22] B. Felszeghy, L. Rónyai, Some meeting points of Gröbner bases and combinatorics, *manuscript*, 2007.

[23] P. Frankl, Traces of antichains, *Graphs Comb.* **Vol 5. No 1.** (1989), 295–299.

[24] P. Frankl, R. M. Wilson, Intersection theorems with geometric consequences, *Combinatorica* **1** (1981), 357–368.

[25] K. Friedl, G. Hegedűs, L. Rónyai, Gröbner bases for complete ℓ-wide families, *to appear in Publ. Math. Debrecen* (2007).

[26] K. Friedl, L. Rónyai, Order shattering and Wilson's theorem, *Discrete Mathematics* **270** (2003), 127–136.

[27] A. M. Garsia, Pebbles and expansions in the polynomial ring, In: *Polynomial identities and combinatorial methods*, Lecture Notes in Pure and Appl. Math. **235** 2003, 261–285.

[28] G.-M. Greuel, G. Pfister, A Singular Introduction to Commutative Algebra (with contributions by O. Bachmann, C. Lossen, and H. Schnemann), *Springer-Verlag* 2002.

[29] G.-M. Greuel, G. Pfister, H. Schönemann, Singular 3.0, A Computer Algebra System for Polynomial Computations, *Centre for Computer Algebra, University of Kaiserslautern* (2005). `http://www.singular.uni-kl.de`.

[30] T. Harima, Characterization of Hilbert functions of Gorenstein Artin algebras with the weak Stanley property, *Proc. Amer. Math. Soc.* **123** (1995), 3631–3638.

[31] G. Hegedűs, A. Nagy, L. Rónyai, Gröbner bases for permutations and oriented trees, *Annales Univ. Sci. Budapest., Sectio Computatorica* **23** (2004), 137–148.

[32] G. Hegedűs, L. Rónyai, Standard monomials for q-uniform families and a conjecture of Babai and Frankl, *Central European Journal of Mathematics* **1** (2003), 198–207.

[33] D. E. Knuth, The art of computer programming, Volume 3., *Addison-Wesley*, Reading 1973.

[34] G. E. Moorhouse, Approaching some problems in finite geometry through algebraic geometry, *to appear.*

[35] D. Pintér, L. Rónyai, On the Hilbert function of complementary set families, *to appear in Annales Univ. Sci. Budapest., Sectio Computatorica.*

[36] J. Qian, D. K. Ray-Chaudhuri, On mod-p Alon–Babai–Suzuki Inequality, *J. of Algebraic Combinatorics* **12** (2000), 85–93.

[37] L. Rédei, Zur Theorie der Gleichungen in endlichen Körpern, *Acta Univ. Szeged Sect. Sci. Math.* **11** (1946), 63–70.

[38] L. Rónyai, On a conjecture of László Rédei, *Acta Univ. Szeged Sect. Sci. Math.* **69** (2003), 523–531.

[39] R. M. Wilson, A diagonal form for the incidence matrices of t-subsets vs. k-subsets, *Europ. J. Combin.* **11** (1990), 609–615.