Gröbner bases in combinatorics

Ph. D. dissertation

Gábor Hegedűs

Thesis advisor: Lajos Rónyai

Budapest

2005

Contents

1 Introduction

First I would like to discuss some results that led to the research reported herein. The main starting points of my work are the linear algebra bound method in combinatorics and the Gröbner basis theory.

The linear algebra bound method yields upper bounds for the size of various combinatorial structures. A general description of this method is as follows. Let $\mathcal{F}$ denote a finite set of points in the affine space $\mathbb{F}^n$ over a field $\mathbb{F}$. Suppose that we can define for each $v \in \mathcal{F}$ a corresponding polynomial $p_v(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$ such that the polynomials $\{p_v : v \in \mathcal{F}\}$ will be linearly independent over the field $\mathbb{F}$. We denote by $\mathcal{T}$ the set of monomials, which occur in the polynomials p_v. Then the linear algebra bound method gives the upper bound $|\mathcal{F}| \le |\mathcal{T}|$.

This method was introduced by D. G. Larman, C. A. Rogers and J. J. Seidel in [62] and T. H. Koornwinder in [61]. Larman, Rogers and Seidel gave the upper bound $\binom{n+2}{2} + \binom{n+1}{1}$ for the size of point sets in $\mathbb{R}^n$ with only two distances.

A. Blokhuis introduced a simple but powerful idea in [21]: he proved that we can enlarge the previous set of polynomials $\{p_v : v \in \mathcal{F}\}$ by some additional functions $\{q_m : m \in \mathcal{M}\}$, and this collection will be still linearly independent. Hence he got the better upper bound $\binom{n+2}{2}$.

Let $[n]$ stand for the set $\{1, 2, \dots, n\}$. Let $0 \le d \le n$ be an integer. Then we denote by $\binom{[n]}{d}$ the family of all d element subsets of $[n]$ and $\binom{[n]}{\le d} = \binom{[n]}{0} \cup \ldots \cup \binom{[n]}{d}$ the subsets of size at most d.

We say that a set system $\mathcal{F}$ is *uniform* if $\mathcal{F} \subseteq \binom{[n]}{d}$ for some d.

Now we define the notion of inclusion matrices. For families $\mathcal{F}, \mathcal{G} \subseteq 2^{[n]}$ the *inclusion matrix* $I(\mathcal{F}, \mathcal{G})$ is a (0,1) 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 ($F \in \mathcal{F}, G \in \mathcal{G}$).

The most important case when $\mathcal{G}$ is the complete s-uniform family $\binom{[n]}{s}$. We call the $|\mathcal{F}| \times \binom{n}{s}$ matrix $I(\mathcal{F}, \binom{[n]}{s})$ *the s-inclusion matrix of $\mathcal{F}$*. We call a set family $\mathcal{F}$ *s-independent* if the rows of $I(\mathcal{F}, \binom{[n]}{s})$ are linearly independent, i.e., the s-inclusion matrix has *full row-rank.*

Let $L \subseteq \mathbb{N}$ be a set of nonnegative integers. A set family $\mathcal{F}$ is L-intersecting, if $|E \cap F| \in L$ for every pair E, F of distinct members of $\mathcal{F}$.

The linear algebra bound method can be applied to give upper bounds for the size of various L-intersecting families. In [14] L. Babai proved this way the Ray-Chaudhuri–Wilson theorem:

Theorem 1.1 *(Ray-Chaudhuri–Wilson, 1975): Let $L \subseteq \mathbb{N}$ be a set of s integers and $\mathcal{F}$ an L-intersecting k-uniform family, where $s \leq \min(k, n-k)$. Then $\mathcal{F}$ is s-independent. Consequently*

$$|\mathcal{F}| \leq \binom{n}{s}.$$

This result and other related modular extensions provided powerful tools for geometric and combinatorial applications.

The first proofs of the Ray-Chaudhuri–Wilson and the Frankl–Wilson theorems in [35] and [73] used inclusion matrices. These matrices are natural generalisations of the incidence matrices. In such proofs one usually shows that the rows of the s-inclusion matrix $I(\mathcal{F}, \binom{[n]}{s})$ are linearly independent, where $s = |L|$, therefore $\mathrm{rank}_{\mathbb{F}}\, I(\mathcal{F}, \binom{[n]}{s})$ yields simple upper bounds for the size of L-intersecting families.

But the inclusion matrix technique and the polynomial methods are just the two sides of the same coin: in the context of Gröbner bases it can be shown that they are equivalent methods. The reduction with the Gröbner bases of combinatorial ideals can give better upper bound for the size of L-intersecting families in the modular case. One interesting example appears in our solution of a conjecture of Babai and Frankl (see Chapter 5).

We recall now some basic facts concerning Gröbner bases in polynomial rings. Let $\mathbb{F}$ be a field and $S = \mathbb{F}[x_1, \ldots, x_n]$ be the ring of polynomials in variables $x_1, \ldots, x_n$. A total order $\prec$ on the monomials (words) composed from variables $x_1, x_2, \ldots, x_n$ is a *term order*, if 1 is the minimal element of $\prec$, and $uw \prec vw$ holds for any monomials u, v, w with $u \prec v$.

The *leading monomial* $\mathrm{lm}(f)$ of a nonzero polynomial $f \in S$ is the largest (with respect to $\prec$) monomial which appears with nonzero coefficient in f when expressed as an $\mathbb{F}$-linear combination of monomials.

Let I be an ideal of S. A finite subset $G \subseteq I$ is a *Gröbner basis* of I if for every $f \in I$ there exists a $g \in G$ such that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$. In other words, the leading monomials of the polynomials from G generate the semi-group ideal of monomials $\{\mathrm{lm}(f) : f \in I\}$. Using that $\prec$ is a well founded order, it follows that G is actually a basis of I, i.e. G generates I as an ideal of S. It is a fundamental fact (cf. [26, Chapter 1, Corollary 3.12] or [1, Corollary 1.6.5, Theorem 1.9.1]) that every nonzero ideal I of S

has a Gröbner basis. We treat the Gröbner basis theory more thoroughly in Chapter 2.

The second source of our results is Gröbner basis theory. This theory has an interesting history. A major step toward Gröbner bases was taken by Macaulay. He introduced total orderings on the set of monomials of a polynomial ring in [63] and used these orders to determine the possible Hilbert function of graded ideals by comparing them with monomial ideals.

Gröbner bases were first introduced in the 1960s by H. Hironaka. He used a division algorithm in his landmark paper on the resolution of singularities and he introduced also the "standard bases", which are analogous to what we call Gröbner bases. Originally Hironaka's work was done for power series, he treated also questions of convergence.

Later B. Buchberger discovered Gröbner bases again, and he treated them in detail in his Ph. D. thesis. Buchberger gave the name "Gröbner bases" to honor his thesis adviser W. Gröbner. His thesis contains also the Buchberger's criterion and the Buchberger's algorithm, now bearing his name, in an implicit form. He made his ideas more explicit in [23] and [24]. He dealt also with the programming of the resulting algorithm.

Buchberger's algorithm is one of the most important tools in computational algebraic geometry. In the 1970s and 1980s Buchberger made a lot of refinements to improve the efficiency of the method.

Although the computation of general Gröbner bases via the Buchberger's algorithm is exponential in the worst case, several polynomial–time algorithms are known for computing the vanishing ideal of a finite set of points. Let $\mathcal{V} = \{P_1, \ldots, P_s\} \subseteq \mathbb{F}^n$ be a finite subset. In [68] Mora and Robbiano defined the Gröbner, Border and Macaulay bases of the ideal $I(\mathcal{V})$ of polynomials vanishing on $\mathcal{V}$, and proposed what is known as the Buchberger–Möller algorithm (see also [25]) for computing the reduced Gröbner basis of $I(\mathcal{V})$. In this algorithm the total number of arithmetical operations in the field $\mathbb{F}$ is $O(ns^3)$, and it needs $O(n^2s^2)$ integer comparisons. This technique in some way is a generalisation of Lagrange interpolation. In [31] Farr and Gao presented an alternate method for the computing the reduced Gröbner bases for finite sets of points. This algorithm builds the Gröbner basis of $I(\mathcal{V})$ step by step and this is equivalent to Newton's interpolation in the univariate case.

Concerning the background of our results, it is appropriate to recall Smolensky's work on Boolean function. Smolensky has observed in [77] that there is a fruitful connection between the complexity theory of Boolean functions and algebraic geometry. His approach was the following.

A Boolean function $f : \{0,1\}^n \to \{0,1\}$ in n variables can be represented as a real multivariate polynomial $g(x_1, \ldots, x_n)$, whose zero set is the same as the set of zeroes of f, together with the polynomials $x_i^2 - x_i$, $i = 1, \ldots, n$. Consider the finite set of points defined by $g = 0$ and $x_i^2 - x_i = 0$, $i = 1, \ldots, n$. This set of points can then be investigated in terms of the Hilbert function of its ideal, and Smolensky showed in [77], that the values of the Hilbert function are related to certain lower bounds in complexity theory.

Now let $0 \leq d_1 < \ldots < d_t \leq n$ be a strictly increasing sequence of nonnegative integers. Let

$$\mathcal{F} := \binom{[n]}{d_1} \cup \ldots \cup \binom{[n]}{d_t}$$

denote a symmetric subset of the Boolean cube $\{0,1\}^n$, i.e., the union of the complete uniform families $\binom{[n]}{d_i}$. Clearly $V(\mathcal{F})$, the set of characteristic vectors of $\mathcal{F}$, is a zero set of a corresponding symmetric Boolean function. In [19] Egidi and Bernasconi determined completely the Hilbert function over $\mathbb{Q}$ of the ideals associated to the zero set of symmetric Boolean functions. They applied this characterisation to analyse the behaviour of the majority function on symmetric subsets of the Boolean cube.

In [2] N. Alon proved the following important Theorem, which he called to Combinatorial Nullstellensatz, because his result is a stronger version of a special case of Hilbert's Nullstellensatz:

Theorem 1.2 *(Combinatorial Nullstellensatz, [2]) Let $\mathbb{F}$ be an arbitrary field and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. Let $S_1, \ldots, S_n$ be nonempty finite subsets of $\mathbb{F}$ and suppose that $|S_i| \geq 2$ for each $1 \leq i \leq n$. Define for $1 \leq i \leq n$*

$$g_i(x_i) := \prod_{s \in S_i} (x_i - s) \in \mathbb{F}[x_1, \ldots, x_n]. \tag{1}$$

If f vanishes on $S_1 \times \ldots \times S_n$, then there are polynomials $h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n]$ satisfying $\deg h_i \leq \deg f - \deg g_i$ so that $f = \sum_{i=1}^n h_i g_i$.

The following result is an immediate consequence of the Combinatorial Nullstellensatz.

Theorem 1.3 *Let $\mathbb{F}$ be an arbitrary field and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. Let $S_1, \ldots, S_n$ be nonempty finite subsets of $\mathbb{F}$ so* *that* $|S_i| \geq 2$ *for each* $1 \leq i \leq n$. *Suppose that* $f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ *such that*

$$deg\ f = \sum_{i=1}^{n} (|S_i| - 1),$$

and the coefficient of $x_1^{|S_1|-1} \cdots x_n^{|S_n|-1}$ *in* f *is not zero. Then there exists a vector* $v \in S_1 \times \ldots \times S_n$ *such that* $F(v) \neq 0$.

This Theorem has surprising applications in graph theory, combinatorial geometry and combinatorial number theory, see for example [6], [7], [8], [9], [10] and [30].

R. P. Anstee, L. Rónyai and A. Sali discovered in [11] an interesting combinatorial description of the lex monomials of the characteristic vectors of set families with the aid of order-shattering (Theorem 2.11). The first application of this description was a new, simpler proof of the following result of Wilson (see also [79]):

Theorem 1.4 *If* $d \leq k \leq n - d$ *are natural numbers and* $\mathbb{F}$ *is an arbitrary field then*

$$rank_{\mathbb{F}}\, I\left(\binom{[n]}{k}, \binom{[n]}{\leq d}\right) = \binom{n}{d}, \tag{2}$$

and

$$rank_{\mathbb{F}}\, I\left(\binom{[n]}{k}, \binom{[n]}{d}\right) = \sum \binom{n}{i} - \binom{n}{i-1}, \tag{3}$$

where the summation is for those indices i, *for which* $\binom{k-i}{d-i}$ *is not 0 in* $\mathbb{F}$.

In [58] A. Kézdy and H. Snevily examined the lex Gröbner basis of the ideal $I(n, t+1) \subseteq \mathbb{C}[x_0, \ldots, x_t]$ consisting of those polynomials in $t+1$ variables that vanish on distinct n^{th} roots of unity. Their research of this ideal was motivated by many combinatorial and graph-theoretical questions involving permutations - such as the existence of latin transversals in latin squares of odd order, Hamiltonian cycles in graphs and perfect matchings in bipartite graphs. They applied Gröbner basis methods to give a Combinatorial Nullstellensatz characterisation of the ideal $I(n, t+1)$.

The results discussed so far point to the importance of polynomial functions, in particular, low degree polynomial functions on finite point sets. With this motivation we started to study polynomial functions on combinatorially interesting finite point sets. As a first step in this direction, it seemed natural to investigate the deglex standard monomials of the ideal of $V\binom{[n]}{d}$, the characteristic vectors of the complete uniform families. We succeeded in describing the reduced Gröbner basis of this ideal, thus we obtained the description of the standard monomials with respect to any term order $\prec$. Next, it was a natural step to generalise our results to the complete ℓ-wide families $\mathcal{F}^{k,\ell}$. Later with a fruitful combination of the linear algebra bound method and a reduction argument we proved a conjecture of L. Babai and P. Frankl about modular L-intersecting families. Then we turned to an other interesting direction: we described the reduced Gröbner bases and the standard monomials of permutations of distinct elements of a field $\mathbb{F}$. This has naturally led to the case when repetitions are allowed among the coordinate values permuted. The resulting point sets V_λ are naturally indexed by partitions λ which describe the multiplicities of the components (see Chapter 7 for a precise formulation). We obtained a characterisation of the lexicographic standard monomials of V_λ and identified the orthogonal complement $(S^\lambda)^\perp$ (with respect to the James scalar product) of the Specht module S^λ in a suitable function space. We used also this identification to describe the deglex standard monomials of V_λ, thus describing a new, simple proof of a result of A. M. Garsia and C. Procesi [39].

In this thesis we follow the general line of Smolensky's approach. We determine the standard monomials of interesting combinatorial sets of points and provide the combinatorial description of the Hilbert function of the ideals of these finite set of points. Then we apply this description to give rank formulae of certain inclusion matrices and obtain applications.

The thesis is organised as follows.

In Chapter 2 we collected preliminaries about Gröbner bases, standard monomials, Hilbert functions and Young tableaux.

In Chapter 3 we describe (reduced) Gröbner bases of the ideal of polynomials over a field, which vanish on the set of characteristic vectors of the complete uniform families $\binom{[n]}{d}$.

Let $n > 0$, k, ℓ be integers with $0 \le \ell - 1 \le k \le n$, and consider the complete *ℓ-wide* family

$$\mathcal{F}^{k,\ell} = \{F \subseteq [n] : k - \ell < |F| \le k\}.$$

In Chapter 4 we describe (reduced) Gröbner bases of the ideal of polynomials over an arbitrary field $\mathbb{F}$, which vanish on the characteristic vectors of the elements of $\mathcal{F}^{k,\ell}$.

As an application, we obtain results on certain inclusion matrices related to $\mathcal{F}^{k,\ell}$. We show in particular, that if $0 \le m \le \min(k, n-k+\ell-1)$ then

$$\mathrm{rank}_{\mathbb{F}}\ I(\mathcal{F}^{k,\ell}, \binom{[n]}{\le m}) = \sum_{i=\max(0,m-\ell+1)}^{m} \binom{n}{i}, \tag{4}$$

where $\mathbb{F}$ is an arbitrary field. We prove also a special case of a conjecture of Frankl related to the determination of the maximum number of subsets of $[n]$ with no shattered set of size t and with no chain of size $\ell+1$.

Let n, k, α be integers, $n, \alpha > 0$, p be a prime and $q = p^\alpha$. Consider the complete q-uniform family

$$\mathcal{F}(k,q) = \{K \subseteq [n] :\ |K| \equiv k \pmod q\}.$$

In Chapter 5 we study certain inclusion matrices attached to $\mathcal{F}(k,q)$ over the field $\mathbb{F}_p$. We show that if $\ell \le q-1$ and $2\ell \le n$ then

$$\mathrm{rank}_{\mathbb{F}_p}\ I(\mathcal{F}(k,q), \binom{[n]}{\le \ell}) \le \binom{n}{\ell}.$$

In the proof we use arguments involving Gröbner bases, standard monomials and reduction. As an application, we solve a problem of L. Babai and P. Frankl related to the size of some L-intersecting families modulo q.

Let $\mathbb{F}$ be a field. In Chapter 6 we describe Gröbner bases for the ideals of polynomials vanishing on the sets $V_{(1^n)}$. Here $V_{(1^n)} = V_{(1^n)}(\alpha_1, \ldots, \alpha_n)$ is the set of all permutations of some $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$. We give also a simple proof of a beautiful generalisation, first obtained by A. Garsia in [38], of the Fundamental Theorem of Symmetric Polynomials.

Let $\alpha_0, \ldots, \alpha_{k-1}$ be k different elements of $\mathbb{F}$. Let $\lambda = (\lambda_1, \ldots, \lambda_k)$ be a partition of n and V_λ be the set of all vectors $v = (v_1, \ldots, v_n) \in \mathbb{F}^n$ such that

$$|\{j \in [n] :\ v_j = \alpha_i\}| = \lambda_{i+1}$$

for $0 \le i \le k-1$.

In Chapter 7 we describe the lexicographic standard monomials of the ideal of polynomials from $\mathbb{F}[x_1, \ldots, x_n]$, which vanish on the set V_λ. In the proof we give a new description of the orthogonal complement $(S^\lambda)^\perp$ (with respect to the James scalar product) of the Specht module S^λ. As applications, a basis of $(S^\lambda)^\perp$ is exhibited, and we obtain a combinatorial description of the Hilbert function of V_λ.

Our approach gives also the deglex standard monomials of V_λ, and hence provides a new proof of a result of A. M. Garsia and C. Procesi [39].

The main results of this thesis appeared in the articles [46], [47], [48], [49], [50].

2 Preliminaries

2.1 The order shattering of set families

First we introduce some notations. Let $[n]$ stand for the set $\{1, 2, \ldots, n\}$. The family of all subsets of $[n]$ is denoted by $2^{[n]}$. For an integer $0 \le d \le n$ we denote by $\binom{[n]}{d}$ the family of all d element subsets of $[n]$, and $\binom{[n]}{\le d} = \binom{[n]}{0} \cup \ldots \cup \binom{[n]}{d}$ the subsets of size at most d.

Recall that a *chain* of size p in $2^{[n]}$ is a sequence $A_1, \ldots, A_p$ of subsets of $[n]$ with $A_1 \subset \ldots \subset A_p$.

Following [11], we recall the notion of order shattering. A set

$$S = \{s_1 < s_2 < \ldots < s_d\} \subseteq [n]$$

is *order shattered* by the family $\mathcal{F} \subseteq 2^{[n]}$ if the following holds: in the case $S = \emptyset$ the family $\mathcal{F}$ has to contain a set; when $|S| > 0$, then there are 2^d sets in $\mathcal{F}$ that can be divided into two families $\mathcal{F}_0$ and $\mathcal{F}_1$ such that $s_d \notin F$ for all $F \in \mathcal{F}_0$, $s_d \in F$ for all $F \in \mathcal{F}_1$, and both $\mathcal{F}_0, \mathcal{F}_1$ order shatter the set $S \setminus \{s_d\}$, furthermore $T \cap F_0 = T \cap F_1$ holds for $T = \{s_d + 1, s_d + 2, \ldots, n\}$ and all $F_0 \in \mathcal{F}_0, F_1 \in \mathcal{F}_1$.

Let

$$\text{osh}\,(\mathcal{F}) = \{S \subseteq [n] : \mathcal{F} \text{ order shatters } S\}.$$

Notice that $\text{osh}\,(\mathcal{F})$ is a down-set, i.e., if $A \in \text{osh}(\mathcal{F})$ and $B \subseteq A$, then $B \in \text{osh}(\mathcal{F})$. We illustrate with the following examples the notion of order shattering.

Examples. 1. If $\mathcal{F} = 2^S$ then clearly $\text{osh}\,(\mathcal{F}) = 2^S$ for $S \subseteq [n]$. More generally, $\text{osh}\left(\binom{[n]}{\le d}\right) = \binom{[n]}{\le d}$.
2. The family $\mathcal{G}$ consisting of all even subsets $F \subseteq [n]$ does not order shatter $\{1\}$. Indeed, there are no $F_0, F_1 \in \mathcal{G}$ such that $1 \in F_1$, $1 \notin F_0$ and $F_1 \cap \{2, \ldots, n\} = F_0$. On the other hand this $\mathcal{G}$ order shatters all subsets of $\{2, \ldots, n\}$, hence $\text{osh}(\mathcal{G}) = \{F \subseteq [n] : \ 1 \notin F\}$.

In [11] it was established for $0 \le d \le n/2$ that

$$\text{osh}\left(\binom{[n]}{d}\right) = \{\{s_1 < \ldots < s_j\} \subset [n] : \ j \le d \text{ and } s_i \ge 2i \text{ for } 1 \le i \le j\}. \tag{5}$$

Actually, it is shown there (Lemma 2.2) that $\mathrm{osh}\binom{[n]}{d}$ is contained in the set on the right side of (5) and that the latter has at most $\binom{n}{d}$ elements (Lemma 2.3). From these (5) follows because $|\mathrm{osh}\,(\mathcal{F})\,| = |\mathcal{F}|$ holds for every $\mathcal{F}$.

It is immediate that for a nonempty family $\mathcal{F} \subseteq 2^{[n]}$ we have

$$\mathrm{osh}\,(\mathrm{co}(\mathcal{F})) = \mathrm{osh}\,(\mathcal{F})\,, \tag{6}$$

where

$$\mathrm{co}(\mathcal{F}) = \{[n] \setminus F : \ F \in \mathcal{F}\}.$$

In particular,

$$\mathrm{osh}\binom{[n]}{d} = \mathrm{osh}\binom{[n]}{n-d}.$$

In Theorem 2.10 we identify the lex standard monomials of the characteristic vectors of a set family $\mathcal{F} \subseteq 2^{[n]}$ with $\mathrm{osh}(\mathcal{F})$. We use this result in the description of the Gröbner bases of (reduced) complete ℓ-wide and complete uniform families.

Consider a family $\mathcal{F}$ of subsets of $[n]$. We say that $\mathcal{F}$ *shatters* S if

$$\{E \cap S : \ E \in \mathcal{F}\} = 2^S. \tag{7}$$

Then define

$$\mathrm{sh}(\mathcal{F}) = \{S \subseteq [n] : \ \mathcal{F} \text{ shatters } S\}. \tag{8}$$

We obtain such properties as $\mathrm{sh}(\mathrm{sh}(\mathcal{F})) = \mathrm{sh}(\mathcal{F})$ and that $\mathrm{sh}(\mathcal{F})$ is a down-set. From the definition it is easy to see that $\mathrm{osh}(\mathcal{F}) \subseteq \mathrm{sh}(\mathcal{F})$, hence using $|\mathrm{osh}(\mathcal{F})| = |\mathcal{F}|$, we get the following result:

Theorem 2.1 *([70]) Let $\mathcal{F}$ be a family of subsets of $[n]$. Then*

$$|\mathcal{F}| \leq |sh(\mathcal{F})|.$$

A family $\mathcal{F}$ has VC-dimension k if there is no shattered set of size k (and hence no larger shattered set). The following theorem is a fundamental result in the theory of shattering:

Theorem 2.2 (Sauer[75],Perles, Shelah[76], Vapnik, Chervonenkis[78]) *Let $\mathcal{F}$ be a family of subsets of $[n]$ with no shattered set of size k. Then*

$$|\mathcal{F}| \leq \sum_{i=0}^{k-1} \binom{n}{i} \tag{9}$$

and (9) is the best possible.

We say that a set system $\mathcal{F}$ is *uniform* if $\mathcal{F} \subseteq \binom{[n]}{\ell}$ for some ℓ.

Using (5) it is easy to prove the following theorem of P. Frankl and J. Pach.

Theorem 2.3 *(Frankl, Pach, [34]) Let $\mathcal{F}$ be a uniform set system with no shattered set of size k. Then*

$$|\mathcal{F}| \leq \binom{n}{k-1}.$$

Let $\mathcal{F}^{k,\ell}$ denote the *complete ℓ-wide* family

$$\mathcal{F}^{k,\ell} = \{F \subseteq [n] : k - \ell < |F| \leq k\}.$$

A set family $\mathcal{F} \subseteq 2^{[n]}$ is *ℓ-wide* if $\mathcal{F} \subseteq \mathcal{F}^{k,\ell}$ for a suitable k.

In Chapter 4 we prove the following generalisation of Theorem 2.3 for ℓ-wide families:

Theorem 2.4 *Suppose that $2t \leq n + \ell$ and let $\mathcal{F} \subseteq 2^{[n]}$ be an ℓ-wide family with no shattered set of size t. Then*

$$|\mathcal{F}| \leq \sum_{i=\max(0,t-\ell)}^{t-1} \binom{n}{i}.$$

Clearly, if $\mathcal{F}$ is an ℓ-wide family of sets, then $\mathcal{F}$ does not contain any chain of size $\ell + 1$. Therefore Theorem 2.4 gives a special case of Frankl's conjecture: Let $g(n, t, d)$ denote the maximum number of subsets of $[n]$ with no shattered set of size t and no chain of size $d + 1$. In [32] Frankl proposed the following conjecture.

Conjecture 1 (Frankl, [32]) *Assume that $2t \leq n + d$. Then*

$$g(n,t,d) \leq \sum_{i=\max(0,t-d)}^{t-1} \binom{n}{i}. \tag{10}$$

2.2 Gröbner bases and standard monomials

We recall now some basic facts concerning Gröbner bases and standard monomials in polynomial rings. For a more thorough study see [28] or [1].

Throughout this thesis $\mathbb{F}$ denotes a fixed (otherwise arbitrary) field. As usual, $\mathbb{F}[x_1,\dots,x_n]$ denotes the ring of polynomials in variables $x_1,\dots,x_n$ over $\mathbb{F}$. Occasionally, we use the shorter notation $S=\mathbb{F}[x_1,\dots,x_n]$.

We denote by $\mathbb{F}[x_1,\dots,x_n]_{\leq s}$ the vector space of all polynomials over $\mathbb{F}$ with degree at most s. Let $\mathrm{Mon}(n,d)$ denote the set of monomials $x^u\in\mathbb{F}[x_1,\dots,x_n]$ of degree d. We write $\mathrm{Mon}(n,\leq d):=\cup_{i=0}^{d}\mathrm{Mon}(n,i)$ and $\mathrm{Mon}:=\cup_{i=0}^{\infty}\mathrm{Mon}(n,i)$ stands for the set of all monomials over $x_1,\dots,x_n$.

To obtain information about polynomial functions on a subset $\mathcal{F}\subseteq\mathbb{F}^n$, it is useful to consider the ideal $I(\mathcal{F})$:

$$I(\mathcal{F}):=\{f\in S:\ f(v)=0 \text{ whenever } v\in\mathcal{F}\}.$$

Let $v_F\in\{0,1\}^n$ denote the characteristic vector of a set $F\subseteq[n]$. For a family of subsets $\mathcal{F}\subseteq 2^{[n]}$, let $V(\mathcal{F})=\{v_F: F\in\mathcal{F}\}\subseteq\{0,1\}^n\subseteq\mathbb{F}^n$. A polynomial $f\in\mathbb{F}[x_1,\dots,x_n]=S$ can be considered as a function from $V(\mathcal{F})$ to $\mathbb{F}$ in the straightforward way.

Several interesting results on finite set systems $\mathcal{F}\subseteq 2^{[n]}$ can be naturally formulated as statements concerning *polynomial functions on* $V(\mathcal{F})$. For instance, certain inclusion matrices (see Chapter 5) can be viewed naturally in this setting. Also, the approach to the complexity theory of Boolean functions, initiated by Smolensky [77] and developed further by Bernasconi and Egidi [19], leads to such questions.

A total order $\prec$ on the monomials composed from variables $x_1,x_2,\dots,x_n$ is a *term order*, if 1 is the minimal element of $\prec$, and if $u\prec v$, then $uw\prec vw$ holds for any monomials u,v,w. We define two important term orders: the lexicographic order $\prec_{lex}$ and the deglex order $\prec_{deg}$. Let $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ and $x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}$ be two monomials. Then

$$x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\prec_{lex}x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}$$

iff $i_k<j_k$ holds for the smallest index k such that $i_k\neq j_k$. For example, $x_1^3x_2^2x_3\prec_{lex}x_1^3x_2^2x_3^5$.

As for deglex, we have $u\prec_{deg}v$ iff either $\deg u<\deg v$, or $\deg u=\deg v$, and $u\prec_{lex}v$. For example, $u=x_1x_2x_3^7\prec_{deg}v=x_1x_2^2x_3^6$, since $\deg u=\deg v=9$ and $x_1x_2x_3^7\prec_{lex}x_1x_2^2x_3^6$. But $v=x_1^2x_2^3\prec_{deg}u=x_1x_2^2x_3^3$, because $\deg u=6>\deg v=5$.

Another (somewhat less intuitive) term order on the monomials is the following special case of a *weight order*, see [71]. Let $u=(u_1,\dots,u_n)$ be a fixed vector in $\mathbb{R}^n$ such that $u_1,\dots,u_n$ are positive and linearly independent over

$\mathbb{Q}$. We say that u is an *independent weight vector*. Then, for the monomials $x^\alpha, x^\beta \in \text{Mon}$, define

$$x^\beta \prec_u x^\alpha \text{ iff } \beta \cdot u < \alpha \cdot u,$$

where the centered dot is the usual scalar product of vectors. We call $\prec_u$ the *weight order* determined by u.

We can easily generalise this definition: we start with a vector $u_1 \in \mathbb{R}^n$, whose entries may not be linearly independent over $\mathbb{Q}$. Then $x^\beta \prec x^\alpha$ if $u_1 \cdot \beta < u_1 \cdot \alpha$. But if we need to break ties, then we use a second weight vector $u_2 \in \mathbb{R}^n$. This means, that $x^\beta \prec x^\alpha$ also holds if $u_1 \cdot \alpha = u_1 \cdot \beta$ and $u_2 \cdot \beta < u_2 \cdot \alpha$. If there are still ties, then we can use a third weight vector in a similar way and so on. In [71] Robbiano proved that *every* term order on the monomials arises in this way.

We say that a term order $\prec$ is an *elimination order*, if x^α is a monomial in which one of $x_1, \ldots, x_i$ appears, then $x^\beta \prec x^\alpha$ for *any* monomial involving only $x_{i+1}, \ldots, x_n$. For example, $\prec_{lex}$ is an elimination order. Elimination orders play an important role in elimination theory.

The *leading monomial* $\text{lm}(f)$ of a nonzero polynomial $f \in S$ is the largest (with respect to $\prec$) monomial which appears with nonzero coefficient in f when expressed as an $\mathbb{F}$-linear combination of monomials. For example, let $f := 4x_1x_2^2x_3 + 4x_3^2 - 5x_1^3 + 7x_1^2x_3^2$. Then $\text{lm}(f) = x_1^3$ with respect to the lex order.

An I ideal of S is a *monomial ideal* if there exists a subset of monomials $G \subseteq \text{Mon}$ such that G generates the ideal I. For example, $I = \langle x_1^3x_2^2, x_3^4, x_2x_3^4 \rangle$ is a monomial ideal.

We can characterise easily *all* monomials of a monomial ideal.

Lemma 2.5 *Let $I = \langle x^\alpha : \ \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I iff there exists an $\alpha \in A$ such that x^β is divisible by x^α.* □

A special case of Hilbert's basis theorem is the following form of Dickson's lemma:

Theorem 2.6 *(Dickson's Lemma) Every monomial ideal*

$$I = \langle x^\alpha : \ \alpha \in A \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$$

has a finite generating set, i.e., $I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle$, where $\alpha(1), \ldots, \alpha(s) \in A$. □

For a proof see Theorem 5 in Chapter 2.4 in Cox, Little, O'Shea [28].

It is easy to verify that two monomial ideals are the same iff they contain the same monomials.

Now we introduce the notion of reduction, which is ubiquitous in the computational applications of Gröbner bases. Let $\mathcal{G}$ be a set of polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ and let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a fixed polynomial. Let $\prec$ be an arbitrary term order. We can reduce f by the set $\mathcal{G}$ with respect to $\prec$. This gives a new polynomial $h \in \mathbb{F}[x_1, \ldots, x_n]$.

Here *reduction* means that we possibly repeatedly replace monomials in f by smaller ones (with respect to $\prec$) as follows: if w is a monomial occurring in f and $\mathrm{lm}(g)$ divides w for some $g \in \mathcal{G}$ (i.e. $w = \mathrm{lm}(g)u$ for some monomial u), then we replace w in f with $u(\mathrm{lm}(g) - g)$. Clearly the monomials in $u(\mathrm{lm}(g) - g)$ are $\prec$-smaller than w.

We can give a division algorithm on the basis of reduction of polynomials:

Theorem 2.7 *(Division Algorithm) Let $\prec$ be a fixed term order. Let $\mathcal{G} = (g_1, \ldots, g_t)$ be an ordered t-tuple of polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. Then every $f \in \mathbb{F}[x_1, \ldots, x_n]$ can be written in the form*

$$f = p_1 f_1 + \ldots + p_t f_t + h \tag{11}$$

and either $h = 0$ or h is a $\mathbb{F}$-linear combination of monomials, none of which is divisible by any $lm(f_i)$. We call h a remainder of f on division by $\mathcal{G}$.

This algorithm is a common generalisation of the Gaussian elimination and the division algorithm of univariate polynomials.

It is easy to show that the remainder h is not uniquely determined by the requirement, that none of its terms be divisible by any $\mathrm{lm}(f_i)$ and a permutation of the t-tuple $(g_1, \ldots, g_t)$ can also change the result of the division algorithm. For instance, if $\mathcal{G} = (x_1^2 x_2 - x_2^2, x_1^4 x_2^2 - x_2^2)$ and $f = x_1^5 x_2$, then using the lex order we have

$$x_1^5 x_2 = (x_1^3 + x_1 x_2)(x_1^2 x_2 - x_2^2) + 0 \cdot (x_1^4 x_2^2 - x_2^2) + x_1 x_2^3,$$

hence the reduction of f by the set $\mathcal{G}$ is $x_1 x_2^3$.

We can define now the ideal of leading monomials as follows. Let I be an ideal of S, $I \neq (0)$. We denote by $\mathrm{Lm}(I)$ the set of leading monomials of I, i.e.,

$$\mathrm{Lm}(I) = \{\mathrm{lm}(f) : \ f \in I\}. \tag{12}$$

The *initial ideal* $\text{in}(I)$ of an ideal I is the ideal in S generated by the elements of $\text{Lm}(I)$. By definition, $\text{in}(I)$ is a monomial ideal.

If we are given a finite generating set for I, say $I = \langle f_1, \ldots, f_s \rangle$, then $\langle \text{lm}(f_1), \ldots, \text{lm}(f_s) \rangle$ and $\text{in}(I)$ may be *different* ideals. It is clear that $\text{lm}(f_i) \in \text{Lm}(I) \subseteq \text{in}(I)$ by definition, which implies $\langle \text{lm}(f_1), \ldots, \text{lm}(f_s) \rangle \subseteq \text{in}(I)$. However $\text{in}(I)$ can be strictly larger. For example, let $I = \langle f_1, f_2 \rangle$, where $f_1 = x_1^3 - 2x_1x_2$ and $f_2 = x_1^2x_2 - 2x_2^2 + x_1$, and use the deglex order on the monomials of $\mathbb{F}[x_1, x_2]$. Then

$$x_1 \cdot (x_1^2x_2 - 2x_2^2 + x_1) - x_2(x_1^3 - 2x_1x_2) = x_1^2,$$

so that $x_1^2 \in I$. Thus, $x_1^2 = \text{lm}(x_1^2) \in \text{in}(I)$. But x_1^2 is not divisible by $\text{lm}(f_1) = x_1^3$ or $\text{lm}(f_2) = x_1^2x_2$, therefore $x_1^2 \notin \langle \text{lm}(f_1), \text{lm}(f_2) \rangle$, by Lemma 2.5.

Let I be an ideal of S and $\prec$ be a fixed term order. A finite subset $\mathcal{G} = \{g_1, \ldots, g_t\} \subseteq I$ is a *Gröbner basis* of I if

$$\langle \text{lm}(g_1), \ldots, \text{lm}(g_t) \rangle = \text{in}(I).$$

Equivalently, a set $\mathcal{G} = \{g_1, \ldots, g_t\} \subseteq I$ is a Gröbner basis of I iff for every $f \in I$ there exists a $g_i \in \mathcal{G}$ such that $\text{lm}(g_i)$ divides $\text{lm}(f)$.

Now we can easily prove here the following fundamental result:

Theorem 2.8 *Let $\prec$ be a fixed term order. Then every ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$, $I \neq (0)$ has a Gröbner basis. Every Gröbner basis for an ideal I is a basis of I.*

Proof. Since $\text{in}(I)$ is generated by the monomials $\text{lm}(g)$ for $g \in I \setminus \{0\}$, Dickson's Lemma implies that

$$\text{in}(I) = \langle \text{lm}(g_1), \ldots, \text{lm}(g_t) \rangle$$

for some $g_1, \ldots, g_t \in I$. Now it is enough to prove that $I = \langle g_1, \ldots, g_t \rangle$. Obviously $\langle g_1, \ldots, g_t \rangle \subseteq I$, because each $g_i \in I$.

Conversely, let $f \in I$ be an arbitrary polynomial. We can reduce f by the set $\{g_1, \ldots, g_t\}$. By Theorem 2.7 we obtain the following expression:

$$f = p_1g_1 + \ldots + p_tg_t + r, \tag{13}$$

where either $r = 0$ or every term of r is not divisible by any of the monomials $\text{lm}(g_1), \ldots, \text{lm}(g_t)$.

We need to prove that $r = 0$.

Clearly $r = f - p_1 g_1 - \ldots - p_t g_t \in I$. If $r \neq 0$, then

$$\mathrm{lm}(r) \in \mathrm{in}(I) = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t) \rangle$$

and Lemma 2.5 implies that the monomial $\mathrm{lm}(r)$ must be divisible by some $\mathrm{lm}(g_i)$. But this contradicts to the meaning of the remainder, therefore r must be zero, i.e., $f = p_1 g_1 + \ldots + p_t g_t \in \langle g_1, \ldots, g_t \rangle$, hence $I \subseteq \langle g_1, \ldots, g_t \rangle$.

□

It is obvious that a Gröbner basis $\mathcal{G}$ for an ideal I with respect to a term order $\prec$ is not unique, in fact, any superset of this $\mathcal{G}$ is also a Gröbner basis.

We can read out easily from the previous proof the famous Hilbert Basis Theorem:

Theorem 2.9 *(Hilbert Basis Theorem): Every ideal* $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ *has a finite basis, i.e.,* $I = \langle g_1, \ldots, g_t \rangle$ *for some* $g_1, \ldots, g_t \in I$.

Consider the ideal $J = \langle x + z, y - z \rangle$. Then it is easy to prove that $g_1 = x + z$ and $g_2 = y - z$ form a Gröbner basis using the lex order in $\mathbb{Q}[x, y, z]$.

Unfortunately, we can get often bigger Gröbner bases with the Buchberger's algorithm than necessary. The first idea to eliminate some unneeded generators is to remove any $p \in \mathbb{F}[x_1, \ldots, x_n]$ polynomial, with

$$\mathrm{lm}(p) \in \langle \mathrm{Lm}(\mathcal{G} \setminus \{p\}) \rangle$$

from the Gröbner basis $\mathcal{G}$.

We call a Gröbner basis $\mathcal{G}$ *minimal*, if the coefficient of $\mathrm{lm}(f_i)$ is 1 and for all $g \in \mathcal{G}$, $\mathrm{lm}(g) \notin \langle \mathrm{Lm}(\mathcal{G} \setminus \{g\}) \rangle$.

But a given ideal may have many minimal Gröbner bases. For example, if $I = \langle x_1^3 - 2x_1x_2, x_1^2x_2 - 2x_2^2 + x_1, -x_1^2 - 2x_1x_2, -2x_2^2 + x_1 \rangle \subseteq \mathbb{Q}[x_1, x_2, x_3]$, then it is easy to check that

$$f_1 = x_1^2 + ax_1x_2, \; f_2 = x_1x_2, \; f_3 = x_2^2 - 0.5x_1$$

is also a minimal Gröbner basis using the deglex order, where $a \in \mathbb{Q}$ is any constant. But we can easily choose out one minimal basis, that has many advantages. We arrived now to the notion of reduced Gröbner bases.

A Gröbner basis $\{f_1, \ldots, f_m\}$ of I is *reduced* if the coefficient of $\mathrm{lm}(f_i)$ is 1, and no nonzero monomial in f_i is divisible by any $\mathrm{lm}(f_j)$, $j \neq i$. By a theorem of Buchberger ([1, Theorem 1.8.7]), for a fixed term order $\prec$, any nonzero ideal of S has a unique reduced Gröbner basis. In the previous example g_1 and g_2 gives a reduced Gröbner basis of the ideal J using the lex order.

Later we shall use the following characterisation of Gröbner bases (see Theorem 3.10 in Chapter 1 of [26], or Theorem 1.9.1 in [1]):

Theorem 2.10 *A nonempty set $\mathcal{G} = \{g_1, \ldots, g_t\}$ of polynomials is a Gröbner basis of the ideal I generated by $\mathcal{G}$ iff every $f \in I$ reduces to zero with respect to $\mathcal{G}$.*

Proof. The division algorithm gives us the expression

$$f = p_1 g_1 + \ldots + p_t g_t + r,$$

where either $r = 0$ or no term of r is divisible by one of $\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t)$. Clearly if the remainder is zero, then $f \in I$.

Conversely, let $f \in I$ be an arbitrary polynomial. Indirectly, suppose that after the division algorithm the remainder $r \neq 0$. Then $f = g + r$, where $g \in I$. Hence $r \in I$, i.e., $\mathrm{lm}(r) \in \mathrm{in}(I) = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t) \rangle$, which is impossible, since by the definition of the remainder no term of r is divisible by one of $\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t)$. □

A monomial $w \in \mathrm{Mon}$ is called a *standard monomial for I* if $w \notin \mathrm{in}(I)$, i.e., it is not a leading monomial of any $f \in I$. Let $\mathcal{V} \subseteq \mathbb{F}^n$ be an arbitrary finite subset. Then let $\mathrm{Sm}(\prec, \mathcal{V})$ stand for the set of all standard monomials of $I(\mathcal{V})$ with respect to the term order $\prec$ over $\mathbb{F}$. It follows from the definition and existence of Gröbner bases (see [26, Chapter 1, Section 4]) that for a nonempty finite set of points $\mathcal{V}$ the set $\mathrm{Sm}(\prec, \mathcal{V})$ is a basis of the $\mathbb{F}$-vector space $S/I(\mathcal{V})$. In fact, every $g \in S$ can be written uniquely as $g = h + f$ where $f \in I(\mathcal{V})$ and h is a unique $\mathbb{F}$-linear combination of monomials from $\mathrm{Sm}(\prec, \mathcal{V})$. Here h is the unique reduction of g by the Gröbner basis $\mathcal{G}$ of the ideal $I(\mathcal{V})$. We write

$$\mathrm{sm}(\prec, \mathcal{V}) := \mathrm{sm}(\prec, \mathcal{V}, \mathbb{F}) = \{\alpha \in \mathbb{N}^n : \ x^\alpha \in \mathrm{Sm}(\prec, \mathcal{V})\} \subseteq \mathbb{N}^n.$$

Let $\mathcal{V}$ be an arbitrary finite subset of $\mathbb{F}^n$. It is immediate that $\mathrm{sm}(\prec, \mathcal{V}, \mathbb{F})$ is a downward closed vector set. By the previous discussion the standard monomials for $I(\mathcal{V})$ form a basis of the functions from $\mathcal{V}$ to $\mathbb{F}$, hence

$$|\mathrm{Sm}(\prec, \mathcal{V})| = |\mathcal{V}|. \qquad (14)$$

If $\mathcal{F} \subseteq 2^{[n]}$, then $x_i^2 - x_i \in I(V(\mathcal{F}))$, hence x_i^2 is a leading term for $I(V(\mathcal{F}))$. It follows that the standard monomials for this ideal are all square-free, i.e. of form x_G for $G \subseteq [n]$. We put

$$\mathrm{stm}(\prec, \mathcal{F}) := \mathrm{stm}(\prec, \mathcal{F}, \mathbb{F}) = \{G \subseteq [n] : \ x_G \in \mathrm{Sm}(\prec, V(\mathcal{F}))\} \subseteq 2^{[n]}.$$

In Theorem 4.3 of [11] R. P. Anstee, L. Rónyai and A. Sali proved the following result.

Theorem 2.11 *Let $\mathcal{F} \subseteq 2^{[n]}$ be a nonempty family and let $\mathbb{F}$ be an arbitrary field. Then $\mathcal{M} = \{x_F : F \in \mathrm{osh}\,(\mathcal{F})\}$ is the set of standard monomials with respect to the lexicographic order $\prec_{lex}$ of the ideal of all polynomials $f \in \mathbb{F}[x_1, \ldots, x_n]$ which vanish on $V(\mathcal{F}) \subseteq \mathbb{F}^n$.*

Theorem 2.11 gives us a combinatorial description of the lex standard monomials of any ideal $I(V(\mathcal{F}))$, which corresponds to the set family $\mathcal{F}$. If we choose a special set family $\mathcal{M}$, then with the concrete description of $\mathrm{osh}(\mathcal{M})$, we can also understand better the rank computation of inclusion matrices or we can investigate without effort the shattered set family $\mathrm{sh}(\mathcal{M})$.

The first applications of the Gröbner basis theory was the ideal membership algorithm: let $I = \langle f_1, \ldots, f_t \rangle$ be a given ideal and $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial. Using reduction by the Gröbner basis of I we can decide whether f lies in I by Theorem 2.10. A second important application of Gröbner bases is the problem of solving polynomial equations over an algebraic closed field. A system of equations in the Gröbner basis with respect to an eliminate term order $\prec$ is easier to solve. It comes out that the last equation contains only one variable. We can apply then well–known one–variable techniques to find the roots of this equation, then we can substitute back into the other equations of the Gröbner bases and similarly solve for the other variables.

2.3 The Hilbert function of ideals

Now we define the affine Hilbert function of an ideal.

Let I be an ideal of $S = \mathbb{F}[x_1, \ldots, x_n]$. The *Hilbert function* of the algebra S/I is the sequence $h_{S/I}(0), h_{S/I}(1), \ldots$. Here $h_{S/I}(m)$ is the dimension over $\mathbb{F}$ of the quotient $\mathbb{F}[x_1, \ldots, x_n]_{\leq m}/(I \cap \mathbb{F}[x_1, \ldots, x_n]_{\leq m})$ (see [28, Section 9.3]).

In the case when $I = I(\mathcal{V})$ for some finite set of points $\mathcal{V} \subseteq \mathbb{N}^n$, the number $h_{\mathcal{V}}(m) := h_{S/I(\mathcal{V})}(m)$ is the dimension of the space of functions from $\mathcal{V}$ to $\mathbb{F}$ which can be represented as polynomials of degree at most m.

The following Proposition gives an easy way to compute the Hilbert function of a monomial ideal.

Proposition 2.12 *Let $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be an arbitrary monomial ideal, $I \neq (0)$.*

(a) Then

$$h_{S/I}(m) = |\{w \in Mon : \ w \notin I \text{ and } \deg w \leq m\}|$$

for each $m \geq 0$, i.e., $h_{S/I}(m)$ is the number of monomials not in I of degree at most m.

(b) There exists a polynomial function $p(x) = \sum_{i=0}^{d} c_i \binom{x}{i} \in \mathbb{Q}[x]$, such that

$$h_{S/I}(m) = p(m)$$

for each sufficiently large m. Here $c_i \in \mathbb{Z}$ and $c_d > 0$.

The previous $p(x)$ polynomial is called the *affine Hilbert polynomial* of the ideal I. It has a central role in the dimension theory: the degree of this polynomial is by definition the dimension of the ideal I.

We say that a term order $\prec$ is a *degree-compatible* order, if $x^\alpha \prec x^\beta$ whenever $\deg x^\alpha < \deg x^\beta$. For example, $\prec_{deg}$ is a degree-compatible term order.

Now we can link the Hilbert function computation problem to the theory of Gröbner bases in the following observation of Macaulay:

Proposition 2.13 *(Macaulay) Let $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be an arbitrary nonzero ideal and $\prec$ be a degree-compatible term order. Then the monomial ideal $in(I)$ and I have the same Hilbert function: $h_{S/I}(m) = h_{S/in(I)}(m)$ for all $m \geq 0$.*

Hence we can relate the problem of Hilbert function computation to the problem of the determination of standard monomials of an ideal I with respect to any $\prec$ degree-compatible term order:

Corollary 2.14 *Let $I = I(\mathcal{V})$ be an ideal of $\mathbb{F}[x_1, \ldots, x_n]$, $I \neq (0)$ and $\prec$ be a degree-compatible term order. Then for all $m \geq 0$, $h_{S/I}(m)$ is the number of standard monomials with respect to $\prec$ of degree at most m, i.e.,*

$$h_{S/I}(m) = |Sm(\prec, \mathcal{V}) \cap Mon(n, \leq m)|. \qquad (15)$$

We examine here an important special case: the Hilbert function of set families. If $\mathcal{F} \subseteq 2^{[n]}$ is a set family and the finite set of points $\mathcal{V} = V(\mathcal{F}) \subseteq \{0,1\}^n \subseteq \mathbb{F}^n$ is the set of characteristic vectors of the set family $\mathcal{F}$, then we put $h_{\mathcal{F}}(m) := h_{S/I(V(\mathcal{F}))}(m)$.

In the combinatorial literature $h_{\mathcal{F}}(m)$ is usually given in terms of inclusion matrices. For families $\mathcal{F}, \mathcal{G} \subseteq 2^{[n]}$ the *inclusion matrix* $I(\mathcal{F}, \mathcal{G})$ is a (0,1) 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 $(F \in \mathcal{F}, G \in \mathcal{G})$.

Of particular interest will be the case when $\mathcal{G}$ is the complete s-uniform family $\binom{[n]}{s}$. We call the $|\mathcal{F}| \times \binom{n}{s}$ matrix $I(\mathcal{F}, \binom{[n]}{s})$ *the s-inclusion matrix of* $\mathcal{F}$.

The first applications of the connection between the order shattering of set families and lex standard monomials (Theorem 2.11) are the following two important results of Wilson, which give the ranks of incidence matrices of complete uniform families:

Theorem 2.15 *If* $d \le k \le n - d$ *are natural numbers and* $\mathbb{F}$ *is an arbitrary field then*

$$rank_{\mathbb{F}}\, I\left(\binom{[n]}{k}, \binom{[n]}{\le d}\right) = \binom{n}{d}, \tag{16}$$

and

$$rank_{\mathbb{F}}\, I\left(\binom{[n]}{k}, \binom{[n]}{d}\right) = \sum \binom{n}{i} - \binom{n}{i-1}, \tag{17}$$

where the summation is for those indices i, for which $\binom{k-i}{d-i}$ *is not 0 in* $\mathbb{F}$.

For proofs see Wilson [79], Bier [14], Frankl [33], Frumkin and Yakir [37], Friedl and Rónyai [36].

In extremal combinatorics one can find a lot of applications of the rank computation of inclusion matrices, see for example [16]. In Chapter 5 we obtain new upper bound for modulo q L-intersecting families.

It is a simple matter to verify that

$$h_{\mathcal{F}}(m) = \mathrm{rank}_{\mathbb{F}}\, I(\mathcal{F}, \binom{[n]}{\le m}). \tag{18}$$

For example, if $\mathcal{F} = 2^{[n]}$ and $\prec$ is an arbitrary term order, then

$$\mathrm{Sm}(\prec, V(\mathcal{F})) = \{x_G : \; G \subseteq [n]\},$$

therefore $h_{\mathcal{F}}(m) = \sum_{i=0}^{m} \binom{n}{i}$, for $0 \le m \le n$.

2.4 Partitions, tableaux

A sequence $\lambda = (\lambda_1, \ldots, \lambda_k)$ of natural numbers is a *partition* of n, if $\lambda_1 + \lambda_2 + \cdots + \lambda_k = n$ and $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k > 0$. If λ is a partition of n, then we denote this fact by $\lambda \vdash n$.

Suppose that $\lambda = (\lambda_1, \ldots, \lambda_k)$ is a partition of n. The Ferrers diagram of λ is an array of n squares (boxes) having k left-justified rows, with row i containing λ_i squares for $1 \leq i \leq k$. A λ-*tableau* t is obtained by filling the squares of the Ferrers diagram of λ with the numbers $1, 2, \ldots, n$ bijectively. There are $n!$ λ-tableaux.

For example, if $n = 7$, $\lambda = (4, 2, 1)$ then

2	5	3	6
4	1		
7			

and

1	2	4	5
3	7		
6			

(19)

are two of the 7! λ-tableaux.

A tableau t is *standard* if the rows and the columns of t are increasing sequences. The second example above is a standard tableau.

S_n denotes the symmetric group (acting on $[n]$). On vectors $v = (v_1, \ldots, v_n) \in \mathbb{F}^n$ we shall consider the action of S_n as the group of place permutations. For $\pi \in S_n$, we set

$$\pi v = (v_{\pi^{-1}(1)}, \ldots, v_{\pi^{-1}(n)}). \tag{20}$$

In the following we work with a partial order $\leq$ on $\mathbb{N}^n$: if

$$u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{N}^n,$$

then set $u \leq v$ iff $u_i \leq v_i$ for $1 \leq i \leq n$.

A subset $W \subseteq \mathbb{N}^n$ is called *downward closed*, if $u \leq v$ and $v \in W$ imply that $u \in W$. We define the *downward hull* of $W \subseteq \mathbb{N}^n$ by:

$$W^{\leq} := \{w \in \mathbb{N}^n : \text{ there exists } v \in W \text{ such that } w \leq v\}.$$

Clearly W is downward closed iff $W^{\leq} = W$. Similarly, if K is a set of monomials, then the downward hull of K is

$$K^{\leq} := \{x^w \in \text{Mon} : \text{ there exists } x^t \in K \text{ such that } w \leq t\}.$$

A *ballot sequence*, or a *lattice permutation*, is a vector of nonnegative integers $m = (i_1, i_2, \ldots, i_n)$ such that, for any prefix $m_k = (i_1, \ldots, i_k)$ and any nonnegative integer l, the number of l's in m_k is at least as large as the number of $(l+1)$'s in that prefix. As an example,

$$m = (0,0,1,0,0,2,1)$$

is a lattice permutation, whereas $(0,1,2,1,0,0,2)$ is not, because the prefix $(0,1,2,1)$ has more ones than zeros.

It is well-known (see [74]) that lattice permutations are in one to one correspondence with standard tableaux. Given a standard tableau t with n elements, form the sequence $m = (i_1, i_2, \dots, i_n)$, where $i_k = i - 1$ if k appears in row i of t. This way we obtain a lattice permutation. It is easy to construct the inverse map. For example, $(0,0,1,0,0,2,1)$ is the lattice permutation corresponding to the standard tableau in (19).

A lattice permutation m has type λ iff the corresponding t is a standard λ-tableau. For $\lambda \vdash n$ we define

$$\mathrm{st}(\lambda) := \{u \in \mathbb{N}^n : \ u \text{ is a lattice permutation of type } \lambda\}$$

and

$$\mathrm{St}(\lambda) := \{x^u : \ u \in \mathrm{st}(\lambda)\}.$$

For example, if $\lambda = (2,2,1)$, then

$$\mathrm{st}(\lambda) = \{(0,0,1,1,2), (0,0,1,2,1), (0,1,0,1,2), (0,1,0,2,1), (0,1,2,0,1)\},$$

and $x_3 x_4 x_5^2 \in \mathrm{St}(\lambda)$.

We write $b_\lambda := \mathrm{st}(\lambda)^{\leq}$ and $B_\lambda = \{x^u : \ u \in b_\lambda\}$. Clearly b_λ is downward closed.

As customary, f^λ denotes the number of standard tableaux of shape λ, i.e., $f^\lambda := |\mathrm{st}(\lambda)|$.

2.5 The polynomials $f_{H,k}$

We introduce a family of polynomials with integral coefficients. These polynomials will be the "nontrivial" elements of the Gröbner bases of the complete uniform and the complete ℓ-wide families.

Let ℓ, t be positive integers. We define $\mathcal{H}(t,\ell)$ as the set of those subsets $H = \{s_1 < \ldots < s_t\}$ of $[n]$ for which t is the smallest index j with $s_j < 2j - \ell + 1$. In the special case $\ell = 1$ we define $\mathcal{H}(t) := \mathcal{H}(t,1)$.

We remark that $\mathcal{H}(t,\ell) = \emptyset$ for $t < \ell$. Indeed, if $H \in \mathcal{H}(t,\ell)$, then $t \le s_t < 2t - \ell + 1$, and $\ell - 1 < t$. Also if $t > (n+\ell)/2$, then $\mathcal{H}(t,\ell) = \emptyset$ again, because then $s_{t-1} \ge 2(t-1) - \ell + 1 > n - 1$ would imply that $s_t > n$.

The elements of $\mathcal{H}(t,\ell)$ are t-subsets of $[n]$, and we have $H \in \mathcal{H}(t,\ell)$ iff $s_1 \ge 3 - \ell, s_2 \ge 5 - \ell, \dots, s_{t-1} \ge 2t - \ell - 1$ and $s_t < 2t - \ell + 1$. It follows that $s_t = 2t - \ell$ (in the case $t = 1$ we have $\ell = 1$ as well). For $t > 1$ we have also $s_{t-1} = 2t - \ell - 1$.

As examples, for n large enough, we have $\mathcal{H}(2,2) = \{\{1,2\}\}$,
$\mathcal{H}(3,2) = \{\{1,3,4\},\{2,3,4\}\}$, and
$\mathcal{H}(4,2) = \{\{1,3,5,6\},\{1,4,5,6\},\{2,3,5,6\},\{2,4,5,6\},\{3,4,5,6\}\}$.

For a subset $J \subseteq [n]$ and an integer $0 \le i \le |J|$ we denote by $\sigma_{J,i}$ the i-th elementary symmetric polynomial of the variables x_j, $j \in J$:

$$\sigma_{J,i} := \sum_{T \subseteq J, |T| = i} x_T \ \in \mathbb{Z}[x_1, \dots, x_n].$$

In particular, $\sigma_{J,0} = 1$.

Now let $0 < \ell \le t < (n+\ell)/2$, $0 \le k \le n$ and $H \in \mathcal{H}(t,\ell)$. Then put $H' = H \cup \{2t - \ell + 1, 2t - \ell + 2, \dots, n\}$.

We write

$$f_{H,k} = f_{H,k}(x_1, \dots, x_n) := \sum_{j=0}^{t} (-1)^{t-j} \binom{k-j}{t-j} \sigma_{H',j}.$$

Note that $f_{H,k}$ depends on t and ℓ through H. Moreover, H uniquely determines t and ℓ. Specifically, we have $f_{\{1\},k} = x_1 + x_2 + \cdots + x_n - k$, and

$$f_{\{2,3\},k} = \sigma_{U,2} - (k-1)\sigma_{U,1} + \binom{k}{2},$$

where $U = \{2, 3, \dots, n\}$.

3 Gröbner bases of complete uniform families

3.1 Introduction

Our aim in this Chapter is to describe (reduced) Gröbner bases for the ideals $I(d) := I(V\binom{[n]}{d})$, i.e. when $\mathcal{F}$ is the full family of d-sets of $[n]$.

A partial result in this direction was obtained in [11], which is based on the notion of order shattering. Here we recall only the facts that are relevant to our discussion. Let $\mathbb{F}$ be an arbitrary field.

In [11] it is established that

$$\mathrm{osh}\binom{[n]}{d} = \{\{s_1 < \ldots < s_j\} \subset [n] : \ j \leq d \text{ and } s_i \geq 2i \text{ for } 1 \leq i \leq j\}. \tag{21}$$

Actually, it is shown there (Lemma 2.2) that $\mathrm{osh}\binom{[n]}{d}$ is contained in the set on the right side of (21) and that the latter has at most $\binom{n}{d}$ elements (Lemma 2.3). From these (21) follows because $|\mathrm{osh}\,(\mathcal{F})\,| = |\mathcal{F}|$ holds for every $\mathcal{F} \subseteq 2^{[n]}$.

If we apply Theorem 2.11 in the case $\mathcal{F} := \binom{[n]}{d}$, then we obtain the following result.

Theorem 3.1 (Anstee, Rónyai, Sali, [11]) *Let $0 \leq d \leq n/2$ and denote by $\mathcal{M} = \mathcal{M}_d$ the set of all monomials x_G such that $G = \{s_1 < s_2 < \ldots < s_j\} \subset [n]$ for which $j \leq d$ and $s_i \geq 2i$ holds for $1 \leq i \leq j$. Then $\mathcal{M}$ is the set of standard monomials for $I(d)$ as well as for $I(n-d)$ with respect to the lexicographic order $\prec_{lex}$. In particular, $|\mathcal{M}| = \binom{n}{d}$ and $\mathcal{M}$ constitutes an $\mathbb{F}$ basis of the space of functions from $V\binom{[n]}{d}$ to $\mathbb{F}$ (from $V\binom{[n]}{n-d}$ to $\mathbb{F}$, resp.).*

For proofs the reader is referred to Theorem 4.3, Lemma 2.2 and 2.3 in [11].

Friedl and Rónyai applied the description of lex standard monomials of the ideals $I(d)$ to give a simpler proof for the following two important results of Wilson:

Theorem 3.2 *If $d \leq k \leq n-d$ are natural numbers and $\mathbb{F}$ is an arbitrary field then*

$$rank_{\mathbb{F}}\, I\left(\binom{[n]}{k}, \binom{[n]}{\leq d}\right) = \binom{n}{d}, \tag{22}$$

and

$$rank_{\mathbb{F}}\, I\left(\binom{[n]}{k},\binom{[n]}{d}\right)=\sum\binom{n}{i}-\binom{n}{i-1}, \qquad (23)$$

where the summation is for those indices i, for which $\binom{k-i}{d-i}$ is not 0 in $\mathbb{F}$.

The organisation of this Chapter is the following. In Section 3.2 we give an explicit description of the initial ideals and the reduced Gröbner bases of the ideals $I(V\binom{[n]}{d})$. In Section 3.3 we prove our main results. Finally we give a simpler proof for theorems of Frankl and Wilson with the aid of deglex standard monomials of $I(V\binom{[n]}{d})$ in Section 3.4.

The results of this Chapter also appeared in [47].

3.2 The main result

The main contribution of this Section is an explicit description of the reduced Gröbner bases for the ideals $I(V\binom{[n]}{d})$.

Our main result follows. We denote the ideal $I(V\binom{[n]}{d})$ by $I(d)$.

Theorem 3.3 *Let d, n be integers, $n > 0$ and $0 \leq d \leq n/2$. Let $\mathbb{F}$ be a field, and $\prec$ be an arbitrary term order on the monomials of $S = \mathbb{F}[x_1, \ldots, x_n]$ for which $x_n \prec x_{n-1} \prec \ldots \prec x_1$. Then the following set $\mathcal{G}$ of polynomials is a Gröbner basis with respect to $\prec$ of the ideal $I(d)$ of S:*

$$\mathcal{G} = \{x_1^2 - x_1, \ldots, x_n^2 - x_n\} \cup \{x_J :\ J \in \binom{[n]}{d+1}\} \cup$$

$$\{f_{H,d} :\ H \in \mathcal{H}(t) \text{ for some } 0 < t \leq d\}.$$

Similarly, the set $\mathcal{G}^*$ below is a Gröbner basis of $I(n-d)$:

$$\mathcal{G}^* = \{x_1^2 - x_1, \ldots, x_n^2 - x_n\} \cup \{x^J :\ J \in \binom{[n]}{d+1}\} \cup$$

$$\{f_{H,n-d} :\ H \in \mathcal{H}(t) \text{ for some } 0 < t \leq d\}.$$

Theorem 3.3 allows us to describe the initial ideals and reduced Gröbner bases of the ideals $I(d)$. Let $n, \mathbb{F}$ and $\prec$ be as in Theorem 3.3. It will be convenient to treat separately the (trivial) cases $d = 0$ or $d = n$. It is immediate that $\mathrm{in}(I(0)) = \mathrm{in}(I(n)) = (x_1, \ldots, x_n)$, and this is a minimal generating set. Similarly, $\{x_1, x_2, \ldots, x_n\}$ and $\{x_1 - 1, x_2 - 1, \ldots, x_n - 1\}$ are the reduced Gröbner bases of $I(0)$ and $I(n)$, respectively.

Let $\mathcal{B}(d)$ denote the collection of subsets $U \subset [n]$, where $U = \{u_1 < \ldots < u_{d+1}\}$ and $u_j \geq 2j$ holds for $j = 1, \ldots, d$.

Corollary 3.4 *Assume that* $0 < d \leq n/2$. *The set of monomials*

$$\cup_{t=1}^{d} \{x_H : \ H \in \mathcal{H}(t)\} \cup \{x_U : \ U \in \mathcal{B}(d)\} \cup \{x_i^2 : \ i = 2, \ldots, n\}$$

minimally generates $in(I(d)) = in(I(n-d))$.

It turns out that a subset of $\mathcal{G}$ ($\mathcal{G}^*$ resp.) is the reduced Gröbner basis of $I(d)$ ($I(n-d)$ resp.).

Corollary 3.5 *Let* $n, \mathbb{F}$, *and* $\prec$ *as in Theorem 3.3, and* $0 < d \leq n/2$. *Then the following set of polynomials is the reduced Gröbner basis with respect to* $\prec$ *of the ideal* $I(d)$:

$$\{x_2^2 - x_2, \ldots, x_n^2 - x_n\} \cup \{x_J : \ J \in \mathcal{B}(d)\} \cup$$
$$\{f_{H,d} : \ H \in \mathcal{H}(t) \text{ for some } 0 < t \leq d\}.$$

Similarly, the following set is the reduced Gröbner basis of $I(n-d)$:

$$\{x_2^2 - x_2, \ldots, x_n^2 - x_n\} \cup \{x^J : \ J \in \mathcal{B}(d)\} \cup$$
$$\{f_{H,n-d} : \ H \in \mathcal{H}(t) \text{ for some } 0 < t \leq d\}.$$

The functions $f_{H,d}$ play a prominent role in our discussion. Next we provide an alternative description for them. Let $H \in \mathcal{H}(t)$, and $H' = H \cup \{2t, 2t+1, \ldots, n\} \subseteq [n]$, as before. Let $l_{H'} = l_{H'}(x_1, \ldots, x_n) := \sum_{j \in H'} x_j$ and denote by $g_{H,d}$ the linear combination of square free monomials obtained from

$$\prod_{j=0}^{t-1} (l_{H'} - d + j)$$

by application of the relations $x_i^2 = x_i$.

Proposition 3.6 *Let* $0 \leq d \leq n$ *and* $H \in \mathcal{H}(t)$ *for some* $0 < t \leq n/2$. *Assume that* char $\mathbb{F} = 0$, *or* char $\mathbb{F} > t$. *Then we have* $f_{H,d} = (1/t!) \cdot g_{H,d}$.

In Section 3.3 we prove the preceding statements. These are followed by some consequences and concluding remarks.

3.3 Proofs

We write $I(d) = I(V\binom{[n]}{d})$.

Lemma 3.7 *Assume that* $0 < t \le n/2$, $H \in \mathcal{H}(t)$, *and* $0 \le d \le n$. *Then* $f_{H,d} \in I(d)$.

Proof. Let $D \in \binom{[n]}{d}$ and let $v = v_D$ be the characteristic vector of D. The set $H' = H \cup \{2t, \ldots, n\}$ has $n - t + 1$ elements, hence

$$|D \cap H'| \in \{d, d-1, \ldots, d-t+1\}. \tag{24}$$

Now

$$f_{H,d}(v) = \sum_{k=0}^{t} (-1)^{t-k} \binom{d-k}{t-k} \sigma_{H',k}(v) = \sum_{k=0}^{t} (-1)^{t-k} \binom{d-k}{t-k} \binom{|D \cap H'|}{k}.$$

We intend to use the following identity involving binomial coefficients

$$\binom{x-d+t-1}{t} = \sum_{k=0}^{t} (-1)^{t-k} \binom{x}{k} \binom{d-k}{t-k}, \tag{25}$$

valid for every $x \in \mathbb{C}$, $d \in \mathbb{Z}$ and $t \in \mathbb{Z}^+$. From (25) we infer that

$$f_{H,d}(v) = \binom{|D \cap H'| - d + t - 1}{t},$$

which is indeed 0 because of (24).

It remains to verify (25). One may start out with a version of the familiar Vandermonde identity ([42], pp. 169-170)

$$\binom{x+s}{t} = \sum_{k=0}^{t} \binom{x}{k} \binom{s}{t-k}, \tag{26}$$

which holds for all $x, s \in \mathbb{C}$ and $t \in \mathbb{Z}^+$. By negating the upper index s on the right-hand side we obtain

$$\binom{x+s}{t} = \sum_{k=0}^{t} \binom{x}{k} (-1)^{t-k} \binom{t-s-k-1}{t-k},$$

from which the substitution $s = t - d - 1$ gives (25). $\square$

Recall that for $0 \leq d \leq n/2$ we denoted by $\mathcal{M} = \mathcal{M}_d$ the set of all monomials x_G such that $G = \{s_1 < s_2 < \ldots < s_j\} \subset [n]$ for which $j \leq d$ and $s_i \geq 2i$ holds for $1 \leq i \leq j$.

Lemma 3.8 *Assume that $0 < t \leq n/2$, $H \in \mathcal{H}(t)$ and $0 \leq d \leq n$. Then $f_{H,d}$ can be written as a linear combination of square free monomials*

$$f_{H,d} = \sum_{U \subseteq H',\ |U| \leq t} \alpha_U x_U, \tag{27}$$

where $\alpha_U \in \mathbb{F}$. The leading monomial of $f_{H,d}$ with respect to $\prec$ is x_H and the leading coefficient is $\alpha_H = 1$. Also we have $x_H \notin \mathcal{M}$, but $x_U \in \mathcal{M}$ for any other nonzero term x_U of (27).

Proof. The statement about the form (27) follows from the fact that the (elementary) symmetric polynomials $\sigma_{H',i}$ $(0 \leq i \leq t)$ are linear combinations of monomials x_U with $U \subset H'$ and $|U| \leq t$. Let $U = \{u_1 < \ldots < u_j\}$ be any such subset and write $H = \{s_1 < \ldots < s_t\}$. By the definition of H' we have $s_i \leq u_i$ for $i = 1, \ldots, j$, hence $x_U \preceq x_{s_1} \cdots x_{s_j} \preceq x_H$. Also, the coefficient of x_H in $f_{H,d}$ is $(-1)^{t-t}\binom{d-t}{t-t} = 1$. These imply that x_H is the leading monomial of $f_{H,d}$.

It is immediate that $x_H \notin \mathcal{M}$ because $s_t = 2t - 1$. Finally, if $U \neq H$, then $2i \leq s_i \leq u_i$ hold for $i \leq \min\{j, t-1\}$, giving the last statement for $j < t$. If $j = t$ then from $U \neq H$ we infer additionally that $u_t > s_t = 2t - 1$. The proof is complete. $\square$

Proof of Theorem 3.3. Let d, n be integers, $n > 0$ and $0 \leq d \leq n/2$. It is immediate that $x_i^2 - x_i \in I(d)$ and $x_J \in I(d)$ if $|J| = d + 1$, hence by Lemma 3.7 $\mathcal{G} \subseteq I(d)$. Similarly we obtain that $\mathcal{G}^* \subseteq I(n - d)$.

To show that $\mathcal{G}$ is a Gröbner basis of $I(d)$ we use the characterisation of Gröbner bases from Theorem 2.10.

Obviously we can reduce any monomial which is divisible by x_i^2 for some i. We can thus assume that f contains only square free monomials x_U, $U \subseteq [n]$. We can also eliminate those x_U for which $|U| > d$.

If x_U $(|U| \leq d,\ U = \{u_1 < u_2 < \ldots < u_j\})$ is a monomial not in $\mathcal{M}_d$, then there is an index $i \leq j$ such that $u_i < 2i$. Let t be the smallest such index i. Then

$$\{u_1 < \ldots < u_t\} =: H \in \mathcal{H}(t)$$

and x_H divides x_U. By Lemma 3.8 x_H is the leading monomial of $f_{H,d} \in \mathcal{G}$, hence via $f_{H,d}$ we can reduce f further.

We have obtained so far that, using $\mathcal{G}$, any $f \in S$ can be reduced to a linear combination

$$\sum_{w \in \mathcal{M}_d} \alpha_w w, \tag{28}$$

where $\alpha_w \in \mathbb{F}$. Let I be the ideal of S generated by $\mathcal{G}$. From (28) and Theorem 3.1 we deduce first that

$$\dim_{\mathbb{F}} S/I \leq |\mathcal{M}_d| = \binom{n}{d} = \dim_{\mathbb{F}} S/I(d). \tag{29}$$

On the other hand, Lemma 3.7 implies that $I \subseteq I(d)$, hence we have $I = I(d)$.

Finally, if we reduce an $f \in I(d)$ into a form (28), then every α_w is zero by Theorem 3.1, because $\mathcal{M}_d$ is a basis of the space of functions from $V\binom{[n]}{d}$ to $\mathbb{F}$. This proves that $\mathcal{G}$ is a Gröbner basis of $I(d)$.

Essentially the same argument works for $I(n-d)$. Note that the leading term of a polynomial x^J, $|J| = d+1$ is x_J and all other terms have degree at most d. These polynomials and $x_i^2 - x_i$ allow us to reduce any polynomial f into one of degree at most d. From here reduction via $f_{H,n-d}$ where $H \in \mathcal{H}(t)$ and $0 < t \leq d$ and $x_i^2 - x_i$ gives a linear combination of type (28). If $f \in I(n-d)$ then every α_w is zero by Theorem 3.1, therefore $\mathcal{G}^*$ is a Gröbner basis of $I(n-d)$. □

Proof of Corollary 3.4. Let $\mathcal{W}$ denote the set of monomials given in the statement. Clearly we have $\mathcal{W} \subset \text{in}(I(d))$ and $\mathcal{W} \subset \text{in}(I(n-d))$. To show that $\mathcal{W}$ is a generating set, it suffices then to verify, that any monomial $w \notin \mathcal{M}_d$ is divisible by an element of $\mathcal{W}$. This is immediate if x_1 divides w because $\{1\} \in \mathcal{H}(1)$. Otherwise if w is not square free, then it is divisible by x_i^2 for some $2 \leq i \leq n$. We can therefore assume that $w = x_U$ for some $U = \{u_1 < \ldots < u_j\} \subseteq [n]$ and either there exists an $0 < i \leq d$ such that $u_i < 2i$, or $j > d$. If the first case occurs here, then let t be the smallest index i with $u_i < 2i$. Then for $H = \{u_1, \ldots, u_t\}$ we have $H \in \mathcal{H}(t)$, hence $x_H \in \mathcal{W}$ and x_H divides w. If only the second case applies to w, then for $H = \{u_1, \ldots, u_{d+1}\}$ we have $H \in \mathcal{B}(d)$, hence $x_H \in \mathcal{W}$, moreover x_H again divides w.

Minimality follows because there are no nontrivial divisibilities among the elements of $\mathcal{W}$. □

Proof of Corollary 3.5. From Corollary 3.4 we see that the leading terms of the sets of polynomials given in the statement are minimal generating sets of the initial ideals of $I(d)$ ($I(n-d)$ respectively). Reducedness follows from the fact that all other (i.e. non-leading) monomials in the polynomials are actually standard monomials for $I(d)$ (and for $I(n-d)$ as well). This has been proven for $f_{H,d}$ and $f_{H,n-d}$ in Lemma 3.8. Also, $x_i \in \mathcal{M}_d$ for $i = 2, \ldots, n$.

Finally let us consider the polynomials x^J, where $J = \{j_1 < \ldots < j_{d+1}\} \in \mathcal{B}(d)$. If $U = \{u_1 < \ldots < u_k\} \subset J$ with $k = |U| \leq d$, then $u_i \geq j_i \geq 2i$ holds whenever $1 \leq i \leq k$, hence $x_U \in \mathcal{M}_d$. We conclude that the non-leading monomials of x^J are standard monomials, and this completes the proof. □

Proof of Proposition 3.6. Let $D \subseteq [n]$ be an arbitrary set, $v = v_D$ the characteristic vector of D. From the definition of $g_{H,d}$ and (37) it is apparent that

$$\frac{1}{t!} \cdot g_{H,d}(v) = \binom{|D \cap H'| - d + t - 1}{t} = f_{H,d}(v).$$

Both $g_{H,d}$ and $f_{H,d}$ are linear combinations of square-free monomials. By the uniqueness of the standard decomposition of a function we conclude that

$$\frac{1}{t!} \cdot g_{H,d} = f_{H,d}.$$

□

3.4 Some consequences

By Theorem 3.3 the set of deglex standard monomials of $\binom{[n]}{d}$ is $\mathcal{M}_k$, where $k = \min\{d, n-d\}$. Now if $0 \leq m \leq k$, then the set of monomials from $\mathcal{M}_k$ of degree at most m is precisely $\mathcal{M}_m$. We have the following

Corollary 3.9 (Wilson, [79]) *Let $0 \leq d \leq n$, $0 \leq m \leq \min\{d, n-d\}$, and $\mathbb{F}$ be an arbitrary field. Then we have*

$$h_{\binom{[n]}{d}}(m) = \binom{n}{m}. \tag{30}$$

□

As a further application we give a simple proof of a theorem of Frankl [33, Theorem 1.1]. Let p be a prime and $d \in \mathbb{Z}$. Let

$$\mathcal{F}(d, p) := \{F \subseteq [n] : \ |F| \equiv d \pmod{p}\}.$$

Corollary 3.10 (Frankl) *Assume that $0 \le m < p$ and $m \le n/2$. Then over $\mathbb{F} = \mathbb{F}_p$ we have*

$$h_{\mathcal{F}(d,p)}(m) \le \binom{n}{m}.$$

Proof. We work over the field $\mathbb{F} = \mathbb{F}_p$. Let $0 < t \le m$ and $H \in \mathcal{H}(t)$. We observe that $f_{H,d} = f_{H,d'}$, as polynomials over $\mathbb{F}_p$, whenever $d \equiv d' \pmod{p}$. This follows because for $0 \le k \le t$ we have

$$\binom{d-k}{t-k} \equiv \binom{d'-k}{t-k} \pmod{p},$$

a consequence of $0 \le t - k \le m < p$.

Now Lemma 3.7 implies that the polynomials $f_{H,d}$ vanish on $V(\mathcal{F}(d,p))$, whenever $H \in \mathcal{H}(t)$ for some $0 < t \le m$. Let $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ be a polynomial of degree at most m. Using the polynomials $f_{H,d}$ above, and $x_i^2 - x_i$, we can reduce f into a linear combination over $\mathbb{F}_p$ of monomials from $\mathcal{M}_m$, as in the proof of Theorem 3.3. This implies that

$$h_{\mathcal{F}(d,p)}(m) \le |\mathcal{M}_m| = \binom{n}{m}.$$

□

4 Gröbner bases for complete ℓ-wide families

4.1 Introduction

Throughout this Chapter n, ℓ are positive integers, k is a nonnegative integer such that $0 \le \ell - 1 \le k \le n$.

Let $\mathcal{F}^{k,\ell}$ denote the *complete ℓ-wide* family

$$\mathcal{F}^{k,\ell} = \{F \subseteq [n] : k - \ell < |F| \le k\}.$$

A set family $\mathcal{F} \subseteq 2^{[n]}$ is *ℓ-wide* if $\mathcal{F} \subseteq \mathcal{F}^{k,\ell}$ for a suitable k.

The main contribution of this Chapter is an explicit description of the initial ideals and the reduced Gröbner bases of complete ℓ-wide families, $\mathcal{F}^{k,l}$. Our results extend those of [47] obtained for the case of complete uniform families, i.e., when $\ell = 1$.

Consider a family $\mathcal{F}$ of subsets of $[n]$. We say that $\mathcal{F}$ *shatters* S if

$$\{E \cap S : \ E \in \mathcal{F}\} = 2^S. \tag{31}$$

Then define

$$\mathrm{sh}(\mathcal{F}) = \{S \subseteq [n] : \ \mathcal{F} \text{ shatters } S\}. \tag{32}$$

From the definition it is easy to see that $\mathrm{osh}(\mathcal{F}) \subseteq \mathrm{sh}(\mathcal{F})$.

Recall that a *chain* of size p in $2^{[n]}$ is a sequence $A_1, \ldots, A_p$ of subsets of $[n]$ with $A_1 \subset \ldots \subset A_p$.

The organisation of this Chapter is the following. In Section 4.2 we state our main results. We give an explicit description of the reduced Gröbner bases and the initial ideals for the ideals $I(V(\mathcal{F}))$, where $\mathcal{F}$ is a complete ℓ-wide family (Theorem 4.2 and its Corollaries). The Gröbner bases turn out to be largely independent of the monomial order and the field. In Section 4.3 we generalise (21) and determine the sets order shattered by ℓ*-wide* families. Then, building on this result, in Section 4.4 we prove our main results. In Section 4.5 we determine the Hilbert function of $S/I(V(\mathcal{F}^{k,\ell}))$, and obtain a special case of a conjecture by Frankl, [32]: Let $g(n,t,d)$ denote the maximum number of subsets of $[n]$ with no shattered set of size t and no chain of size $d+1$. In [32] Frankl conjectured the following Theorem.

Conjecture 2 (Frankl, [32]) *Assume that* $2t \leq n + d$. *Then*

$$g(n,t,d) \leq \sum_{i=\max(0,t-d)}^{t-1} \binom{n}{i}. \tag{33}$$

Clearly, if $\mathcal{F}$ is an ℓ-wide family of sets, then $\mathcal{F}$ does not contain any chain of size $\ell + 1$. We prove the following special case of this conjecture.

Theorem 4.1 *Suppose that* $2t \leq n + \ell$ *and let* $\mathcal{F} \subseteq 2^{[n]}$ *be an* ℓ*-wide family with no shattered set of size* t*. Then*

$$|\mathcal{F}| \leq \sum_{i=\max(0,t-\ell)}^{t-1} \binom{n}{i}.$$

The results presented in this Chapter also appeared in [49].

4.2 The main results

Recall that we have $n > 0$, and $0 \leq \ell - 1 \leq k \leq n$. We denote by $I(k, \ell)$ the ideal $I(V(\mathcal{F}^{k,\ell}))$. The main contribution of the paper is an explicit description of the reduced Gröbner bases for the ideals $I(k, \ell)$. First we state the following

Theorem 4.2 *Let $n > 0$, k and ℓ be integers such that $0 < \ell - 1 \leq k \leq n$. Let $\mathbb{F}$ be a field, and $\prec$ be an arbitrary term order on the monomials of $S = \mathbb{F}[x_1, \ldots, x_n]$ for which $x_n \prec x_{n-1} \prec \ldots \prec x_1$. If $k < (n + \ell)/2$, then the following set $\mathcal{G}$ of polynomials is a Gröbner basis with respect to $\prec$ of the ideal $I(k, \ell)$ of S:*

$$\mathcal{G} = \{x_1^2 - x_1, \ldots, x_n^2 - x_n\} \cup \{x_J : \ J \in \binom{[n]}{k+1}\} \cup$$

$$\{f_{H,k} : \ H \in \mathcal{H}(t, \ell) \text{ for some } \ t, \ \ell \leq t \leq k\}.$$

Similarly, if $k \geq (n+\ell)/2$, then the set $\mathcal{G}^*$ below is a Gröbner basis of $I(k, \ell)$:

$$\mathcal{G}^* = \{x_1^2 - x_1, \ldots, x_n^2 - x_n\} \cup \{x^J : \ J \in \binom{[n]}{n-(k-\ell)}\} \cup$$

$$\{f_{H,k} : \ H \in \mathcal{H}(t, \ell) \text{ for some } \ t, \ \ell \leq t \leq n - (k - \ell + 1)\}.$$

Theorem 4.2 allows us to describe the initial ideals and reduced Gröbner bases of the ideals $I(k, \ell)$. Let $n, \mathbb{F}$ and $\prec$ be as in Theorem 4.2. Uniform families (i.e. $\ell = 1$) have been treated in Section 3.2. Here we focus on the case $\ell > 1$. This differs slightly from the uniform case because there x_1 is a leading monomial.

For $0 < \ell \leq k + 1$ let $\mathcal{B}(k, \ell)$ denote the collection of subsets $U \subseteq [n]$, where $U = \{u_1 < \ldots < u_{k+1}\}$ and $u_j \geq 2j - \ell + 1$ holds for $j = 1, \ldots, k$.

Corollary 4.3 *Let $1 < \ell \leq k + 1$. Assume that $k < (n + \ell)/2$. Then*

$$\{x_i^2 : \ i = 1, \ldots, n\} \cup \{x_U : \ U \in \mathcal{B}(k, \ell)\} \cup$$

$$\{x_H : \ H \in \mathcal{H}(t, \ell) \text{ for some } \ t, \ \ell \leq t \leq k\}$$

generates minimally $\text{in}(I(k, \ell))$.

Next assume that $k \geq (n+\ell)/2$. *Then*

$$\{x_i^2 : \ i=1,\dots,n\} \cup \{x_U : \ U \in \mathcal{B}(n-k+\ell-1,\ell)\} \cup$$

$$\{x_H : \ H \in \mathcal{H}(t,\ell) \textit{ for some } \ t, \ \ell \leq t \leq n-k+\ell-1\}$$

minimally generates $\mathrm{in}(I(k,\ell))$.

It turns out that a subset of $\mathcal{G}$ ($\mathcal{G}^*$ resp.) is the reduced Gröbner basis of $I(k,\ell)$.

Corollary 4.4 *Let* $n, \mathbb{F}$, *and* $\prec$ *as in Theorem 4.2, and* $1 < \ell \leq k+1$. *Assume that* $k < (n+\ell)/2$. *Then the following set is the reduced Gröbner basis with respect to* $\prec$ *of the ideal* $I(k,\ell)$:

$$\{x_1^2 - x_1, \dots, x_n^2 - x_n\} \cup \{x_J : \ J \in \mathcal{B}(k,\ell)\} \cup$$

$$\{f_{H,k} : \ H \in \mathcal{H}(t,\ell) \textit{ for some } \ell \leq t \leq k\}.$$

In the case $k \geq (n+\ell)/2$ *the following set is the reduced Gröbner basis with respect to* $\prec$ *of the ideal* $I(k,\ell)$:

$$\{x_1^2 - x_1, \dots, x_n^2 - x_n\} \cup \{x^J : \ J \in \mathcal{B}(n-k+\ell-1,\ell)\} \cup$$

$$\{f_{H,k} : \ H \in \mathcal{H}(t,\ell) \textit{ for some } \ell \leq t \leq n-k+\ell-1\}.$$

The functions $f_{H,k}$ are quite important in our discussion. Next we provide an alternative description for them. Let $H \in \mathcal{H}(t,\ell)$, and $H' = H \cup \{2t-\ell+1, 2t-\ell+2, \dots, n\} \subseteq [n]$, where $0 < \ell \leq t \leq (n+\ell)/2$. Let $l_{H'} = l_{H'}(x_1,\dots,x_n) := \sum_{j \in H'} x_j$ and denote by $g_{H,k}$ the linear combination of square-free monomials obtained from

$$\prod_{j=0}^{t-1} (l_{H'} - k + j)$$

by application of the relations $x_i^2 - x_i$.

Proposition 4.5 *Assume that char* $\mathbb{F} = 0$, *or char* $\mathbb{F} > t$. *Then we have*

$$f_{H,k} = \frac{1}{t!} \cdot g_{H,k}.$$

We prove these statements in Section 4.4.

4.3 Order shattering by ℓ-wide families

In this Section we describe the sets order shattered by the ℓ-wide families $\mathcal{F}^{k,\ell}$. For $0 \leq \ell - 1 \leq k \leq n$ we write

$$D(k,\ell) = \{\{g_1 < \ldots < g_t\} \subseteq [n] : \; t \leq k \text{ and } g_j \geq 2j - \ell + 1 \text{ if } 1 \leq j \leq t\}.$$

In particular $\emptyset \in D(k,\ell)$. The following theorem is the combinatorial core of our results; it is an extension of (5).

We shall distinguish two cases: $k < (n+\ell)/2$ and $k \geq (n+\ell)/2$. The second case can be reduced to the first one by (6).

Theorem 4.6 *(a) Let* $0 \leq k < (n+\ell)/2$*. Then*

$$\operatorname{osh}(\mathcal{F}^{k,\ell}) = D(k,\ell)$$

(b) If $k \geq (n+\ell)/2$*, then*

$$\operatorname{osh}(\mathcal{F}^{k,\ell}) = D(n-k+\ell-1,\ell).$$

Proof. Part (b) follows from part (a) by complementarity. Indeed, $\operatorname{co}(\mathcal{F}^{k,\ell}) = \mathcal{F}^{n-(k-\ell+1),\ell}$, hence by (6)

$$\operatorname{osh}(\mathcal{F}^{k,\ell}) = \operatorname{osh}(\operatorname{co}(\mathcal{F}^{k,\ell})) = \operatorname{osh}(\mathcal{F}^{n-k+\ell-1,\ell}).$$

On the other hand, $n - (k-\ell+1) < (n+\ell)/2$ follows from $n \leq 2k - \ell$, and hence case (a) applies for the ℓ-wide family $\mathcal{F}^{n-(k-\ell+1),\ell}$.

We turn to the proof of case (a) now. First we verify that $\operatorname{osh}(\mathcal{F}^{k,\ell}) \subseteq D(k,\ell)$. For this it is enough to check that if $D \notin D(k,\ell)$, then $D \notin \operatorname{osh}(\mathcal{F}^{k,\ell})$.

Assume that $D = \{d_1 < \ldots < d_s\} \notin D(k,\ell)$. Then either $s > k$ or there is an index $i \leq s \leq k$ such that $d_i < 2i - \ell + 1$. In the first case $D \notin \operatorname{osh}(\mathcal{F}^{k,\ell})$, because $\operatorname{osh}(\mathcal{F}^{k,\ell}) \subseteq \operatorname{osh}(\binom{[n]}{\leq k}) = \binom{[n]}{\leq k}$. In the second case let t be the smallest such index i. Let $H := \{d_1, \ldots, d_t\} \subseteq D$. Then obviously $\ell \leq t \leq k$, hence $H \in \mathcal{H}(t,\ell)$. Also, $D \in \operatorname{osh}(\mathcal{F}^{k,\ell})$ would imply that $H \in \operatorname{osh}(\mathcal{F}^{k,\ell})$, because $\operatorname{osh}(\mathcal{F}^{k,\ell})$ is downward closed. From the latter fact we derive a contradiction below.

Indeed, suppose that there exists $H \in \mathcal{H}(t,\ell) \cap \operatorname{osh}(\mathcal{F}^{k,\ell})$, where $0 < \ell \leq t \leq k < (n+\ell)/2$. Let $H = \{h_1 < \ldots < h_t\}$, then $h_t = 2t - \ell$ and $h_i \geq 2i - \ell + 1$ for each $1 \leq i \leq t-1$. Since $H \in \operatorname{osh}(\mathcal{F}^{k,\ell})$, the definition of order-shattering gives us two subsets $F_0, F_1 \in \mathcal{F}^{k,\ell}$ such that $F_0 \cap T = F_1 \cap T$, where $T = \{h_t + 1, \ldots, n\}$, and $F_0 \cap H = \emptyset$, $F_1 \cap H = H$.

Let $P := [n] \setminus (T \cup H)$. Clearly $|P| = t - \ell$. By definition

$$F_0 = (F_0 \cap T) \cup (F_0 \cap H) \cup (F_0 \cap P)$$

is a decomposition into disjoint sets. Let $r := |F_0 \cap T|$. Then

$$|F_0| = |F_0 \cap T| + |F_0 \cap H| + |F_0 \cap P| \leq r + t - \ell,$$

because $|F_0 \cap P| \leq |P| = t - \ell$. Similarly

$$|F_1| = |F_1 \cap T| + |F_1 \cap H| + |F_1 \cap P| \geq r + t,$$

because $|F_1 \cap H| = |H| = t$. Hence $|F_1| - |F_0| \geq \ell$, which contradicts to $F_0, F_1 \in \mathcal{F}^{k,\ell}$.

Now we prove that $D(k,\ell) \subseteq \mathrm{osh}(\mathcal{F}^{k,\ell})$. Let $D = \{d_1 < \ldots < d_t\} \in D(k,\ell)$. This means that $d_i \geq 2i - \ell + 1$ for $1 \leq i \leq t$.

We extend the base set $[n]$ by $\ell - 1$ new elements: let

$$X = \{-\ell + 2, -\ell + 3, \ldots, 0, \ldots, n\}.$$

We intend to establish that $D \in \mathrm{osh}\binom{X}{k}$. We note first that in the definition of order-shattering only the ordering of the elements of the ground set is what matters, not the elements themselves. From $0 \leq k < (n + \ell)/2$ we have $0 \leq k \leq |X|/2$. In view of (5), $D \in \mathrm{osh}\binom{X}{k}$ holds iff there are at least $2i - 1$ elements of X which are smaller than s_i. This is indeed true because $D \in D(k,\ell)$.

Let $F \in \binom{X}{k}$ be an arbitrary subset. We define $F' := F \cap [n]$. Then we have $F' \in \mathcal{F}^{k,\ell}$, because we dropped at most $\ell - 1$ elements from F, and $|F| = k$. Let $\mathcal{G} = \{F' : \ F \in \binom{X}{k}\}$. Then $\mathcal{G} \subseteq \mathcal{F}^{k,\ell}$, and hence $D \in \mathrm{osh}\binom{X}{k} \cap 2^{[n]} = \mathrm{osh}(\mathcal{G}) \subseteq \mathrm{osh}(\mathcal{F}^{k,\ell})$. This completes the proof. □

For $k < (n + \ell)/2$ we denote by $\mathcal{M}(k,\ell)$ the set of all monomials x_G such that $G \in D(k,\ell)$. For $k \geq (n+\ell)/2$ we set $\mathcal{M}(k,\ell)$ to be $\mathcal{M}(n-(k-\ell+1),\ell)$.

Theorems 2.11 and 4.6 give us the lexicographic standard monomials of ℓ-wide families.

Corollary 4.7 *Let $n > 0$, k, ℓ be integers, $0 \leq \ell - 1 \leq k \leq n$. Then $\mathcal{M}(k,\ell)$ is the set of standard monomials for $I(k,\ell)$ with respect to the lexicographic order $\prec_{lex}$. In particular,*

$$|\mathcal{M}(k,\ell)| = \sum_{i=k-\ell+1}^{k} \binom{n}{i} \tag{34}$$

and $\mathcal{M}(k,\ell)$ constitutes an $\mathbb{F}$ basis of the space of functions from $V(\mathcal{F}^{k,\ell})$ to $\mathbb{F}$. □

Remark. One can obtain (34) by lattice path counting techniques (see [67] for an excellent account on those methods). This provides an alternative way to prove Theorem 4.6.

4.4 Proofs of the main results

Let $\mathbb{F}$ be a fixed field and let $\prec$ be an arbitrary term order on the monomials of $S = \mathbb{F}[x_1, \ldots, x_n]$ for which $x_n \prec x_{n-1} \prec \ldots \prec x_1$. Let $0 \leq \ell - 1 \leq k \leq n$. For $t > 0$ and $G \subseteq [n]$ we put

$$\mathcal{F}^{k,t}(G) = \{D \subseteq [n] : k - t < |D \cap G| \leq k\}.$$

Theorem 4.8 *Assume that $0 < \ell \leq t \leq (n+\ell)/2$, $H \in \mathcal{H}(t,\ell)$, and $0 \leq k \leq n$. Then $f_{H,k} \in I(V(\mathcal{F}^{k,t}(H')))$.*

Proof. Let $D \in \mathcal{F}^{k,t}(H')$ and let $v = v_D$ be the characteristic vector of D. By definition

$$|D \cap H'| \in \{k, k-1, \ldots, k-t+1\}. \tag{35}$$

Now

$$f_{H,k}(v) = \sum_{i=0}^{t} (-1)^{t-i} \binom{k-i}{t-i} \sigma_{H',i}(v) = \sum_{i=0}^{t} (-1)^{t-i} \binom{k-i}{t-i} \binom{|D \cap H'|}{i}.$$

We use the following identity

$$\binom{x-k+t-1}{t} = \sum_{i=0}^{t} (-1)^{t-i} \binom{x}{i} \binom{k-i}{t-i}, \tag{36}$$

which holds for every $x \in \mathbb{C}$, $k \in \mathbb{Z}$ and $t \in \mathbb{Z}^+$. From (36) we infer that

$$f_{H,k}(v) = \binom{|D \cap H'| - k + t - 1}{t}, \tag{37}$$

which is indeed 0 because of (35).

□

Lemma 4.9 *Assume that* $0 \leq k \leq n$, $0 < \ell \leq t \leq \min(k, n-k+\ell-1)$, *and* $H \in \mathcal{H}(t, \ell)$. *Then* $f_{H,k}$ *can be written as a linear combination of square-free monomials*

$$f_{H,k} = \sum_{U \subseteq H',\ |U| \leq t} \alpha_U x_U, \tag{38}$$

where $\alpha_U \in \mathbb{F}$. *The leading monomial of* $f_{H,k}$ *with respect to* $\prec$ *is* x_H *and the leading coefficient is* $\alpha_H = 1$. *Also we have* $x_H \notin \mathcal{M}(k, \ell)$, *but* $x_U \in \mathcal{M}(k, \ell)$ *for* $U \subseteq H'$, $|U| \leq t$, $U \neq H$. *The latter monomials* x_U *are precisely the non-leading monomials in (38).*

Proof. First suppose that $k < (n + \ell)/2$.

The statement about the form (38) follows from the fact that the (elementary) symmetric polynomials $\sigma_{H',i}$ $(0 \leq i \leq t)$ are linear combinations of monomials x_U with $U \subseteq H'$ and $|U| \leq t$. Let $U = \{u_1 < \ldots < u_j\}$ be any such subset and write $H = \{s_1 < \ldots < s_t\}$. By the definition of H' we have $s_i \leq u_i$ for $i = 1, \ldots, j$, hence $x_U \preceq x_{s_1} \cdots x_{s_j} \preceq x_H$. Also, the coefficient of x_H in $f_{H,k}$ is $(-1)^{t-t}\binom{k-t}{t-t} = 1$. These imply that x_H is the leading monomial of $f_{H,k}$.

It is immediate that $x_H \notin \mathcal{M}(k, \ell)$ because $s_t = 2t - \ell$. Next suppose that $U \subseteq H'$, $|U| = j \leq t$, and $U \neq H$. If $j < t$, then $2i - \ell + 1 \leq s_i \leq u_i$ for $1 \leq i \leq j$, and $j \leq k$ imply $x_U \in \mathcal{M}(k, \ell)$. If $|U| = t$ then from $U \neq H$ we infer additionally that $u_t > s_t = 2t - \ell$, giving that $x_U \in \mathcal{M}(k, \ell)$.

In the case $k \geq (n + \ell)/2$ we can give a similar proof, using the relations $\mathcal{M}(n - (k - \ell + 1), \ell) = \mathcal{M}(k, \ell)$ and $t \leq n - k + \ell - 1$. This concludes the proof. □

Corollary 4.10 *Assume that* $0 \leq k \leq n$, $0 < \ell \leq t \leq \min(k, n-k+\ell-1)$, *and* $H \in \mathcal{H}(t, \ell)$. *Then* $x_H \notin Sm(\prec, \mathcal{F}^{k,t}(H'))$.

Proof. This is obvious from Theorem 4.8 and Lemma 4.9, because x_H is the leading term of $f_{H,k}$, a polynomial vanishing on $V(\mathcal{F}^{k,t}(H'))$. $\square$

Lemma 4.11 *Let* $0 < \ell \leq t \leq (n+\ell)/2$, $0 \leq k \leq n$, *and* $H \in \mathcal{H}(t, \ell)$. *Then* $\mathcal{F}^{k,\ell} \subseteq \mathcal{F}^{k,t}(H')$.

Proof. Let $D \in \mathcal{F}^{k,\ell}$. We know that $H' = H \cup \{2t-\ell+1, 2t-\ell+2, \ldots, n\}$ has $n - t + \ell$ elements, hence the size of $[n] \setminus H'$ is $t - \ell$. Using also, that $k - \ell + 1 \leq |D|$, we obtain

$$k - t + 1 \leq |D| - |[n] \setminus H'| \leq |D \cap H'| \leq |D| \leq k,$$

hence $D \in \mathcal{F}^{k,t}(H')$. $\square$

Corollary 4.12 *Let* $0 < \ell \leq t \leq (n + \ell)/2$, $0 \leq k \leq n$, *and* $H \in \mathcal{H}(t, \ell)$. *Then* $f_{H,k} \in I(k, \ell)$.

Proof. We know that $f_{H,k} \in I(V(\mathcal{F}^{k,t}(H')))$ by Theorem 4.8 and $\mathcal{F}^{k,\ell} \subseteq \mathcal{F}^{k,t}(H')$ by Lemma 4.11. We conclude that $f_{H,k} \in I(V(\mathcal{F}^{k,t}(H'))) \subseteq I(k, \ell)$. $\square$

Proof of Theorem 4.2: Let k, $0 < n$ and ℓ be integers, such that $0 \leq \ell - 1 \leq k \leq n$. We consider first the case $k < (n+\ell)/2$. It is immediate that $x_i^2 - x_i \in I(k, \ell)$ and $x_J \in I(k, \ell)$ if $|J| = k + 1$, hence by Corollary 4.12, $\mathcal{G} \subseteq I(k, \ell)$.

To show that $\mathcal{G}$ is a Gröbner basis of $I(k, \ell)$ we use the characterisation of Gröbner bases from Theorem 2.10. Let I be the ideal of S generated by $\mathcal{G}$.

Lemma 4.13 $I = I(k, \ell)$.

Proof. It is immediate that $I \subseteq I(k, \ell)$, because $\mathcal{G} \subseteq I(k, \ell)$.

Now let $f \in S$ be an arbitrary polynomial. Obviously we can reduce by $\mathcal{G}$ any monomial of f which is divisible by x_i^2 for some i. We can thus assume that f contains only square-free monomials x_U, $U \subseteq [n]$. We can also eliminate those x_U for which $|U| > k$.

Suppose now that x_U is a monomial ($|U| \leq k$, $U = \{u_1 < u_2 < \ldots < u_j\}$) appearing in f which is not in $\mathcal{M}(k,\ell)$. Then there exists an index $i \leq j$ such that $u_i < 2i - \ell + 1$. Let t be the smallest such index i and put $H := \{u_1, \ldots, u_t\}$. Then necessarily $\ell \leq t$ and $H \in \mathcal{H}(t,\ell)$ and x_H divides x_U by definition. By Lemma 4.9 x_H is the leading monomial of $f_{H,k} \in \mathcal{G}$, hence via $f_{H,k}$ we can reduce f further.

What we obtained is that any $f \in S$ can be $\mathcal{G}$-reduced to a linear combination

$$\sum_{w \in \mathcal{M}(k,\ell)} \alpha_w \cdot w, \tag{39}$$

where $\alpha_w \in \mathbb{F}$. From (39) and Corollary 4.7 we deduce that

$$\dim_{\mathbb{F}} S/I \leq |\mathcal{M}(k,\ell)| = \sum_{i=k-\ell+1}^{k} \binom{n}{i} = \dim_{\mathbb{F}} S/I(k,\ell), \tag{40}$$

which, together with $I \subseteq I(k,\ell)$, implies that $I = I(k,\ell)$. The Lemma is proved. $\square$

If we consider the reduced form (39) of an $f \in I(k,\ell)$, then every α_w is zero by Corollary 4.7, because $\mathcal{M}(k,\ell)$ is basis of the space of functions from $V(\mathcal{F}^{k,\ell})$ to $\mathbb{F}$. This proves that $\mathcal{G}$ is a Gröbner basis of $I(k,\ell)$, when $k < \frac{n+\ell}{2}$.

Essentially the same argument works when $k \geq (n+\ell)/2$.

It is immediate that $x_i^2 - x_i \in I(k,\ell)$. We know that if $H, J \subseteq [n]$, then $x^J(v_H) = 0$ iff $H \cap J \neq \emptyset$. Now if $H \in \mathcal{F}^{k,\ell}$ and $J \in \binom{[n]}{n-(k-\ell)}$, then H and J must intersect because

$$|H| + |J| \geq k - \ell + 1 + n - k + \ell = n + 1.$$

Assume now that t is an integer, such that $\ell \leq t \leq n - k + \ell - 1$. Then $k \geq \frac{n+\ell}{2}$ implies that $n-k+\ell-1 < \frac{n+\ell}{2}$, showing that $t < \frac{n+\ell}{2}$. Corollary 4.12 applies, giving that $f_{H,k} \in I(k,\ell)$, whenever $H \in \mathcal{H}(t,\ell)$. We have therefore $\mathcal{G}^* \subseteq I(k,\ell)$.

From here we can prove that the ideal I generated by $\mathcal{G}^*$ is $I(k,\ell)$ as in Lemma 4.13. For this, one observes first that the leading term of a polynomial x^J, $|J| = n-(k-\ell)$ is x_J and all other terms have degree at most $n-k+\ell-1$. These polynomials and $x_i^2 - x_i$ allow us to reduce any polynomial f into one of degree at most $n - (k - \ell + 1)$.

Reduction via polynomials $f_{H,k}$, where $H \in \mathcal{H}(t,\ell)$ gives a linear combination of type (39). From (39) we obtain (40) and $I = I(k,\ell)$ as before.

Finally, if $f \in I(k,\ell)$ then every α_w is zero by Corollary 4.7, therefore $\mathcal{G}^*$ is a Gröbner basis of $I(k,\ell)$. □

Corollary 4.14 *Let $\mathbb{F}$, $\prec$, k, n, and ℓ be as in Theorem 4.2. Then*

$$\mathrm{Sm}(\prec, \mathcal{F}^{k,\ell}) = \mathcal{M}(k,\ell).$$

Remark. This was established in Corollary 4.7 for the lexicographic order $\prec_{lex}$. The point here is that the statement holds for *any* term order $\prec$ on the monomials for which $x_n \prec x_{n-1} \prec \ldots \prec x_1$.

Proof. The argument of Theorem 4.2 shows that any monomial $w \notin \mathcal{M}(k,\ell)$ can be $\mathcal{G}$-reduced to $\prec$-smaller monomials. This means that w is a leading monomial for $I(k,\ell)$, giving the containment $\subseteq$. Equality then follows because by (14) and Corollary 4.7 both sides have the same size $|\mathcal{F}^{k,\ell}|$. □

Proof of Corollary 4.3. We assume first that $k < (n+\ell)/2$. Let $\mathcal{W}$ denote the set of monomials given in the statement. Clearly we have $\mathcal{W} \subset \mathrm{in}(I(k,\ell))$. First we show that $\mathcal{W}$ is a generating set. For this it suffices to verify, that any monomial $w \notin \mathcal{M}(k,\ell)$ is divisible by an element of $\mathcal{W}$. If w is not square-free, then it is divisible by x_i^2 for some $1 \le i \le n$. We can therefore assume that $w = x_U$ for some $U = \{u_1 < \ldots < u_j\} \subseteq [n]$ and either there exists an $0 < i \le k$ such that $u_i < 2i - \ell + 1$, or $j > k$. In the first case let t be the smallest index i with $u_i < 2i - \ell + 1$. Then for $H = \{u_1, \ldots, u_t\}$ we have $H \in \mathcal{H}(t,\ell)$, where $\ell \le t \le k$, hence $x_H \in \mathcal{W}$ and x_H divides w. In the case $j > k$ for $H = \{u_1, \ldots, u_{k+1}\}$ we have $H \in \mathcal{B}(k,\ell)$, hence $x_H \in \mathcal{W}$, moreover x_H again divides w.

Using, that $2 \le \ell \le t$, it is easy to verify, that there are no nontrivial divisibilities among the elements of $\mathcal{W}$. This settles the minimality.

The case $k \ge (n+\ell)/2$ is reduced to the preceding one by using the following obvious consequence of Corollary 4.14:

$$\mathrm{in}(I(k,\ell)) = \mathrm{in}(I(n-k+\ell-1,\ell)).$$

□

Proof of Corollary 4.4. It follows from Corollary 4.3 that the leading terms of the sets of polynomials given in the statement are minimal generating sets of the initial ideal of $I(k,\ell)$. We have proven for $f_{H,k}$ and $f_{H,n-(k-\ell+1)}$ in Lemma 4.9 that all other (i.e. non-leading) monomials in these polynomials are actually standard monomials for $I(k,\ell)$ (and for $I(n-(k-\ell+1),k)$ as well). Also, because of $\ell > 1$ we have $x_i \in \mathcal{M}(k,\ell)$ for $i = 1,\ldots,n$.

It remains to check that the non-leading monomials of the polynomial x^J, where $J \in \mathcal{B}(k,\ell)$, are elements of $\mathcal{M}(k,\ell)$. Let $J = \{j_1 < \ldots < j_{k+1}\} \in \mathcal{B}(k,\ell)$. Then the non-leading monomials of x^J are x_U, where $U = \{u_1 < \ldots < u_m\} \subseteq J$ with $m = |U| \le k$. Clearly $u_i \ge j_i \ge 2i-\ell+1$ holds whenever $1 \le i \le m$, hence $x_U \in \mathcal{M}(k,\ell)$. The proof is complete. □

Proof of Proposition 4.5. Let $D \subseteq [n]$ be an arbitrary set, $v = v_D$ the characteristic vector of D. From the definition of $g_{H,k}$ and (37) it is apparent that

$$\frac{1}{t!}g_{H,k}(v) = \binom{|D \cap H'| - k + t - 1}{t} = f_{H,k}(v).$$

Both $g_{H,k}$ and $f_{H,k}$ are linear combinations of square-free monomials. Square-free monomials are precisely the standard monomials for $\mathcal{F}^{n,n+1} = 2^{[n]}$. By the uniqueness of the standard decomposition of a function we conclude that

$$\frac{1}{t!}g_{H,k} = f_{H,k}.$$

□

4.5 The Hilbert function of $\mathcal{F}^{k,\ell}$

Here we give the values $h_{\mathcal{F}^{k,\ell}}(m)$ of the Hilbert function of the complete ℓ-wide family $\mathcal{F}^{k,\ell}$. We need first a useful fact of combinatorial nature about $\mathrm{osh}(\mathcal{F}^{k,\ell})$. As before $n > 0$, ℓ, k are integers, and $0 \le \ell - 1 \le k \le n$.

Theorem 4.15 *Suppose that* $0 \le i \le \min(k, n-k+\ell-1)$. *Then*

$$|\mathrm{osh}(\mathcal{F}^{k,\ell}) \cap \binom{[n]}{i}| = \binom{n}{i} - \binom{n}{i-\ell}.$$

Remark. The binomial coefficient $\binom{n}{j}$ is understood to be 0 if $j < 0$.

Proof. We use the description of $\mathrm{osh}(\mathcal{F}^{k,\ell})$ given in Theorem 4.6. With $d = \min(k, n-k+\ell-1)$ we have $d < \frac{n+\ell}{2}$ and $\mathrm{osh}(\mathcal{F}^{k,\ell}) = D(d,\ell)$. We consider first the case $0 \le i < \ell$. Then

$$\mathrm{osh}(\mathcal{F}^{k,\ell}) \cap \binom{[n]}{i} = D(d,\ell) \cap \binom{[n]}{i} = \binom{[n]}{i}, \tag{41}$$

giving the claim of the Theorem in this case. We turn now to the case $\ell \le i \le d$. The case (a) of Theorem 4.6 applies to $\mathcal{F}^{i,\ell}$, giving that $\mathrm{osh}(\mathcal{F}^{i,\ell}) = D(i,\ell)$. Directly from the definition we see that

$$D(d,\ell) \cap \binom{[n]}{i} = D(i,\ell) \cap \binom{[n]}{i},$$

hence

$$\mathrm{osh}(\mathcal{F}^{k,\ell}) \cap \binom{[n]}{i} = D(d,\ell) \cap \binom{[n]}{i} = D(i,\ell) \cap \binom{[n]}{i} = \mathrm{osh}(\mathcal{F}^{i,\ell}) \cap \binom{[n]}{i}. \tag{42}$$

We have also the following consequences of Theorem 4.6:

$$\mathrm{osh}(\mathcal{F}^{i-1,\ell}) \subseteq \mathrm{osh}(\mathcal{F}^{i,\ell}) \tag{43}$$

and

$$\mathrm{osh}(\mathcal{F}^{i,\ell}) \cap \binom{[n]}{i} = \mathrm{osh}(\mathcal{F}^{i,\ell}) \setminus \mathrm{osh}(\mathcal{F}^{i-1,\ell}). \tag{44}$$

Corollary 4.7, applied to both $\mathcal{F}^{i,\ell}$ and $\mathcal{F}^{i-1,\ell}$ gives that the size of the set in (44) is

$$\sum_{j=i-\ell+1}^{i} \binom{n}{j} - \sum_{s=i-\ell}^{i-1} \binom{n}{s} = \binom{n}{i} - \binom{n}{i-\ell}.$$

This, together with (42), proves the statement. □

We turn now to the computation of the Hilbert function $h_{\mathcal{F}^{k,\ell}}(m)$. By (18), h gives the rank of certain important inclusion matrices:

$$\mathrm{rank}_{\mathbb{F}}\ I(\mathcal{F}^{k,\ell}, \binom{[n]}{\le m}) = h_{\mathcal{F}^{k,\ell}}(m).$$

Theorem 4.16 *Let $n > 0$, ℓ, k, m be integers, Let $0 \le \ell - 1 \le k \le n$, and $0 \le m \le \min(k, n-k+\ell-1)$. Let $\mathbb{F}$ be an arbitrary field. Then we have*

$$h_{\mathcal{F}^{k,\ell}}(m) = |\mathrm{osh}(\mathcal{F}^{k,\ell}) \cap \binom{[n]}{\le m}| = \sum_{i=\max(0,m-\ell+1)}^{m} \binom{n}{i}. \tag{45}$$

Proof. For short we write $\mathcal{F} = \mathcal{F}^{k,\ell}$. From (15) we infer that

$$h_{\mathcal{F}}(m) = |\mathrm{Sm}(\prec_{deg}, \mathcal{F}) \cap \binom{[n]}{\le m}|,$$

where $\prec_{deg}$ is the deglex order (or any other term order which refines the partial ordering by degree). From Corollary 4.14 and Theorem 4.6 we have

$$\mathrm{Sm}(\prec_{deg}, \mathcal{F}) = D(t, \ell) = \mathrm{osh}(\mathcal{F}),$$

where $t = \min(k, n-k+\ell+1)$. We consider the following decomposition into a disjoint union

$$\mathrm{osh}(\mathcal{F}) \cap \binom{[n]}{\le m} = \cup_{j=0}^{m} \left(\mathrm{osh}(\mathcal{F}) \cap \binom{[n]}{j} \right).$$

Turning to the sizes of the above sets, Theorem 4.15 gives that

$$h_{\mathcal{F}}(m) = | \cup_{j=0}^{m} \left(\mathrm{osh}(\mathcal{F}) \cap \binom{[n]}{j} \right) | = \sum_{j=0}^{m} \binom{n}{j} - \binom{n}{j-\ell} = \sum_{j=r}^{m} \binom{n}{j},$$

where $r = \max(0, m-\ell+1)$. This finishes the proof. □

4.6 A conjecture of Frankl

Finally we prove Theorem 4.1. It turns out to be a simple consequence of Theorem 4.16.

Proof of Theorem 4.1: $\mathcal{F}$ is an ℓ-wide family, therefore we have $\mathcal{F} \subseteq \mathcal{F}^{k,\ell}$ for some k, ℓ, with $0 \le \ell - 1 \le k \le n$. Put $r = \min(k, n-k+\ell-1, t-1)$. Theorem 4.6, the assumption on t together with $\mathrm{osh}(\mathcal{F}) \subseteq \mathrm{sh}(\mathcal{F})$ imply that the family $\mathcal{F} \subseteq \mathcal{F}^{k,\ell}$ has no order-shattered sets of size $> r$. We have thus

$$\mathrm{osh}(\mathcal{F}) \subseteq \mathrm{osh}(\mathcal{F}^{k,\ell}) \cap \binom{[n]}{\le r}.$$

Theorem 4.16 implies that

$$|\mathrm{osh}(\mathcal{F})| \leq |\mathrm{osh}(\mathcal{F}^{k,\ell}) \cap \binom{[n]}{\leq r}| = \sum_{i=\max(0,r-\ell+1)}^{r} \binom{n}{i} \leq \sum_{i=\max(0,t-\ell)}^{t-1} \binom{n}{i}.$$

The last inequality follows from $r \leq t-1$ and $t \leq \frac{n+\ell}{2}$. The proof is complete.

□

5 A conjecture of Babai and Frankl

5.1 Introduction

In extremal combinatorics we may find a lot of applications of rank computation of inclusion matrices. In the following we deal with the most demonstrative example: with L-intersecting families.

First we give some definitions. For families $\mathcal{F}, \mathcal{G} \subseteq 2^{[n]}$ the *inclusion matrix* $I(\mathcal{F}, \mathcal{G})$ is a (0,1) 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 $(F \in \mathcal{F}, G \in \mathcal{G})$.

Of particular interest will be the case when $\mathcal{G}$ is the complete s-uniform family $\binom{[n]}{s}$. Further we call the $|\mathcal{F}| \times \binom{n}{s}$ matrix $I(\mathcal{F}, \binom{[n]}{s})$ *the s-inclusion matrix of $\mathcal{F}$*. We call a set family $\mathcal{F}$ *s-independent* if the rows of $I(\mathcal{F}, \binom{[n]}{s})$ are linearly independent, which means that the s-inclusion matrix has *full row-rank.*

It is easy to prove the following Proposition.

Proposition 5.1 *If the family $\mathcal{F}$ is s-independent, then $|\mathcal{F}| \leq \binom{n}{s}$.* □

Now we define the L-intersecting families.

Definition 5.2 *Let $L \subseteq \mathbb{N}$ be a set of nonnegative integers. The family $\mathcal{F}$ is L-intersecting, if $|E \cap F| \in L$ for every pair E, F of distinct members of $\mathcal{F}$.*

Let $L \subseteq \mathbb{N}$ be a fix subset of nonnegative integers and $k \geq 1$. It would be very important to answer for the following open problem: what is the maximum number of members in a k-uniform L-intersecting family of subsets of a set of n elements?

No general answer to this problem has been found, but a lot of partial results are known. Now we state here the first result in the theory of L-intersecting families: the Ray-Chaudhuri–Wilson theorem:

Theorem 5.3 *(Ray-Chaudhuri–Wilson, 1975): Let $L \subseteq \mathbb{N}$ be a set of s integers and $\mathcal{F}$ an L-intersecting k-uniform family, where $s \leq \min(k, n-k)$. Then $\mathcal{F}$ is s-independent. Consequently*

$$|\mathcal{F}| \leq \binom{n}{s}.$$

This result and other related modular extensions of the Ray-Chaudhuri–Wilson theorem gave the basis of beautiful for geometric and combinatorial applications.

We may deal also with the modular extensions of Theorem 5.3. First we give some modular terminology.

Definition 5.4 *For a set $L \subseteq \mathbb{Z}$ and integers r, t, we shall say that*

$$t \in L \ (\ mod\ r)$$

if there exists an $l \in L$ such that $t \equiv l \pmod r$.

The negation of this statement will be written as $t \notin L \pmod r$.

In 1981 Frankl and Wilson obtained in [35] the following extension of the Ray-Chaudhuri–Wilson theorem:

Theorem 5.5 *(Frankl–Wilson, 1981) Let L be a set of s integers and p a prime number. Assume $\mathcal{F}$ is a k-uniform family of subsets of a set of n elements such that*

$$(a)\ k \notin L \pmod p$$

and

$$(b)\ |E \cap F| \in L \pmod p \text{ for } E, F \in \mathcal{F}, E \neq F.$$

Then $\mathcal{F}$ is s-independent. Consequently

$$|\mathcal{F}| \leq \binom{n}{s}.$$

Frankl and Wilson applied this result to give an exponential lower bound for the chromatic number of the unit distance graph on $\mathbb{R}^n$.

In 1992 Alon, Babai and Suzuki generalised further this theorem with the aid of the linear algebra bound method in [5]:

Theorem 5.6 *(Alon, Babai, Suzuki, 1992): Let p be a prime number and L a set of $s \leq p-1$ integers. Let k be an integer such that $k \notin L \pmod p$. Assume that $s + k \leq n$. Let $\mathcal{F}$ be a family of subsets of a set of n elements such that*

$$(a)\ |E| \equiv k \pmod p \text{ for } E \in \mathcal{F}$$

and

$$(b)\ |E \cap F| \in L \pmod p \text{ for } E, F \in \mathcal{F}, E \neq F.$$

Then

$$|\mathcal{F}| \leq \binom{n}{s}.$$

In the thesis we prove the following conjecture of Babai and Frankl (see [16], p. 115).

Theorem 5.7 *Let k be an integer and $q = p^\alpha$, $\alpha \geq 1$, a prime power. Suppose that $2(q-1) \leq n$. Assume that $\mathcal{F} = \{A_1, \ldots, A_m\}$ is a family of subsets of $[n]$ such that*

$$(a)\ |A_i| \equiv k \ (\text{mod } q) \text{ for } i = 1, \ldots, m$$

$$(b)\ |A_i \cap A_j| \not\equiv k \ (\text{mod } q) \text{ for } 1 \leq i, j \leq m,\ i \neq j.$$

Then

$$m \leq \binom{n}{q-1}.$$

In the proof we combine the linear algebra bound method with an argument involving Gröbner-standard monomials and the corresponding reduction.

Let p be a prime and k an integer. Let $q = p^\alpha$, $\alpha \geq 1$. We write

$$\mathcal{F}(k, q) = \{K \subseteq [n] : \ |K| \equiv k \ (\text{mod } q)\}.$$

In Theorem 1.1 of [33] Frankl proved the following Theorem.

Theorem 5.8 *Let p be a prime and k an integer. If $\ell \leq p-1$ and $2\ell \leq n$, then*

$$rank_{\mathbb{F}_p}\ I(\mathcal{F}(k,p), \binom{[n]}{\leq \ell}) \leq \binom{n}{\ell}.$$

Our proof of Theorem 5.7 relies on the following generalisation of Theorem 5.8.

Theorem 5.9 *Let p be a prime and k an integer. Let $q = p^\alpha$, $\alpha \geq 1$. If $\ell \leq q-1$ and $2\ell \leq n$, then*

$$rank_{\mathbb{F}_p}\ I(\mathcal{F}(k,q), \binom{[n]}{\leq \ell}) \leq \binom{n}{\ell}.$$

We give an equivalent form of Theorem 5.9 in Section 5.2 with the aid of standard monomials. The bound in Theorem 5.9 is sharp. We have equality here if $\ell \leq k \leq n - \ell$ or if $k + \ell + q \leq n$. Indeed, by a theorem of Wilson [79] (see also Corollary 3.1 in [47]) the sub-matrix $I(\binom{[n]}{m}, \binom{[n]}{\leq \ell})$ has rank $\binom{n}{\ell}$, where $m = k$ if $\ell \leq k \leq n - \ell$ and $m = k + q$ if $k + q + \ell \leq n$.

The results presented in this Chapter also appeared in [48].

5.2 A generalisation of Frankl's Theorem

Assume that $0 \leq d \leq n/2$. We write

$$D(d) := \{\{s_1 < \ldots < s_j\} \subset [n] : \ j \leq d \text{ and } s_i \geq 2i \text{ for } 1 \leq i \leq j\}. \qquad (46)$$

In particular $\emptyset \in D(d)$. The sets $D(d)$ were studied in [11], [36] and [47] in connection with order shattering and Gröbner bases for uniform families. In Theorem 1.4 and Lemma 2.3 of [11] it was proved that

$$|D(d)| = \binom{n}{d}$$

holds for $0 \leq d \leq n/2$.

The following statement is from [47]. Characteristic vectors are interpreted now as elements of $\mathbb{Z}^n$.

Proposition 5.10 *Assume that* $0 < t \leq n/2$*,* $H \in \mathcal{H}(t)$ *and* $0 \leq d \leq n$*.*
(a) The degree of $f_{H,d}$ *is* t*,* $\mathrm{lm}(f_{H,d}) = x_H$*, and the leading coefficient is 1.*
(b) If $D \subseteq [n]$*,* $|D| = d$*, then* $f_{H,d}(v_D) = 0$*.*

The next statement is a slight generalisation of an argument from [47].

Proposition 5.11 *Assume that* $0 \leq \ell \leq n/2$ *and let*

$$\mathcal{G}_\ell = \{g_H : \ H \in \mathcal{H}(t), 0 < t \leq \ell\} \cup \{x_1^2 - x_1, \ldots, x_n^2 - x_n\} \subset \mathbb{F}[x_1, \ldots, x_n]$$

be a collection of polynomials such that the degree of g_H *is* t *and* $\mathrm{lm}(g_H) = x_H$*. Let* $f \in \mathbb{F}[x_1, \ldots, x_n]$ *be a polynomial,* $\deg f \leq \ell$*, which is irreducible with respect to* $\mathcal{G}_\ell$ *and* $\prec$*. Then* f *is an* $\mathbb{F}$*-linear combination of monomials from*

$$\mathcal{M}_\ell := \{x_G : \ G \in D(\ell)\} \subset \mathbb{F}[x_1, \ldots, x_n].$$

Remark. The term *irreducible* means here that no reduction of f by any element of $\mathcal{G}_\ell$ is possible.

Proof. Assume for contradiction that f contains a monomial w not in $\mathcal{M}_\ell$. We have $\deg w \le \ell$. Also, w is square-free; otherwise we could reduce it further by some binomial $x_i^2 - x_i$. We have therefore $w = x_U$ for some $U = \{u_1 < \ldots < u_m\}$ with $m \le \ell$. The condition $U \notin \mathcal{M}_\ell$ means now that there is an index $i \le m \le \ell$ such that $u_i < 2i$. Let t be the smallest such index i. Then by the definition of t we have $u_i \ge 2i$ for $1 \le i < t$, hence $\{u_1 < \ldots < u_t\} := H \in \mathcal{H}(t)$. Also, we see that $H \subseteq U$. But then the leading term x_H of g_H divides w, hence f is reducible with respect to $\mathcal{G}_\ell$, a contradiction. This proves the statement. □

In view of (18) and the subsequent remark, Theorem 5.8 follows from the next statement.

Theorem 5.12 *Let $\prec$ be the deglex order, p be a prime and k an integer. If $\ell \le p-1$ and $2\ell \le n$, then*

$$|Sm(\prec, \mathcal{F}(k,p), \mathbb{F}_p) \cap \binom{[n]}{\le \ell}| \le \binom{n}{\ell}.$$

We give a generalisation to q-uniform families. It is slightly stronger than Theorem 5.9.

Theorem 5.13 *Let $\prec$ be the deglex order, p be a prime and $q = p^\alpha > 1$. Suppose that $k, \ell \in \mathbb{N}$ for which $0 \le k, \ell < q$, and $2\ell \le n$. Then*

$$Sm(\prec, \mathcal{F}(k,q), \mathbb{F}_p) \cap \binom{[n]}{\le \ell} \subseteq D(\ell),$$

hence

$$|Sm(\prec, \mathcal{F}(k,q), \mathbb{F}_p) \cap \binom{[n]}{\le \ell}| \le \binom{n}{\ell}.$$

Proof. We intend to use Proposition 5.11. We exhibit a set of polynomials $\mathcal{G}_\ell \subset \mathbb{F}_p[x_1, \ldots, x_n]$ satisfying the conditions of the Proposition, with the additional property that all elements of $\mathcal{G}_\ell$ vanish on the characteristic vectors of the family $\mathcal{F}(k,q)$. This suffices, because the standard monomials for $V(\mathcal{F}(k,q))$ must be irreducible with respect to any set of polynomials which vanish on the set, in particular, with respect to $\mathcal{G}_\ell$. On the other hand, the $\mathcal{G}_\ell$-irreducible monomials are in $\mathcal{M}_\ell$ by Proposition 5.11. These allow us to conclude that the standard monomials of degree at most ℓ for the complete q-uniform family are in $\mathcal{M}_\ell$.

We thus turn to the construction of $\mathcal{G}_\ell$. Obviously the binomials $x_i^2 - x_i \in \mathbb{F}_p[x_1, \ldots, x_n]$ vanish on $V(\mathcal{F}(k,q))$. For $0 < t \leq \ell$ and $H \in \mathcal{H}(t)$ we define $g_H \in \mathbb{F}_p[x_1, \ldots, x_n]$ as the modulo p reduction of the polynomial (with integer coefficients) $f_{H,k}$. By Proposition 5.10 (a) the degree of g_H is t and the leading term of g_H is x_H.

It suffices to verify that $g_H(v_D) = 0$ for the characteristic vectors v_D of elements $D \in \mathcal{F}(k,q)$. We recall the following simple fact.

Lemma 5.14 *Let $q = p^\alpha > 1$ a prime power. Let x, j be integers, $0 \leq j < q$. Then*

$$\binom{x+q}{j} \equiv \binom{x}{j} \pmod{p}.$$

Proof. The congruence follows from the Vandermonde identity (26) with $s = q$ and $t = j$, by noting that the binomial coefficients $\binom{q}{i}$ vanish modulo p for $1 \leq i < q$. □

Now let $D \in \mathcal{F}(k,q)$, and write $v = v_D$. Then $|D| = k'$ for some k' such that $0 \leq k' \leq n$ and $k \equiv k' \pmod{q}$. We observe that $f_{H,k} \equiv f_{H,k'} \pmod{p}$, i.e., the coefficients of the two polynomials are the same modulo p. This holds because for $0 \leq i \leq t$ we have

$$\binom{k-i}{t-i} \equiv \binom{k'-i}{t-i} \pmod{p},$$

a consequence of $0 \leq t - i \leq q - 1$ and Lemma 5.14.

We conclude that

$$g_H(v) \equiv f_{H,k}(v) \equiv f_{H,k'}(v) = 0 \pmod{p}.$$

Here the last equality follows from Lemma 5.10 (b). The proof is complete. □

5.3 The proof of the conjecture of Babai and Frankl

We prove Theorem 5.7 by a combination of the linear algebra argument presented in Theorem 5.30 of [16] with Theorem 5.13. We make first some preparations. The following fact was proved in Proposition 5.31 of [16].

Proposition 5.15 *Let $q = p^\alpha$, p a prime, and $\alpha \geq 1$. For any integer r, the binomial coefficient $\binom{r-1}{q-1}$ is divisible by p iff r is not divisible by q.* $\square$

Let $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ be a polynomial. The *square-free reduction* f' of f is obtained by reducing f with respect to the set of polynomials $\{x_1^2 - x_1, \ldots, x_n^2 - x_n\}$. In other words, we replace x_i^2 with x_i as long as it is possible. Clearly f' is a $\mathbb{Q}$-linear combination of monomials x_U, $U \subseteq [n]$. It is immediate that $\deg f' \leq \deg f$ and $f(v) = f'(v)$ for every vector $v \in \{0,1\}^n$.

Lemma 5.16 *Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$ be a polynomial such that $f(v) \in \mathbb{Z}$ for every $v \in \{0,1\}^n$. Let f' be the square-free reduction of f. Then $f' \in \mathbb{Z}[x_1, \ldots, x_n]$.*

Proof. We have

$$f'(x_1, \ldots, x_n) = \sum_{H \subseteq [n]} \alpha_H \cdot x_H, \tag{47}$$

where $\alpha_H \in \mathbb{Q}$. Suppose for contradiction that $f' \notin \mathbb{Z}[x_1, \ldots, x_n]$. Then there exists $G \subseteq [n]$ such that $\alpha_G \in \mathbb{Q} \setminus \mathbb{Z}$. Let K be minimal with respect to inclusion among those subsets G. Obviously $\alpha_K \notin \mathbb{Z}$. Then $f(v_K) = f'(v_K) = \sum_{Y \subseteq K} \alpha_Y x_Y(v_K) = \sum_{Y \subset K} \alpha_Y + \alpha_K \in \mathbb{Z}$. Also $\sum_{Y \subset K} \alpha_Y \in \mathbb{Z}$, by the minimality of K. These imply that $\alpha_K = f'(v_K) - \sum_{Y \subset K} \alpha_Y$ is also in $\mathbb{Z}$, a contradiction. This proves the claim. $\square$

Proof of Theorem 5.7. Let v_i denote the characteristic vector of the set A_i. Let us consider the polynomials

$$f_i(x_1, \ldots, x_n) = \binom{x \cdot v_i - k - 1}{q - 1}$$

in n rational variables $x = (x_1, \ldots, x_n) \in \mathbb{Q}^n$ $(i = 1, \ldots, m)$, where $a \cdot b$ denotes the scalar product in $\mathbb{Q}^n$. Denote by f_i' the square-free reduction of f_i for $i = 1, \ldots, m$. Then $f_i' \in \mathbb{Z}[x_1, \ldots, x_n]$, because $f_i(v) \in \mathbb{Z}$ for each $v \in \{0,1\}^n$, and hence Lemma 5.16 applies.

Let $g_i \in \mathbb{F}_p[x_1, \ldots, x_n]$ denote the reduction of f_i' modulo p and $h_i \in \mathbb{F}_p[x_1, \ldots, x_n]$ the reduction of g_i by a 'deglex Gröbner basis for the ideal $I := I(V(\mathcal{F}(k,q)))$ of polynomials vanishing on $V(\mathcal{F}(k,q))$ (actually reduction by $\mathcal{G}_{q-1}$ suffices here). Obviously we have

$$f_i(v_j) = f_i'(v_j) \equiv g_i(v_j) \equiv h_i(v_j) \pmod{p} \text{ for } 1 \leq j \leq m. \tag{48}$$

Here the (first) equality is valid for any 0,1-vector, while the second congruence holds because $A_j \in \mathcal{F}(k,q)$. Next note that by Proposition 5.15 the integer

$$f_i(v_j) = \binom{|A_i \cap A_j| - k - 1}{q-1}$$

will be divisible by p iff $i \neq j$. Then (48) implies that $h_i(v_j)$ will be 0 in $\mathbb{F}_p$ iff $i \neq j$. We thus found that the $m \times m$ matrix $H = (h_i(v_j))_{i,j=1}^m$ is a diagonal matrix over $\mathbb{F}_p$ with no zeroes in the diagonal. From Proposition 2.7 of [16] (Determinant Criterion) it follows that the polynomials $h_1, \ldots, h_m$ are linearly independent over $\mathbb{F}_p$.

Moreover, being reduced polynomials with respect to a Gröbner basis, the h_i are linear combinations of standard monomials for I and $\deg h_i \leq q-1$ because $\deg f_i = q-1$, and the reductions (modulo p, and deglex) involved can not increase the degree. By Theorem 5.13 we infer that the linearly independent polynomials $h_1, \ldots, h_m$ are in the $\mathbb{F}_p$-space spanned by $\mathcal{M}_{q-1}$, and hence

$$|\mathcal{F}| = m \leq |\mathcal{M}_{q-1}| = \binom{n}{q-1},$$

which was to be proved. □

6 Gröbner bases for permutations

6.1 Introduction

Let $\mathbb{F}$ be a fix, but otherwise arbitrary field.

In this Chapter we consider an another type of interesting finite subsets of $\mathbb{F}^n$. Let $\alpha_1, \dots, \alpha_n$ be n different elements of $\mathbb{F}$ and put

$$V_{(1^n)} := V_{(1^n)}(\alpha_1, \dots, \alpha_n) := \{(\alpha_{\pi(1)}, \dots, \alpha_{\pi(n)}) : \ \pi \in S_n\}.$$

Then $V_{(1^n)}$ is the set of all permutations of the α_i, viewed as a subset of $\mathbb{F}^n$.

We denote by

$$\mathcal{M} := \{x_1^{\alpha_1} \dots x_n^{\alpha_n} : \ 0 \le \alpha_i \le i-1 \ \text{ for } 1 \le i \le n\} \tag{49}$$

the set of Artin monomials.

We give here the most important previous results in the theme of the determination of Gröbner bases of permutations. In [13] E. Artin proved that $\mathcal{M}$ is a basis of the quotient ring

$$\mathbb{F}[x_1, \dots, x_n]/(\sigma_1, \dots, \sigma_n),$$

where we wrote σ_i for the i-th elementary symmetric polynomial:

$$\sigma_i(x_1, \dots, x_n) = \sum_{S \subset [n], \ |S|=i} x_S.$$

In [40] Garsia and Wallach gave an expansion of every polynomial

$$p(x_1, \dots, x_n) \in \mathbb{Q}[x_1, \dots, x_n]$$

modulo the ideal $(\sigma_1, \dots, \sigma_n)$, as a linear combination of Artin monomials. Later, Mora and Sala in [69] determined the Gröbner basis of the ideal J, which is generated by all symmetric functions in $\mathbb{F}[x_1, \dots, x_n]$, with respect to any term order $\prec$.

In Theorem 6.2 we describe the reduced Gröbner bases and the standard monomials with respect to any term order $\prec$, for which $x_1 \prec \ldots \prec x_n$, for the ideal $I(V_{(1^n)})$.

In [38] Garsia obtained a beautiful generalisation of the Fundamental Theorem of Symmetric Polynomials. Here we present a simple proof of his result.

6.2 Permutations

We recall the definition of the complete symmetric polynomials. Let i be a nonnegative integer and write

$$h_i(x_1, \ldots, x_n) = \sum_{a_1+\cdots+a_n=i} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}.$$

Thus, $h_i \in \mathbb{F}[x_1, \ldots, x_n]$ is the sum of all monomials of total degree i. For $0 \leq i \leq n$ we write σ_i for the i-th elementary symmetric polynomial:

$$\sigma_i(x_1, \ldots, x_n) = \sum_{S \subset [n],\ |S|=i} x_S.$$

$\sigma_i \in \mathbb{F}[x_1, \ldots, x_n]$ is the sum of all square free monomials of degree i in the variables $x_1, \ldots, x_n$.

Let $\alpha_1, \ldots, \alpha_n$ be n different elements of $\mathbb{F}$, and $V_{(1^n)} = V_{(1^n)}(\alpha_1, \ldots, \alpha_n) \subseteq \mathbb{F}^n$ be the set of permutations of $\alpha_1, \ldots, \alpha_n$.

For $1 \leq k \leq n$ we introduce the polynomials $f_k \in S$ as follows:

$$f_k = \sum_{i=0}^{k} (-1)^i h_{k-i}(x_k, x_{k+1}, \ldots, x_n) \sigma_i(\alpha_1, \ldots, \alpha_n).$$

We remark, that $f_k \in \mathbb{F}[x_k, x_{k+1}, \ldots, x_n]$. Moreover, $\deg f_k = k$ and the leading monomial of f_k is x_k^k with respect to any term order $\prec$ for which $x_1 \succ x_2 \succ \ldots \succ x_n$.

Proposition 6.1 *Let $v \in V_{(1^n)}$. Then $f_k(v) = 0$ for $1 \leq k \leq n$.*

Proof. The statement is immediate from the following known (see, e.g. [28, p 314]) identities. Let $1 \leq k \leq n$. Then

$$\sum_{i=0}^{k} (-1)^i h_{k-i}(x_k, \ldots, x_n) \sigma_i(x_1, \ldots, x_n) = 0. \tag{50}$$

For the convenience of the reader we sketch a proof of (50). For a fixed k one verifies first that

$$\sigma_i(x_1, \ldots, x_n) = \sum_{S \subseteq [k-1]} x_S \sigma_{i-|S|}(x_k, \ldots, x_n), \tag{51}$$

where we understand $\sigma_j = 0$ for $j < 0$.

We need also the fundamental relation connecting complete symmetric polynomials to the elementary ones, see [74, Theorem 4.3.7] or [64, p 14]. If t, m are positive integers then, with the convention $\sigma_i = 0$ for $i > m$, we have

$$\sum_{i=0}^{t}(-1)^i h_{t-i}(w_1, \dots, w_m)\sigma_i(w_1, \dots, w_m) = 0. \tag{52}$$

Now using (51), we obtain

$$\sum_{i=0}^{k}(-1)^i h_{k-i}(x_k, \dots, x_n)\sigma_i(x_1, \dots, x_n) =$$

$$= \sum_{S\subseteq[k-1]} x_S \sum_{j=|S|}^{k}(-1)^i h_{k-i}(x_k, \dots, x_n)\sigma_{i-|S|}(x_k, \dots, x_n).$$

To establish (50), it suffices to verify that the coefficient of x_S is 0 for every $S \subseteq [k-1]$. For this we can apply (52) with $t = k - |S| > 1$, and $m = n - k + 1$. □

We can state now the main result of this section. A related weaker statement is given in [28, Proposition 5, Chapter 7].

Theorem 6.2 *Let $\mathbb{F}$ be a field and let $\prec$ be an arbitrary term order on the monomials of $\mathbb{F}[x_1, \dots, x_n]$ such that $x_n \prec \dots \prec x_1$. Then the reduced Gröbner basis of $I(V_{(1^n)})$ is*

$$\{f_i : \ 1 \le i \le n\}.$$

Moreover the set of standard monomials is

$$\mathrm{Sm}(\prec, I(V_{(1^n)}) = \{x_1^{\alpha_1} \dots x_n^{\alpha_n} : \ 0 \le \alpha_i \le i-1, \text{ for } 1 \le i \le n\}. \tag{53}$$

Proof. Let $\mathcal{M}$ denote the set of monomials on the right hand side of (53). The leading monomial of f_k is x_k^k, hence if a monomial w is not in $\mathcal{M}$ then w is clearly a leading term for $I(V_{(1^n)})$. We infer that the standard monomials are a subset of $\mathcal{M}$. The reverse inclusion follows at once from $|\mathcal{M}| = n! = |V_{(1^n)}|$ and (39). Now (53) implies that the monomials x_k^k, $(1 \le k \le n)$ generate the initial ideal for $I(V_{(1^n)})$, therefore $\{f_1, \dots f_n\}$ is a Gröbner basis for $I(V_{(1^n)})$.

Reducedness is immediate: on one hand, there are no divisibilities among the x_k^k. On the other hand, except for the leading term, all monomials in f_k are standard monomials. □

There is a useful and simple bijection between permutations and Artin monomials, more precisely their exponent vectors. This is the Hall map [59, Section 5.1.1.]. To a permutation π of $\{1, \ldots, n\}$ the Hall map associates the sequence of integers $b_n, b_{n-1}, \ldots, b_1$ where b_j is the number elements $k \in [n]$ such that $k > j$ and k appears in π to the left of j. Clearly we have $b_i \leq n - i$ for $i = 1, \ldots, n$, hence $x_1^{b_n} x_2^{b_2} \cdots x_n^{b_1} \in \mathcal{M}$. It is not hard to show that this map is invertible. Monomials of degree k correspond under the Hall map to permutations with exactly k inversions. These latter objects have been studied intensively. Writing simply $h(m)$ for the Hilbert function $h_{S/I(V_{(1^n)})}(m)$, we have

$$h(m) - h(m-1) = I_m(n), \quad m = 1, 2, \ldots, \binom{n}{2},$$

where $I_m(n)$ is the number of permutations of n symbols with m inversions. In [59, Section 5.1.1.] there are some explicit formulae for $I_m(n)$, $m \leq n$. Asymptotic estimates are given in [27] and [65].

The Fundamental Theorem on Symmetric Polynomials asserts that every symmetric polynomial $f \in \mathbb{F}[y_1, \ldots, y_n]$ admits a unique expression of the form

$$f = \sum_{p \geq 0} a_p \sigma_1^{p_1} \sigma_2^{p_2} \cdots \sigma_n^{p_n},$$

where $p = (p_1, p_2, \ldots, p_n)$, $a_p \in \mathbb{F}$, and the σ_i are the elementary symmetric polynomials in the y_i. Here we prove the following generalisation: Let $\mathcal{N}$ be the set of Artin monomials in the y_i (we substitute y_i in the place of x_i for every $w \in \mathcal{M}$).

Corollary 6.3 *Every polynomial $f \in \mathbb{F}[y_1, \ldots, y_n]$ has a unique expansion of the form*

$$f(y_1, \ldots, y_n) = \sum_{w \in \mathcal{N}} \sum_{p \geq 0} a_{w,p} w \sigma_1^{p_1} \sigma_2^{p_2} \cdots \sigma_n^{p_n},$$

where $a_{w,p} \in \mathbb{F}$.

Proof. Let $\{y_1, \ldots, y_n\}$ be variables, and consider the set of permutations $V_{(1^n)} = V_{(1^n)}(y_1, \ldots, y_n)$ in $\mathbb{K}^n$, where $\mathbb{K}$ is the function field $\mathbb{F}(y_1, \ldots, y_n)$. The polynomial $f(x_1, \ldots, x_n)$ can be considered as an element of $\mathbb{K}[x_1, \ldots, x_n]$. We apply the preceding Theorem with $\mathbb{K}$ in the place of $\mathbb{F}$ and $\alpha_i = y_i$. The reduction of $f(x_1, \ldots, x_n)$ with respect to $f_1, \ldots, f_n$ shows the existence of a unique expansion of the form

$$f(x_1, \ldots, x_n) = \sum_{w \in \mathcal{M}} w g_w, \tag{54}$$

where $g_w \in \mathbb{F}[y_1, \ldots, y_n]$ are symmetric polynomials in the y_i. This holds because the leading coefficient of an f_i is 1, and the non leading terms of f_i are of the form $w g_w$ as above. The two sides of (54) are equal as functions on $V_{(1^n)}$. Now the substitutions $x_i = y_i$ and the Fundamental Theorem on Symmetric Polynomials gives the claim. □

Remark. The Corollary, together with the proof we presented here, offers an algorithmic version of the fact that $\mathbb{F}[y_1, \ldots, y_n]$ is a free module of rank $n!$ over the ring of symmetric polynomials. The reduction procedure gives an expression of f in terms of the Artin basis.

7 The standard monomials of the ideal $I(V_\lambda)$.

7.1 Introduction

First we give some notations. We use also in this Chapter without reference the definitions of Section 2.4.

Recall that a sequence $\lambda = (\lambda_1, \dots, \lambda_k)$ of natural numbers is a *partition* of n, if $\lambda_1 + \lambda_2 + \dots + \lambda_k = n$ and $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k > 0$. If λ is a partition of n, then we denote this fact by $\lambda \vdash n$.

Let $\alpha_0, \dots, \alpha_{k-1}$ be k different elements of $\mathbb{F}$, $\lambda \vdash n$ and V_λ be the set of all vectors $v = (v_1, \dots, v_n) \in \mathbb{F}^n$ such that

$$|\{j \in [n] : \ v_j = \alpha_i\}| = \lambda_{i+1}$$

for $0 \leq i \leq k-1$.

Example: if $\alpha_0 = 0$, $\alpha_1 = 1$, and $\lambda = (n-d, d)$, then V_λ is the set of $0-1$ vectors of length n and Hamming weight d.

In their study of the q-Kostka polynomials [39] A. M. Garsia and C. Procesi have obtained that $\mathrm{Sm}(\prec_{deg}, V_\lambda) = B_\lambda$ holds for any partition λ (Proposition 3.2 in [39]). They worked over $\mathbb{Q}$, but their argument is valid over an arbitrary field. The associated graded ring gr $S/I(V_\lambda)$ is also described there.

The main contribution of this Chapter is Theorem 7.8 which states that $\mathrm{Sm}(\prec_{lex}, V_\lambda) = B_\lambda$, where $\mathbb{F}$ is an arbitrary field and λ is an arbitrary partition. This extends the above result of Garsia and Procesi to the lexicographic order.

Note that both in the lex and deglex cases the standard monomials are independent of the specific choice of $\alpha_0, \dots, \alpha_{k-1}$ or the field $\mathbb{F}$ itself.

From Theorem 7.8 we obtain a new, perhaps simpler proof of the result of Garsia and Procesi on the deglex standard monomials of V_λ (Theorem 7.12). In particular, we avoid the use of Tanisaki's ideals (see (1.5) in [39]).

The claims of Theorems 7.8 and 7.12 have been known in the special cases $\lambda = (n-d, d)$ and $\lambda = (1^n)$. In the former case we have necessarily $d \leq n/2$, and it is not difficult to see that B_λ consists of the monomials $x_{i_1} x_{i_2} \dots x_{i_j}$, where $j \leq d$, $i_1 < i_2 < \ldots < i_j$ and $i_\ell \geq 2\ell$ for $1 \leq \ell \leq j$. In [11] it is shown that $\mathrm{Sm}(\prec_{lex}, V_\lambda) = B_\lambda$. In [47] this is generalised to an arbitrary term order $\prec$, for which $x_n \prec \ldots \prec x_1$.

Now let $\alpha_1, \dots, \alpha_n$ be n different elements of $\mathbb{F}$, put $\lambda = (1^n)$ and consider $V_\lambda = \{(\alpha_{\pi(1)}, \dots, \alpha_{\pi(n)}) :\ \pi \in S_n\}$.

Let $\prec$ be an arbitrary term-order on the monomials of $\mathbb{F}[x_1, \dots, x_n]$ such that $x_n \prec \dots \prec x_1$. We proved in Theorem 2.2 of [46] that

$$\mathrm{Sm}(\prec, V_\lambda) = \{x_1^{\beta_1} \dots x_n^{\beta_n} :\ 0 \le \beta_i \le i-1 \text{ for } 1 \le i \le n\}. \tag{55}$$

Clearly $g = (0, 1, \dots, n-1)$ is the only lattice permutation of type $\lambda = (1^n)$, that is, $\mathrm{st}(\lambda) = \{g\}$. By (55) we have in this case $\mathrm{Sm}(\prec, V_\lambda) = B_\lambda$.

The rest of this Chapter organised as follows: In Section 7.2 we describe some technical lemmas about standard monomials for the lex and deglex orders. In Section 7.3 we prove an orthogonality relation connecting a space of functions on V_λ to the Specht module S^λ. In Section 7.4 we settle first the lex case (Theorem 7.8). Next we give an apparently new characterisation of $(S^\lambda)^\perp$ (Theorem 7.10). This will be used to infer the result of Garsia and Procesi on the deglex standard monomials of V_λ (Theorem 7.12). Some other consequences are also discussed, including a combinatorial description of the Hilbert function of the algebra $S/I(V_\lambda)$, and an explicit basis of the module $(S^\lambda)^\perp$.

7.2 Standard monomials

In the following we shall consider the term orders $\prec_{lex}$ and $\prec_{deg}$.

Lemma 7.1 *Let $\mathcal{F} \subseteq \mathbb{F}^n$ be a finite subset and let $d \in \mathbb{N}$ be a natural number such that $\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \subseteq \mathrm{Mon}(n, \le d)$. Then*

$$\mathrm{Sm}(\prec_{deg}, \mathcal{F}) \cap \mathrm{Mon}(n, d) \subseteq \mathrm{Sm}(\prec_{lex}, \mathcal{F}) \cap \mathrm{Mon}(n, d).$$

Proof. Let $w \in \mathrm{Sm}(\prec_{deg}, \mathcal{F})$ of degree d. If $w \notin \mathrm{Sm}(\prec_{lex}, \mathcal{F})$, then w is the lex-leading term of a polynomial $f \in S$ vanishing on $\mathcal{F}$:

$$f = w + \sum_u \gamma_u \cdot u + \sum_v \beta_v \cdot v,$$

where u runs through the elements of $\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \cap \mathrm{Mon}(n, d)$ and v runs through the elements $\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \cap \mathrm{Mon}(n, \le (d-1))$. But here we have also $u \prec_{deg} w$ and $v \prec_{deg} w$ by the definitions of the orders $\prec_{lex}$ and $\prec_{deg}$, hence w is a leading term for $\prec_{deg}$, a contradiction. $\square$

The following (technical) result will be our primary tool when passing from the lexicographic case to deglex.

Proposition 7.2 *Let $\mathcal{F} \subseteq \mathbb{F}^n$ be a finite subset. Suppose that $d \in \mathbb{N}$ is a natural number such that*

$$(a)\ (\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \cap \mathrm{Mon}(n, d))^{\leq} = \mathrm{Sm}(\prec_{lex}, \mathcal{F})$$

and

$$(b)\ |\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \cap \mathrm{Mon}(n, \leq d-1)| = |\mathrm{Sm}(\prec_{deg}, \mathcal{F}) \cap \mathrm{Mon}(n, \leq d-1)|.$$

Then $\mathrm{Sm}(\prec_{lex}, \mathcal{F}) = \mathrm{Sm}(\prec_{deg}, \mathcal{F})$.

Proof. By (a) $\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \subseteq \mathrm{Mon}(n, \leq d)$. Let $w \in \mathrm{Sm}(\prec_{deg}, \mathcal{F})$. As a function on $\mathcal{F}$ we can express w as

$$w = \sum_y \gamma_y y,$$

where y ranges over $\mathrm{Sm}(\prec_{lex}, \mathcal{F})$ and $\gamma_y \in \mathbb{F}$. Here w can not be the leading term with respect to $\prec_{deg}$ because it is a standard monomial. We infer that some y must be the deglex leading term, hence $\deg w \leq \deg y \leq d$, giving that $\mathrm{Sm}(\prec_{deg}, \mathcal{F}) \subseteq \mathrm{Mon}(n, \leq d)$ as well. Also by (14) we have

$$|\mathcal{F}| = |\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \cap \mathrm{Mon}(n, d)| + |\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \cap \mathrm{Mon}(n, \leq d-1)|, \quad (56)$$

and

$$|\mathcal{F}| = |\mathrm{Sm}(\prec_{deg}, \mathcal{F}) \cap \mathrm{Mon}(n, d)| + |\mathrm{Sm}(\prec_{deg}, \mathcal{F}) \cap \mathrm{Mon}(n, \leq d-1)|. \quad (57)$$

From the above two equations and (b) we infer that

$$|\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \cap \mathrm{Mon}(n, d)| = |\mathrm{Sm}(\prec_{deg}, \mathcal{F}) \cap \mathrm{Mon}(n, d)|,$$

whence by Lemma 7.1 we obtain

$$\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \cap \mathrm{Mon}(n, d) = \mathrm{Sm}(\prec_{deg}, \mathcal{F}) \cap \mathrm{Mon}(n, d).$$

But $\mathrm{Sm}(\prec_{deg}, \mathcal{F})$ is downward closed, hence by (a) we obtain $\mathrm{Sm}(\prec_{lex}, \mathcal{F}) \subseteq \mathrm{Sm}(\prec_{deg}, \mathcal{F})$. The latter two sets have the same size $|\mathcal{F}|$, giving the conclusion desired. □

We shall apply Proposition 7.2 for the set $\mathcal{F} = V_\lambda$. Condition (b) will be verified with the aid of Specht modules. Moreover, we shall prove (a) by combinatorial arguments.

7.3 Specht modules and spaces of functions

Following James [54] we call two tableaux t and t' associated with the same partition λ *row equivalent* if t' can be obtained from t by permuting numbers in the same rows. The equivalence classes are called *tabloids*. The tabloid of a tableau t is denoted by $\{t\}$. We depict the tabloid $\{t\}$ in a way similar to the tableau t, by erasing the vertical lines separating the boxes of t. The tabloids corresponding to the tableaux of (19) may be drawn as

2	5	3	6
4	1		
7			

and

1	2	4	5
3	7		
6			

A λ-*array* is an array t obtained by putting n nonnegative integers in the boxes of the Ferrers diagram of λ. An array differs from a tableau in that repeated or large entries are allowed here.

Let $\mathbb{F}$ be a field, λ be a partition of n. We denote by M^λ the linear space over $\mathbb{F}$ whose basis elements are the λ-tabloids. M^λ carries an $\mathbb{F}S_n$ module structure: for $\pi \in S_n$ and a λ-tableau t we set $\pi\{t\} := \{\pi t\}$. There is a convenient S_n-invariant non degenerate bilinear form $\langle , \rangle$ on M^λ, the James scalar product, which is defined by

$$\langle \{t\}, \{t'\} \rangle := \delta_{\{t\},\{t'\}}$$

for λ-tabloids $\{t\}$, $\{t'\}$.

Let $w = x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}$ be a monomial and $\lambda = (\lambda_1, \dots, \lambda_k) \vdash n$. We say that w is of type λ, if $\lambda_i = |\{j \in [n] : \ \beta_j = i - 1\}|$ for $1 \le i \le k$. We denote by $\mathrm{Mon}(\lambda)$ the set of all monomials of type λ.

For a partition $\lambda \vdash n$ let $P^\lambda \subseteq \mathbb{F}[x_1, \dots, x_n]$ denote the $\mathbb{F}$-subspace spanned by the monomials of type λ. P^λ is an $\mathbb{F}S_n$ module by the rule $\pi(x_1^{\beta_1} \dots x_n^{\beta_n}) = x_{\pi(1)}^{\beta_1} \dots x_{\pi(n)}^{\beta_n}$. It is immediate that $\dim_{\mathbb{F}} P^\lambda = n!/\lambda!$, where $\lambda! := \prod_{i=1}^k (\lambda_i)!$.

We define now an $\mathbb{F}S_n$ module isomorphism $\phi^\lambda : M^\lambda \to P^\lambda$.

Let $\{t\} \in M^\lambda$. We define $\phi^\lambda(\{t\}) = x_1^{\beta_1} \dots x_n^{\beta_n}$ by the rule

$$\beta_i = j - 1 \text{ iff } i \text{ appears in } \{t\} \text{ in the } j^{th} \text{ row.} \tag{58}$$

Actually, ϕ^λ can be turned into an isometry as well, by defining $\langle x^u, x^v \rangle := \delta_{u,v}$ for monomials x^u, x^v of type λ.

We denote by $F(V_\lambda)$ the $\mathbb{F}$-space of functions from V_λ to $\mathbb{F}$ and let $F(\leq d, V_\lambda)$ stand for the $\mathbb{F}$-space of functions from V_λ to $\mathbb{F}$ which are linear combinations of monomials of degree at most d. It is immediate that $\dim_{\mathbb{F}} F(V_\lambda) = |V_\lambda| = n!/\lambda!$.

For $v \in V_\lambda$, we denote by $\chi_v : V_\lambda \to \mathbb{F}$ the characteristic function of v, i.e., $\chi_v(v) = 1$ and $\chi_v(w) = 0$ for $w \in V_\lambda$, $w \neq v$. Obviously $\{\chi_v : \ v \in V_\lambda\}$ is a basis of the $\mathbb{F}$-space $F(V_\lambda)$.

Clearly $F(V_\lambda)$ and $F(\leq d, V_\lambda)$ are $\mathbb{F}S_n$ modules: a permutation $\pi \in S_n$ acts on $f \in F(V_\lambda)$ as

$$\pi f(v) := f(\pi v), \tag{59}$$

where πv is the place permutation action given in (20).

Now we define an anti-isomorphism $\theta^\lambda : F(V_\lambda) \to P^\lambda$ of $\mathbb{F}S_n$ modules. First we give a map $t^\lambda : V_\lambda \to \mathbb{N}^n$. For $v \in V_\lambda$ we set $t^\lambda : V_\lambda \to \mathbb{N}^n$ by the rule

$$t^\lambda(v)_i := j \text{ iff } v_i = \alpha_j$$

for $1 \leq i \leq n$. If $\lambda = (\lambda_1, \ldots, \lambda_k)$ is a partition of n, then

$$t^\lambda(V_\lambda) \subseteq \{0, \ldots, k-1\}^n.$$

Now let $\theta^\lambda(\chi_v) := x^{t^\lambda(v)}$, for $v \in V_\lambda$. The linear extension of θ^λ to $F(V_\lambda)$ is an $\mathbb{F}$-space isomorphism, because $\{x^{t^\lambda(v)} : \ v \in V_\lambda\}$ is an $\mathbb{F}$-basis of P^λ. We note that $\theta^\lambda(\pi f) = \pi^{-1}\theta^\lambda(f)$ for each $\pi \in S_n$, $f \in F(V_\lambda)$.

We write

$$P^{\lambda, \leq d} := \theta^\lambda(F(\leq d, V_\lambda)) \leq P^\lambda.$$

Let λ be a partition n. Suppose that t is a tableau of shape λ. Then let $e_t^\lambda = \sum \operatorname{sgn}(t')\{t'\}$, where the sum is over those tableaux t' obtained from t by permuting the numbers in the columns of t, and $\operatorname{sgn}(t')$ is the signature of the permutation.

Example. Let $n = 6$, $\lambda = (4, 2)$ and

$$t = \begin{array}{|c|c|c|c|} \hline 2 & 5 & 3 & 6 \\ \hline 1 & 4 \\ \cline{1-2} \end{array}.$$

Then

$$e_t^\lambda = \begin{array}{l} \hline 2\ \ 5\ \ 3\ \ 6 \\ \hline 1\ \ 4 \\ \hline \end{array} - \begin{array}{l} \hline 1\ \ 5\ \ 3\ \ 6 \\ \hline 2\ \ 4 \\ \hline \end{array} - \begin{array}{l} \hline 2\ \ 4\ \ 3\ \ 6 \\ \hline 1\ \ 5 \\ \hline \end{array} + \begin{array}{l} \hline 1\ \ 4\ \ 3\ \ 6 \\ \hline 2\ \ 5 \\ \hline \end{array}. \tag{60}$$

Let S^λ denote the linear subspace of M^λ spanned by the tabloid sums e_t^λ. We have $\pi(e_t^\lambda) = e_{\pi(t)}^\lambda$, hence S^λ is an $\mathbb{F}S_n$-submodule of M^λ. The modules S^λ are called *Specht modules* (see James [54] and Section 7.1 in James, Kerber [56]).

To simplify notation, we denote also by S^λ the isomorphic image $\phi^\lambda(S^\lambda) \leq P^\lambda$ of the module $S^\lambda \leq M^\lambda$.

For $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n$ we write

$$m(\lambda) := \sum_{i=1}^{k} \lambda_i \cdot (i-1).$$

Lemma 7.3 *Let $\lambda = (\lambda_1, \ldots, \lambda_k)$ be a partition of n and $x = x_1^{\beta_1} \ldots x_n^{\beta_n}$ a monomial such that deg $x = \sum_{j=1}^n \beta_j < m(\lambda) = \sum_{i=1}^k \lambda_i(i-1)$. Let t be an arbitrary tableau of shape λ. Then there exist indices $l_1 \neq l_2$ such that $\beta_{l_1} = \beta_{l_2}$ and l_1, l_2 are in the same column of t.*

Proof. Fill out a diagram t' of shape λ with $\beta_1, \ldots, \beta_n$: if i appears in a box of the diagram of t, then write β_i in the same box of t'. As a result, t' will be an array of type λ. Next fill out a diagram of shape λ by writing $i-1$ to all of the λ_i boxes in the i^{th} row. This procedure gives an array s.

Suppose for contradiction that for all d, the indices j for which $\beta_j = d$ are all in different columns of t. This implies that the elements are pairwise different in each of the columns of the array t'. Permute now the entries in each column of t' in such a way that the columns of the new array t'' are strictly increasing sequences.

Then it is obvious from the definition of t'' and s that the value of each box of t'' is at least as large as the entry of the corresponding box of s. The sum of the elements of t'' is deg $x = \sum_{i=1}^n \beta_i$ and the sum of the elements of s is $m(\lambda)$, hence

$$\deg x \geq m(\lambda) = \sum_{i=1}^{k} \lambda_i(i-1).$$

This contradiction proves the Lemma. □

The main result of this section is the following:

Proposition 7.4 $P^{\lambda, \leq m(\lambda)-1} \leq (S^\lambda)^\perp$.

Proof. By the definition of S^λ the set $\{e_t^\lambda : t \text{ is a tableau of shape } \lambda\}$ spans the module S^λ. For this reason, it is enough to prove that if t has shape λ, and $x \in F(V_\lambda)$ is an arbitrary monomial such that

$$\deg x < m(\lambda) = \sum_{i=1}^{k} \lambda_i \cdot (i-1), \tag{61}$$

then

$$\langle \theta^\lambda(x), \phi^\lambda(e_t^\lambda)\rangle = 0.$$

By the definition of the map θ^λ

$$\theta^\lambda(x) = \sum_{v \in V_\lambda} x(v) \cdot x^{t^\lambda(v)}. \tag{62}$$

We apply Lemma 7.3 with $x = x_1^{\beta_1} \dots x_n^{\beta_n}$ and t. There exist indices $l \neq m$ such that $\beta_l = \beta_m$ and l, m are in the same column of t. Let $\tau \in S_n$ denote the transposition (lm).

Now we introduce an equivalence relation on the set $\mathrm{Mon}(\lambda)$. Let $v, w \in \mathrm{Mon}(\lambda)$. We define $v \sim w$ iff $v = w$ or $v = \tau w$. Let A be the set of monomials $w \in \mathrm{Mon}(\lambda)$ for which $\tau w = w$, and let B be a complete set of representatives for the set of equivalence classes of $\sim$ with two elements.

Let $v \in V_\lambda$ be an arbitrary vector. Then

$$x(v) = \tau x(v) = x(\tau v), \tag{63}$$

because $\beta_l = \beta_m$.

It is an immediate consequence of (62) and (63), that if γ_v is the coefficient of $x^v \in B$ in $\theta^\lambda(x)$, then the coefficient of τx^v is the same γ_v. Hence

$$\theta^\lambda(x) = \sum_{x^v \in B} \gamma_v (x^v + \tau x^v) + \sum_{x^v \in A} \epsilon_v x^v \in P^{\lambda, m(\lambda)-1},$$

where $\gamma_v, \epsilon_v \in \mathbb{F}$.

Let δ_w be the coefficient of $x^w \in \mathrm{Mon}(\lambda)$ in $\phi^\lambda(e_t^\lambda)$. Clearly we have $\delta_w = 0$ for $w \in A$. More generally, the coefficient of τx^w is $-\delta_w$. This holds, because if a tabloid $\{t^*\}$ appears in the sum defining e_t^λ, then $\{\pi t^*\}$ appears also, but with opposite sign. Here we used that l and m are in the same column of t. We may therefore write

$$\phi^\lambda(e_t^\lambda) = \sum_{x^w \in B} \delta_w (x^w - \tau x^w) \in P^\lambda.$$

We see in particular, that $\phi^\lambda(e_t^\lambda)$ is orthogonal to any monomial from A, hence

$$\langle \phi^\lambda(e_t^\lambda), \theta^\lambda(x)\rangle = \langle \sum_{x^w \in B} \delta_w(x^w - \tau x^w), \sum_{x^v \in B} \gamma_v(x^v + \tau x^v)\rangle =$$

$$= \sum_{x^w, x^v \in B} \delta_w \gamma_v \langle x^w - \tau x^w, x^v + \tau x^v\rangle$$

$$= \sum_{x^w, x^v \in B} \delta_w \gamma_v (\langle x^w, \tau x^v\rangle - \langle \tau x^w, x^v\rangle + \langle x^w, x^v\rangle - \langle \tau x^w, \tau x^v\rangle) = 0,$$

because $\langle x^w, \tau x^v\rangle = \langle \tau x^w, x^v\rangle$ and $\langle x^w, x^v\rangle = \langle \tau x^w, \tau x^v\rangle$. This finishes the proof. □

Remark. The proof extends without much difficulty to generalised Specht modules S^{λ_1,λ_2} (see James [54], Chapter 17). We have

$$P^{\lambda_2, \leq m(\lambda_1)-1} \leq (S^{\lambda_1,\lambda_2})^\perp.$$

We omit the details because we do not need this relation here.

7.4 Some combinatorial lemmas

Here we establish a bijection between B_λ and V_λ, and some other useful facts on the structure of the sets b_λ.

We recall the notion of inner and outer corner of a diagram (see Section 2.8 in Sagan [74]). If λ is a Ferrers diagram, then an *inner corner* of λ is a box of λ, whose removal leaves the Ferrers diagram of a partition. An *outer corner* of λ is a box b not in λ, whose addition produces the Ferrers diagram of a partition.

Suppose $\lambda = (\lambda_1, \ldots, \lambda_l)$ and $\mu = (\mu_1, \ldots, \mu_m)$ are partitions of n. Then λ *dominates* μ, written $\lambda \trianglerighteq \mu$, if $\sum_{j=1}^i \lambda_j \geq \sum_{j=1}^i \mu_j$ for all $i \geq 1$ (see Section 2.2 in Sagan [74]). If $i > l$ (respectively $i > m$), then we take λ_i (respectively μ_i) to be zero.

Lemma 7.5 *Let λ, $\mu \vdash n+1$ be diagrams of partitions such that $\lambda \cap \mu$ has n boxes. Then $\lambda \cap \mu$ is a partition as well. Let p be the box in $\lambda \setminus \mu$ and q be the box in $\mu \setminus \lambda$. Assume that p is in row α, q is in row β and $\alpha > \beta$. Then $b_\mu \subseteq b_\lambda$.*

Proof. It is enough to prove that for each $v \in \mathrm{st}(\mu)$ there exists a $w \in \mathrm{st}(\lambda)$ such that $v \leq w$. Indeed, then let $t \in b_\mu$ be an arbitrary sequence. Then there exists a $v \in \mathrm{st}(\mu)$ such that $t \leq v$. Hence there exists a $w \in \mathrm{st}(\lambda) \subseteq b_\lambda$ such that $v \leq w$. This means that $t \leq v \leq w \in b_\lambda$, giving that $t \in b_\lambda$.

Let $v \in \mathrm{st}(\mu)$ be an arbitrary lattice permutation and let t be the standard tableau corresponding to v. Take the entry e in the box q of μ. Consider the union of $\{e\}$ and the row of t one below. Arrange the elements in increasing order in the boxes of that row so that the largest element, say e_1, is left out. Consider the union of $\{e_1\}$ and the entries of the next row and repeat the procedure here. When the row of p is reached, then the largest element stays in p rather than being handed down, and the process stops. It is easy to see that the tableau t' we obtained is a standard tableau of type λ. Indeed, the rows of t' are obviously increasing. Let e, e' be entries of t' such that e' is in the box b, which is just under the box holding e. If b held an element $e_1 \neq e'$ in t, this means that we needed to arrange e' in increasing order in the boxes of the row below e'. Therefore e' is greater than any of the elements of the preceding row of t', hence $e' > e$. If $e_1 = e'$, i.e. we did not need to move e' in the process, then we have again $e' > e$, because the entry in the box over b did not increase during the process.

Let $w \in \mathrm{st}(\lambda)$ be the lattice permutation of t'. We have $v \leq w$, because the entries of t do not move upwards during the process. This completes the proof. □

Remark. The process in the proof above bears resemblance to the widely used row insertion algorithm from the theory of tableaux (see Section 3.1 in [74]).

Proposition 7.6 $|V_\lambda| = |B_\lambda|$ *for all* $\lambda \vdash n$.

Proof. We proceed by induction on the number of boxes of the diagram λ. It is immediate that $|V_\lambda| = |B_\lambda|$, if $\lambda \vdash 1$ or $\lambda \vdash 2$.

Suppose that $|V_{\lambda'}| = |B_{\lambda'}|$ for all $\lambda' \vdash n$. Let $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n+1$. From λ we construct a diagram $\lambda^i \vdash n$ for each $1 \leq i \leq k$.

Let λ^i be the diagram obtained from λ by removing the highest inner corner which is located at, or under the i^{th} row. (The row index of the corner is $j \geq i$, and it is the smallest possible such index.) Clearly we obtain a diagram $\lambda^i \vdash n$.

We partition V_λ as

$$V_\lambda = V_0 \cup V_1 \cup \ldots \cup V_{k-1}, \tag{64}$$

where

$$V_i = \{u = (u_1, \ldots, u_{n+1}) \in V_\lambda : \; u_{n+1} = \alpha_i\}. \tag{65}$$

For $u = (u_1, \ldots, u_n) \in V_i$, the vector of the multiplicities of the α_j in $u_1, \ldots, u_n$, when arranged in a decreasing order, defines a partition of type λ^{i+1}. We have therefore $|V_i| = |V_{\lambda^{i+1}}|$ and

$$|V_\lambda| = \sum_{i=0}^{k-1} |V_i| = \sum_{i=1}^{k} |V_{\lambda^i}|. \tag{66}$$

We know that $\lambda^i \vdash n$, hence

$$|V_{\lambda^i}| = |B_{\lambda^i}| = |b_{\lambda^i}|, \tag{67}$$

for $1 \le i \le k$ by induction. Now

$$b_\lambda = \cup_{i=0}^{k-1} \{v \in b_\lambda : \; v_{n+1} = i\}, \tag{68}$$

where the sets on the right side are pairwise disjoint. It is therefore sufficient to prove that the projection map ϕ which sends a sequence $(v_1, \ldots, v_{n+1})$ to $(v_1, \ldots, v_n)$ gives a

$$\phi : \{v \in b_\lambda : \; v_{n+1} = i\} \to b_{\lambda^{i+1}}$$

bijection for $0 \le i \le k-1$. Indeed, then

$$|B_\lambda| = |b_\lambda| = \sum_{i=0}^{k-1} |\{v \in b_\lambda : \; v_{n+1} = i\}| = \sum_{i=1}^{k} |b_{\lambda^i}| = \sum_{i=1}^{k} |V_{\lambda^i}| = |V_\lambda|$$

by equations (66), (67), (68). The argument will be complete, if we prove the next statement:

Lemma 7.7 *ϕ is a bijection between the sets $\{v \in b_\lambda : \; v_{n+1} = i\}$ and $b_{\lambda^{i+1}}$ for $0 \le i \le k-1$.*

Proof. We observe first that ϕ is an injective map. Indeed, if $w, u \in \{v \in b_\lambda : \ v_{n+1} = i\}$ and $w \neq u$, then

$$\phi(w) = (w_1, \ldots, w_n) \neq (u_1, \ldots, u_n) = \phi(u).$$

The surjectivity of ϕ: first we prove that if $y = (y_1, y_2, \ldots, y_n) \in \mathrm{st}(\lambda^{i+1})$, then $v = (y_1, \ldots, y_n, i) \in b_\lambda$. Clearly then $\phi(v) = y$.

Let p be the node (the inner corner) of λ we removed to obtain λ^{i+1}. The row index j of p is at least $i+1$ by construction. Fill out λ according to the sequence $(y_1, y_2, \ldots, y_n, j-1)$. This gives a λ-tableau. Indeed the rows and columns are increasing in $\lambda^{i+1} \subseteq \lambda$, because y is a lattice permutation for λ^{i+1}. Moreover, in node p we have $n+1$. As p is an inner corner of λ, this element can not violate the ordering condition either.

We proved that $(y_1, \ldots, y_n, j-1) \in \mathrm{st}(\lambda)$, hence $(y_1, \ldots, y_n, j-1) \geq (y_1, \ldots, y_n, i) \in b_\lambda$. Obviously $\phi(y_1, \ldots, y_n, i) = y$. This proves that there exists a $v \in b_\lambda$ such that $\phi(v) = y$, whenever $y \in \mathrm{st}(\lambda^{i+1})$.

Now let $y \in b_{\lambda^{i+1}}$ be an arbitrary sequence. Then there exists $y' \in \mathrm{st}(\lambda^{i+1})$ such that $y \leq y'$. We know that there exists $v' \in b_\lambda$ such that $v'_{n+1} = i$, $\phi(v') = y'$. Let $v := (y, i) \in \mathbb{N}^{n+1}$. Then $v \in b_\lambda$, because $v = (y, i) \leq (y', i) = v' \in b_\lambda$. Clearly $v_{n+1} = i$ and $\phi(v) = y$. This proves that ϕ is surjective.

It remains to check that $\phi(v) \in b_{\lambda^{i+1}}$ when $v \in b_\lambda$, and $v_{n+1} = i$. Let $y := (v_1, \ldots, v_n) = \phi(v)$. There exists $v' \in \mathrm{st}(\lambda)$ such that $v \leq v'$.

As v' is a lattice permutation of type λ, we know that there exists an inner corner of λ in the $v'_{n+1} + 1^{st}$ row. From $i = v_{n+1} \leq v'_{n+1}$, we obtain $v'_{n+1} + 1 \geq j$, where j is the row index of the box we removed from λ to obtain λ^{i+1}. Let $z := (v'_1, \ldots, v'_n)$. Then z is a lattice permutation of type μ for some $\mu \vdash n$, because v' was a lattice permutation.

From the definition of μ and λ^{i+1} we see that either $\lambda^{i+1} = \mu$ or $|\lambda^{i+1} \setminus \mu| = |\mu \setminus \lambda^{i+1}| = 1$. If $\lambda^{i+1} = \mu$, then $b_{\lambda^{i+1}} = b_\mu$. If $|\lambda^{i+1} \setminus \mu| = |\mu \setminus \lambda^{i+1}| = 1$, then $v'_{n+1} + 1 > j$ and the node of $\lambda^{i+1} \setminus \mu$ is in the $v'_{n+1} + 1^{st}$ row, while the node of $\mu \setminus \lambda^{i+1}$ is in the j^{th} row, hence we can apply Lemma 7.5. We infer that $b_\mu \subseteq b_{\lambda^{i+1}}$. From $z \in \mathrm{st}(\mu) \subseteq b_\mu$, we obtain $z \in b_{\lambda^{i+1}}$. But $z \geq y = \phi(v)$, because $v' \geq v$, giving that $\phi(v) \in b_{\lambda^{i+1}}$. $\square$

7.5 The lex standard monomials of $I(V_\lambda)$

Theorem 7.8 $\mathrm{Sm}(\prec_{lex}, V_\lambda) = B_\lambda$, *where* $\mathbb{F}$ *is an arbitrary field and* λ *is an arbitrary partition of* n.

Proof. In the proof we use again the diagrams λ^i introduced in Proposition 7.6. Let $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n+1$ be a fixed partition. Let $1 \le i < j \le k$. Then from the definitions we see, that λ^i, $\lambda^j \vdash n$ are diagrams such that either $\lambda^i = \lambda^j$ or $|\lambda^i \setminus \lambda^j| = |\lambda^j \setminus \lambda^i| = 1$, and if the box of $\lambda^i \setminus \lambda^j$ is in the α^{th} row of λ^i and the box of $\lambda^j \setminus \lambda^i$ is in the β^{th} row of λ^j, then $\beta < \alpha$. We obtain that

$$B_{\lambda^j} \subseteq B_{\lambda^i} \tag{69}$$

by applying Lemma 7.5 with $\lambda = \lambda^i$ and $\mu = \lambda^j$.

We prove the Theorem by induction on the number n of boxes of the diagram λ, the case $n = 1$ being immediate.

Suppose that we have the claim for all $\lambda' \vdash n$. Let $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n+1$ be a partition. We consider again the decomposition

$$V_\lambda = V_0 \cup V_1 \cup \ldots \cup V_{k-1}, \tag{70}$$

where

$$V_i = \{u = (u_1, \ldots, u_{n+1}) \in V_\lambda : \; u_{n+1} = \alpha_i\}. \tag{71}$$

Clearly V_i is a set of points of type $V_{\lambda^{i+1}}$ (we use the suitable permutation of $\alpha_0, \ldots, \alpha_{k-1}$ to obtain V_i as a set of the form $V_{\lambda^{i+1}}$). We have $\lambda^i \vdash n$ for $1 \le i \le k$, hence by induction we have

$$\mathrm{Sm}(\prec_{lex}, V_{i-1}) = B_{\lambda^i}$$

for $1 \le i \le k$.

It is enough to prove that $b_\lambda \subseteq \mathrm{sm}(\prec_{lex}, V_\lambda)$, because

$$|b_\lambda| = |V_\lambda| = |\mathrm{sm}(\prec_{lex}, V_\lambda)|,$$

by Proposition 7.6 and (14). As before, $\phi : \mathbb{N}^{n+1} \to \mathbb{N}^n$ denotes the projection onto the first n components: $\phi(v_1, \ldots, v_{n+1}) := (v_1, \ldots, v_n)$.

Let $v = (v_1, \ldots, v_{n+1}) \in b_\lambda$ be arbitrary. Let $i := v_{n+1}$ and $w := \phi(v)$. We proved in Proposition 7.6 that $w = \phi(v) \in b_{\lambda^{i+1}}$. By (69) we have $w \in \cap_{j=1}^{i+1} b_{\lambda^j}$, hence $x^w \in \cap_{j=0}^{i} \mathrm{Sm}(\prec_{lex}, V_j)$ by induction. We intend to use the following simple criterion to show that $x^v \in \mathrm{Sm}(\prec_{lex}, V_\lambda)$:

Proposition 7.9 *Let I be a nonzero ideal of $\mathbb{F}[x_1, \ldots, x_m]$, $\prec$ a term order. Then for a monomial $z \in \mathbb{F}[x_1, \ldots, x_m]$ we have $z \notin \mathrm{Sm}(\prec, I)$ iff there exists a finite subset M of monomials $y \prec z$ and $\beta_y \in \mathbb{F}$ such that $z - \sum_{y \in M} \beta_y y \in I$.*

The argument below is an extension of an idea from the proof of Theorem 4.3 in [11]. Suppose for contradiction that $x^v \notin \mathrm{Sm}(\prec_{lex}, V_\lambda)$. Then by Proposition 7.9 there are $\beta_y \in \mathbb{F}$ such that

$$x^v - \sum_{y \prec_{lex} x^v} \beta_y y = 0,$$

as functions on V_λ. We group the terms of the above equation as follows

$$x^v = \sum_{y \prec_{lex} x^v} \beta_y y = \sum_{0 \leq \ell < i} \beta_\ell \cdot x^w \cdot x_{n+1}^\ell + \sum_{h:\ \phi(h) \prec_{lex} w} \beta_h x^h. \tag{72}$$

Here we relied on the following property of $\prec_{lex}$: for $u, u' \in \mathbb{N}^{n+1}$ we have $u \prec_{lex} u'$ iff $\phi(u) \prec_{lex} \phi(u')$ or $\phi(u) = \phi(u')$ and $u_{n+1} < u'_{n+1}$.

Substitute now $x_{n+1} := \alpha_j$ into (72) for $0 \leq j \leq i$. With suitable $\beta_{h,j} \in \mathbb{F}$ this gives equations of the form

$$x^w \cdot \alpha_j^i = x^w \cdot \sum_{0 \leq \ell < i} \beta_\ell \alpha_j^\ell + \sum_{h: \phi(h) \prec_{lex} w} \beta_{h,j} x^{\phi(h)}, \tag{73}$$

for $0 \leq j \leq i$, as functions on the set V_j. But $x^w \in \cap_{m=0}^i \mathrm{Sm}(\prec_{lex}, V_m)$, hence these equations can be valid only if

$$\alpha_j^i = \sum_{0 \leq \ell < i} \beta_\ell \alpha_j^\ell, \tag{74}$$

for $0 \leq j \leq i$. This holds, because otherwise for some j we could express x^w with $\prec_{lex}$-smaller monomials on V_j, which is impossible by Proposition 7.9. But from (74) we infer that the polynomial $t^i - \sum_{0 \leq \ell < i} \beta_\ell t^\ell$ has degree i, and has $i+1$ roots in the field $\mathbb{F}$, namely $\alpha_0, \alpha_1, \ldots, \alpha_i$. This contradiction proves that $x^v \in \mathrm{Sm}(\prec_{lex}, V_\lambda)$. □

7.6 The orthogonal complement of the Specht Module

We are in a position to show that $(S^\lambda)^\perp$ coincides with the image of $F(\leq m(\lambda)-1, V_\lambda)$ with respect to θ^λ.

Theorem 7.10 $P^{\lambda,\leq m(\lambda)-1} = (S^\lambda)^\perp$.

Proof. By Proposition 7.4 we have

$$P^{\lambda,\leq m(\lambda)-1} \leq (S^\lambda)^\perp,$$

hence it suffices to show that the two sides have the same dimension over $\mathbb{F}$. It is known (see Theorem 2.6.5 in [74]) that $\dim_{\mathbb{F}} S^\lambda = f^\lambda$, where f^λ is the number of standard λ-tableaux, hence

$$\dim_{\mathbb{F}} (S^\lambda)^\perp = \frac{n!}{\lambda!} - f^\lambda. \tag{75}$$

To conclude, we prove that

$$\dim_{\mathbb{F}} P^{\lambda,m(\lambda)-1} \geq \frac{n!}{\lambda!} - f^\lambda.$$

This will follow from

$$\dim_{\mathbb{F}} F(\leq m(\lambda)-1, V_\lambda) \geq \frac{n!}{\lambda!} - f^\lambda, \tag{76}$$

because $\theta^\lambda : F(\leq m(\lambda)-1, V_\lambda) \to P^{\lambda,\leq m(\lambda)-1}$ is an $\mathbb{F}$-linear isomorphism. But (76) is an immediate consequence of Theorem 7.8: B_λ contains $\frac{n!}{\lambda!} - f^\lambda$ monomials of degree at most $m(\lambda)-1$. These are lex standard monomials for V_λ, hence they induce linearly independent functions on V_λ. This verifies (76), and the Theorem follows. □

Corollary 7.11 *We have*

$$|\mathrm{Sm}(\prec_{deg}, V_\lambda) \cap \mathrm{Mon}(n, \leq m(\lambda)-1)| = \frac{n!}{\lambda!} - f^\lambda.$$

Proof. It is apparent from the proof of Theorem 7.10 that we have equality in (76). The statement then follows by (15). □

7.7 The deglex standard monomials of $I(V_\lambda)$

We can now easily prove the result of A. M. Garsia and C. Procesi [39] on the deglex standard monomials of $I(V_\lambda)$.

Theorem 7.12 $\mathrm{Sm}(\prec_{deg}, V_\lambda) = B_\lambda$ *holds for every field* $\mathbb{F}$ *and partition* $\lambda \vdash n$.

Proof. We have $\mathrm{Sm}(\prec_{lex}, V_\lambda) = B_\lambda$ by Theorem 7.8. It is enough now to verify that the conditions of Proposition 7.2 are satisfied with $\mathcal{F} = V_\lambda$ and $d = m(\lambda)$. Condition (a) is immediate, because by Theorem 7.8 we have

$$\mathrm{Sm}(\prec_{lex}, V_\lambda) \cap \mathrm{Mon}(n, m(\lambda)) = B_\lambda \cap \mathrm{Mon}(n, m(\lambda)) = \mathrm{St}(\lambda),$$

and $\mathrm{St}(\lambda)^{\leq} = B_\lambda = \mathrm{Sm}(\prec_{lex}, V_\lambda)$.

As for condition (b), we have

$$|\mathrm{Sm}(\prec_{lex}, V_\lambda) \cap \mathrm{Mon}(n, \leq m(\lambda) - 1)| = \frac{n!}{\lambda!} - f^\lambda$$

by Theorem 7.8. Moreover, Corollary 7.11 gives that

$$|\mathrm{Sm}(\prec_{deg}, V_\lambda) \cap \mathrm{Mon}(n, \leq m(\lambda) - 1)| = \frac{n!}{\lambda!} - f^\lambda.$$

This finishes the proof. □

The knowledge of deglex standard monomials for V_λ provides a combinatorial description of the Hilbert function of $S/I(V_\lambda)$.

Corollary 7.13 $h_{V_\lambda}(m) = |B_\lambda \cap \mathrm{Mon}(n, \leq m)|$ *if* $m \geq 0$.

Proof. From (15) and Theorem 7.12 we have

$$h_{V_\lambda}(m) = |\mathrm{Sm}(\prec_{deg}, V_\lambda) \cap \mathrm{Mon}(n, \leq m)| = |B_\lambda \cap \mathrm{Mon}(n, \leq m)|.$$

□

Theorem 7.12 allows us to exhibit a nice basis of $(S^\lambda)^\perp$.

Corollary 7.14 $\{\sum_{v\in V_\lambda} y(v)\cdot x^{t^\lambda(v)} :\ y \in B_\lambda \cap \mathrm{Mon}(n, \leq m(\lambda)-1)\}$ *is a basis over* $\mathbb{F}$ *of the linear space* $(S^\lambda)^\perp \leq P^\lambda$.

Proof. We know that $\theta^\lambda : F(V_\lambda) \to P^\lambda$ is a linear isomorphism. Using that

$$(S^\lambda)^\perp = P^{\lambda, \leq m(\lambda)-1} = \theta^\lambda(F(\leq m(\lambda)-1, V_\lambda)),$$

and that $B_\lambda \cap \mathrm{Mon}(n, \leq m(\lambda)-1)$ is a basis of the $\mathbb{F}$-space $F(\leq m(\lambda)-1, V_\lambda)$, we obtain that $\{\theta^\lambda(y) :\ y \in B^\lambda \cap \mathrm{Mon}(n, \leq m(\lambda)-1)\}$ is a basis of the $\mathbb{F}$-space $(S^\lambda)^\perp$. □

In a similar fashion, we obtain a basis for the dual of S^λ:

Corollary 7.15 *The (image of the) set* $\{\theta^\lambda(w) :\ w \in \mathrm{St}(\lambda)\}$ *is a basis of the vector space* $P^\lambda/(S^\lambda)^\perp$.

Proof. $\theta^\lambda : F(V_\lambda) \to P^\lambda$ is an $\mathbb{F}$-linear isomorphism. B_λ is a basis of $F(V_\lambda)$, hence $B' = \{\theta^\lambda(w) :\ w \in B_\lambda\}$ is a basis of P^λ. By Corollary 7.14 $B'' := \{\theta^\lambda(w) :\ w \in B_\lambda \setminus \mathrm{St}(\lambda)\}$ is a basis of $(S^\lambda)^\perp$. It follows that $B' \setminus B''$ is mapped to a basis at the canonical map $P^\lambda \to P^\lambda/(S^\lambda)^\perp$. □

The inductive combinatorial description for b_λ, provided by Lemma 7.7, leads to a polynomial time algorithm to recognise the standard monomials of V_λ.

Corollary 7.16 *Let a partition* $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n$ *and a monomial* x^u *with exponent vector* $u = (u_1, \ldots, u_n)$ *be given as input. Then in time* $O(n^2 + \sum_{i=1}^n \log_2(1+u_i))$ *we can check if* $x^u \in B_\lambda$.

Proof. For $n = 1$ we check if $u_1 = 0$. Suppose now that $n > 1$. If $u_n > k-1$, then obviously $x^u \notin B_\lambda$. Else by Lemma 7.7 we have $x^u \in B_\lambda$ if and only if $x^{\phi(u)} \in B_{\lambda^{i+1}}$, where $\phi(u) = (u_1, \ldots, u_{n-1})$, and $i = u_n$. We thus reduce the problem to a partition having $n-1$ boxes. The cost of this reduction is $O(n + \log_2(1+u_n))$, the time needed for the comparison of u_n and $k-1$, and the generation of λ^{i+1} from λ. The statement follows by induction on n. □

8 Concluding remarks

In this thesis we have presented a complete description of the reduced Gröbner bases of the complete ℓ-wide families $\mathcal{F}^{k,l}$. We have provided new applications of this description: we computed the rank of the inclusion matrices $I(\mathcal{F}^{k,l}, \binom{[n]}{\leq t})$ and a simple proof of a special case of Frankl's conjecture.

It would be desirable to obtain similar results for other families $\mathcal{F} \subseteq 2^{[n]}$, with possible applications to inclusion matrices and to the complexity of Boolean functions (see [19] for the latter). In particular, Gröbner bases for symmetric families (i.e., which are invariant under the action of the symmetric group on $[n]$) would be of interest.

Aigner [2] gave a remarkable explicit decomposition of $2^{[n]}$ into symmetric chains. The bottommost elements of the chains are exactly the sets $U \subseteq [n]$ for which $x_U \in \mathcal{M}_{\lfloor n/2 \rfloor}$, the set of standard monomials for $\binom{[n]}{\lfloor n/2 \rfloor}$. It would perhaps be interesting to obtain an algebraic explanation of the results in [2].

One might be interested in solving via Gröbner bases the following q-analog of Wilson's theorem: consider the incidence matrix formed by the k– and the l-dimensional subspaces of a t-dimensional vector space over the finite field $\mathbb{F}_q$. Then the rank of this matrix has been known over the rationals $\mathbb{Q}$ since Kantor [60]. Frumkin and Yakir in [37] gave a rank formula for primes not dividing q, their result is in fact analogous to Wilson's rank formula. But the answer is still open for the p prime, where $q = p^\alpha$, $\alpha \geq 1$.

In this thesis we gave an upper bound on the rank of inclusion matrices $I(\mathcal{F}(k,q), \binom{[n]}{\leq \ell})$ over $\mathbb{F}_p$, where $0 \leq \ell \leq q-1$. In fact, for n sufficiently large, we determined the rank precisely. It would be interesting to describe the set of standard monomials $\mathrm{Sm}(\prec, \mathcal{F}(k,q), \mathbb{F}_p)$ with respect to any term order $\prec$ in a fashion similar to the uniform case given in [47]. This could give bounds on the rank of inclusion matrices $I(\mathcal{F}(k,q), \binom{[n]}{\leq \ell})$ over $\mathbb{F}_p$, where $\ell > q-1$.

We determined also the lex and the deglex standard monomials of the ideal $I(V_\lambda)$. It would be desirable to extend these results to other interesting term orders $\prec$.

We propose the following

Conjecture 3 *Let $\prec$ be an arbitrary term-order with $x_1 \succ x_2 \succ \ldots \succ x_n$ and $\mathbb{F}$ be an arbitrary field. Then*

$$\mathrm{Sm}(\prec, V_\lambda) = B_\lambda.$$

Further work to be done includes a determination the initial ideals and the (reduced) Gröbner bases of the ideals $I(V_\lambda)$.

The Hall map [59, Section 5.1.1.] is a useful and simple bijection between permutations and Artin monomials (i.e. the monomials $\{x_1^{b_1} \dots x_n^{b_n} : 0 \leq b_i \leq i-1$ for each $1 \leq i \leq n\}$). Do there exist such simple bijections $\phi^\lambda : V_\lambda \to B_\lambda$ for partitions λ, other than (1^n)?

Finally we suggest another possible extension of the results of [46]. Let $\alpha_1, \dots, \alpha_n$ be n different elements of $\mathbb{F}$ and let $G \leq S_n$ be a fixed subgroup of S_n. We put

$$V_G = V_G(\alpha_1, \dots, \alpha_n) = \{(\alpha_{\pi(1)}, \dots, \alpha_{\pi(n)}) : \ \pi \in G\} \subseteq \mathbb{F}^n.$$

It would be interesting to relate the standard monomials of the group theoretic ideal $I(V_G)$ to the representation theory of G.

Acknowledgements

I am most grateful to my teacher, Lajos Rónyai, who taught me so much and guided my research with care and love.

I am indebted to Alex Küronya for introducing me to the theory of tableaux.

References

[1] W. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases,* American Mathematical Society, 1994.

[2] M. Aigner, Lexicographic matching in Boolean algebras; *Journal of Combinatorial Theory, Ser. B,* **14** (1973), 187–194.

[3] R.E.L. Aldred and R.P. Anstee, On the Density of Sets of Divisors, *Discrete Math.* **137** (1995), 345-349.

[4] N. Alon, Combinatorial Nullstellensatz, *Combin. Probability and Computing* **8** (1999), 7–29.

[5] N. Alon, L. Babai, H. Suzuki, Multilinear polynomials and Frankl–Ray-Chaudhuri–Wilson type intersections theorems, *J. Combin. Theory A* **58** (1991), 165–180.

[6] N. Alon, S. Friedland, G. Kalai, Regular subgraphs of almost regular graphs, *Journal of Combinatorial Theory, Ser. B,* **37** (1984), 79–91.

[7] N. Alon, Z. Füredi, Covering the cube by affine hyperplanes, *European J. Combinatorics* **14** (1993), 79–83.

[8] N. Alon, M. B. Nathanson, I. Z. Ruzsa, The polynomial method and restricted sums of congruence classes, *J. Number Theory* **56** (1996), 404–417.

[9] N. Alon, M. Tarsi, A nowhere-zero point in linear mappings, *Combinatorica* **9** (1989), 393–395.

[10] N. Alon, M. Tarsi, Colorings and orientations of graphs, *Combinatorica* **12** (1992), 125–134.

[11] R.P. Anstee, L. Rónyai, A. Sali, Shattering news, *Graphs and Combinatorics* **18** (2002), 59–73.

[12] R.P. Anstee and A. Sali, Sperner Families of Bounded VC-dimension, *Discrete Math.* **175** (1997), 13-21.

[13] E. Artin, *Galois theory,* University of Notre Dame, 1942.

[14] L. Babai, A short proof of the non-uniform Ray-Chaudhuri–Wilson inequality, *Combinatorica* **8** (1988), 122-135.

[15] D. A. Barrington, R. Beigel, S. Rudich, *Representing boolean functions modulo composite numbers,* in Proc. 24^{th} Annual ACM Symposium on Theory of Computing, Victoria, BC, Canada, 1992, pp. 455–461.

[16] L. Babai, P. Frankl, *Linear algebra methods in combinatorics,* September 1992.

[17] T. Becker, V. Weispfenning, *Gröbner bases - a computational approach to commutative algebra,* Springer-Verlag, Berlin, Heidelberg, 1993.

[18] S. Bell, J. Siemens, P. Jones, On modular homology in the Boolean algebra II, *J. of Algebra* **199** (1998) 556–580.

[19] A. Bernasconi, L. Egidi, Hilbert function and complexity lower bounds for symmetric Boolean functions, *Information and Computation* **153**(1999), 1–25.

[20] T. Bier, Remarks on recent formulas of Wilson and Frankl, *Europ. J. Combin.* **14**(1993), 1–8.

[21] A. Blockhuis, A new upper bound for the cardinality of 2-distance sets in Euclidean space, *Eindhoven Univ. Technology Mem.* 1981–04.

[22] A. Blockhuis, Few distance sets, *C. W. I. Tracts* No. **7**, (1984) Mathematisch Centrum, Amsterdam.

[23] B. Buchberger, An algorithmic criterion for the solvability of algebraic systems of equations, *Aequationes Math.* **4** (1970), 374–383.

[24] B. Buchberger, A theoretical basis for the reduction of polynomials to canonical forms, *ACM SIGSAM Bull.* **39** (1976), 19–29.

[25] B. Buchberger, H. M. Möller, The construction of multivariate polynomials with preassigned zeros, *Comp. algebra*, EUROCAM '82, 24-31, Lecture Notes in Comput. Sci., **144**, Springer-Verlag, 1982

[26] A. M. Cohen, H. Cuypers, H. Sterk (eds.), *Some Tapas of Computer Algebra,* Springer-Verlag, Berlin, Heidelberg, 1999.

[27] L. Clark, An asymptotic expansion for the number of permutations with a certain number of inversions. *Electron. J. Combin.* **7**, (2000), no. 1, Research Paper 50, 5 pp. (electronic).

[28] D. Cox, J. Little, D. O'Shea, *Ideals, varieties, and algorithms,* Springer-Verlag, Berlin, Heidelberg, 1992.

[29] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Graduate Text in Mathematics **150**, Springer-Verlag, 1995.

[30] J. A. Dias da Silva, Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26**, 140–146

[31] J. Farr, D. Gao, Computing Gröbner bases for vanishing ideals of finite sets of points, manuscript

[32] P. Frankl, Traces of antichains, *Graphs Combin.* **5** (1989), 295-299.

[33] P. Frankl, Intersection theorems and mod p rank of inclusion matrices, *J. Combin. Theory A* **54**(1990), 85–94.

[34] P. Frankl and J. Pach, On disjointly representable sets, *Combinatorica* **4** (1984), 39-45.

[35] P. Frankl, R. M. Wilson, Intersection theorems with geometric consequences, *Combinatorica* **1** (1981), 357–368.

[36] K. Friedl, L. Rónyai, Order-shattering and Wilson's theorem, *Discrete Mathematics,* **270** (2003), 127–136..

[37] A. Frumkin, A. Yakir, Rank of inclusion matrices and modular representation theory, *Israel Journal of Math.* **71** (1990), 309–320.

[38] A. M. Garsia, Pebbles and expansions in the polynomial ring, *Polynomial identities and combinatorial methods (Pantelleria 2001)*, 261–285, Lecture Notes in Pure and Appl. Math., 235, Dekker, New York, 2003.

[39] A. M. Garsia, C. Procesi, On certain graded S_n-modules and the q-Kostka polynomials, *Advances in Mathematics,* **94** (1992), 82–138.

[40] A. M. Garsia, N. Wallach, Qsym over Sym is free, *J. Combin. Theory Ser. A* **104** (2003), no. 2, 217–263.

[41] C. D. Godsil, Problems in algebraic combinatorics, *The Electronic Journal of Comb.*, **2**, (1995), 1-20.

[42] R.L. Graham, D.E. Knuth, O. Patashnik, *Concrete Mathematics,* Addison-Wesley, 1989.

[43] M. Haiman, Commutative algebra of n points in the plane, manuscript

[44] M. Hall, Combinatorial Theory, Blaisdell, Waltham, Mass., 1967.

[45] J. Harris, *Algebraic geometry. A first course.* Graduate Texts in Mathematics **133**, Springer-Verlag, 1992.

[46] G. Hegedűs, A. Nagy, L. Rónyai, Gröbner bases for permutati‘ons and oriented trees, *Annales Univ. Sci. Budapest*, Sect. Comp. 23 (2004), 137–148.

[47] G. Hegedűs, L. Rónyai, Gröbner bases for complete uniform families, *J. of Algebraic Combinatorics* **17** (2003), 171–180.

[48] 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.

[49] G. Hegedűs, L. Rónyai, Gröbner bases for complete ℓ-wide families, manuscript

[50] G. Hegedűs, L. Rónyai, Standard monomials for partitions, submitted to the Acta Math. Hungarica

[51] H. Hironaka, Resolution of singularities of an algebraic variety over a field of characteristic zero, I, II. *Ann. of Math. (2)* **79** (1964), 109–203, ibid. (2) **79** (1964) 205–326.

[52] D. Hilbert, Über die Theorie der algebraischen Formen, *Math. Annalen* **36** (1890), 473–534. Reprinted in Gesammelte Abhandlungen Volume II, Chelsea, New York, 1965.

[53] G. D. James, A Characteristic-Free Approach to the Representation Theory of S_n, *Journal of Algebra,* **46** *(1977), 430–450.*

[54] G. D. James, *The Representation Theory of the Symmetric Groups,* Springer Lecture Notes in Mathematics 682, Springer-Verlag, 1978.

[55] G. D. James, The Module Orthogonal to the Specht Module, *Journal of Algebra,* **46***(1977), 451–456.*

[56] G. D. James, A. Kerber, *The Representation Theory of the Symmetric Group,*, Encyclopedia of Mathematics and its Applications, Vol. 16, Addison-Wesley Publishing Co., 1981.

[57] P. Jones, J. Siemens, On modular homology of the Boolean algebra III, submitted to J. of Algebra

[58] A. E. Kézdy, H. S. Snevily, Polynomials that Vanish on Distinct nth Roots of Unity, *Combin. Probability and Computing* **13** (2004), 37–59.

[59] D. E, Knuth, *The art of computer programming, Volume 3, Sorting and searching,* Addison-Wesley, 1973.

[60] W. Kantor, On incidence matrices of finite projective and affine spaces, *Math. Z.*, **124** (1972) 315–318.

[61] T. H. Koornwinder, A note on the absolute bound for systems of lines, *Proc. Konink. Nederl. Akad. Wet. Ser. A* **79** (1976), 152–153.

[62] D. G. Larman, C. A. Rogers, J. J. Seidel, On two-distance sets in Euclidean space, *Bull. London Math. soc.* **9** (1977), 261–267.

[63] F. S. Macaulay, Some properties of enumeration in the theory of modular systems, *Proc. London Math. Soc.* **26** (1927) 531–555.

[64] I. G. Macdonald, *Symmetric functions and Hall polynomials,* Clarendon Press, Oxford, 1979.

[65] B. H. Margolius, Permutations with inversions. *Journal of Integer Sequences* **4**, (2001), no. 2, Article 01.2.4, 13 pp. (electronic).

[66] V. B. Mnulkin, I. J. Siemens, On the modular homology in the Boolean Algebra, *Jour. of Algebra* **179** (1996) 191–199.

[67] G. Mohanty, *Lattice path counting and Applications*, Academic Press, 1979.

[68] T. Mora, L. Robbiano, Points in affine and projective spaces, in Computational Algebraic Geometry and Commutative Algebra, Cambridge Press, 1994.

[69] T. Mora, M. Sala, On the Groebner bases of some symmetric systems and their applications to Coding Theory, submitted to J. of Alg. Combin.

[70] A. Pajor, Sous-espaces 2_1^n des espaces de Banach, Travaux en Cours, Hermann, Paris, 1985

[71] L. Robbiano, On the theory of graded structures, *J. Symbolic Comput. 2* **2** (1986), 139–170.

[72] J. Riordan, Combinatorial Identities, John Wiley and Sons, New York, 1968

[73] D. K. Ray-Chaudhuri, R. M. Wilson, On t-designs, *Osaka J. Math.* **12** (1975), 737–744.

[74] B. E. Sagan, *The symmetric group, representations, combinatorial algorithms, and symmetric functions,* GTM 203, Springer-Verlag, Berlin, Heidelberg, 2001.

[75] N. Sauer, On the Density of Families of Sets, *J. Combin. Th. A* **13** (1972), 145-147.

[76] S. Shelah, A Combinatorial Problem: Stability and Order for Models and Theories in Infinitary Language, *Pac. J. Math.* **41** (1972), 247-261.

[77] R. Smolensky, On representations by low-degree polynomials, *Proc. of the 34th IEEE Symposium on the Foundations of Computer Science,* 1993, pp. 130–138.

[78] V.N. Vapnik and A.Ya. Chervonenkis, On the Uniform Convergence of Relative Frequencies of Events to their Probabilities, *Theory Prob. Applics.* **16** (1971), 264-280.

[79] R. M. Wilson, A diagonal form for the incidence matrices of t-subsets vs. k-subsets, *European Journal of Combinatorics* **11**(1990), 609–615.

[80] T. Tanisaki, Defining ideals of the closures of conjugacy classes and representations of the Weyl groups, *Tôhoku Math. J.* **34** (1982), 575–585.