Some meeting points of Gröbner bases and combinatorics

Bálint Felszeghy and Lajos Rónyai

Computer and Automation Institute, Hungarian Academy of Science and
Institute of Mathematics, Budapest University of Technology and Economics
fbalint@math.bme.hu, lajos@ilab.sztaki.hu

Summary. Let $\mathbb{F}$ be a field, $V \subseteq \mathbb{F}^n$ be a set of points, and denote by $I(V)$ the vanishing ideal of V in the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$. Several interesting algebraic and combinatorial problems can be formulated in terms of some finite V, and then Gröbner bases and standard monomials of $I(V)$ yield a powerful tool for solving them.

We present the Lex Game method, which allows one to efficiently compute the lexicographic standard monomials of $I(V)$ for any finite set $V \subseteq \mathbb{F}^n$. We apply this method to determine the Gröbner basis of $I(V)$ for some V of combinatorial and algebraic interest, and present four applications of this type. We give a new easy proof of a theorem of Garsia on a generalization of the fundamental theorem of symmetric polynomials. We also reprove Wilson's theorem concerning the modulo p rank of some inclusion matrices. By examining the Gröbner basis of the vanishing ideal of characteristic vectors of some specific set systems, we obtain results in extremal combinatorics. Finally, we point out a connection among the standard monomials of $I(V)$ and $I(V^c)$, where $V \subseteq \{0,1\}^n$ and $V^c = \{0,1\}^n \setminus V$. This has immediate consequences in combinatorial complexity theory.

The main results have appeared elsewhere in several papers. We collected them into a unified account to demonstrate the usefulness of Gröbner basis methods in combinatorial settings.

Key words: Gröbner basis, standard monomial, lexicographic order, vanishing ideal, Hilbert function, inclusion matrix, rank formula

---

Part of this work was done during the Special Semester on Gröbner Bases (February 1 - July 31, 2006), organized by RICAM, Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz, Austria. The authors are pleased to acknowledge Prof. Bruno Buchberger and the coordinators of the Special Semester for their hospitality and attention to this project.
Research supported in part by OTKA grants NK72845 and NK63066.

1 Introduction

Throughout the paper n will be a positive integer, and $[n]$ stands for the set $\{1, 2, \ldots, n\}$. The set of all subsets of $[n]$ is denoted by $2^{[n]}$. Subsets of $2^{[n]}$ are called *set families* or *set systems*. Let $\binom{[n]}{m}$ denote the family of all m-*subsets* of $[n]$ (subsets which have cardinality m), and $\binom{[n]}{\leq m}$ is the family of those subsets that have at most m elements. By $\mathbb{N}$ we mean the nonnegative integers, $\mathbb{Z}$ is the set of integers, $\mathbb{Q}$ is the field of rational numbers, and $\mathbb{F}_p$ is the field of p elements, where p is a prime.

Let $\mathbb{F}$ be a field. As usual, we denote by $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[\mathbf{x}]$ the ring of polynomials in variables $x_1, \ldots, x_n$ over $\mathbb{F}$. To shorten our notation, we write $f(\mathbf{x})$ for $f(x_1, \ldots, x_n)$. Vectors of length n are denoted by boldface letters, for example $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}^n$. If $\mathbf{w} \in \mathbb{N}^n$, we write $\mathbf{x}^{\mathbf{w}}$ for $x_1^{w_1} \ldots x_n^{w_n} \in \mathbb{F}[\mathbf{x}]$. For a subset $M \subseteq [n]$, the monomial x_M is $\prod_{i \in M} x_i$ (and $x_\emptyset = 1$). We say that a polynomial is *multilinear* if it is a linear combination of some x_M ($M \subseteq [n]$).

Suppose that $V \subseteq \mathbb{F}^n$. Then the *vanishing ideal* $I(V)$ *of* V consists of polynomials in $\mathbb{F}[\mathbf{x}]$, which as functions vanish on V. In our applications, we consider finite sets V, and use the Gröbner bases, or standard monomials of $I(V)$ (see the next subsection for the definitions) to prove claims on V.

Let $\mathbf{v}_F \in \{0,1\}^n$ denote the *characteristic vector of a set* $F \subseteq [n]$, that is the ith coordinate of $\mathbf{v}_F$ is 1 iff $i \in F$. For a system of sets $\mathcal{F} \subseteq 2^{[n]}$, let us put $V_{\mathcal{F}}$ for the set of the characteristic vectors of elements of $\mathcal{F}$. By $I(\mathcal{F})$ we understand the vanishing ideal $I(V_{\mathcal{F}})$, as it will make no confusion.

In Section 2 we collected the definitions and basic facts we need about Gröbner bases and Hilbert functions.

We develop a combinatorial description of the lexicographic standard monomials of $I(V)$ in the subsequent Section via a two player game. Lea and Stan play the Lex Game with some fixed parameters $V \subseteq \mathbb{F}^n$ and $\mathbf{w} \in \mathbb{N}^n$. We show that $\mathbf{x}^{\mathbf{w}}$ is a lexicographic standard monomial of $I(V)$ if and only if Stan has a winning strategy in the game. This description proves to be more then just a toy. It yields a fast algorithm to determine the standard monomials of $I(V)$ for an arbitrary finite V. On the other hand, it is also applicable in the 'symbolic' computation of the standard monomials for some particular sets V. We shall see several examples of such calculations in Section 4, which is devoted to combinatorial and algebraic applications.

We give a new easy proof of a theorem of Garsia on a generalization of the fundamental theorem of symmetric polynomials. We also reprove Wilson's theorem concerning the modulo p rank of some inclusion matrices. In the direction of extremal combinatorics, we obtain results on the maximal cardinality of some set systems. To be a bit more specific, we will consider modulo q L-avoiding L-intersecting families, and families that do not shatter large sets. The last application is to point out a connection among the standard monomials and Hilbert functions of $I(V)$ and $I(V^c)$, where $V \subseteq \{0,1\}^n$

and $V^c = \{0,1\}^n \setminus V$. An immediate consequence of this in combinatorial complexity theory is shown.

Much of the results described here have already appeared elsewhere, most notably in [FRR06], [HNR04], [FR03], [FHR1], [FHR2], and [PR]. In some cases the way of exposition, which is based primarily on the Lex Game, is new and considerably simpler than the original one. We collected the material to point out interesting combinatorial applications of Gröbner basis methods.

2 Preliminaries

2.1 Gröbner bases and standard monomials

We recall now some basic facts concerning Gröbner bases in polynomial rings over fields. More detailed exposition can be found in the classic papers by prof. Bruno Buchberger [B65], [B70], [B85], and in the textbook [CLO92].

A total order $\prec$ on the monomials composed from variables $x_1, x_2, \ldots, x_n$ is a *term order*, if 1 is the minimal element of $\prec$, and $\prec$ is compatible with multiplication with monomials. Two important term orders are the *lexicographic* (*lex* for short) and the *degree compatible lexicographic* (*deglex*) orders. We have $\mathbf{x^w} \prec_{\text{lex}} \mathbf{x^u}$ if and only if $w_i < u_i$ holds for the smallest index i such that $w_i \neq u_i$. As for deglex, we have that a monomial of smaller degree is smaller in deglex, and among monomials of the same degree lex decides the order. Also in general, $\prec$ is *degree compatible*, if $\deg(\mathbf{x^w}) < \deg(\mathbf{x^u})$ implies $\mathbf{x^w} \prec \mathbf{x^u}$.

The *leading monomial* (or *leading term*) $\mathrm{lm}(f)$ of a nonzero polynomial $f \in \mathbb{F}[\mathbf{x}]$ is the largest monomial (with respect to $\prec$) which appears with nonzero coefficient in f, when written as the usual linear combination of monomials. It is easy to verify that the leading monomial of a product $f \cdot g$ of nonzero polynomials is $\mathrm{lm}(f) \cdot \mathrm{lm}(g)$. We denote the set of all leading monomials of polynomials of a given ideal $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ by $\mathrm{Lm}(I) = \{\mathrm{lm}(f) : f \in I\}$, and we simply call them the *leading monomials of* I.

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

Obviously, $\mathrm{Sm}(I)$ is a *downset* with respect to division, that is, a divisor of a standard monomial is again in $\mathrm{Sm}(I)$.

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 $\mathrm{lm}(f)$.

Using that $\prec$ is a well founded order, it follows that G is actually a basis of I, that is, G generates I as an ideal of $\mathbb{F}[\mathbf{x}]$. It is a fundamental fact that every nonzero ideal I of $\mathbb{F}[\mathbf{x}]$ has a Gröbner basis.

A Gröbner basis $G \subseteq I$ is *reduced* if for all $g \in G$, the *leading coefficient* of g (i.e. the coefficient of $\mathrm{lm}(g)$) is 1, and $g \neq h \in G$ implies that no nonzero

monomial in g is divisible by $\mathrm{lm}(h)$. This is clearly equivalent to saying that every $g \in G$ has leading coefficient 1, $\{\mathrm{lm}(g) : g \in G\}$ is the set of minimal elements of $\mathrm{Lm}(I)$ (with respect to division), and the polynomial $g - \mathrm{lm}(g)$ is a linear combination of standard monomials. For any fixed term order and any nonzero ideal of $\mathbb{F}[\mathbf{x}]$ there exists a unique reduced Gröbner basis.

Suppose that $f \in \mathbb{F}[\mathbf{x}]$ contains a monomial $\mathbf{x}^{\mathbf{w}} \cdot \mathrm{lm}(g)$, where g is some other polynomial with leading coefficient c. Then we can *reduce f with g* (and get $\hat{f}$), that is, we can replace $\mathbf{x}^{\mathbf{w}} \cdot \mathrm{lm}(g)$ in f with $\mathbf{x}^{\mathbf{w}} \cdot \left(\mathrm{lm}(g) - \frac{1}{c}g\right)$. Clearly if $g \in I$, then f and $\hat{f}$ represent the same coset in $\mathbb{F}[\mathbf{x}]/I$. Also note that $\mathrm{lm}\left(\mathbf{x}^{\mathbf{w}} \cdot \left(\mathrm{lm}(g) - \frac{1}{c}g\right)\right) \prec \mathbf{x}^{\mathbf{w}} \cdot \mathrm{lm}(g)$. As $\prec$ is a well founded order, this guarantees that if we reduce f repeatedly with a set of polynomials G, then we end up with a *reduced* $\hat{f}$ in finitely many steps, that is a polynomial such that none of its monomials is divisible by any $\mathrm{lm}(g)$ $(g \in G)$.

Assume now that G is a Gröbner basis of some ideal I. In this case, it can be shown that the reduction of any polynomial with G is unique. We see from the definitions that the reduction $\hat{f}$ of a polynomial f is a linear combination of standard monomials of I. From these, it follows directly that for a nonzero ideal I the set $\mathrm{Sm}(I)$ is a linear basis of the $\mathbb{F}$-vectorspace $\mathbb{F}[\mathbf{x}]/I$. If $I(V)$ is a vanishing ideal of a finite set V of points in $\mathbb{F}^n$, then $\mathbb{F}[\mathbf{x}]/I(V)$ can be interpreted as the space of functions $V \to \mathbb{F}$. An immediate consequence is that the number of standard monomials of $I(V)$ is $|V|$. In particular for every family of sets we have $|\mathcal{F}| = |\mathrm{Sm}(I(\mathcal{F}))|$.

Another property of the standard monomials of $I(\mathcal{F})$ will be needed several times: for an arbitrary set family $\mathcal{F}$, one has $x_i^2 - x_i \in I(\mathcal{F})$, therefore all the elements of $\mathrm{Sm}(I(\mathcal{F}))$ are multilinear monomials.

2.2 The Hilbert function

We write $\mathbb{F}[\mathbf{x}]_{\leq m}$ for the vector space of polynomials over $\mathbb{F}$ with degree at most m. Similarly, if $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ is an ideal then $I_{\leq m} = I \cap \mathbb{F}[\mathbf{x}]_{\leq m}$ stands for the linear subspace of polynomials from I with degree at most m. The *Hilbert function* of the $\mathbb{F}$-algebra $\mathbb{F}[\mathbf{x}]/I$ is $H_I : \mathbb{N} \to \mathbb{N}$, where

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

Let $\prec$ be any degree compatible term ordering (deglex for instance). One can easily see that the set of standard monomials with respect to $\prec$ of degree at most m forms a linear basis of $\mathbb{F}[\mathbf{x}]_{\leq m}/I_{\leq m}$. Hence we can obtain $H_I(m)$ by determining the set $\mathrm{Sm}(I)$ with respect to any degree compatible term ordering.

When $\mathcal{F}$ is a system of sets, we call $H_{I(\mathcal{F})}(m)$ the Hilbert function of $\mathcal{F}$ and denote it by $H_{\mathcal{F}}(m)$, as it makes no confusion. In the combinatorial literature $H_{\mathcal{F}}(m)$ is usually given in terms of inclusion matrices.

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

It is a simple matter to verify that the Hilbert function of $\mathcal{F}$ is given by

$$H_{\mathcal{F}}(m) = \dim_{\mathbb{F}} \left(\mathbb{F}[\mathbf{x}]_{\leq m} \big/ I(\mathcal{F})_{\leq m} \right) = \operatorname{rank}_{\mathbb{F}} I\left(\mathcal{F}, \binom{[n]}{\leq m}\right). \tag{1}$$

We will benefit from a similar statement in Subsection 4.2, which claims that

$$\dim_{\mathbb{F}} \left(\mathcal{P}_{\mathcal{F},m} \right) = \operatorname{rank}_{\mathbb{F}} I\left(\mathcal{F}, \binom{[n]}{m}\right), \tag{2}$$

where $\mathcal{P}_{\mathcal{F},m}$ is the linear space of functions from $V_{\mathcal{F}}$ to $\mathbb{F}$ which can be represented as homogeneous multilinear polynomials of degree m. (With a slight abuse of notation we could have written $\mathcal{P}_{\mathcal{F},m} = \mathbb{F}[\mathbf{x}]_{=m} \big/ I(\mathcal{F})_{=m}$.)

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

3 Computation of the lex standard monomials

In this section we sketch a purely combinatorial description of the lexicographic standard monomials of vanishing ideals of finite sets of points. This is the main tool which can be applied to compute lex standard monomials of sets of combinatorial interest. The original source is [FRR06], and the interested reader can find an extension to general zero dimensional ideals in [FB06].

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

As before, let $\mathbb{F}$ be a field, $V \subseteq \mathbb{F}^n$ a finite set and $\mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{N}^n$ an n dimensional vector of natural numbers. With these data fixed, we define the Lex Game $\operatorname{Lex}(V; \mathbf{w})$, which is played by two persons, Lea and Stan. Both Lea and Stan know V and $\mathbf{w}$.

1 Lea chooses w_n elements of $\mathbb{F}$.
  Stan picks a value $y_n \in \mathbb{F}$, different from Lea's choices.
2 Lea now chooses w_{n-1} elements of $\mathbb{F}$.
  Stan picks a $y_{n-1} \in \mathbb{F}$, different from Lea's (last w_{n-1}) choices.
... (The game goes on in this same fashion.)
n Lea chooses w_1 elements of $\mathbb{F}$.
  Stan finally picks a $y_1 \in \mathbb{F}$, different from Lea's (last w_1) choices.

The winner is Stan if he could pick $\mathbf{y} = (y_1, \ldots, y_n)$ such that $\mathbf{y} \in V$, otherwise Lea wins the game. (Also, if in any step there is no proper choice y_i for Stan, then Lea wins.)

Example 1. Let $n = 5$, and $\alpha, \beta \in \mathbb{F}$ be different elements. Let V be the set of all α-β sequences in $\mathbb{F}^5$ in which the number of the α coordinates is 1, 2 or 3. We claim that Lea can win with the question vector $\mathbf{w} = (11100)$, but with $\mathbf{w} = (01110)$ Stan has a chance to win.

Indeed, let $\mathbf{w} = (11100)$. To have $\mathbf{y} \in V$, Stan is forced to select values from $\{\alpha, \beta\}$. If Stan gives only β for the last 2 coordinates, then Lea will choose α in the first three, therefore $\mathbf{y}$ cannot contain any α coordinates. However if Stan gives at least one α for the last 2 coordinates, then Lea, by keeping on choosing β, can prevent $\mathbf{y}$ to have at least two β coordinates.

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

It is quite clear that, being a finite deterministic game, in $\mathrm{Lex}(V; \mathbf{w})$ either Lea or Stan has a winning strategy. We will simply say that Lea or Stan wins $\mathrm{Lex}(V; \mathbf{w})$ accordingly. The main theorem of this section is the following.

Theorem 2. *Let $V \subseteq \mathbb{F}^n$ be a finite set and $\mathbf{w} \in \mathbb{N}^n$. Stan wins $\mathrm{Lex}(V; \mathbf{w})$ if and only if $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$.*

An immediate consequence is that Lea wins the game iff $\mathbf{x}^{\mathbf{w}}$ is a leading monomial for $I(V)$.

There is a fast algorithm[1] which lists those $\mathbf{w} \in \mathbb{N}^n$, for which Stan wins $\mathrm{Lex}(V; \mathbf{w})$ for a given V. In view of Theorem 2, it actually computes the lex standard monomials of $I(V)$. In this paper we intend to use the Theorem to obtain explicit combinatorial description of $\mathrm{Sm}\,(I(V))$ for some interesting sets V.

Also, note that the game does not use anything more from the properties of the base field than its cardinality. That is, we can conclude that the set of lex standard monomials of a vanishing ideal is rather a combinatorial object, than an algebraic one.

In line with the recursive nature of the game, we will use induction on n to prove the theorem. The following notation will be useful.

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

[1] It uses constant times $|V|\, nk$ comparisons of field elements in the worst case, where k is the maximum number of different elements which appear in a fixed coordinate of points of V; see [FRR06].

Let $y \in \mathbb{F}$, suppose that $n \geq 2$, and set

$$V_y = \left\{ \overline{\mathbf{y}} \in \mathbb{F}^{n-1} \,:\, (\overline{\mathbf{y}}, y) \in V \right\}.$$

It is clear that if Stan picks $y_n = y$ in the first step, then they continue as if they have just started a $\mathrm{Lex}(V_y; \overline{\mathbf{w}})$ game.

Proof (Theorem 2). We prove the statement by induction on n.

The case $n = 1$ is easy. Let $w \geq 0$ be an integer. Then $x^w \in \mathrm{Sm}\,(I(V))$ if and only if $w < |\mathrm{Sm}\,(I(V))| = |V|$ by the fact that $\mathrm{Sm}\,(I(V))$ is a downset with respect to division. But this means precisely that there has to be a $y \in V$ which is not among Lea's guesses, thus Stan wins the game by picking that y.

Suppose that $n \geq 2$, and that the theorem is true for $n-1$. Set

$$Z = \left\{ y \in \mathbb{F} \,:\, \overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \mathrm{Sm}\,(I(V_y)) \right\}.$$

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

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

Suppose first that $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$, and let $f(\mathbf{x}) \in I(V)$ be a witness of this fact, that is $\mathrm{lm}(f) = \mathbf{x}^{\mathbf{w}}$. By collecting together the terms of the form $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^i$ $(i \in \mathbb{N})$ we get a decomposition $f(\mathbf{x}) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} g(x_n) + h(\mathbf{x})$, where all monomials of $h(\mathbf{x})$ are lexicographically smaller than $\overline{\mathbf{x}}^{\overline{\mathbf{w}}}$, and $\deg(g) = w_n$.

If $y \in \mathbb{F}$ is not a root of $g(x_n)$, then $\hat{f}(\overline{\mathbf{x}}) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}} g(y) + h(\overline{\mathbf{x}}, y)$ is a polynomial which vanishes on V_y, and has the property that $\mathrm{lm}(\hat{f}) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}}$. Thus, if y is not a root of g, then $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \mathrm{Lm}\,(I(V_y))$. In other words there are at most $\deg(g) = w_n$ elements $y \in \mathbb{F}$ such that $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \mathrm{Sm}\,(I(V_y))$.

For the other direction, assume that $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$. First note that by the finiteness of V, we have $V_y = \emptyset$ (and then $\mathrm{Sm}\,(I(V_y)) = \emptyset$) with finitely many exceptions $y \in \mathbb{F}$, hence $|Z| < \infty$. Now, it suffices to show that $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{|Z|} \in \mathrm{Lm}\,(I(V))$, since in this case $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{|Z|}$ cannot be a divisor of $\mathbf{x}^{\mathbf{w}}$, that is $w_n < |Z|$.

Set $F = \{ y \in \mathbb{F} \,:\, V_y \neq \emptyset \}$ and $y \in F \setminus Z$. On one hand, $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \mathrm{Lm}\,(I(V_y))$ implies the existence of a polynomial $f_y(\overline{\mathbf{x}})$ such that all monomials of $f(\overline{\mathbf{x}})$ are less than $\overline{\mathbf{x}}^{\overline{\mathbf{w}}}$, and $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} + f_y(\overline{\mathbf{x}}) \in I(V_y)$. On the other hand, let $\chi_y(x_n)$ be a polynomial such that for $y' \in F \setminus Z$

$$\chi_y(y') = \begin{cases} 1, & y' = y \\ 0 & \text{otherwise} \end{cases}. \tag{3}$$

Since F is finite, such a polynomial does exist.

And finally let

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

By the properties of the lex order $\operatorname{lm}\left(\overline{\mathbf{x}}^{\overline{\mathbf{w}}} + \sum_{y \in F} \chi_y(x_n) f_y(\overline{\mathbf{x}}) \right) = \overline{\mathbf{x}}^{\overline{\mathbf{w}}}$, therefore we have that the leading monomial of $s(\mathbf{x})$ is $\overline{\mathbf{x}}^{\overline{\mathbf{w}}} x_n^{|Z|}$. It remains to verify $s(\mathbf{x}) \in I(V)$.

Let $\mathbf{y} = (\overline{\mathbf{y}}, y) \in V$ be arbitrary. Clearly $V_y \neq \emptyset$, that is $y \in F$. We may suppose that $y \notin Z$ for otherwise the second term of $s(\mathbf{x})$ vanishes on $\mathbf{y}$. Property (3) of the polynomials $\chi_{y'}(x_n)$ gives (for some $\alpha \in \mathbb{F}$)

$$s(\overline{\mathbf{x}}, y) = \left(\overline{\mathbf{x}}^{\overline{\mathbf{w}}} + \sum_{y' \in F \setminus Z} \chi_{y'}(y) f_{y'}(\overline{\mathbf{x}}) \right) \cdot \alpha = \left(\overline{\mathbf{x}}^{\overline{\mathbf{w}}} + f_y(\overline{\mathbf{x}}) \right) \cdot \alpha,$$

which vanishes on $\overline{\mathbf{y}} \in V_y$ by the definition of f_y, thus $s(\mathbf{x})$ is zero on $\mathbf{y}$. This completes the proof. □

For those, who do not like playing whilst doing math, we emphasize below the main point of Theorem 2, a fact first noted by Cerlienco and Mureddu [CM92].

Corollary 3. *If $V \subseteq \mathbb{F}^n$ is finite, $n \geq 2$, and $\mathbf{w} \in \mathbb{N}^n$ then*

$$\mathbf{x}^{\mathbf{w}} \in \operatorname{Sm}_{\text{lex}}(I(V)) \iff w_n < \left| \left\{ y \in \mathbb{F} \,:\, \overline{\mathbf{x}}^{\overline{\mathbf{w}}} \in \operatorname{Sm}_{\text{lex}}(I(V_y)) \right\} \right|.$$

Theorem 2 has the immediate consequence that the standard monomials are largely independent of the base field $\mathbb{F}$ and of the precise embedding of V into $\mathbb{F}^n$. As here we consider more than one field, let us temporarily put $I_{\mathbb{F}}(V)$ for the polynomial ideal $I(V)$ in $\mathbb{F}[\mathbf{x}]$.

Corollary 4. *Assume that $V \subseteq V_1 \times \cdots \times V_n$ for some finite sets $V_i \subseteq \mathbb{F}$. Let $\hat{\mathbb{F}}$ be any field and suppose that $\varphi_i \colon V_i \to \hat{\mathbb{F}}$ are injective maps for $i \in [n]$. Let $\hat{V}$ be the image of V, that is*

$$\hat{V} = \{ (\varphi_1(y_1), \ldots, \varphi_n(y_n)) \,:\, \mathbf{y} \in V \}.$$

Then $\operatorname{Sm}(I_{\mathbb{F}}(V)) = \operatorname{Sm}\left(I_{\hat{\mathbb{F}}}\left(\hat{V} \right) \right)$. In particular, if $V \subseteq \{0,1\}^n$ then the set $\operatorname{Sm}(I_{\mathbb{F}}(V))$ is independent of the base field $\mathbb{F}$.

Proof. The $\operatorname{Lex}(V; \mathbf{w})$ game is essentially the same as the $\operatorname{Lex}(\hat{V}; \mathbf{w})$ game since we have changed only the names of the elements (bijectively). The second part follows from the first, because $0 \neq 1$ in $\mathbb{F}$ for any field $\mathbb{F}$. □

The second part of the corollary concerning sets $V \subseteq \{0,1\}^n$ has been proven in [ARR02] by a different method. We now show that the reduced lexicographic Gröbner basis of $I_{\mathbb{F}}(V)$ for a set $V \subseteq \{0,1\}^n$ is essentially the same over any field. We remark that this can be generalized to finite sets with more than two integer coordinate values.

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

Corollary 5. *If $V \subseteq \{0,1\}^n$, then the reduced lex Gröbner basis G of $I_{\mathbb{Q}}(V)$ has integer coefficients. For an arbitrary field $\mathbb{F}$, the set in $\mathbb{F}[\mathbf{x}]$ corresponding to G is the reduced lex Gröbner basis of the ideal $I_{\mathbb{F}}(V)$.*

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

Let $z \in \mathbb{Z}$ such that $zg(\mathbf{x})$ has relatively prime integer coefficients. If a prime p divides z, then reduce $zg \in \mathbb{Z}[\mathbf{x}]$ modulo p to get a polynomial over $\mathbb{F}_p$. It is a nonzero polynomial which (modulo p) vanishes on V, as $z\mathbf{x}^{\mathbf{w}} + zg(\mathbf{x})$ vanishes on V and $p \mid z$. Thus the leading monomial of $zg(\mathbf{x})$ is in $\mathrm{Lm}\left(I_{\mathbb{F}_p}(V)\right) = \mathrm{Lm}\left(I_{\mathbb{Q}}(V)\right)$, by Corollary 4. That is a contradiction.

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

Before going on to present mathematical (mostly combinatorial) applications of the Lex Game, we briefly comment on the algorithmic problem of actually computing standard monomials, or more generally a basis of $\mathrm{Sm}\left(I_{\mathbb{F}}(V)\right)$ over $\mathbb{F}$. The problem has had a long history starting with the outstanding paper by Buchberger and Möller [BM82]. Their algorithm, as well as the subsequent methods of Marinari, Möller and Mora [MMM93] and Abbott, Bigatti, Kreuzer and Robbiano [ABKR00] give also a Gröbner basis of $I_{\mathbb{F}}(V)$. For the arithmetic complexity of these methods we have the bound $O(n^2m^3)$ when V is a subset of $\mathbb{F}^n$ and $|V| = m$ (see Section 3 in [FG06] for a related discussion). The Lex Game provides only the standard monomials, but in return it appears to lead to a much faster algorithm (see [FRR06] for the details). In general we have the bound $O(nm^2)$. In some important special cases, such as the case of small finite ground fields which appear naturally in coding applications, one can even have a linear bound $O(nm)$ on the time demand of the algorithm.

4 Applications

4.1 Generalization of the fundamental theorem of symmetric polynomials

Following [HNR04], we present an easy proof of a theorem by Garsia [G03], which is a generalization of the fundamental theorem of symmetric polynomials.

The *ith elementary symmetric polynomial* is

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

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

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

The fundamental theorem of symmetric polynomials claims that if $f(\mathbf{x})$ is a symmetric polynomial, then it can be written uniquely as a finite sum

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

where $\alpha_\mathbf{u} \in \mathbb{F}$, and $\boldsymbol{\sigma}(\mathbf{x})^\mathbf{u}$ stands for $\prod_{i=1}^{n} \sigma_i(\mathbf{x})^{u_i}$.

We intend to prove the following generalization, which was obtained by A. Garsia [G03].

Theorem 6. *Any polynomial* $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ *can be written uniquely as a finite sum*

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

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

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

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

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

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

Proposition 7. *For the set of points V defined above, we have that $\mathbf{x}^{\mathbf{w}}$ is a lexicographic standard monomial of $I(V)$ if and only if $\mathbf{w} \leq (0, 1, \ldots, n-1)$.*

Proof. One can get the lexicographic standard monomials of V using the Lex Game (Theorem 2). Suppose that $\mathbf{w} \leq (0, 1, \ldots, n-1)$. Then Stan's strategy will be to pick in the $(n-i+1)$th step (for y_i) any element from the set $\{z_1, \ldots, z_n\} \setminus \{y_n, \ldots, y_{i+1}\}$. This set has exactly i elements, so $w_i < i$ guarantees that Lea cannot choose all of them, that is there will always be a proper choice for Stan.

On the other hand, if for example $w_i \geq i$, then in the $(n-i+1)$th step Lea can choose all the elements of $\{z_1, \ldots, z_n\} \setminus \{y_n, \ldots, y_{i+1}\}$, thus y_i will either be the same as a previously selected y_j (and then $\mathbf{y} \notin V$) or an element different from all z_j (again $\mathbf{y} \notin V$). □

We use the following easy fact without proof (see for example [CLO92]) which holds for all $i \in [n]$:

$$\sum_{j=0}^{i} (-1)^j h_{i-j}(x_i, \ldots, x_n)\sigma_j(\mathbf{x}) = 0. \tag{4}$$

Let $i \in [n]$ and set

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

Proposition 8. *The set of polynomials $\{f_i : i \in [n]\}$ is the reduced Gröbner basis of V for all term orders, such that the order of the variables is $x_1 \succ x_2 \succ \cdots \succ x_n$.*

Proof. Clearly, if $x_1 \succ x_2 \succ \cdots \succ x_n$ holds for a term order, then $\mathrm{lm}(f_i) = x_i^i$. It is also obvious by Proposition 7 that every monomial of $f_i(\mathbf{x}) - x_i^i$ is a lex standard monomial. Equation (4) implies that f_i vanishes on V. As the minimal lex leading monomials (again by Proposition 7) are $\{x_i^i : i \in [n]\}$, we have that $\{f_i : i \in [n]\}$ is indeed a reduced lex Gröbner basis. But the leading monomials of the f_i for all term orders $\prec$ considered in the statement are the same, thus $\mathrm{Sm}_{\mathrm{lex}}(I(V)) \supseteq \mathrm{Sm}_{\prec}(I(V))$. Due to the equality of the cardinalities of the two sides, we have that the standard monomials are the same for all term orders considered. We conclude that $\{f_i : i \in [n]\}$ is a reduced Gröbner basis also with respect to $\prec$. □

Proof (Theorem 6). We had a good reason for not choosing base field for V until now. Let $\mathbb{F}(\mathbf{z})$ be the function field over $\mathbb{F}$ in n variables $z_1, \ldots, z_n$ and let $V \subseteq \mathbb{F}(\mathbf{z})$ be the set of all permutations of these variables, as before.

Let $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}] \subseteq \mathbb{F}(\mathbf{z})[\mathbf{x}]$ be any polynomial, and reduce $f(\mathbf{x})$ by the Gröbner basis $\{f_i(\mathbf{x}) \in \mathbb{F}(\mathbf{z})[\mathbf{x}] : i \in [n]\}$ of V. The result is an $\mathbb{F}(\mathbf{z})$-linear combination of monomials $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))$. Furthermore, since actually $f_i \in$

$\mathbb{F}[\mathbf{z}][\mathbf{x}]$, and f_i is symmetric in the variables $z_1, \ldots, z_n$, the coefficients of the $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V))$ in this $\mathbb{F}(\mathbf{z})$-linear combination are symmetric polynomials from $\mathbb{F}[\mathbf{z}]$. Thus as functions on V, we have an equality

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

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

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

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

Uniqueness now follows: suppose that

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

Then as functions on V we have

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

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

It is instructive to compare our approach here to the one followed by Buchberger and Elias in [BE92]. They used Gröbner bases to detect and guess identities among polynomials, which involved Fermat polynomials and elementary symmetric polynomials. Subsequently they went on, generalized these to obtain conjectures and then proved these conjectures by traditional inductive means. Here we employ Gröbner bases as a proof technique to establish the generalized identity constituting Theorem 6.

4.2 Wilson's rank formula

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

A famous theorem of Richard M. Wilson [W90, Theorem 2] describes a diagonal form of A over $\mathbb{Z}$. A is shown to be row-column equivalent over $\mathbb{Z}$ to a diagonal matrix with diagonal entries $\binom{d-i}{m-i}$ with multiplicity $\binom{n}{i} - \binom{n}{i-1}$ for $0 \leq i \leq m$. As a corollary, the following rank formula holds:

Theorem 9. *Let p be a prime. Then*

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

We shall outline a simple proof which uses polynomial functions, and some simple notions related to Gröbner bases. We note first that the rank of A is exactly the dimension of the linear space $\mathcal{P}_{d,m}$ over $\mathbb{F}_p$ of the functions from $V_{\binom{[n]}{d}}$ to $\mathbb{F}_p$ which are spanned by the monomials x_M with $|M| = m$.

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

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

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

Lemma 10. *The collection of polynomials y_M, where $x_M \in \mathrm{Sm}(I)$, is a linear basis of P_m over $\mathbb{F}_p$.*

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

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

Theorem 11. *Let p be a prime, suppose that $m \le d \le n - m$ and put $I = I\left(\binom{[n]}{m}\right)$. A basis of the space $\mathcal{P}_{d,m}$ of $\mathbb{F}_p$-valued functions on $V_{\binom{[n]}{d}}$, which are $\mathbb{F}_p$-linear combinations of monomials x_M, $|M| = m$ is*

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

In particular,

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

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

$$y_M(\mathbf{v}_F) = \binom{d-|M|}{m-|M|} \cdot x_M(\mathbf{v}_F). \tag{5}$$

We obtain that, as a function on $V_{\binom{[n]}{d}}$, y_M is a scalar multiple of x_M. This, together with the linear independence of the x_M gives that B is an independent set. Also, B spans $\mathcal{P}_{d,m}$, because P_m spans $\mathcal{P}_{d,m}$ by definition, and the y_M span P_m by Lemma 10. To conclude, it remains to verify that for $0 \leq i \leq m$ there are exactly $\binom{n}{i} - \binom{n}{i-1}$ monomials of degree i in $\mathrm{Sm}\,(I)$. This will be proven in Lemma 12. □

Lemma 12. *For an arbitrary term order and any integers $0 \leq i \leq m \leq \frac{n}{2}$, there are exactly $\binom{n}{i} - \binom{n}{i-1}$ monomials of degree i in $\mathrm{Sm}\left(I\left(\binom{[n]}{m}\right)\right)$.*

Proof. We will restrict ourselves to the lex order. Note that this is enough for completing the proof of Theorem 11. The full proof could be carried out by the same ideas we use in Proposition 8 or outline after Theorem 13.

We say that a vector $\mathbf{w} \in \{0,1\}^n$ is a *ballot sequence* if in every prefix of $\mathbf{w}$ there are at least as many 0, as 1 coordinates. We shall prove that $\mathbf{x}^{\mathbf{w}}$ is a lex standard monomial for $I = I\left(\binom{[n]}{m}\right)$ iff $\deg(\mathbf{x}^{\mathbf{w}}) \leq m$ and $\mathbf{w}$ is a ballot sequence. By Theorem 2, we can use the Lex Game $\mathrm{Lex}\left(V_{\binom{[n]}{m}}; \mathbf{w}\right)$ to show this.

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

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

Next we show how Stan can win if $\mathbf{w}$ is a ballot sequence with at most m ones. Set $J = \{j \in [n] : w_j = 1\}$. For all $j \in J$ let us pick an $\ell(j) \in [n]$, such that $w_{\ell(j)} = 0$, $\ell(j) < j$, and $\ell : J \to [n]$ is injective. (This can be done if $\mathbf{w}$ is a ballot sequence.) Let us put $L = \{\ell(j) : j \in J\}$, and $K = [n] \setminus (J \cup L)$. Stan's strategy to choose y_i is the following. If $i \in J$, then Lea will guess something, so he just claims the opposite (in $\{0,1\}$). If $i \in L$, say $i = \ell(j)$, then he picks $y_{\ell(j)}$, such that $\{y_j, y_{\ell(j)}\} = \{0,1\}$. (Note that when choosing

the $\ell(j)$th coordinate, he already fixed y_j by $\ell(j) < j$.) This way, Stan will have exactly $|J|$ ones in $(y_i : i \in J \cup L)$. Therefore he picks $m - |J|$ ones from the y_k $(k \in K)$, and wins.

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

The approach given here allows a considerable generalization of the rank formula. We present without proof a result of this type (for details, see [FR03]). Suppose that $0 \le m_1 < m_2 \cdots < m_r \le d \le n - m_r$ and let p be a prime. Consider the set family $\mathcal{F} = \binom{[n]}{m_1} \cup \binom{[n]}{m_2} \cup \cdots \cup \binom{[n]}{m_r}$. Then

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

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

4.3 Applications to modulo q ℓ-wide families

In this subsection we give two applications of the Gröbner methods to extremal set theory. We prove upper bounds on the cardinality of a family of subsets of $[n]$ with certain restrictions: we will consider modulo q L-intersecting, L-avoiding families, and families that do not shatter large sets. We shall omit a part of the proof, but give the ideas. A detailed proof can be found in [FHR1].

Let us consider the following family of sets. Let q, d, and ℓ be integers, such that $1 \le \ell < q$. Then the *modulo q complete ℓ-wide family* is

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

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

The following theorem will be crucial in both applications.

Theorem 13. *Let p be a prime, and q be a power of p. Denote by $H_{\mathcal{G}}(m)$ the Hilbert-function over $\mathbb{F}_p$ of a modulo q complete ℓ-wide family $\mathcal{G}$. If $0 \le m \le \frac{n+\ell}{2}$, then*

$$H_{\mathcal{G}}(m) \le \sum_{j=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m - jq - k}.$$

A sketch of the proof is the following. One can obtain the lex standard monomials of $I(\mathcal{G})$ by the Lex Game method. Then also the lexicographic Gröbner basis can be constructed: for each minimal lex leading monomial $\mathbf{x}^{\mathbf{w}}$, we can exhibit a polynomial $f_{\mathbf{w}}$ in the ideal, such that $\mathrm{lm}(f_{\mathbf{w}}) = \mathbf{x}^{\mathbf{w}}$. It turns out that the lex and deglex leading monomials of these polynomials are the same. From this fact it follows that what we got is a deglex Gröbner basis as well, and that the lex and deglex standard monomials are the same. (This is the same way to compute the deglex Gröbner basis as in Proposition 8.) This is good news, since by counting the deglex standard monomials of degree at most m, we obtain the exact value of $H_{\mathcal{G}}(m)$. The formula in Theorem 13 is then a convenient upper bound of that value.

One may compare this result to Lemma 12, noting that if $q > n$ and $\ell = 1$, then the modulo q complete ℓ-wide family is just $\binom{[n]}{d}$.

Modulo q L-intersecting, L-avoiding families

Let L be a subset of integers and $\mathcal{F}$ be a system of sets. We say that $\mathcal{F}$ is *modulo q L-avoiding* if $F \in \mathcal{F}$ and $f \in L$ implies $|F| \not\equiv f \pmod q$. We call $\mathcal{F}$ *modulo q L-intersecting* if for any two distinct sets $F_1, F_2 \in \mathcal{F}$ a congruence $|F_1 \cap F_2| \equiv f \pmod q$ holds for some $f \in L$.

The maximum number of sets a modulo q L-avoiding, L-intersecting set family can contain has been studied extensively, see [FHR1] for more details. We have the following result in this direction.

We call a set $L \subseteq \{0, \ldots, q-1\}$ a *modulo q interval* if it is either an interval of integers, or a union of two intervals L_1 and L_2, such that $0 \in L_1$ and $q - 1 \in L_2$.

Theorem 14. *Let q be a power of a prime, L be a modulo q interval and $\mathcal{F} \subseteq 2^{[n]}$ be a modulo q L-avoiding, L-intersecting family of sets. If $|L| \leq n - q + 2$, then*

$$|\mathcal{F}| \leq \sum_{k=|L|}^{q-1} \binom{n}{k}.$$

The following lemma is left as an exercise for the reader.

Lemma 15. *If f is an integer, q is a power of a prime p, then*

$$\binom{f-1}{q-1} \equiv \begin{cases} 0 \pmod p, \text{ if } f \not\equiv 0 \pmod q \\ 1 \pmod p, \text{ if } f \equiv 0 \pmod q. \end{cases}$$

Proof (Theorem 14). Put $\ell = q - |L|$. If L is an interval of integers, then set $d = \max L + 1$, otherwise, when L is the union of two (separate) intervals L_1, L_2 and $0 \in L_1$, set $d = \max L_1 + 1$. Denote by $\mathcal{G}$ the modulo q complete ℓ-wide family with this parameter d. Then by the definitions $\mathcal{F} \subseteq \mathcal{G}$.

For any $F \in \mathcal{F}$ we define the polynomial $\hat{f}_F(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ to be

$$\hat{f}_F(\mathbf{x}) = \left(\sum_{\substack{k=0 \\ k \notin L}}^{q-1} \binom{\mathbf{x} \cdot \mathbf{v}_F - k - 1}{q-1} \right) \text{ reduced by } x_i^2 - x_i \ (i \in [n]),$$

where $\mathbf{x} \cdot \mathbf{v} = \sum_{i=1}^{n} x_i v_i$ is the usual scalar product of row vectors.

We claim that $\hat{f}_F \in \mathbb{Z}[\mathbf{x}]$. Since we have reduced with $x_i^2 - x_i$, we have that $\hat{f}_F(\mathbf{x})$ is multilinear, thus $\hat{f}_F = \sum_{G \subseteq [n]} \alpha_G x_G$ with some coefficients $\alpha_G \in \mathbb{Q}$. If $\hat{f}_F \notin \mathbb{Z}[\mathbf{x}]$, then let G be a minimal set with respect to inclusion, such that $\alpha_G \notin \mathbb{Z}$. Clearly, the reduction with the polynomials $x_i^2 - x_i$ does not change the value of the original polynomial on 0-1 vectors, therefore $f_F(\mathbf{v}_G)$ is an integer. Thus substituting $\mathbf{v}_G$ we get that $f_F(\mathbf{v}_G) = \sum_{G' \subsetneq G} \alpha_{G'} + \alpha_G$, a contradiction since the coefficients $\alpha_{G'}$ are integers. We have proven that $\hat{f}_F \in \mathbb{Z}[\mathbf{x}]$.

Suppose that q is a power of a prime p and let $F' \in \mathcal{F}$ be a set. Then

$$\hat{f}_F(\mathbf{v}_{F'}) = \sum_{\substack{k=0 \\ k \notin L}}^{q-1} \binom{|F' \cap F| - k - 1}{q-1}. \tag{6}$$

If $F' \neq F$, then, as $\mathcal{F}$ is modulo q L-intersecting, $|F' \cap F| - k$ cannot be congruent to 0 modulo q for $k \notin L$. That is (by Lemma 15), if $F' \neq F$, then all terms of the sum in (6) are zero modulo p. If $F' = F$, then using that $\mathcal{F}$ is modulo q L-avoiding, we have exactly one nonzero term modulo p, which is actually congruent to 1. Write f_F for the polynomial in $\mathbb{F}_p[\mathbf{x}]$ we obtain from $\hat{f}_F$ by reducing its integer coefficients modulo p. The above argument yields

$$f_F(\mathbf{v}_{F'}) = \begin{cases} 0 \text{ if } F \neq F' \\ 1 \text{ if } F = F' \end{cases}.$$

Since the degree of $\hat{f}_F$ is at most $q-1$, the same is true for f_F as well. Using our earlier notation, this means that $f_F \in \mathbb{F}_p[\mathbf{x}]_{\leq q-1}$. We claim that the images $\overline{f}_F$ of the f_F in the quotient space $\mathbb{F}_p[\mathbf{x}]_{\leq q-1} / I(\mathcal{G})_{\leq q-1}$ are linearly independent over $\mathbb{F}_p$. Indeed, suppose that

$$\sum_{F \in \mathcal{F}} \alpha_F \overline{f}_F = 0 \tag{7}$$

for some $\alpha_F \in \mathbb{F}_p$. The elements of $\mathbb{F}_p[\mathbf{x}] / I(\mathcal{G})$ are functions on the characteristic vectors of $\mathcal{G}$. In particular equation (7) still holds if we substitute $\mathbf{v}_F$ for some $F \in \mathcal{F} \subseteq \mathcal{G}$. The substitution gives $\alpha_F = 0$ immediately.

To conclude, note that the number of the polynomials f_F is bounded by the dimension of $\mathbb{F}_p[\mathbf{x}]_{\leq q-1} / I(\mathcal{G})_{\leq q-1}$, that is

$$|\mathcal{F}| \leq \dim_{\mathbb{F}_p}\left(\mathbb{F}_p[\mathbf{x}]_{\leq q-1}/I(\mathcal{G})_{\leq q-1}\right) = H_{\mathcal{G}}(q-1) \leq \sum_{j=0}^{\infty}\sum_{k=0}^{\ell-1}\binom{n}{q-1-jq-k} = \sum_{k=|L|}^{q-1}\binom{n}{k}.$$

by Theorem 13 (which we are allowed to use as $|L| \leq n-q+2$ implies the assumption $q-1 \leq \frac{n+\ell}{2}$ of the Theorem). □

Set families which do not shatter large sets

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

$$\{F \cap M \,:\, F \in \mathcal{F}\} = 2^M.$$

The system of sets $\mathcal{F}$ is an ℓ-*antichain* if it does not contain $\ell+1$ distinct sets $F_0, F_1, \ldots, F_\ell$ such that $F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_\ell$.

Frankl [F89] conjectured that if an ℓ-antichain $\mathcal{F}$ shatters no set of size $m+1$ for some integer $0 \leq m \leq \frac{n+\ell}{2}-1$, then $|\mathcal{F}| \leq \sum_{k=0}^{\ell-1}\binom{n}{m-k}$ must hold.

An ℓ-wide family (which of course can be understood as a modulo q ℓ-wide family for some q large enough) is an ℓ antichain. In their manuscript [FHR2], Friedl, Hegedűs and Rónyai showed that the upper bound is valid for ℓ-wide families. The next theorem is a generalization of that result, the special case follows by choosing $q > n$.

Theorem 16. *Let $\mathcal{F} \subseteq 2^{[n]}$ be a modulo q ℓ-wide family of sets, where q is a prime power. If $\mathcal{F}$ shatters no set of size $m+1$ for some integer $0 \leq m \leq \frac{n+\ell}{2}$, then*

$$|\mathcal{F}| \leq \sum_{j=0}^{\infty}\sum_{k=0}^{\ell-1}\binom{n}{m-jq-k}.$$

Proof. We first prove that if x_M is a standard monomial of any set system $\mathcal{F}$, then $\mathcal{F}$ shatters M. Suppose that $N \subseteq M$, but $N \notin \{F \cap M \,:\, F \in \mathcal{F}\}$. Let $\mathbf{v} = \mathbf{v}_N$ be the characteristic vector of N. Then the polynomial

$$\prod_{i \in M}(x_i + v_i - 1)$$

vanishes on $V_{\mathcal{F}}$ and its leading monomial is x_M, thus $x_M \in \mathrm{Lm}\,(I(\mathcal{F}))$. We conclude that $x_M \in \mathrm{Sm}\,(I(\mathcal{F}))$ implies $|M| \leq m$ for a family $\mathcal{F}$ which does not shatter any set of size $m+1$.

Recall that $\mathcal{F} \subseteq \mathcal{G}$, where $\mathcal{G}$ is a modulo q complete ℓ-wide family. This gives $\mathrm{Sm}\,(I(\mathcal{F})) \subseteq \mathrm{Sm}\,(I(\mathcal{G}))$, and so we can bound the cardinality of the standard monomials of $\mathcal{F}$ with the number of standard monomials of $\mathcal{G}$ of degree at most m. This latter is exactly $H_{\mathcal{G}}(m)$, if we consider a degree compatible

term ordering. (Actually, in this case, we can take any term order, see the discussion after Theorem 13.) Therefore

$$|\mathcal{F}| = |\mathrm{Sm}\,(I(\mathcal{F}))| \leq H_{\mathcal{G}}(m),$$

and hence Theorem 13 gives the desired bound. □

The inequality in Theorem 16 is sharp. Choose $d = m+\ell-1$ for a modulo q complete ℓ-wide family $\mathcal{G}$, and put $\mathcal{F} = \mathcal{G} \cap \binom{[n]}{\leq m}$. Then the fact that $\mathcal{F}$ does not contain any set of size $m+1$ implies that it cannot shatter any set of cardinality $m+1$. The size of $\mathcal{F}$ is precisely $\sum_{j=0}^{\infty} \sum_{k=0}^{\ell-1} \binom{n}{m-jq-k}$.

4.4 Harima's theorem for set families

Here we prove an important special case of a theorem by T. Harima. It establishes a connection among the Hilbert functions of complementary set families.

Theorem 17. *Suppose $\mathcal{F} \subseteq 2^{[n]}$ and $\mathcal{G} = 2^{[n]} \setminus \mathcal{F}$ are nonempty set families. Then for their Hilbert functions we have*

$$\sum_{i=0}^{m} \binom{n}{i} = |\mathcal{G}| + H_{\mathcal{F}}(m) - H_{\mathcal{G}}(n-1-m)$$

for every $m = 0, 1, \ldots, n$.

Theorem 17 was proved by Tadahito Harima for much more general point sets. In formula (3.1.5) of [H95] the result is given for two disjoint finite point sets $\mathbb{X}, \mathbb{Y} \subset \mathbf{P}^n(\mathbb{F})$ in the projective n-space over $\mathbb{F}$, instead of $V_{\mathcal{F}}$ and $V_{\mathcal{G}}$, such that $\mathbb{X} \cup \mathbb{Y}$ is a complete intersection. The formula was used in his characterization of the Hilbert functions of Artinian Gorenstein algebras with the weak Stanley property.

Here we focus on 0,1-vectors only. Our approach is based on direct computations with polynomial functions.

Proof. For a subset $M \subseteq [n]$, let M^c stand for the set $[n] \setminus M$.

We claim that a monomial x_M is a leading monomial for $I(\mathcal{F})$ if and only if x_{M^c} is a standard monomial for $I(\mathcal{G})$.

Among the monomials of the form x_M, the number of leading monomials for $I(\mathcal{F})$ is the same as the number of standard monomials for $I(\mathcal{G})$, namely $2^n - |\mathcal{F}| = |\mathcal{G}|$, hence the claim will follow if we show that $x_M \in \mathrm{Lm}\,(I(\mathcal{F}))$ implies $x_{M^c} \in \mathrm{Sm}\,(I(\mathcal{G}))$. Indeed, suppose for contradiction that we have polynomials $f \in I(\mathcal{F})$ and $g \in I(\mathcal{G})$ with leading terms x_M and x_{M^c}, respectively. Then $f \cdot g$ vanishes on $V_{2^{[n]}}$ and its leading term is $x_{[n]}$. This is impossible, because $\left|\mathrm{Sm}\left(I\left(2^{[n]}\right)\right)\right| = 2^n = |\{x_{M'} : M' \subseteq [n]\}|$ implies that every multilinear monomial is a standard monomial for $V_{2^{[n]}}$.

Let $\prec$ be a degree compatible term order on $\mathbb{F}[\mathbf{x}]$. Now the number of multilinear leading monomials of degree i for $I(\mathcal{F})$ is $\binom{n}{i}-(H_{\mathcal{F}}(i)-H_{\mathcal{F}}(i-1))$. By the claim above, this is $H_{\mathcal{G}}(n-i)-H_{\mathcal{G}}(n-i-1)$, the number of standard monomials of degree $n-i$ for $I(\mathcal{G})$. We have

$$\binom{n}{i} = H_{\mathcal{F}}(i) - H_{\mathcal{F}}(i-1) + H_{\mathcal{G}}(n-i) - H_{\mathcal{G}}(n-i-1),$$

for every $0 \leq i \leq n$ (we use the convention $H_{\mathcal{F}}(-1) = H_{\mathcal{G}}(-1) = 0$). By adding these up for $i = 0, \ldots, m$, we obtain

$$\sum_{i=0}^{m} \binom{n}{i} = H_{\mathcal{F}}(m) + H_{\mathcal{G}}(n) - H_{\mathcal{G}}(n-m-1).$$

The Theorem follows now from $H_{\mathcal{G}}(n) = |\mathcal{G}|$. □

Theorem 17 allows us to formulate an interesting min-max relation. Let $\mathcal{F} \subset 2^{[n]}$ be a family different from $\emptyset$ and $2^{[n]}$. Let $a(\mathcal{F})$ stand for the smallest degree of a nonzero multilinear polynomial from $\mathbb{F}[\mathbf{x}]$ which vanishes on $V_{\mathcal{F}}$. We have $1 \leq a(\mathcal{F}) \leq n$.

Also, we define $b(\mathcal{F})$ to be the smallest integer k such that $H_{\mathcal{F}}(k) = |\mathcal{F}|$. In other words, $b(\mathcal{F})$ is the smallest degree k such that every function from $V_{\mathcal{F}}$ to $\mathbb{F}$ can be represented by a polynomial from $\mathbb{F}[\mathbf{x}]$ of degree at most k. We have $0 \leq b(\mathcal{F}) \leq n$.

It is easily seen that any polynomial $\chi_{\mathbf{v}} \in \mathbb{F}[\mathbf{x}]$ which is 1 on the vector $\mathbf{v} \in \{0,1\}^n$, and 0 on all other vectors from $\{0,1\}^n$ must have degree at least n. From that we readily infer that

$$a(\mathcal{F}) + b(2^{[n]} \setminus \mathcal{F}) \geq n. \tag{8}$$

Theorem 17 implies that, in fact, we have an equality here.

Corollary 18. *Let $\mathcal{F} \subset 2^{[n]}$ and $\mathcal{G} = 2^{[n]} \setminus \mathcal{F}$. Assume that both $\mathcal{F}$ and $\mathcal{G}$ are nonempty. Then we have*

$$a(\mathcal{F}) + b(\mathcal{G}) = n.$$

Proof. We apply Theorem 17 with $m = a(\mathcal{F}) - 1$. Note first, that $m \geq 0$ and $H_{\mathcal{F}}(m) = H_{2^{[n]}}(m)$, because the multilinear monomials of degree $\leq m$ are linearly independent over $\mathbb{F}$, as functions on $V_{\mathcal{F}}$. Theorem 17 gives now that $H_{\mathcal{G}}(n-m-1) = |\mathcal{G}|$, hence $b(\mathcal{G}) \leq n-m-1 = n-a(\mathcal{F})$. This, together with (8) proves the assertion. □

In [PR] Theorem 17 is proved over more general coefficient rings, rather than fields, which include the rings $\mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z}$, where k is a positive integer. An application to the (modular weak degree) complexity of Boolean functions is also given there.

References

[ABKR00] Abbott, J.; Bigatti, A.; Kreuzer, M.; Robbiano,L.: Computing ideals of points. J. Symbolic Comput. **30**, 341–356 (2000)

[ARR02] Anstee, R.P., Rónyai, L., Sali, A.: Shattering news. Graphs and Combinatorics, **18**, 59–73 (2002)

[B65] Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Doctoral thesis, University of Innsbruck, 1965. *English Translation:* An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal. Journal of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science: Interactions. **41**, 475-511 (2006)

[B70] Buchberger, B.: Ein algorithmisches Kriterium fur die Lösbarkeit eines algebraischen Gleichungssystems. Aequationes mathematicae **4**, 374-383 (1970) *English translation:* An algorithmic criterion for the solvability of algebraic systems of equations. In: B. Buchberger, F. Winkler (eds.), Gröbner Bases and Applications, London Mathematical Society Lecture Note Series, Vol. 251, Cambridge University Press, 535 -545 (1998)

[B85] Buchberger, B.: Gröbner-Bases: An algorithmic method in polynomial ideal theory. Chapter 6 in: N.K. Bose (ed.), Multidimensional systems theory - progress, directions and open problems in multidimensional systems theory, Reidel Publishing Company, Dodrecht - Boston - Lancaster, pp. 184-232 (1985)

[BE92] Buchberger, B.; Elias, J.: Using Gröbner bases for detecting polynomial identities: a case study on Fermat's ideal. J. Number Theory, **41**, 272–279 (1992)

[CM92] Cerlienco, L., Mureddu, M.: From algebraic sets to monomial linear bases by means of combinatorial algorithms. Discrete Mathematics, **139**, 73–87 (1995)

[CLO92] Cox, D., Little, J., O'Shea, D.: Ideals, varieties, and algorithms. Springer-Verlag, Berlin, Heidelberg (1992)

[FG06] Farr, J. B.; Gao, S-: Computing Gröbner bases for vanishing ideals of finite sets of points. Applied algebra, algebraic algorithms and error-correcting codes, 118–127, Lecture Notes in Comput. Sci., 3857, Springer, Berlin (2006)

[FHR1] Felszeghy, B., Hegedűs, G., Rónyai, L.: Algebraic properties of modulo q complete ℓ-wide families. Combinatorics, Probability and Computing, to appear.

[FRR06] Felszeghy, B., Ráth, B., Rónyai, L.: The lex game and some applications. J. Symbolic Computation, **41**, 663–681 (2006)

[FB06] Felszeghy, B., Rónyai, L.: On the lexicographic standard monomials of zero dimensional ideals. Proc. 10th Rhine Workshop on Computer Algebra (RWCA), 95–105 (2006)

[F89] Frankl, P.: Traces of antichains. Graphs and Combinatorics, **5**, 295–299 (1989)

[FHR2] Friedl, K., Hegedűs, G., Rónyai, L.: Gröbner bases for complete ℓ-wide families. Publ. Math. Debrecen, **70**, 271–290 (2007)

[FR03] Friedl, K., Rónyai, L.: Order shattering and Wilson's theorem. Discrete Mathematics **270**, 127–136 (2003)

[G03] Garsia, A.M.: Pebbles and expansions in the polynomial ring. In: Polynomial identities and combinatorial methods. Lecture Notes in Pure and Appl. Math., **235**, 261–285 (2003)

[H95] Harima, T.: Characterization of Hilbert functions of Gorenstein Artin algebras with the weak Stanley property. Proc. Amer. Math. Soc., **123**, 3631–3638 (1995)

[HNR04] Hegedűs, G., Nagy, A., Rónyai, L.: Gröbner bases for permutations and oriented trees. Annales Univ. Sci. Budapest., Sectio Computatorica, **23**, 137–148 (2004)

[MMM93] Marinari, M. G.; Möller, H. M.; Mora, T.: Göbrner bases of ideals defined by functionals with an application to ideals of projective points. Appl. Algebra Engrg. Comm. Comput. **4**, 103–145 (1993)

[M] Moorhouse, G.E.: Approaching some problems in finite geometry through algebraic geometry. This volume.

[BM82] Möller, H. M.; Buchberger, B.: The construction of multivariate polynomials with preassigned zeros. Computer algebra (Marseille, 1982), 24–31, Lecture Notes in Comput. Sci., 144, Springer, Berlin-New York (1982)

[PR] Pintér, D., Rónyai, L.: On the Hilbert function of complementary set families. Annales Univ. Sci. Budapest., Sectio Computatorica **29**, 175–198 (2008)

[W90] Wilson, R.M.: A diagonal form for the incidence matrices of t-subsets vs. k-subsets. Europ. J. Combin., **11** 609–615 (1990)