The lex game and some applications

Bálint Felszeghy, Balázs Ráth and Lajos Rónyai
Computer and Automation Institute
Hungarian Academy of Sciences
and
Department of Algebra
Budapest University of Technology and Economics

November 12, 2005

Abstract

Let $\mathbb{F}$ be a field, V a finite subset of $\mathbb{F}^n$. We introduce the lex game, which yields a combinatorial description of the lexicographic standard monomials of the ideal $I(V)$ of polynomials vanishing on V.

As a consequence, we obtain a fast algorithm which computes the lexicographic standard monomials of $I(V)$.

We apply the lex game to calculate explicitly the standard monomials for special types of subsets of $\{0,1\}^n$. For $D \subseteq \mathbb{Z}$ let V_D denote the vectors $\mathbf{y} \in \{0,1\}^n$ in which the number of ones (the Hamming weight of $\mathbf{y}$) is in D. We calculate the lexicographic standard monomials of V_D, where

$$D = D(d,\ell,r) = \left\{a \in \mathbb{Z} : \exists\, a' \in \mathbb{Z} \text{ with } d \le a' \le d+\ell-1 \text{ and } a' \equiv a \pmod{r}\right\},$$

for $d, \ell, r \in \mathbb{N}$ fixed with $0 \le d < r$ and $0 < \ell < r$. This extends results of [3], [6] and [10].

1 Introduction

Throughout the paper $\mathbb{N}$ denotes the set of nonnegative integers, and $\mathbb{Z}$ stands for the integers. We write $[n]$ for the set $\{1, 2, \ldots, n\}$. We use boldface letters for vectors and we denote their coordinates by the same letter indexed with respective numbers, for example $\mathbf{w} = (w_1, \ldots, w_n)$.

Let $\mathbb{F}$ be a field, n be a positive integer and $\mathbb{F}[x_1, \ldots, x_n]$ be the ring of polynomials in the n variables $x_1, \ldots, x_n$ over $\mathbb{F}$. For $\mathbf{w} \in \mathbb{N}^n$ we write $\mathbf{x}^{\mathbf{w}}$ for the monomial $x_1^{w_1} x_2^{w_2} \ldots x_n^{w_n}$. A polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ can be considered as a function from $\mathbb{F}^n$ to $\mathbb{F}$ in a straightforward way. If $V \subseteq \mathbb{F}^n$, then the polynomials that vanish on V form an ideal $I(V)$ in $\mathbb{F}[x_1, \ldots, x_n]$. We will study the ideal $I(V)$ and the ring of polynomial functions $\mathbb{F}[x_1, \ldots, x_n]/I(V)$ on V in

[0] *Key words and phrases:* standard monomials, Gröbner basis, combinatorial algorithm
Research supported in part by OTKA grants T42481, T42706, NWO-OTKA grant N34010, the EU-COE Grant of MTA SZTAKI, and the Center for Applied Mathematics and Computational Physics of the BUTE.

the case that V is finite. More precisely, we investigate a special monomial linear basis of $\mathbb{F}[x_1, \ldots, x_n]/I(V)$, the set of the lexicographic standard monomials of $I(V)$. Certain properties of V can be formulated in terms of polynomial functions on V, and can be proven using standard monomials and Gröbner bases (see Subsection 1.1 for the definitions). Examples of such applications can be found in [7] and [11].

We introduce the lex game $\mathrm{Lex}(V; \mathbf{w})$ in Section 2, where V is a finite subset of $\mathbb{F}^n$ and $\mathbf{w} \in \mathbb{N}^n$. By determining the player who has winning strategy in $\mathrm{Lex}(V; \mathbf{w})$ we can decide if $\mathbf{x}^{\mathbf{w}}$ is a standard monomial of $I(V)$. As a consequence we show that the set of the lexicographic standard monomials is a combinatorial object, as it is largely independent of the base field.

These facts suggest that the lexicographic standard monomials can be calculated by purely combinatorial methods. Indeed, such an algorithm was given by Cerlienco and Mureddu [5]. In Section 3 we present a computationally more efficient variant. Here we shall use an observation that connects lexicographic standard monomials to the well known data structure *trie* in computer science.

In the last section we give some theoretical applications. For some interesting sets V, a good description of the standard monomials yields combinatorial consequences (see for example [7] or [11] for results of this type). We describe the lexicographic standard monomials of some sets having combinatorial significance. To be more specific, let D be a set of integers and put

$$V_D = \{\mathbf{v} \in \{0,1\}^n \,:\, \text{the Hamming weight of } \mathbf{v} \text{ is in } D\}\,.$$

We study the standard monomials of V_D. We are particularly interested in the case when d, ℓ, r are nonnegative integers, $0 \le d < r$, $0 < \ell < r$ and

$$D = \{a \in \mathbb{Z} \,:\, \exists\, a' \in \mathbb{Z} \text{ with } d \le a' \le d + \ell - 1 \text{ and } a' \equiv a \pmod{r}\}\,.$$

We obtain a simple characterization of the lexicographic standard monomials of V_D. As a special case we recover the description of the lex standard monomials for complete uniform and complete ℓ-wide families, and hence extend results of [3], [6] and [10].

1.1 Standard monomials

A *term order* is a total order $\prec$ on the monomials such that for every monomials $\mathbf{x}^{\mathbf{u}}$, $\mathbf{x}^{\mathbf{v}}$ and $\mathbf{x}^{\mathbf{w}}$ we have

$$1 \preceq \mathbf{x}^{\mathbf{w}},$$

and if $\mathbf{x}^{\mathbf{u}} \prec \mathbf{x}^{\mathbf{v}}$ then

$$\mathbf{x}^{\mathbf{u}} \cdot \mathbf{x}^{\mathbf{w}} \prec \mathbf{x}^{\mathbf{v}} \cdot \mathbf{x}^{\mathbf{w}}.$$

It follows that a term order is a well founded order and that it is a refinement of the partial order given by divisibility of monomials.

We will use the *lexicographic order* (or *lex order* for short), where $\mathbf{x}^{\mathbf{w}} \prec \mathbf{x}^{\mathbf{u}}$ if and only if $\mathbf{w}$ is lexicographically smaller than $\mathbf{u}$, that is, if the least coordinate is i where $w_i \neq u_i$, then $w_i < u_i$. In particular, every monomial in $\mathbb{F}[x_{i+1}, \ldots, x_n]$ is smaller than every monomial in $\mathbb{F}[x_1, \ldots, x_i] \setminus \{1\}$, and $x_1 \succ x_2 \succ \cdots \succ x_n$. For the rest of the paper $\prec$ denotes the lexicographic order.

The *leading monomial of a nonzero polynomial* $f \in \mathbb{F}[x_1, \ldots, x_n]$ is the largest monomial (with respect to the lexicographic order) which appears in f

with nonzero coefficient. The *leading monomials of an ideal* I of $\mathbb{F}[x_1, \ldots, x_n]$ are monomials which occur as leading monomials of some nonzero $f \in I$. We denote the set of leading monomials of I by $\mathrm{Lm}(I)$. The complement of $\mathrm{Lm}(I)$ in the set of all monomials of $\mathbb{F}[x_1, \ldots, x_n]$ is the set of *standard monomials of* I and is denoted by $\mathrm{Sm}(I)$. In other words

$$\mathrm{Sm}(I) = \{\mathbf{x}^{\mathbf{w}} : \text{ there is no } f \in I \text{ whose leading monomial is } \mathbf{x}^{\mathbf{w}}\}.$$

We will use the simple fact that $\mathrm{Sm}(I)$ is a downset with respect to division, which follows easily from the definition.

It can be proven (see for example in [1] or [4]) that for every nonzero ideal I there is a finite subset H of $\mathrm{Lm}(I)$ such that for every monomial $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}(I)$ there exists a monomial in H which divides $\mathbf{x}^{\mathbf{w}}$. A finite set $G \subseteq I$ such that for all $\mathbf{x}^{\mathbf{w}} \in H$ there exists an $f \in G$ with leading monomial $\mathbf{x}^{\mathbf{w}}$ is called a Gröbner basis of I. It is a basic fact that $\mathrm{Sm}(I)$ forms a linear basis of $\mathbb{F}[x_1, \ldots, x_n]/I$.

Suppose now that $I = I(V)$ is the ideal of the polynomials vanishing on a set $V \subseteq \mathbb{F}^n$. By substitution, we can assign a function $V \to \mathbb{F}$ to every polynomial g. The kernel of this homomorphism is $I(V)$ and hence $\mathbb{F}[x_1, \ldots, x_n]/I(V)$ is the ring of polynomial functions on V. Furthermore, if V is finite then for every function $f : V \to \mathbb{F}$ there exists a polynomial which is identical to f as a function (for a simple proof see Subsection 1.2). This means that in fact $\mathbb{F}[x_1, \ldots, x_n]/I(V)$ is the ring of $\mathbb{F}$-valued functions on V. In particular $\dim_{\mathbb{F}}(\mathbb{F}[x_1, \ldots, x_n]/I(V)) = |V|$, which, together with the basis property of standard monomials discussed above, gives that

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

1.2 Interpolation

We have already used the fact that a function $f\colon V \to \mathbb{F}$ can be realized by a polynomial if V is finite. As we will need this fact several times, we sketch a simple proof here.

Suppose that $f\colon V \to \mathbb{F}$ is a function, $V \subseteq \mathbb{F}^n$ is nonempty and finite. If the set of the coordinates of the elements of V is $\mathcal{B}$ and $\beta \in \mathbb{F}$ then put

$$\chi_\beta(x) = \prod_{\alpha \in \mathcal{B} \setminus \{\beta\}} \frac{x - \alpha}{\beta - \alpha},$$

and for $\boldsymbol{\beta} \in V$

$$\chi_{\boldsymbol{\beta}}(\mathbf{x}) = \chi_{(\beta_1, \ldots, \beta_n)}(x_1, \ldots, x_n) = \prod_{i=1}^{n} \chi_{\beta_i}(x_i).$$

Clearly $\chi_{\boldsymbol{\beta}}(\boldsymbol{\gamma}) = 0$ for $\boldsymbol{\gamma} \in V$ unless $\boldsymbol{\beta} = \boldsymbol{\gamma}$ and $\chi_{\boldsymbol{\beta}}(\boldsymbol{\beta}) = 1$. Then the polynomial

$$g(\mathbf{x}) = \sum_{\boldsymbol{\beta} \in V} \Big(f(\boldsymbol{\beta}) \cdot \chi_{\boldsymbol{\beta}}(\mathbf{x}) \Big)$$

is identical to f as a function on V.

2 The lex game

Let $\mathbb{F}$ be a field, $V \subseteq \mathbb{F}^n$ a finite nonempty 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 $\mathrm{Lex}(V; \mathbf{w})$.

We have two players named Lea and Stan. They both know V and $\mathbf{w}$. Stan thinks of a point $\mathbf{y} = (y_1, \ldots, y_n) \in V$. Lea has to find out one coordinate of $\mathbf{y}$ under the following rules. First she can guess w_n elements of $\mathbb{F}$ for the value of y_n. If she succeeds by giving y_n, then Lea wins and the game is over. Otherwise Stan lets her know the real value of y_n. In the next round Lea tries to find out y_{n-1} with w_{n-1} guesses. The game goes on in the same fashion. We stop when either Lea correctly declares one of the y_i (and then wins the game), or Stan reveals y_1. In that case Stan wins.

We extend the game to the case $V = \emptyset$ as well. For every question vector $\mathbf{w} \in \mathbb{N}^n$ we declare that Lea wins $\mathrm{Lex}(\emptyset; \mathbf{w})$.

2.1 Who wins the lex game?

Due to its recursive construction, our primary tool to prove statements on the game will be induction on n. For this reason the following notation will be useful.

For $\beta \in \mathbb{F}$ we set

$$V_\beta = \left\{(\beta_1, \ldots, \beta_{n-1}) \in \mathbb{F}^{n-1} \,:\, (\beta_1, \ldots, \beta_{n-1}, \beta) \in V\right\}.$$

It is clear that if Lea could not find out y_n in a $\mathrm{Lex}(V; (w_1, \ldots, w_n))$ game then they continue as if they have just started a $\mathrm{Lex}(V_{y_n}; (w_1, \ldots, w_{n-1}))$ game. More generally for $\beta_i, \beta_{i+1}, \ldots, \beta_n$ put

$$V_{\beta_n \beta_{n-1} \ldots \beta_i} = \left\{(\beta_1, \ldots, \beta_{i-1}) \in \mathbb{F}^{i-1} \,:\, (\beta_1, \ldots, \beta_{i-1}, \beta_i, \ldots \beta_n) \in V\right\}.$$

Let $\mathcal{B} \subseteq \mathbb{F}$ be the set of coordinate values that occur in the elements of V and $k = |\mathcal{B}|$. We thus have

$$V \subseteq \mathcal{B}^n.$$

We may always assume that Lea's guesses for y_n are all from the set $\mathcal{B}$, because it is pointless for her to select other values. Denote by

$$V^c = \mathcal{B}^n \setminus V$$

the complement of V in $\mathcal{B}^n$.

First we address the question of existence of a winning strategy for Lea. To simplify the arguments we use the adversary method for Stan's strategy. The adversary method is an important technique for proving lower bounds in computer science (see for example Section 5.3.2 in [13]). In our case Stan's strategy is the following. He does not really think of a fixed $\mathbf{y} \in V$. The only thing he has to adhere to is consistency. He keeps on responding 'no' as long as the suffix known to Lea is consistent with some $\mathbf{y} \in V$. In this sense we can also speak about Stan's strategy. The next lemma is quite straightforward.

Lemma 1. *If $n > 1$ then Stan has winning strategy in* $\mathrm{Lex}(V; (w_1, \ldots, w_n))$ *if and only if there exist at least $w_n + 1$ elements $\beta \in \mathcal{B}$ such that he has winning strategy in* $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$. *Similarly if $n > 1$ then Lea does not have winning strategy in* $\mathrm{Lex}(V; (w_1, \ldots, w_n))$ *if and only if there exist at least $w_n + 1$ elements β of $\mathcal{B}$ such that she has no winning strategy in* $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$.

Proof. Suppose that there exist at least $w_n + 1$ elements β such that Stan has winning strategy in $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$. Then his winning strategy in $\mathrm{Lex}(V; (w_1, \ldots, w_n))$ is to respond 'no' to all of Lea's guesses and then state $y_n = \beta$ with a β which was not guessed by Lea and for which he wins $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$. As Lea named only at most w_n elements, such a β does exist.

Conversely, suppose that there are at most w_n elements β such that Stan has winning strategy in $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$. If now Lea guesses for all those β, then Stan either has to respond 'yes' or reveal a β, such that he does not have winning strategy in $\mathrm{Lex}(V_\beta; (w_1, \ldots, w_{n-1}))$. This means, that he does not have a winning strategy in $\mathrm{Lex}(V; (w_1, \ldots, w_n))$.

The statement concerning Lea can be proved in the same way. □

We have a finite deterministic game which can never end in a draw. It follows that for any selection of V and $\mathbf{w}$ one of the players has a winning strategy for $\mathrm{Lex}(V; \mathbf{w})$. In particular, Lea has no winning strategy if and only if Stan has. This fact can also be proved directly by induction on n, with Lemma 1 providing the induction step.

If Lea has a winning strategy for a fixed V and $\mathbf{w}$ we say that Lea wins $\mathrm{Lex}(V; \mathbf{w})$, otherwise we say that Stan wins, since, as the preceding discussion shows, he can actually win.

The main theorem of this section characterizes winning strategies from the viewpoint of standard monomials. For some interesting sets V this will allow us to obtain explicit combinatorial description of $\mathrm{Sm}\,(I(V))$.

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

We have the following equivalent form of Theorem 2.

Theorem 3. *Stan wins* $\mathrm{Lex}(V; \mathbf{w})$ *if and only if $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$.*

Example. 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. One can easily see that Lea can win with the question vector $\mathbf{w} = (11100)$, but she has no winning strategy for $\mathbf{w} = (01110)$. In view of Theorem 2 this means that $x_1x_2x_3$ is a leading monomial, while $x_2x_3x_4$ is a standard monomial for $I(V)$.

Proof of Theorem 2, first part. If Lea wins $\mathrm{Lex}(V; \mathbf{w})$ then $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$.

Since every monomial of $x_1, \ldots, x_n$ is in $\mathrm{Lm}\,(I(\emptyset))$, the statement is trivial in that case. Assume that $V \neq \emptyset$.

Let $f_{j,1}$, $f_{j,2}$, $\ldots$, f_{j,w_j} be Lea's guesses for y_j $(j = 1, 2, \ldots, n)$ according to her winning strategy. When Lea tries to find out y_j, she already knows $y_{j+1}, y_{j+2}, \ldots, y_n$, hence $f_{j,i}$ is a function depending on the $n - j$ variables $x_{j+1}, x_{j+2}, \ldots, x_n$. The domain of $f_{j,i}$ is finite, because every possible sequence

$(y_{j+1}, y_{j+2}, \ldots, y_n)$ is the suffix of some $\mathbf{y} \in V$ and V is finite by assumption. For this reason we can suppose that $f_{j,i}(x_{j+1}, x_{j+2}, \ldots, x_n)$ is a polynomial over $\mathbb{F}$. Consider the polynomial

$$l(\mathbf{x}) = \left(\prod_{i=1}^{w_n} (x_n - f_{n,i})\right) \cdot \left(\prod_{i=1}^{w_{n-1}} (x_{n-1} - f_{n-1,i}(x_n))\right) \ldots$$
$$\left(\prod_{i=1}^{w_j} (x_j - f_{j,i}(x_{j+1}, x_{j+2}, \ldots, x_n))\right) \ldots \left(\prod_{i=1}^{w_1} (x_1 - f_{1,i}(x_2, \ldots, x_n))\right). \quad (1)$$

We see that $l(\mathbf{x})$ vanishes on V since for all $\mathbf{y} \in V$ Lea can find out a coordinate y_j, hence the corresponding $x_j - f_{j,i}(x_{j+1}, x_{j+2}, \ldots, x_n)$ is 0 on $\mathbf{y}$. Thus $l(\mathbf{x})$ is in $I(V)$.

The polynomial $f_{j,i}$ does not depend on $x_1, \ldots, x_j$, hence the leading monomial of $x_j - f_{j,i}(x_{j+1}, x_{j+2}, \ldots, x_n)$ is x_j, giving that $\mathbf{x}^{\mathbf{w}}$ is the leading monomial of $l(\mathbf{x})$. Together with $l(\mathbf{x}) \in I(V)$ this yields $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$ as we stated.

For the converse we need an easy lemma.

Lemma 4. *Let $n > 1$, $l(\mathbf{x})$ be a polynomial with leading monomial $\mathbf{x}^{\mathbf{w}}$. Then there exist polynomials $g \in \mathbb{F}[x_n]$ and $h \in \mathbb{F}[x_1, \ldots, x_n]$ such that $\deg g = w_n$, every monomial of h is lexicographically smaller than $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}}$ and*

$$l(x_1, \ldots, x_n) = x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} g(x_n) + h(x_1, \ldots, x_n).$$

Proof. By collecting every monomial of $l(\mathbf{x})$ in which the exponent of x_j is w_j for each $1 \leq j \leq n-1$, we obtain the first term $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} g(x_n)$ of the decomposition. Clearly $\deg g = w_n$ since among these monomials the lexicographic order is given by the exponent of x_n and on the other hand we know that the largest monomial is $\mathbf{x}^{\mathbf{w}} = x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} x_n^{w_n}$.

We put $h(\mathbf{x}) = l(\mathbf{x}) - x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} g(x_n)$. Suppose that $\mathbf{x}^{\mathbf{u}}$ is a monomial of $l(\mathbf{x})$.

If $\mathbf{x}^{\mathbf{u}} \succeq x_1^{w_1} \ldots x_{n-1}^{w_{n-1}}$ then $u_j = w_j$ for $j = 1, \ldots, n-1$ since otherwise $\mathbf{x}^{\mathbf{u}} \succ \mathbf{x}^{\mathbf{w}}$. But this means that $\mathbf{x}^{\mathbf{u}}$ belongs to the first term $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}} g(x_n)$. This proves the required property of h. □

Proof of Theorem 2, second part: If $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$ then Lea wins $\mathrm{Lex}(V; \mathbf{w})$.

Again, the case $V = \emptyset$ is trivial, so we can suppose that $V \neq \emptyset$. We proceed by induction on n.

If $n = 1$ then $x^w \in \mathrm{Sm}\,(I(V)) \iff w < |V|$. This follows because $\mathrm{Sm}\,(I(V))$ is a downset with respect to division and $|V| = |\mathrm{Sm}\,(I(V))|$. We infer that Lea has at least $|V|$ questions for y which is obviously enough for her to win.

Assume now that the statement is true for $n-1$. Let $V \subseteq \mathbb{F}^n$ and $l(\mathbf{x})$ be a polynomial in $I(V)$ with leading monomial $\mathbf{x}^{\mathbf{w}}$. Set the polynomials g and h as in Lemma 4 and let

$$\hat{l}(x_1, \ldots, x_{n-1}) = l(x_1, \ldots, x_{n-1}, y_n),$$

where y_n is the last coordinate of the $\mathbf{y} \in V$ Stan reveals to Lea (if the game progresses that far). If $g(y_n) \neq 0$ then by Lemma 4 it follows that the leading monomial of $\hat{l}$ is $x_1^{w_1} \ldots x_{n-1}^{w_{n-1}}$. Since l vanishes on V, it is clear that $\hat{l}$ vanishes

on V_{y_n}. This yields that $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} \in \operatorname{Lm}(I(V_{y_n}))$, hence by the induction hypothesis Lea has a winning strategy for $\operatorname{Lex}(V_{y_n}; (w_1, \dots, w_{n-1}))$.

Note also, that g has at most w_n roots in $\mathbb{F}$ because $\deg g = w_n$. With these in mind, Lea can win $\operatorname{Lex}(V; \mathbf{w})$ in the following way. She includes among her guesses for y_n the roots of g. If she does not win at the last coordinate, then we must have $g(y_n) \neq 0$. But then by the preceding paragraph, she can find out a coordinate of the remaining $(y_1, \dots, y_{n-1}) \in V_{y_n}$. Note that the argument is valid also for $w_n = 0$. This proves the theorem. □

The polynomial in (1) encodes a strategy for Lea. Here we prove an analogous statement about Stan's strategy. This proposition also tells us that if $\mathbf{x}^{\mathbf{w}} \in \operatorname{Sm}(I(V))$ then $\mathbf{x}^{\mathbf{k-1-w}} := x_1^{k-1-w_1} \dots x_n^{k-1-w_n} \in \operatorname{Lm}(I(V^c))$, where $k = |\mathcal{B}|$. The converse is also true, we will show it later in this section.

Proposition 5. *If Stan wins* $\operatorname{Lex}(V; \mathbf{w})$ *then* $\mathbf{x}^{\mathbf{k-1-w}} \in \operatorname{Lm}(I(V^c))$.

Proof. Let $f_{j,1}, f_{j,2}, \dots, f_{j,w_j+1}$ be some of Stan's possible answers when he has to reveal y_j. Clearly there has to be at least $w_j + 1$ of those, since otherwise Lea could win the game in the j^{th} step by asking for all the possibilities. When Lea is guessing for y_j then $y_{j+1}, y_{j+2}, \dots, y_n$ are already known, hence $f_{j,i}$ depends on $n - j$ variables $x_{j+1}, x_{j+2}, \dots, x_n$. For j fixed put

$$\{g_{j,1}, g_{j,2}, \dots, g_{j,k-1-w_j}\} = \{f_{j,1}, f_{j,2}, \dots, f_{j,w_j+1}\}^c.$$

$g_{j,i} = g_{j,i}(x_{j+1}, x_{j+2}, \dots, x_n)$ is again a function with finite domain (that is the set of the suffices of length $n - j$ of all $\mathbf{y} \in V$). There exists a polynomial which is identical to $g_{j,i}$ as a function on $\mathcal{B}^j$. We may therefore assume that $g_{j,i}(x_{j+1}, x_{j+2} \dots x_n)$ is a polynomial.

The polynomial that encodes Stan's strategy is

$$s(\mathbf{x}) = \left(\prod_{i=1}^{k-1-w_n} (x_n - g_{n,i}) \right) \cdot \left(\prod_{i=1}^{k-1-w_{n-1}} (x_{n-1} - g_{n-1,i}(x_n)) \right) \dots$$
$$\left(\prod_{i=1}^{k-1-w_j} (x_j - g_{j,i}(x_{j+1}, \dots, x_n)) \right) \dots \left(\prod_{i=1}^{k-1-w_1} (x_1 - g_{1,i}(x_2, \dots, x_n)) \right). \quad (2)$$

Clearly the leading monomial of $s(\mathbf{x})$ is $\mathbf{x}^{\mathbf{k-1-w}}$. To prove that $s(\mathbf{x}) \in I(V^c)$, suppose that $s(\mathbf{y}) \neq 0$ for some $\mathbf{y} \in \mathcal{B}^n$. By the definition of $s(\mathbf{x})$ and $g_{j,i}$ it is clear that for all j there exists an i_j such that $y_j = f_{j,i_j}(y_{j+1}, \dots, y_n)$. This yields that $\mathbf{y}$ is a possible choice for Stan. In particular, $\mathbf{y} \in V$. This proves that $s(\mathbf{x}) \in I(V^c)$, and hence $x_1^{k-1-w_1} \dots x_n^{k-1-w_n} \in \operatorname{Lm}(I(V^c))$. □

The following is a part of Theorem 3, which we have already proved. Here we give an alternative proof, which reveals a winning strategy for Stan.

Proposition 6. *If* $\mathbf{x}^{\mathbf{w}} \in \operatorname{Sm}(I(V))$ *then Stan wins* $\operatorname{Lex}(V; \mathbf{w})$.

Proof. We prove the statement by induction. The case $n = 1$ is immediate. Indeed, $x^w \in \operatorname{Sm}(I(V))$ implies $|V| > w$, and thus Stan can safely respond *no* to all the w guesses of Lea.

Suppose now that $n > 1$. Put

$$Y = \left\{\beta \in \mathcal{B} : x_1^{w_1} \dots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\left(I(V_\beta)\right)\right\}$$

We claim that $|Y| > w_n$. If this is true then Stan's strategy is quite simple. Respond *no* to the w_n guesses of Lea, then choose a y_n which was not among the guesses of Lea but which is in Y. Such y_n exists since $|Y| > w_n$. By construction $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\left(I(V_{y_n})\right)$, hence by the induction hypothesis, Stan wins the game $\mathrm{Lex}(V_{y_n}; (w_1, \dots, w_{n-1}))$.

To verify $|Y| > w_n$ it suffices to show $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} x_n^{|Y|} \in \mathrm{Lm}\left(I(V)\right)$, since $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} x_n^{w_n} \in \mathrm{Sm}\left(I(V)\right)$ and $\mathrm{Sm}\left(I(V)\right)$ is a downset with respect to division.

For each $\beta \in \mathcal{B} \setminus Y$ there exists a polynomial $f_\beta(x_1, \dots, x_{n-1})$ for which $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} + f_\beta(x_1, \dots, x_{n-1})$ vanishes on V_β and all the monomials of f_β are less than $x_1^{w_1} \dots x_{n-1}^{w_{n-1}}$. This holds by the definition of Y.

Put

$$f(x_1, \dots, x_n) = \sum_{\beta \in \mathcal{B} \setminus Y} \chi_\beta(x_n) f_\beta(x_1, \dots, x_{n-1}),$$

where $\chi_\beta(x_n)$ is a polynomial vanishing on the set $\mathcal{B} \setminus \{\beta\}$, and $\chi_\beta(\beta) = 1$. Clearly $f(x_1, \dots, x_{n-1}, \beta) = f_\beta(x_1, \dots, x_{n-1})$ for $\beta \in \mathcal{B} \setminus Y$. From the properties of the lexicographic order it follows that the monomials of f are less than $x_1^{w_1} \dots x_{n-1}^{w_{n-1}}$.

It is immediate now that

$$s(\mathbf{x}) = \left(x_1^{w_1} \dots x_{n-1}^{w_{n-1}} + f(\mathbf{x})\right) \prod_{\beta \in Y} (x_n - \beta)$$

vanishes on V, and the leading monomial of $s(\mathbf{x})$ is $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} x_n^{|Y|}$. □

2.2 Combinatorial properties of lex standard monomials

Theorem 3 has some immediate consequences for the standard monomials of a finite subset of $\mathbb{F}^n$. Corollaries 7 and 8 are implicit in [5]. The next statement means that the standard monomials are largely independent of the base field $\mathbb{F}$ and of the precise embedding of V into $\mathbb{F}^n$.

Corollary 7. *Let $\hat{\mathbb{F}}$ be any field and suppose that $\varphi_j \colon \mathcal{B} \to \hat{\mathbb{F}}$ are injective mappings for $j = 1, 2, \dots, n$. Let $\hat{V}$ be the image of V, that is*

$$\hat{V} = \left\{(\varphi_1(\beta_1), \dots, \varphi_n(\beta_n)) : (\beta_1, \dots, \beta_n) \in V\right\}.$$

Then the standard monomials of V in $\mathbb{F}[x_1, \dots, x_n]$ are the same as the standard monomials of $\hat{V}$ in $\hat{\mathbb{F}}[x_1, \dots, x_n]$. In particular, if $V \subseteq \{0,1\}^n$ then the standard monomials of V are independent of the base field.

Proof. The $\mathrm{Lex}(V; \mathbf{w})$ game is essentially the same as the $\mathrm{Lex}(\hat{V}; \mathbf{w})$ 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 $\mathbb{F}$. □

We now give a reformulation of Lemma 1. Recall that $k = |\mathcal{B}|$.

Corollary 8. *(i) If $n > 1$ then $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$ if and only if there exist at least $w_n + 1$ elements $\beta \in \mathcal{B}$ such that $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\,(I(V_\beta))$.*
(ii) If $n > 1$ then $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$ if and only if there exist at least $k - w_n$ elements $\beta \in \mathcal{B}$ such that $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} \in \mathrm{Lm}\,(I(V_\beta))$.

Proof. (i) is immediate from Lemma 1 and Theorem 3.

To prove (ii), consider the following statements.

1. $\mathbf{x}^{\mathbf{w}} \notin \mathrm{Sm}\,(I(V))$
2. There are at most w_n elements $\beta \in \mathcal{B}$ such that $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\,(I(V_\beta))$
3. There exist at least $k - w_n$ elements $\beta \in \mathcal{B}$ for which $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} \notin \mathrm{Sm}\,(I(V_\beta))$

They are all equivalent as one can easily check it by using part (i) of the present corollary. This proves the statement. □

Next we describe the standard (and leading) monomials of the complement $V^c = \mathcal{B}^n \setminus V$. As before $|\mathcal{B}| = k$ and $\mathbf{x}^{\mathbf{k-1-w}} = x_1^{k-1-w_1} \dots x_n^{k-1-w_n}$.

Corollary 9. $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$ *if and only if* $\mathbf{x}^{\mathbf{k-1-w}} \in \mathrm{Lm}\,(I(V^c))$.

Proof. We employ induction on n. The case $n = 1$ is clear, since we have then $x^w \in \mathrm{Sm}\,(I(V)) \iff w < |V| \iff k-1-w > k-1-|V| \iff k-1-w \geq |V^c| \iff x^{k-1-w} \in \mathrm{Lm}\,(I(V^c))$.

Assume now that $n > 1$ and that the statement is true for $n-1$. We note first that for $\beta \in \mathcal{B}$ we have

$$(V_\beta)^c = \left\{(\beta_1, \dots, \beta_{n-1}) \in \mathcal{B}^{n-1} \,:\, (\beta_1, \dots, \beta_{n-1}, \beta) \notin V\right\} = (V^c)_\beta\,,$$

hence we can simply write V_β^c.

Corollary 8 (i) tells us that $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}\,(I(V))$ if and only if there are at least $w_n + 1$ elements $\beta \in \mathcal{B}$ such that $x_1^{w_1} \dots x_{n-1}^{w_{n-1}} \in \mathrm{Sm}\,(I(V_\beta))$. By the induction hypothesis this is equivalent to the existence of at least w_n+1 elements $\beta \in \mathcal{B}$ such that $x_1^{k-1-w_1} \dots x_{n-1}^{k-1-w_{n-1}} \in \mathrm{Lm}\left(I(V_\beta^c)\right)$. Finally an application of Corollary 8 (ii) (with $k-1-w_n$ in the place of w_n) gives the conclusion desired. The proof is complete. □

2.3 Without the game

Here we outline a notational setting, which avoids the language of the lex game, but still allows us to show constructively that a monomial is a leading monomial for $I(V)$. This approach employs a more traditional and precise language, but, in our view, is less transparent. The notation introduced below will not be used in the later parts of the paper.

As before, let $\mathcal{B}$ be a finite subset of $\mathbb{F}$ and $V \subseteq \mathcal{B}^n$. For $0 \leq i < n$ we set

$$V_i = \{(\beta_{i+1}, \dots, \beta_n) \in \mathcal{B}^{n-i} \,:\, (\beta_1, \dots, \beta_n) \in V \text{ for some } \beta_1, \dots, \beta_i \in \mathcal{B}\}.$$

Also, put $V_0^{(\mathbf{w})} = V$, and recursively

$$V_i^{(\mathbf{w})} = \left\{(\beta_{i+1}, \dots, \beta_n) \in V_i \,:\, \left|\{\beta \,:\, (\beta, \beta_{i+1} \dots, \beta_n) \in V_{i-1}^{(\mathbf{w})}\}\right| > w_i\right\},$$

for $i = 1, 2, \ldots, n-1$.

In terms of the game, $V_i^{(\mathbf{w})}$ consists of the projections to the last $n-i$ coordinates of those vectors $\mathbf{y} \in V$ for which Lea can not win by finding out one of the first i coordinates $y_1, \ldots, y_i$.

It follows that $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$ if and only if $\left|V_{n-1}^{(\mathbf{w})}\right| \leq w_n$. Suppose now that this latter condition is satisfied. Then without referring to the game we exhibit a polynomial which proves that $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$.

For $1 \leq i < n$ and $(\beta_{i+1}, \ldots, \beta_n) \in V_i \setminus V_i^{(\mathbf{w})}$ let

$$\{b_{i,j}^{(\beta_{i+1},\ldots,\beta_n)} \in \mathcal{B} : \ j = 1, \ldots, w_i\}$$

be an arbitrary superset of

$$\{\beta \in \mathcal{B} : \ (\beta, \beta_{i+1} \ldots \beta_n) \in V_{i-1}^{(\mathbf{w})}\}.$$

Also we let $\{\gamma_1, \ldots, \gamma_{w_n}\}$ be a superset of $V_{n-1}^{(\mathbf{w})}$ in $\mathbb{F}$. The supersets defined above may be multisets: repetitions are allowed among the elements.

Let $\chi_{(\beta_{i+1},\ldots,\beta_n)}(x_{i+1}, \ldots, x_n)$ be a polynomial which vanishes on $\mathcal{B}^{n-i} \setminus \{(\beta_{i+1}, \ldots, \beta_n)\}$, and $\chi_{(\beta_{i+1},\ldots,\beta_n)}(\beta_{i+1}, \ldots, \beta_n) = 1$.

Next we define an array of polynomials $f_{i,j} = f_{i,j}(x_i, \ldots, x_n)$ for $1 \leq i \leq n$ and $1 \leq j \leq w_i$ as follows: $f_{n,j} = x_n - \gamma_j$, and

$$f_{i,j} = x_i - \sum_{(\beta_{i+1},\ldots,\beta_n) \in V_i \setminus V_i^{(\mathbf{w})}} b_{i,j}^{(\beta_{i+1},\ldots,\beta_n)} \chi_{(\beta_{i+1},\ldots,\beta_n)}(x_{i+1}, \ldots, x_n),$$

whenever $1 \leq i \leq n-1$ and $1 \leq j \leq w_i$. Now

$$l(\mathbf{x}) := \prod_{i=1}^{n} \prod_{j=1}^{w_i} f_{i,j}$$

shows that $\mathbf{x}^{\mathbf{w}} \in \mathrm{Lm}\,(I(V))$. Indeed, suppose that $(\beta_1, \ldots, \beta_n) \in V$. Then either $f_{n,1} \cdots f_{n,w_n}$ vanishes on $(\beta_1, \ldots, \beta_n)$, or there exists an index i ($1 \leq i \leq n-1$) such that $(\beta_i, \ldots, \beta_n) \in V_{i-1}^{(\mathbf{w})}$ but $(\beta_{i+1}, \ldots, \beta_n) \notin V_i^{(\mathbf{w})}$. By the definition of the $b_{i,j}^{(\beta_{i+1},\ldots,\beta_n)}$ there exists a j with $b_{i,j}^{(\beta_{i+1},\ldots,\beta_n)} = \beta_i$, hence $f_{i,j}$ vanishes on $(\beta_1, \ldots, \beta_n)$. Moreover, it is immediate from the construction that the leading monomial of $l(\mathbf{x})$ is $\mathbf{x}^{\mathbf{w}}$.

3 A fast algorithm for lex standard monomials

In this section we give a combinatorial algorithm to compute the lexicographic standard monomials of the vanishing ideal $I(V)$ of a finite subset V of $\mathbb{F}^n$. Such an algorithm was first given by Cerlienco and Mureddu in [5]. Here we present a computationally more efficient variant.

The method in [5] is combinatorial in the sense that algebraic operations in $\mathbb{F}$ are not needed. The algorithm uses merely the equality and inequality of coordinate values for points $\mathbf{v} \in V$. Algorithm MB in [5] determines $\mathrm{Sm}\,(I(V))$ in an incremental fashion. Suppose that $V = \{\mathbf{v_1}, \ldots, \mathbf{v_m}\}$ and set $V_i = \{\mathbf{v_1}, \ldots, \mathbf{v_i}\}$.

Starting out from V_1, they proceed to calculate $\mathrm{Sm}\,(I(V_i))$ for $i = 2, \ldots, m$. Implementation details and complexity are not discussed in [5]. It appears that a straightforward implementation of MB takes at least cm^2n^2 steps for some fixed positive c.

Here we take a somewhat different approach. First we carry out some preprocessing of V by building a reverse trie (see below for the definitions or Subsection 6.3 in [13] for more detailed discussion). This way, we organize the relevant information about V in a data structure which allows afterwards a very fast computation of the lexicographic standard monomials for $I(V)$.

Throughout we use the *uniform cost* measure ([2] Section 1.3) to discuss bounds on the running time of the algorithms. In this setting the cost of an elementary instruction is 1. Here we assume that reading or writing an element of $\mathbb{F}$ and testing the equality of two elements of $\mathbb{F}$ are elementary operations and hence have unit costs. With this concept of speed our method runs in time $O(mnk)$, where $m = |V|$ and k is the maximum number of coordinate values for the points of V which appear at an arbitrary coordinate position. At the end of this section we discuss even better upper bounds for the complexity of our algorithm.

The algorithm has been implemented in Singular [8] and can be downloaded from `http://www.math.bme.hu/~fbalint/publ/singular.html`

3.1 A naive approach

First we remind the reader of the definitions related to the data structure trie. A *rooted tree* is a tree in the graph theoretical sense, with a special vertex called *root*. We say that a vertex is on the i^{th} *level* of the tree if its distance from the root is i. If the last level of the tree is the i^{th}, we say that the depth of the tree is i. If v is a vertex, v is not the root, and u is the vertex preceding v on the way from the root, then u is the *parent* of v and v is a *child* of u. The root has no parent. A vertex without a child is called a *leaf*. If v is a vertex different from the root and u is on the path from v to the root, then u is an *ancestor* of v and v is a *descendant* of u.

A *trie* is a rooted tree in which there is a symbol written on every edge from a fixed alphabet. For every vertex v, the labels on the edges from v to its children are all different. One can associate words over the alphabet to the vertices of a trie by assigning to a vertex v the word we get by concatenating the letters written on the edges on the way from the root to v. Furthermore we sometimes identify the vertices with their words. In our case the alphabet will be either the set $\mathcal{B} \subseteq \mathbb{F}$ or the natural numbers $\mathbb{N}$.

We write $|V| = m$ and for the rest of this section we suppose that $m > 0$. Let T be the trie built for the reverse sequences of V. If $(\beta_1, \ldots, \beta_n) \in V$ then T will contain a unique path from the root to a leaf whose edge labels are $\beta_n, \beta_{n-1}, \ldots, \beta_1$ in turn. T is called the reverse trie for V. (See Figure 1 as an example.) Obviously the depth of T is n and T has leaves only on the n^{th} level, where there are exactly m leaves.

If $V_{\beta_n\beta_{n-1}\ldots\beta_i} \neq \emptyset$, then there is a unique vertex v on the $(n-i+1)^{st}$ level of T, which corresponds to $(\beta_i\beta_{i+1}\ldots\beta_n)$. Note that the (reverse) trie of $V_{\beta_n\beta_{n-1}\ldots\beta_i}$ is the subtree of T containing all the descendants of v and having v as root. These descendants correspond to those vectors in V which end in the suffix $\beta_i, \beta_{i+1}, \ldots, \beta_n$. We shall use the shorter form S_v instead of writing

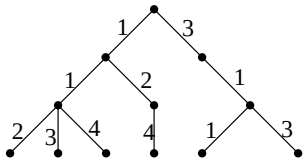


Figure 1: The reverse trie T for the set $V = \{(2,1,1), (3,1,1), (4,1,1), (4,2,1), (1,1,3), (3,1,3)\}$.

$\mathrm{Sm}\left(I(V_{\beta_n\beta_{n-1}\ldots\beta_i})\right)$, keeping in mind that the path from v to the root leads on edges marked by $\beta_i, \beta_{i+1}, \ldots, \beta_n$ respectively. Clearly if v is on the $(n-i)^{th}$ level of T, then all the elements of S_v are monomials in the variables $x_1, \ldots, x_i$.

It follows readily from Corollary 8, that we can compute the standard monomials S_v of v, if we already know the standard monomial sets $S_{v_1}, \ldots, S_{v_r}$ of the children $v_1, \ldots, v_r$ of v. Indeed, for all monomials $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}}$ which occur in at least one of the S_{v_j} we put the monomial $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^w$ in S_v, if there are at least $w+1$ vertices v_j among the children of v such that $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} \in S_{v_j}$.

If v is a leaf then we set $S_v = \{1\}$. Suppose that we have all the standard monomials of the vertices at the $(n-i+1)^{st}$ level. Let v be a vertex on the $(n-i)^{th}$ level and suppose that its children are $v_1, \ldots, v_r$. Now S_v can be computed as follows. Initialize S_v to be the empty set. For $j = 1, \ldots, r$ and for each $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} \in S_{v_j}$ set $w := 1 + \max\left(\{\ell \geq 0 : x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^\ell \in S_v\} \cup \{-1\}\right)$ and put $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^w$ in S_v. Note that in the first round, that is, when $i = 1$, the empty product $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}}$ is defined to be 1.

When we put $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^w$ in S_v, then we know that $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^{w-1}$ is already in S_v (if $w > 0$) implying that there were w occurrences of the monomial $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}}$ in $S_{v_1}, \ldots, S_{v_{j-1}}$. Thus, together with S_{v_j} there are $w+1$ of those, hence $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^w$ is indeed a standard monomial for v.

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

3.2 Another try

We intend to build a trie for the exponent vectors of $\mathrm{Sm}\,(I(V))$. We construct this trie U level by level. The edges of U are numbered by natural numbers. This way, the vertices on the i^{th} level of U will correspond to monomials in variables $x_1, \ldots, x_i$. (Here we read the exponent vectors from left to right, hence U is *not* a reverse trie.)

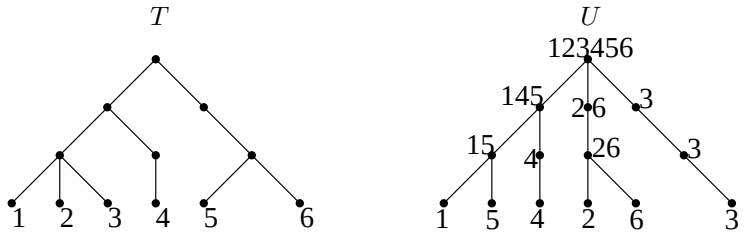
Furthermore, we assign some leaves of T to vertices of U. When the $(i-1)^{st}$ level of U has been constructed, then we use T together with the leaves assigned to the $(i-1)^{st}$ level of U to build the i^{th} level of U. In the following pseudo code of the algorithm we record (a part of) this assignment in an array A. Upon completion of the i^{th} phase leaf l of T is assigned to vertex $A[l]$ on the i^{th} level of U.

```
Let U be a tree consisting of a single root r;
For l ∈ {leaves of T} do A[l] := r; endfor;
For i = 1,...,n do
   //We now build the i^th level of U
   For v ∈ {vertices on the (n−i)^th level of T} do
      For l ∈ {leaves of T which are descendants of v} do
         b[A[l]] := 0;
      endfor;
      For l ∈ {leaves of T which are descendants of v} do
         b[A[l]] := b[A[l]] + 1;
         A[l] := (the child of A[l] given by edge number b[A[l]] − 1);
         //If such an edge does not exist, we create a new child
      endfor;
   endfor;
endfor;
```

We also have to slightly modify the first trie T to get the nodes of T in the same level and the descendant leaves of a vertex v in constant time. For this purpose every vertex has three additional pointers to other nodes. One points to a vertex in the same level in such a way that the vertices of a level form a linked list. In particular all the leaves of T are in a linked list L and moreover the descendant leaves of any vertex form a contiguous sublist of L. The other two pointers of a vertex gives the first and the last leaf of L belonging the corresponding vertex.

For a given V we build T in a incremental fashion. We start with an empty trie and insert the elements of V in turn. Suppose that we have a trie T. Adding the new element $\mathbf{v}$ to the structure implies the creation of a new root-to-leaf path in T. When the path is ready we have to modify the pointers. To this end denote the first new vertex by v. The first and last leaves of all the new vertices are the only new leaf as well as the last leaf of all the vertices on the way from v to the root. The first leaves of the vertices above v remain unchanged. To maintain the linked list of the vertices of the i^{th} level we simply insert the new node between the former last descendant of v on the i^{th} level and its successor. Doing this proceeding downwards from v requires not much extra work.

The following example gives the result of our new algorithm applied to the set V of Figure 1. We numbered the leaves of T to make the assignement visible and we do not show the labels of the edges of U as they can be reconstructed easily: number the edges leaving a vertex from left to right with $0, 1, \ldots,$ respectively.



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

To prove the correctness of the algorithm, we have to verify three basic properties of the assignment of leaves of T to vertices of U. If a leaf l of T is assigned to a vertex u then we also say that u *contains* l.

Lemma 10. *For every leaf l of T, the vertices in U which contain l form a path from the root to a leaf of U.*

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

Lemma 11. *If two leaves l_1 and l_2 of T are assigned to the same vertex on the i^{th} level of U then the ancestors of l_1 and l_2 on the $(n-i)^{th}$ level of T are different.*

Proof. Suppose for contradiction that l_1 and l_2 satisfies the condition of the lemma but they have a common ancestor v on the $(n-i)^{th}$ level of T. By Lemma 10 we know that l_1 and l_2 are assigned to the same vertex on the $(i-1)^{th}$ level of U as well. When building the i^{th} level of U and working in the

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

loop with the common ancestor v, then we have $A[l_1] = A[l_2]$, hence the counter b will separate them on the i^{th} level of U. □

Lemma 12. *Let l be a leaf of T and for some $0 \leq i \leq n$ let v be the ancestor of l on the $(n-i)^{th}$ level of T. Suppose that we assigned l to a vertex on the i^{th} level of U, to which the path from the root is marked by $w_1, \ldots, w_i$ respectively. Then*

$$x_1^{w_1} \ldots x_i^{w_i} \in S_v.$$

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

Suppose that the statement is true for the $(i-1)^{st}$ level of U, and let l be a leaf of T assigned to the vertex $w_1 \ldots w_{i-1}w$ on the i^{th} level of U, with ancestor v on the $(n-i)^{th}$ level of T. We have to prove $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^w \in S_v$.

By the algorithm there exist leaves $l_0, l_1, \ldots, l_{w-1}, l_w = l$ of T, such that they are all assigned to the vertex $w_1 \ldots w_{i-1}$ of U, and their common ancestor on the $(n-i)^{th}$ level of T is v. Denote the ancestor of l_j on the $(n-i+1)^{st}$ level of T by v_j. By Lemma 11, the v_j are pairwise different. The induction hypothesis gives that $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} \in S_{v_j}$ for $j = 0, \ldots, w$, hence $x_1^{w_1} \ldots x_{i-1}^{w_{i-1}} x_i^w \in S_v$ by Corollary 8. □

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

Theorem 13. *The trie U given by the above algorithm is the trie of the exponent vectors of* $\mathrm{Sm}\,(I(V))$.

Proof. On the one hand, we apply Lemma 12 with $i = n$: the root v of T is an ancestor of every leaf, and $S_v = \mathrm{Sm}\,(I(V))$. These imply that every monomial corresponding to a leaf of U is in $\mathrm{Sm}\,(I(V))$.

On the other hand, since the root of T is a common ancestor for every leaf of T, Lemma 11 yields that every leaf of U contains exactly one leaf l of T. Together with Lemma 10 this gives that U has exactly m leaves, where $m = |V| = |\mathrm{Sm}\,(I(V))|$, proving our claim. □

To sum up, our algorithm consists of two major stages. First we construct the reverse trie T of V together with pointers needed in the second stage. Then we build the trie U by the algorithm above. In particular, we do not compute every S_v explicitly, though it would not require too much extra work.

Theorem 14. *Let $r+1$ be the maximal degree of the trie T and $|V| = m$. Then the above algorithm computes $\mathrm{Sm}\,(I(V))$ in $O(nmr)$ time. If we assume that there exists an ordering on the coordinate set $\mathcal{B} \subseteq \mathbb{F}$ of V which can be tested in constant time then the algorithm makes $O(nm \log r)$ steps.*

Proof. We claim that the second stage can be done in $O(nm)$ time.

Consider the two `For` loops

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

  `For` $l \in \{$`leaves of` T `which are descendants of` $v\}$ `do`

As every leaf l of T has exactly one ancestor v on the $(n-i)^{th}$ level of T, we work with every l only once, and so building of the i^{th} level of U requires $O(m)$ steps. This proves that the second stage can be done in $O(nm)$ time.

Unlike the second, the first stage of the algorithm does depend largely on the assumptions on $\mathbb{F}$ and r. The computational cost of inserting a point $\mathbf{y}$ to a trie depends on the way we can compare elements of $\mathcal{B}$. If there is no easily checkable ordering on $\mathcal{B}$, then in the worst case we need r comparisons to determine the next edge of the path describing $\mathbf{y}$. This gives an $O(nr)$ time bound for each point of V. Once the new path is given it requires $O(n)$ time to rebuild the pointers. Thus inserting all the m points of V can be realised in $O(mnr)$ uniform time.

If we assume that there is an ordering on $\mathcal{B}$, and we can compare two elements in constant time, then we get $O(mn \log r)$ time for building T, by using binary search when looking for a coordinate value among the children of an existing vertex.

□

4 Theoretical applications

It is of interest to obtain explicit descriptions of the standard monomials of some sets $V \subseteq \mathbb{F}^n$. Applications of such results can be found in [7] or [11]. Here we demonstrate that in some cases Theorem 3 allows one to obtain a nice description of $\mathrm{Sm}\,(I(V))$. As a first example, consider the case $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$, $|\mathcal{B}| = n$ and

$$V = \left\{ \left(\alpha_{\pi(1)}, \alpha_{\pi(2)}, \ldots, \alpha_{\pi(n)}\right) \,:\, \pi \text{ is a permutation of } [n] \right\}.$$

The standard monomials and Gröbner bases of the ideal $I(V)$ have been studied in [9] and [12]. Their description of the lexicographic standard monomials follows easily from our approach. Lea can find out y_i if and only if she can guess at least i times, since Stan can always choose any of the remaining i possibilities for y_i. This means that $\mathbf{x}^{\mathbf{w}}$ is a standard monomial of $I(V)$ if and only if $w_i < i$ for all $i \in [n]$.

The case $|\mathcal{B}| = 2$, that is, when $V \subseteq \{\alpha_1, \alpha_2\}^n$, is of special interest in combinatorics. Let $\mathcal{F}$ be a family of subsets of $[n]$. We can represent $\mathcal{F}$ in $\mathbb{F}^n$ as the set V of the characteristic vectors of the sets in $\mathcal{F}$. In this section we present

a theorem that allows us to describe the lexicographic standard monomials of a symmetric family. This result extends previous work from [3], [10] and [6].

Let D be a subset of the integers. We denote by $V_{D,n}$ the set of all 0-1 vectors of length n whose Hamming weight is in D. Note that $V_{D,n}$ is the set of characteristic vectors of the set family $\mathcal{F}_{D,n}$, where

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

We need some more notation. For $t \in \mathbb{Z}$ and $A \subseteq \mathbb{Z}$ we put

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

For any $A \subseteq \mathbb{Z}$, we set $A^{(0)} = A \cup (A-1)$ and $A^{(1)} = A \cap (A-1)$. If $\mathbf{w} = (w_1, \ldots, w_n) \in \{0,1\}^n$ then

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

It turns out that $D^{(\mathbf{w})}$ is a quite convenient tool to see if $\mathbf{x}^{\mathbf{w}}$ a standard monomial of $V_{D,n}$. In fact, we shall prove that $\mathbf{x}^{\mathbf{w}} \in \mathrm{Sm}(I(V_{D,n}))$ if and only if $0 \in D^{(\mathbf{w})}$. We illustrate this point by taking another look at our old example from Section 2.

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

Theorem 15. *$\mathbf{x}^{\mathbf{w}}$ is a standard monomial of $I(V_{D,n})$ with respect to the lexicographic order if and only if $\mathbf{w} \in \{0,1\}^n$ and $0 \in D^{(\mathbf{w})}$.*

Proof. We prove that Stan wins the lex game $\mathrm{Lex}(V_{D,n}; \mathbf{w})$ if and only if $\mathbf{w} \in \{0,1\}^n$ and $0 \in D^{(\mathbf{w})}$. By Theorem 3 this yields our statement.

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

We prove by induction on n that

$$A := \{t \in \mathbb{Z} \,:\, \text{Stan wins } \mathrm{Lex}(V_{D-t,n}; \mathbf{w})\} = D^{(\mathbf{w})}. \tag{3}$$

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

To prove (3), first we consider the case $n = 1$. If $w = 0$ then Stan wins $\mathrm{Lex}(V_{D-t,1}; w)$ if and only if $V_{D-t,1} \neq \emptyset$, since Lea is not allowed to guess anything. This means $(D-t) \cap \{0,1\} \neq \emptyset$, so $t \in D \cup (D-1) = D^{(w)}$. If $w = 1$ then Stan wins if and only if $|V_{D-t,1}| = 2$, since Lea can check only one of the two possibilities. Thus $\{0,1\} \subseteq (D-t)$ hence $t \in D \cap (D-1) = D^{(w)}$.

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

$$C := \{t \in \mathbb{Z} \,:\, \text{Stan wins } \mathrm{Lex}(V_{D-t,n-1}; (w_1, \ldots, w_{n-1}))\}\,,$$

we have $C = D^{(w_1,\ldots,w_{n-1})}$. We have to prove that $C^{(w_n)} = A$.

When Stan and Lea play a $\mathrm{Lex}(V_{D-t,n}; \mathbf{w})$ game and Stan reveals the last coordinate y_n, then they keep on playing either a $\mathrm{Lex}(V_{D-t,n-1}; (w_1, \ldots, w_{n-1}))$ game (if $y_n = 0$) or a $\mathrm{Lex}(V_{D-t-1,n-1}; (w_1, \ldots, w_{n-1}))$ game (if $y_n = 1$).

If $w_n = 0$ then Stan wins $\mathrm{Lex}(V_{D-t,n}; \mathbf{w})$ if and only if he wins either $\mathrm{Lex}(V_{D-t,n-1}; (w_1, \ldots, w_{n-1}))$ or $\mathrm{Lex}(V_{D-t-1,n-1}; (w_1, \ldots, w_{n-1}))$, since he can choose y_n accordingly.

If $w_n = 1$ then Stan wins $\mathrm{Lex}(V_{D-t,n}; \mathbf{w})$ if and only if he wins both of the games

$$\mathrm{Lex}(V_{D-t,n-1}; (w_1, \ldots, w_{n-1})) \text{ and } \mathrm{Lex}(V_{D-t-1,n-1}; (w_1, \ldots, w_{n-1})),$$

since in this case Lea can force either of the above alternatives by a suitable guess for y_n.

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

4.1 ℓ-wide families modulo r

We now calculate explicitly $D^{(\mathbf{w})}$ for some specific sets D. This will extend and generalize known results on standard monomials for some symmetric set families.

Let d, r and ℓ be integers with $0 \leq d < r$ and $1 \leq \ell < r$. Set

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

Consider a square grid with coordinate axes corresponding to 1 (horizontal X axis) and 0 (vertical Y axis). A *lattice path* is a polygon which starts at the origin and proceeds in unit length steps. A step can be either to the right or to the upwards direction. We can associate a lattice path $\hat{\mathbf{w}}$ to any $\mathbf{w} \in \{0,1\}^n$ in a straightforward way. For each i $(1 \leq i \leq n)$ the i^{th} step of $\hat{\mathbf{w}}$ is horizontal if $w_i = 1$ and vertical otherwise. We have the following:

Proposition 16. *Let d' be the integer for which $d' \equiv d \pmod{r}$ and*

$$\frac{n - r - \ell}{2} < d' \leq \frac{n + r - \ell}{2}.$$

Then $0 \in D^{(\mathbf{w})}$ if and only if $\hat{\mathbf{w}}$ does not touch the line $Y = X - \ell$ before touching the line $Y = X + r - \ell$ and in the case where $\hat{\mathbf{w}}$ does not reach these two lines, the X coordinate of its endpoint n_1 (which is in fact the number of the 1 coordinates in $\mathbf{w}$) satisfies

$$n_1 \leq \min\{n - d', d' + \ell - 1\}.$$

Every $\hat{\mathbf{w}}$ intersects one of the thick lines in Figure 2. Proposition 16 states that if $\hat{\mathbf{w}}$ reaches the thicker line first then $\mathbf{x}^{\mathbf{w}}$ is a leading monomial, otherwise $\mathbf{x}^{\mathbf{w}}$ is a standard monomial.

Proof of Proposition 16. Let a, b be integers. We define the interval $[a, b]$ as

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

in particular if $a > b$ then $[a, b] = \emptyset$. If $[a, b] \neq \emptyset$ then $[a, b]^{(0)} = [a - 1, b]$ and $[a, b]^{(1)} = [a, b - 1]$. More generally suppose that in $\mathbf{w} \in \{0,1\}^n$ there are n_1

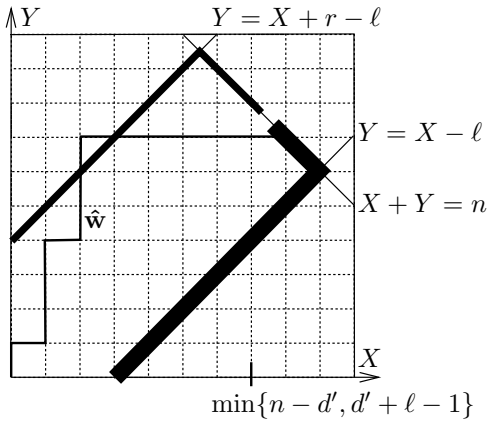


Figure 2: An example with $n = 15$, $r = 7$, $\ell = 3$ and $d = 1$ or $d = 5$. We see that $\mathbf{x}^{\mathbf{w}} = x_2x_6x_{10}x_{11}x_{12}x_{13}x_{14}x_{15}$ is a standard monomial.

one and $n - n_1 = n_0$ zero coordinates, and for every proper prefix $\mathbf{w}'$ of $\mathbf{w}$ we have $[a,b]^{(\mathbf{w}')} \neq \emptyset$. Then

$$[a,b]^{(\mathbf{w})} = [a - n_0, b - n_1]. \tag{4}$$

Here $[a - n_0, b - n_1]$ is empty if and only if $a - n_0 > b - n_1$, that is, the length $b - a + 1$ of the interval $[a,b]$ is at most $n_1 - n_0$. From $[a,b]^{(w_1,\ldots,w_{n-1})} \neq \emptyset$ and $[a,b]^{(\mathbf{w})} = \emptyset$ it follows that $w_n = 1$ and $a - n_0 \leq b - (n_1 - 1)$. Therefore if $\mathbf{w}$ is as above, then $[a - n_0, b - n_1] = \emptyset$ if and only if $b - a + 1 = n_1 - n_0$. We summarize these observations as follows: if $\mathbf{w}^*$ is the shortest prefix of $\mathbf{w} \in \{0,1\}^n$ for which $[a,b]^{(\mathbf{w}^*)} = \emptyset$ then $\mathbf{w}^*$ has exactly $b - a + 1$ more one coordinates than zeros.

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

$$A^{(w)} = \bigcup_{i\in\Gamma} [a_i, b_i]^{(w)} \quad \text{for } w \in \{0,1\}. \tag{5}$$

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

$$(A - r)^{(\mathbf{w})} = A^{(\mathbf{w})} - r. \tag{6}$$

In our case we have $D = \cup_{i\in\mathbb{Z}}(A - ir)$, with $A = [d, d + \ell - 1]$. By the assumption $\ell < r$ one can see that the intervals $A - ir = [d - ir, d + \ell - 1 - ir]$ are separated. From (5) and (6) easy induction on n gives that

$$D^{(\mathbf{w})} = \bigcup_{i\in\mathbb{Z}} \left(A^{(\mathbf{w})} - ir \right), \tag{7}$$

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

Thus (7) allows us to reduce the calculation of $D^{(\mathbf{w})}$ to that of the interval $A^{(\mathbf{w})}$. In particular $D^{(\mathbf{w})} = \emptyset$ if and only if $A^{(\mathbf{w})} = \emptyset$ and there is no prefix $\mathbf{w}'$ of $\mathbf{w}$ such that $\left|A^{(\mathbf{w}')}\right| = r$. Let $\mathbf{w}^*$ be the shortest prefix of the above $\mathbf{w}$ for which $A^{(\mathbf{w}^*)} = \emptyset$. We have seen that $\mathbf{w}^*$ has ℓ more 1 coordinates than zeros, that is, the path $\hat{\mathbf{w}}^*$ reaches the line $Y = X - \ell$ at its endpoint. The condition $\left|A^{(\mathbf{w}')}\right| < r$ for every prefix $\mathbf{w}'$ of $\mathbf{w}^*$ together with the condition on $\mathbf{w}^*$ is equivalent to that $\mathbf{w}'$ has less than $r - \ell$ more zeros than ones, or equivalently, the path $\hat{\mathbf{w}}'$ stays under the line $Y = X + r - \ell$.

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

It remains to consider the case when $\hat{\mathbf{w}}$ stays between the two lines. Let the endpoint of $\hat{\mathbf{w}}$ be (n_1, n_0). Here $D^{(\mathbf{w})}$ can be calculated according to (7). By (4) we have

$$A^{(\mathbf{w})} = [d, d + \ell - 1]^{(\mathbf{w})} = [d - n_0, d + \ell - 1 - n_1],$$

hence we obtain that

$$D^{(\mathbf{w})} = \bigcup_{i \in \mathbb{Z}} [d + ir - n_0, d + ir + \ell - 1 - n_1]. \tag{8}$$

The intersection of the lines $Y = X + r - \ell$ and $X + Y = n$ is the point $\left(\frac{n-r+\ell}{2}, \frac{n+r-\ell}{2}\right)$. Since (n_1, n_0) is on $X + Y = n$, and below $Y = X + r - \ell$, it follows that

$$n_0 \leq \frac{n + r - \ell}{2} \quad \text{and} \tag{9}$$

$$n_1 \geq \frac{n - r + \ell}{2} \ . \tag{10}$$

Thus by (8) we have $0 \in D^{(\mathbf{w})}$ if and only if there exists an $i \in \mathbb{Z}$ such that $d + ir - n_0 \leq 0 \leq d + \ell - 1 + ir - n_1$. From this we infer

$$d + ir \leq n_0 \leq \frac{n + r - \ell}{2}$$

by (9) and

$$d + ir \geq n_1 - \ell + 1 \geq \frac{n - r + \ell}{2} - \ell + 1 > \frac{n - r - \ell}{2}$$

follows from (10). These yield that $d' = d + ir$. Therefore $0 \in D^{(\mathbf{w})}$ if and only if $d' - n_0 \leq 0 \leq d' + \ell - 1 - n_1$ which is precisely the condition $n_1 \leq \min\{n - d', d' + \ell - 1\}$ by $n_0 = n - n_1$. □

By selecting r greater than n, we obtain an important special case of Proposition 16, the standard monomials of a complete ℓ-wide family. This was first described in [6] together with the respective reduced Gröbner basis and some combinatorial applications. In the case $r > n$ the selection of an even larger r does not alter $V_{D,n}$, hence we can suppose that $r > n + \ell$. With this setting of the parameters, the line $Y = X + r - \ell$ does not play any role. We obtain the following simple characterization of the standard monomials.

Corollary 17. *Let $\mathcal{F}$ be a complete ℓ-wide family with $0 \leq d \leq d+\ell-1 \leq n$, that is*

$$\mathcal{F} = \{Z \subseteq [n] \,:\, d \leq |Z| \leq d+\ell-1\}\,,$$

and V be the set of characteristic vectors of the elements of $\mathcal{F}$. Then the monomial $\mathbf{x}^{\mathbf{w}}$ is a standard monomial of $I(V)$ if and only if the path $\hat{\mathbf{w}}$ does not reach the line $Y = X - \ell$ and the X coordinate of its endpoint n_1 is at most $\min\{n-d, d+\ell-1\}$. □

Another interesting special case is $\ell = 1$, when $\mathcal{F}$ is the collection of all subsets X of $[n]$ whose size is d modulo r. Then we have the lines $Y = X - 1$ and $Y = X + r - 1$. The upper bound for n_1 is $\min\{n - d', d'\}$ with the appropriate d'. If $\mathbf{w}$ is the exponent vector of a standard monomial, then the property that $\hat{\mathbf{w}}$ stays over the line $Y = X - 1$ means that there are at least as many zeros in every prefix of $\mathbf{w}$ as ones, in other words, $\mathbf{w}$ is a ballot sequence.

Acknowledgement We are grateful to Balázs Rácz and Dömötör Pintér for their remarks on the algorithm of Section 3. We thank the anonymous referee for useful suggestions.

References

[1] W. W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, *American Mathematical Society*, 1994.

[2] A. V. Aho, J. E. Hopcroft, J. D. Ullman, The design and analysis of computer algorithms, *Addison-Wesley*, Reading, Massachusetts, 1978.

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

[4] T. Becker, V. Weispfenning, Gröbner bases – a computational approach to commutative algebra, *Springer-Verlag*, Berlin, Heidelberg, 1993.

[5] L. Cerlienco, M. Mureddu, From algebraic sets to monomial linear bases by means of combinatorial algorithms, Formal power series and algebraic combinatorics, (Montreal, PQ, 1992) *Discrete Mathematics* **139** (1995), no. 1–3, 73–87.

[6] K. Friedl, G. Hegedűs, L. Rónyai, Gröbner bases for complete ℓ-wide families, *to appear.*

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

[8] G.-M. Greuel, G. Pfister, H. Schönemann, Singular 3.0. A Computer Algebra System for Polynomial Computations, *Centre for Computer Algebra, University of Kaiserslautern* (2005). `http://www.singular.uni-kl.de`.

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

[10] G. Hegedűs, L. Rónyai, Gröbner bases for complete uniform families, *J. of Algebraic Combinatorics* **17** (2003), 171–180.

[11] 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.

[12] A. E. Kézdy, H. S. Snevily, Polynomials that vanish on distinct n^{th} roots of unity, *Combinatorics, Probability and Computing* **13** (2004), 37–59.

[13] D. E. Knuth, The art of computer programming, Volume 3., *Addison-Wesley*, Reading 1973.