*Annales Univ. Sci. Budapest., Sect. Comp. 42 (2014) 249–260*

# A NOTE ON ALON'S COMBINATORIAL NULLSTELLENSATZ

**Tamás Mészáros** (Budapest, Hungary)

**Lajos Rónyai** (Budapest, Hungary)

*This note is dedicated to András Benczúr on the occasion of his 70th birthday*

Communicated by János Demetrovics

(Received June 1, 2014; accepted July 1, 2014)

**Abstract.** Alon's Combinatorial Nullstellensatz (Theorem 1.1 from [2]), and in particular the resulting nonvanishing criterion (Theorem 1.2 from [2]) is a very useful algebraic tool in combinatorics. It has several remarkable applications, see [4], [5], [7], [9], [10], [14], [15] for some recent examples. It is a theorem on polynomial functions on a discrete box $\mathbf{S} = S_1 \times \cdots \times S_n$, where $S_i$, $i = 1, \ldots, n$ are finite subsets of a field $\mathbb{F}$. It is a natural question to ask: what other finite subsets $X \subseteq \mathbb{F}$ allow a similar result? Here we characterize those sets $X \subseteq \mathbb{F}^n$, whose vanishing ideal $I(X)$ has a Gröbner basis similar to the Gröbner basis of $I(\mathbf{S})$.

## 1. Introduction

We introduce first some notations. $\mathbb{F}$ will stand for an arbitrary field, the ring of polynomials over $\mathbb{F}$ in variables $x_1, \ldots, x_n$ will be denoted by $\mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[\mathbf{x}]$ and, to shorten our notation, we will write $f(\mathbf{x})$ for

*Key words and phrases*: Combinatorial Nullstellensatz, Nonvanishing Theorem, Gröbner basis, reduction.
*2010 Mathematics Subject Classification*: 05-xx, 05E40, 12D10, 13P10.
The project is supported in part by OTKA Grant NK 105 645.
https://doi.org/10.71352/ac.42.249

$f(x_1, \ldots, x_n)$. Vectors of length $n$ will be denoted by boldface letter, for example $\mathbf{s} = (s_1, \ldots, s_n)$.

Let $S_1, S_2, \ldots, S_n$ be finite nonempty subsets of $\mathbb{F}$ and let

$$\mathbf{S} = S_1 \times S_2 \times \cdots \times S_n \subseteq \mathbb{F}^n.$$

For $i = 1, \ldots, n$ put

$$g_i = g_i(x_i) = \prod_{s \in S_i} (x_i - s) \in \mathbb{F}[\mathbf{x}].$$

Alon's Combinatorial Nullstellensatz (Theorem 1.1 in [2]) is a specialized and strengthened version of the Hilbertsche Nullstellensatz for the ideal $I(\mathbf{S})$ of all polynomial functions vanishing on $\mathbf{S}$. It states that if a polynomial $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ vanishes over all the common zeros of $g_1, \ldots, g_n$ (i.e. $f \in I(\mathbf{S})$), then there are polynomials $h_1, \ldots, h_n \in \mathbb{F}[\mathbf{x}]$, satisfying $deg(h_i) \leq deg(f) - deg(g_i)$, so that

$$f = \sum_{i=1}^{n} h_i g_i.$$

From this a simple and widely applicable nonvanishing criterion (Theorem 1.2 in [2]) has been deduced. It provides a sufficient condition for a polynomial $f \in \mathbb{F}[\mathbf{x}]$ for not vanishing everywhere on $\mathbf{S}$.

The usefulness of the Combinatorial Nullstellensatz leads naturally to the question: what finite point sets $X \subseteq \mathbb{F}^n$ (other than discrete boxes) allow a similar, possibly not much weaker, theorem to hold. Here we formulate a weaker version of the Theorem (Theorem 3.1 (ii)) in terms of lexicographic standard monomials. Moreover we characterize those finite point sets $X$ for which the weaker Nullstellensatz holds. In fact, we give two characterizations, one in terms of the vanishing ideal $I(X)$ of $X$, and one other in terms of some combinatorial properties of $X$.

This note is organized as follows. After the introduction in Section 2 we present the basic notions and facts from the theory of Gröbner bases and vanishing ideals. Next in Section 3 we state our main result, Theroem 3.1, and provide some important examples. Section 4 is devoted to the proof of Theorem 3.1. At the end, in Section 5, we make some possible suggestions for further study.

## 2. Preliminaries

A total order $\prec$ on the monomials of $\mathbb{F}[\mathbf{x}]$ is a *term order*, if 1 is the minimal element of $\prec$, and $\prec$ is compatible with multiplication with monomials. For an

example of term orders consider the *lexicographic ordering* of monomials (*lex order* for short). We have $x_1^{w_1} \dots x_n^{w_n} \prec_{\text{lex}} x_1^{u_1} \dots x_n^{u_n}$ if and only if $w_i < u_i$ holds for the smallest index $i$ such that $w_i \neq u_i$.

The *leading monomial* $lm(f)$ of a nonzero polynomial $f \in \mathbb{F}[\mathbf{x}]$ is the largest monomial (with respect to a fixed term order $\prec$) which appears with nonzero coefficient in $f$, when written as the usual linear combination of monomials. The leading monomial of a polynomial $f$ together with its coefficient is called the *leading term* of $f$ and is denoted by $lt(f)$. We denote the set of all leading monomials of polynomials of a given ideal $I \lhd \mathbb{F}[\mathbf{x}]$ by $Lm(I) = \{lm(f) : f \in I\}$. A monomial is called a *standard monomial* of $I$, if it is not a leading monomial of any $f \in I$. $Sm(I)$ denotes the set of standard monomials of $I$. Standard monomials have some very nice properties, among other things they form a linear basis of the $\mathbb{F}$-vector space $\mathbb{F}[\mathbf{x}]/I$. The *vanishing ideal* of a point set $X \subseteq \mathbb{F}^n$, denoted by $I(X)$, is the collection of all polynomials $f \in \mathbb{F}[\mathbf{x}]$ for which $f(\mathbf{v}) = 0$ for all $\mathbf{v} \in X$. In the case of vanishing ideals of finite point sets $|Sm(I(X))| = |X|$, in particular $Sm(I(X))$ is finite. Ideals, where $Sm(I)$ is finite, i.e. $\mathbb{F}[\mathbf{x}]/I$ is a finite dimensional $\mathbb{F}$-vector space, are called called *zero dimensional ideals*. For further details on term orders and standard monomials see [1].

In [6] Felszeghy, Ráth and Rónyai proposed an efficient algorithm for determining the standard monomials of the vanishing ideal of a finite point set $X \subseteq \mathbb{F}$ when $\prec$ is the lexicographic order. Their method revealed that the family of standard monomials is independent, in a sense explained below, from $\mathbb{F}$ and from the embedding of $X$ in $\mathbb{F}^n$, it depends only on the property whether 2 points coincide at some coordinate or not: if $A \subseteq \mathbb{F}$ is the collection of all field elements that occur as coordinates in $X$, $m = |A| - 1$ and if $\varphi_i : A \to \{0, 1, \dots, m\} \subseteq \mathbb{R}$, $i = 1, 2, \dots, n$ are real valued injective functions, then the standard monomials of the vanishing ideal $I(\widehat{X}) \lhd \mathbb{R}[\mathbf{x}]$ of the point set

$$\widehat{X} = \{(\varphi_1(s_1), \varphi_2(s_2), \dots, \varphi_n(s_n)) \mid (s_1, s_2, \dots, s_n) \in X\} \subseteq \{0, 1, \dots, m\}^n \subseteq \mathbb{R}^n$$

with respect to the lexicographic term order are the same as those of the vanishing ideal $I(X) \lhd \mathbb{F}[\mathbf{x}]$.

For $1 \leq i \leq n$, the $i$-section of $Y \subseteq \{0, 1, \dots, m\}^n$ for $n - 1$ arbitrary elements

$$\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_n \in \{0, 1, \dots, m\}$$

is defined as

$$Y_i(\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_n) = \{\alpha \mid (\alpha_1, \dots, \alpha_{i-1}, \alpha, \alpha_{i+1}, \dots, \alpha_n) \in Y\}.$$

Using $i$-sections one can define $D_i$, the *downshift operation at coordinate* $i$. For any finite point set $Y \subseteq \{0, 1, \dots, m\}^n$, $D_i(Y)$ is the unique point set in

$\{0,1,\ldots,m\}^n$, for which

$$(D_i(Y))_i(\alpha_1,..,\alpha_{i-1},\alpha_{i+1},..,\alpha_n)=\{0,1,..,|Y_i(\alpha_1,..,\alpha_{i-1},\alpha_{i+1},..,\alpha_n)|-1\}$$

whenever $Y_i(\alpha_1,\ldots,\alpha_{i-1},\alpha_{i+1},\ldots,\alpha_n)$ is nonempty, otherwise it is empty as well.

From Section 10 of [13] we know that if $Y\subseteq\{0,1,\ldots,m\}^n$ and $\prec$ is the lexicographic term order, then for the vanishing ideal $I(Y)\lhd\mathbb{R}[\mathbf{x}]$ we have

$$Sm(I(Y))=\{\mathbf{x}^{\mathbf{u}}\mid\mathbf{u}\in D_n(D_{n-1}(\ldots D_1(Y)\ldots))\}.$$

For an ideal $I\lhd\mathbb{F}[\mathbf{x}]$ a finite subset $\mathcal{G}\subseteq I$ is a *Gröbner basis* of $I$ with respect to a term order $\prec$, if for every $f\in I$ there exists $g\in\mathcal{G}$ such that $lm(g)$ divides $lm(f)$. It is not hard to verify that $\mathcal{G}$ is actually a basis of $I$, that is, $\mathcal{G}$ generates $I$ as an ideal of $\mathbb{F}[\mathbf{x}]$.

Let $f,g\in\mathbb{F}[\mathbf{x}]$ and consider an arbitrary term order $\prec$. Suppose that there is a monomial $\mathbf{x}^{\mathbf{w}}$ in $f$ with nonzero coefficient $c_f$ that is divisible by $lm(g)$. Let the coefficient of $lm(g)$ in $g$ be $c_g$ and let

$$\widehat{f}(\mathbf{x})=f(\mathbf{x})-\tfrac{c_f\cdot\mathbf{x}^{\mathbf{w}}}{c_g\cdot lm(g)}g(\mathbf{x}).$$

This operation is called a *reduction* of $f$ with $g$. We replace $\mathbf{x}^{\mathbf{w}}$ in $f$ by monomials strictly less (with respect to $\prec$) than $\mathbf{x}^{\mathbf{w}}$. A Gröbner basis is called *reduced* if no polynomial $g$ from $\mathcal{G}$ can be reduced with $\mathcal{G}\backslash\{g\}$.

It is a fundamental fact that every nonzero ideal $I$ of $\mathbb{F}[\mathbf{x}]$ has a Gröbner basis (and a unique reduced Gröbner basis). The existence can be proven using S-polynomials. The *S-polynomial* of nonzero polynomials $f,g\in\mathbb{F}[\mathbf{x}]$ is

$$S(f,g)=\frac{L}{lt(f)}f-\frac{L}{lt(g)}g,$$

where $L$ is the least common multiple of the monomials $lm(f)$ and $lm(g)$. Buchberger's theorem (Theorem 1.7.4. in [1]) states that a finite set $\mathcal{G}$ of polynomials in $\mathbb{F}[\mathbf{x}]$ is a Gröbner basis for the ideal generated by $\mathcal{G}$ iff the S-polynomial of any two polynomials from $\mathcal{G}$ can be reduced to 0 using $\mathcal{G}$.

For proofs and a detailed introduction to Gröbner bases see [1].

If a finite set $\mathcal{G}$ of polynomials is a Gröbner basis of $I$ for every term order, then $\mathcal{G}$ is called a *universal Gröbner basis*. In terms of Gröbner bases Alon's Combinatorial Nullstellensatz actually states that the polynomials $g_1,\ldots,g_n$ form a universal Gröbner basis of the vanishing ideal $I(\mathbf{S})$ and that

$$Sm(I(S))=\{\mathbf{x}^{\mathbf{s}}\mid s_i<|S_i|\text{ for all }i\}$$

for every term order.

## 3. Main result

The main result of this note is a generalization of Alon's Combinatorial Nullstellensatz to a wider class of finite sets, not merely discrete boxes.

Let $X \subseteq \mathbb{F}^n$ be a finite point set. For $1 \leq k \leq n$ define the projection of $X$ to the last $n-k+1$ coordinates as

$$X_k = \{(s_k, \ldots, s_n) \mid \exists s_1, \ldots, s_{k-1} \in \mathbb{F} \text{ such that } (s_1, \ldots, s_n) \in X)\} \subseteq \mathbb{F}^{n-k+1}.$$

**Theorem 3.1.** *For a nonempty finite set $X \subseteq \mathbb{F}^n$ and for positive integers $d_1, \ldots, d_n$ the following are equivalent:*

*(i)* $Sm(I(X)) = \{\mathbf{x^u} \mid u_i < d_i \text{ for all } 1 \leq i \leq n\}$ *with respect to the lex order.*

*(ii) With respect to the lex order the reduced Gröbner basis of $I(X)$ is of the form $\{F_1, \ldots, F_n\}$, where for all $1 \leq i \leq n$ we have $lm(F_i) = x_i^{d_i}$.*

*(iii) For all $k = 1, \ldots, n-1$ the size of*

$$\{s \in \mathbb{F} \mid (s, s_{k+1}, \ldots, s_n) \in X_k\}$$

*is $d_k$ for all $(s_{k+1}, \ldots, s_n) \in X_{k+1}$, and $|X_n| = d_n$.*

■

Several examples of such point sets can be found:

**Example 3.2.** *Let $\mathbf{S} = S_1 \times \cdots \times S_n$ be a discrete box as in Alon's original Nullstellensatz. Here we have $d_i = |S_i|$ and $F_i(x_i, \ldots, x_n) = F_i(x_i) = \prod_{s \in S_i} (x_i - s)$ for all $i$. This example shows that Theorem 3.1 is indeed a generalization of the Combinatorial Nullstellensatz.*

**Example 3.3.** *Let $a_1, \ldots, a_n$ be different elements from $\mathbb{F}$, and consider all possible permutations of these elements as vectors in $\mathbb{F}^n$.*

$$P_n(a_1, \ldots, a_n) = \{(a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)}) \mid \pi \in S_n\},$$

*where $S_n$ is the symmetric group of degree $n$. In [8] the reduced Gröbner basis of $I(P_n(a_1, \ldots, a_n))$ was determined with respect to the lex order, where we have $d_i = i$ for $1 \leq i \leq n$. For the precise polynomials and proofs see [8].*

**Example 3.4.** *Let $A$ be an $n \times n$ matrix with entries $a_{i,j}$, $1 \leq i, j \leq n$ from the field $\mathbb{F}$, and suppose that each column contains $n$ different elements, i.e. $a_{i_1 j} \neq a_{i_2 j}$ for all $j$ and $i_1 \neq i_2$. Put*

$$\mathcal{P}(A) = \{(a_{1\pi(1)}, a_{2\pi(2)}, \ldots, a_{n\pi(n)}) \mid \pi \in S_n\},$$

*where $S_n$ is the symmetric group of degree $n$. Sets of the form $\mathcal{P}(A)$ are the generalizations of permutations, and clearly satisfy the the combinatorial condition (iii) from Theorem 3.1.*

*In connection with norm graphs ([3]), the polynomials*

$$f_i(x_1, \ldots, x_n) = \prod_{j=1}^{n} (x_j - a_{ij}), i = 1, \ldots, n$$

*turn up, where the field elements $a_{ij}$ satisfy the same condition as above. Their set of common zeros is exactly $\mathcal{P}(A)$.*

**Example 3.5.** *For this example let $\mathbb{F} = \mathbb{C}$ and for $n$ different nonzero complex numbers $z_1, z_2, \ldots, z_n$ put*

$$f(x, y) = x^n - y,$$

$$g(y) = (y - z_1)(y - z_2) \cdots (y - z_n).$$

*For $1 \leq i \leq n$ let $w_i$ be one $n^{th}$ root of $z_i$, and let $\varepsilon$ be a primitive $n^{th}$ root of unity. The vanishing set of $I = \langle f, g \rangle \lhd \mathbb{C}[x, y]$ is*

$$X = \{(\varepsilon^k w_i, z_i) \mid 1 \leq i, k \leq n\} \subseteq \mathbb{C}^2,$$

*clearly possesses the desired combinatorial property with $d_1 = d_2 = n$, and hence by Theorem 3.1 for the lex order we have $Sm(I(X)) = \{x^\alpha y^\beta \mid \alpha, \beta < n\}$. $f, g \in I(X)$ by definition, moreover, using $f$ and $g$ any polynomial $h \in \mathbb{C}[x, y]$ can be reduced to some polynomial $\widetilde{h}$ whose degree is smaller than $n$ both in $x$ and in $y$, and so $\widetilde{h}$ is a linear combination of standard monomials. This implies that $f$ and $g$ form a reduced Gröbner basis of $I(X)$ with respect to the lex order, in particular $I(X) = \langle f, g \rangle$.*

Similar examples can be given in higher dimensions as well.

**Example 3.6.** *For our last example suppose that for $1 \leq i \leq N$ we are given a positive integer $n_i$, a point set $X^{(i)} \subseteq \mathbb{F}^{n_i}$ satisfying property (iii) from Theorem 3.1 and a reduced Gröbner basis $\mathcal{G}_i = \{F_{i1}, \ldots, F_{in_i}\}$ of the vanishing ideal $I(X^{(i)}) \lhd \mathbb{F}[x_{i1}, \ldots, x_{in_i}]$ with respect to the lex order such that $lm(F_{ij}) = x_{ij}^{d_{ij}}$, $1 \leq j \leq n_i$. Now let*

$$X = X^{(1)} \times X^{(2)} \times \cdots \times X^{(N)} \subseteq \mathbb{F}^{\sum_{i=1}^{N} n_i}$$

*and*

$$\mathcal{G} = \bigcup_{i=1}^{N} \mathcal{G}_i.$$

*From the construction it follows that $X$ satisfies the given combinatorial property as well, and so by Theorem 3.1 for the lex order we have*

$$Sm(X) = \{\mathbf{x}^{\mathbf{u}} \mid u_{ij} < d_{ij} \text{ for all } 1 \le i \le N \text{ and } 1 \le j \le n_i\}.$$

*On the other hand using $\mathcal{G}$ any polynomial $f$ in the variables $x_{ij}$, $1 \le i \le N$, $1 \le j \le n_i$ can be reduced to a form $\widetilde{f}$ where the degree in each variable $x_{ij}$ is less than $d_{ij}$, and so $\widetilde{f}$ is the linear combination of standard monomials. This implies that $\mathcal{G}$ is a reduced Gröbner basis of $I(X)$.*

This direct product construction allows us to combine the earlier examples and to obtain more complicated ones.

**Remark 3.1.** *A Gröbner basis $\mathcal{G}$ is called* degree reducing*, if for every element $g \in \mathcal{G}$ the leading monomial $lm(g)$ is the unique monomial of maximal degree, i.e. $deg(lm(g)) = deg(g)$ and for any other monomial $\mathbf{x}^{\mathbf{u}}$ occurring in $g$ with nonzero coefficient we have $deg(\mathbf{x}^{\mathbf{u}}) < deg(lm(g))$.*

*If $X \subseteq \mathbb{F}^n$ is such that $I(X)$ has a degree reducing Gröbner basis, then the original proof of the Nonvanishing Theorem from [2] applies to obtain*

**Proposition 3.7.** *Let $X \subseteq \mathbb{F}^n$ be a nonempty set such that $I(X)$ has a degree reducing Gröbner basis for some term order. If a polynomial $f \in \mathbb{F}[\mathbf{x}]$ of degree $d$ contains a standard monomial for $I(X)$ of degree $d$ with nonzero coefficient, then there is some point $\mathbf{s} \in X$ where $f$ does not vanish, i.e. $f(\mathbf{s}) \neq 0$.*

*Note that in the original case of the Nonvanishing Theorem in [2] the polynomials $g_1, \ldots, g_n$ formed a universal degree reducing Gröbner basis. An interesting feature of Example 3.5 is that it provides an example of a point set that is not a discrete box, but we still have a degree reducing Gröbner basis and hence a Nonvanishing Theorem. Moreover in this case by Theorem 3.1 the condition in Proposition 3.7 reduces to a simple degree bound as in the original Nonvanishing Theorem.*

## 4. The proof of Theorem 3.1

In the rest of the paper $\prec$ will always stand for the lexicographic term order (though the statement of Lemma 4.1 holds for any term order). First we

prove, that $(i)$ and $(ii)$ in Theorem 3.1 are actually equivalent for every zero dimensional ideal.

**Lemma 4.1.** *Let $I \lhd \mathbb{F}[\mathbf{x}]$ be an ideal and $d_1, \ldots, d_n$ positive integers. Then*

$$Sm(I) = \{\mathbf{x^u} \mid u_i < d_i \text{ for all } 1 \leq i \leq n\}$$

*iff the reduced Gröbner basis of $I$ is of the form $\{F_1, \ldots, F_n\}$, where for all $1 \leq i \leq n$ we have $lm(F_i) = x_i^{d_i}$.*

**Proof.** First suppose that $Sm(I) = \{\mathbf{x^u} \mid u_i < d_i \text{ for all } i\}$. By assumption $x_i^{d_i}$ is a leading monomial, hence for all $i$ there is a polynomial $F_i \in I$ such that $lm(F_i) = x_i^{d_i}$. The fact that the leading monomial of $F_i$ is $x_i^{d_i}$ just means, that $x_j$ with $j < i$ does not occur in $F_i$, i.e.

$$F_i \in \mathbb{F}[x_i, \ldots, x_n] \subseteq \mathbb{F}[x_1, \ldots, x_n] = \mathbb{F}[\mathbf{x}],$$

and the degree of $x_i$ in any other monomial in $F_i$ is smaller than $d_i$. Take an arbitrary polynomial $f$ from $I$. As its leading monomial is not a standard one, there must an index $i$, such that $lm(F_i) = x_i^{d_i} | lm(f)$, meaning that the set of polynomials $\mathcal{G} = \{F_1, F_2, \ldots, F_n\}$ is a Gröbner basis of $I$ with respect to $\prec$. Moreover we may also assume that they form a reduced Gröbner basis, otherwise take the polynomials one-by-one, starting with $F_n$, and when dealing with $F_i$ reduce it with respect to $\{F_{i+1}, \ldots, F_n\}$.

For the other direction, suppose that the reduced Gröbner basis of $I \lhd \mathbb{F}[\mathbf{x}]$ is of the form $\{F_1, F_2, \ldots, F_n\}$, where for all $1 \leq i \leq n$ we have that $lm(F_i) = x_i^{d_i}$. By the properties of Gröbner bases for any leading monomial $\mathbf{x^u} \in Lm(I)$ there is an index $i$ such that $lm(F_i) = x_i^{d_i} | \mathbf{x^u}$. On the other hand, if for some monomial $\mathbf{x^u}$ there is an index $i$ such that $x_i^{d_i} | \mathbf{x^u}$ (i.e. $d_i \leq u_i$), then $\mathbf{x^u}$ is the leading monomial of the polynomial $\frac{\mathbf{x^u}}{x_i^{d_i}} F_i \in I$. These facts together imply that $Sm(I) = \{\mathbf{x^u} \mid u_i < d_i \text{ for all } 1 \leq i \leq n\}$. ■

For $(ii) \Longrightarrow (iii)$ suppose that $X \subseteq \mathbb{F}^n$ is such that the reduced Gröbner basis of $I(X)$ is of the form $\mathcal{G} = \{F_1, \ldots, F_n\}$, where for all $1 \leq i \leq n$ we have that $lm(F_i) = x_i^{d_i}$. As observed in the proof of Lemma 4.1, $lm(F_i) = x_i^{d_i}$ implies that $F_i \in \mathbb{F}[x_i, \ldots, x_n]$. For $k = 1, 2, \ldots, n$ put $\mathcal{G}_k = \{F_k, F_{k+1}, \ldots, F_n\}$ and $I_k = \langle \mathcal{G}_k \rangle \lhd \mathbb{F}[x_k, \ldots, x_n]$. As a special case we have that $\mathcal{G} = \mathcal{G}_1$ and $I(X) = I_1$.

**Lemma 4.2.** *If a polynomial $f \in \mathbb{F}[x_k, \ldots, x_n]$ reduces to $0$ using $\mathcal{G}$ inside $\mathbb{F}[x_1, \ldots, x_n]$, then it reduces to $0$ using $\mathcal{G}_k$ inside $\mathbb{F}[x_k, \ldots, x_n]$.*

**Proof.** The first step in the reduction of $f$ by $\mathcal{G}$ can only be by a polynomial $g \in \mathcal{G}_k \subseteq \mathcal{G}$, as only these have their leading term in $\mathbb{F}[x_k, \ldots, x_n]$. For the

polynomial $\widetilde{f}$, obtained after the first reduction step we have $\widetilde{f} \in \mathbb{F}[x_k, \ldots, x_n]$ as $\mathcal{G}_k \subseteq \mathbb{F}[x_k, \ldots, x_n]$. The claim now follows by induction on the length of the reduction process. ■

**Lemma 4.3.** *$\mathcal{G}_k$ is the reduced Gröbner basis of $I_k$ for $1 \leq k \leq n$.*

**Proof.** Recall that by Buchberger's theorem $\mathcal{G}_k$ is a Gröbner basis of $I_k$ iff the S-polynomial of any two polynomials in $\mathcal{G}_k$ can be reduced to 0 using $\mathcal{G}_k$ inside $\mathbb{F}[x_k, \ldots, x_n]$. Now take $F_i, F_j$, $k \leq i < j \leq n$, and let $S(F_i, F_j)$ be their S-polynomial. Since $\mathcal{G}$ is a Gröbner basis of $I(X)$, $S(F_i, F_j) \in \mathbb{F}[x_i, \ldots, x_n]$ can be reduced to 0 using $\mathcal{G}$ inside $\mathbb{F}[x_1, \ldots, x_n]$, and so by Lemma 4.2 it can be reduced to 0 using $\mathcal{G}_i \subseteq \mathcal{G}_k$ inside $\mathbb{F}[x_i, \ldots, x_n] \subseteq \mathbb{F}[x_k, \ldots, x_n]$.

The fact that $\mathcal{G}_k$ is a reduced Gröbner basis easily follows as it is a subset of $\mathcal{G}$ which is a reduced basis. ■

It is easily seen that $I_k$ is a zero dimensional ideal, however a bit more is true.

**Lemma 4.4.** $I(X_k) = I_k$

**Proof.** $I_k \subseteq I(X_k)$ follows directly from the definitions. For the other direction let $f$ be an arbitrary polynomial in $I(X_k) \lhd \mathbb{F}[x_k, \ldots, x_n]$. Since $\mathcal{G}_k$ is a Gröbner basis of $I_k$, to prove that $f \in I_k$ it suffices to show that it can be reduced to 0 using $\mathcal{G}_k$. $f \in I(X_k)$ implies that $f \in I(X)$, and hence it can be reduced to 0 using $\mathcal{G}$ inside $\mathbb{F}[x_1, \ldots, x_n]$. Again by Lemma 4.2 this means that it can be reduced to 0 using $\mathcal{G}_k$ inside $\mathbb{F}[x_k, \ldots, x_n]$ as well. ■

Lemma 4.3 and 4.4 together imply that $\mathcal{G}_k = \{F_k, \ldots, F_n\}$ is the reduced Gröbner basis of the vanishing ideal $I(X_k) \lhd \mathbb{F}[x_k, \ldots, x_n]$. Now Lemma 4.1 implies that

$$Sm(I(X_k)) = \{x_k^{u_k} \cdots x_n^{u_n} \mid u_i < d_i \text{ for all } k \leq i \leq n\},$$

and hence by the properties of standard monomials of vanishing ideals we get that $|X_k| = |Sm(I(X_k))| = \prod_{i=k}^{n} d_i$, in particular $|X_n| = d_n$.

**Remark 4.1.** *From the general properties of elimination term orders (Theorem 2.3.4. in [1]) we know that $\mathcal{G}_k$ is a Gröbner basis (and hence an ideal basis) of the elimination ideal $I(X) \cap \mathbb{F}[x_k, \ldots, x_n]$ as well, and hence*

$$I(X) \cap \mathbb{F}[x_k, \ldots, x_n] = I(X_k).$$

Now fix $1 \leq k \leq n-1$, let $(s_{k+1}, \ldots, s_n) \in X_{k+1}$ and put $h(x_k) = F_k(x_k, s_{k+1}, \ldots, s_n)$. $h$ is a polynomial in $\mathbb{F}[x_k]$ of degree $d_k$. If $s \in \mathbb{F}$ is

such that $(s, s_{k+1}, \ldots, s_n) \in X_k$, then $h(s) = F_k(s, s_{k+1}, \ldots, s_k) = 0$, i.e. $s$ is a root of $h$. By the degree bound on $h$, the number of such elements $s$ is at most $d_k$. However $|X_k| = d_k \cdot |X_{k+1}|$, what is possible only if for all fixed $(s_{k+1}, \ldots, s_n) \in X_{k+1}$ the number of suitable elements $s$ is exactly $d_k$. This finishes the $(ii) \Longrightarrow (iii)$ part of the proof.

To complete the proof of Theorem 3.1, suppose that the finite set $X \subseteq \mathbb{F}^n$ satisfies the given combinatorial condition, i.e. for all $k = 1, \ldots, n-1$ the size of

$$\{s \in \mathbb{F} \mid (s, s_{k+1}, \ldots, s_n) \in X_k\}$$

is $d_k$ for all $(s_{k+1}, \ldots, s_n) \in X_{k+1}$, and $|X_n| = d_n$. Let $A$ be the set of all field elements occurring as a coordinate in $X$ and put $m = |A| - 1$. Fix some injective functions $\varphi_i : A \longrightarrow \{0, 1, \ldots, m\} \subseteq \mathbb{R}$, $i = 1, \ldots, n$, and using them, define $\widehat{X} \subseteq \{0, 1, \ldots, m\}^n \subseteq \mathbb{R}^n$ as in Section 2. By the injectivity of the $\varphi_i$'s $\widehat{X}$ inherits from $X$ its structural property, i.e. for all $1 \leq k \leq n-1$ the number of elements $\alpha$ for which $(\alpha, \alpha_{k+1}, \ldots, \alpha_n) \in \widehat{X}_k$ is $d_k$ for all $(\alpha_{k+1}, \ldots, \alpha_n) \in \widehat{X}_{k+1}$, and $|\widehat{X}_n| = d_n$. However in this case it is immediately seen that

$$D_n(D_{n-1}(\ldots D_1(\widehat{X})\ldots)) = \{\mathbf{u} \in \mathbb{N}^n \mid u_i < d_i \text{ for all } i\},$$

and hence

$$Sm(I(X)) = Sm(I(\widehat{X})) = \{\mathbf{x}^{\mathbf{u}} \mid u_i < d_i \text{ for all } 1 \leq i \leq n\}.$$

This finishes the proof of Theorem 3.1. ■

**Remark 4.2.** *By earlier arguments one can also observe that for all fixed* $(s_{k+1}, \ldots, s_n) \in X_{k+1}$ *we have*

$$h(x_k) = F_k(x_k, s_{k+1}, \ldots, s_n) = \prod_{s \,:\, (s, s_{k+1}, \ldots, s_n) \in X_k} (x_k - s).$$

## 5. Concluding remarks

Theorem 3.1 and our examples suggest two related problems for further study.

In [11] and [12] the authors proved several generalizations of the Combinatorial Nullstellensatz and the Nonvanishing Theorem, in particular a version for multisets. It would be interesting to obtain an analogue of Theorem 3.1 in

the multiset case as well, that relates the combinatorial properties of a given multiset to the algebraic properties of its vanishing ideal.

In Example 3.5 we introduced a wider class of point sets, not merely discrete boxes, where the Nonvanishig Theorem holds in its full generality. The conditions of Theorem 3.1 are in general not sufficient for the Nonvanishing Theorem to hold, for example in the case of permutations, if $n > 1$ and the $a_i$'s are all different, the polynomial

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} a_i$$

has standard monomials in its maximal degree part ($x_2, x_3, \ldots, x_n$ are all standard monomials), but it vanishes on the whole set of permutations (it is actually a member of the reduced Gröbner basis). It would be interesting to develop an understanding of the finite sets $X \subseteq \mathbb{F}^n$ for which a version of the Nonvanishing Theorem holds.

## References


[1] **Adams, W.W. and P. Loustaunau,** *An Introduction to Gröbner Bases,* Graduate Studies in Mathematics **3**, American Mathematical Society, 1994.

[2] **Alon, N.,** Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing*, **8** (1999), 7–29.

[3] **Alon, N., L. Rónyai, and T. Szabó,** Norm-graphs: Variations and applications, *Journal of Combinatorial Theory, Series B,* **76** (2) (1999), 280–290.

[4] **Cámara, M., A. Lladó, and J. Moragas,** On a conjecture of Graham and Häggkvist with the polynomial method, *European Journal of Combinatorics,* **30** (2009), 1585–1592.

[5] **Felszeghy, B.,** On the solvability of some special equations over finite fields, *Publ. Math. Debrecen,* **68** (2006), 15–23.

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

[7] **Green, B. and T. Tao,** The distribution of polynomials over finite fields, with applications to the Gowers norms, *Contributions to Discrete Mathematics,* **4** (2009), 1–36.

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

[9] **Károlyi, Gy.,** Restricted set addition: the exceptional case of the Erdős-Heilbronn conjecture, *Journal of Combinatorial Theory, Ser. A* **116** (2009), 741–746.

[10] **Károlyi, Gy., Z.L. Nagy, F.V. Petrov, and V. Volkov,** A new approach to constant term identities and Selberg-type integrals, *arXiv:1312.6369*

[11] **Kós, G. and L. Rónyai,** Alon's Nullstellensatz for multisets, *Combinatorica,* **32** (5) (2012), 589–605.

[12] **Kós, G., T. Mészáros, and L. Rónyai,** Some extensions of Alon's Nullstellensatz, *Publ. Math. Debrecen,* **79** (3-4) (2011), 507–519.

[13] **Mészáros, T.,** *S-extremal set systems and Gröbner bases,* Diploma Thesis at Budapest University of Technology and Economics, 2010. `http://www.math.bme.hu/~slovi/thesiswork.pdf`

[14] **Pan, H. and Z.-W. Sun,** A new extension of the Erdős-Heilbronn conjecture, *Journal of Combinatorial Theory, Ser. A,* **116** (2009), 1374–1381.

[15] **Sun, Z-W.,** On value sets of polynomials over a field, *Finite Fields and Applications,* **14** (2008), 470–481.

**Tamás Mészáros**
Department of Mathematics
Central European University and
Institute of Mathematics, Budapest University of Technology and Economics
Budapest, Hungary
`Meszaros_Tamas@ceu-budapest.edu` or `tmeszaros87@gmail.com`

**Lajos Rónyai**
Computer and Automation Research Institute
Hungarian Academy of Sciences and
Institute of Mathematics, Budapest University of Technology and Economics
Budapest, Hungary
`lajos@ilab.sztaki.hu`