Bull. Aust. Math. Soc. **103** (2021), 369–378
doi:10.1017/S0004972720001197

THE NUMBER OF ROOTS OF A POLYNOMIAL SYSTEM

NGUYEN CONG MINH, LUU BA THANG✉ and TRAN NAM TRUNG

(Received 2 July 2020; accepted 6 September 2020; first published online 9 November 2020)

Abstract

Let I be a zero-dimensional ideal in the polynomial ring $K[x_1, \ldots, x_n]$ over a field K. We give a bound for the number of roots of I in K^n counted with combinatorial multiplicity. As a consequence, we give a proof of Alon's combinatorial Nullstellensatz.

2020 *Mathematics subject classification*: primary 05D40; secondary 05C90, 05E40, 05E45, 13D45.

Keywords and phrases: combinatorial Nullstellensatz, multiplicity, multiset, root.

1. Introduction

Let $R = K[x_1, \ldots, x_n]$ denote the ring of polynomials in variables $x_1, \ldots, x_n$ over a field K. Consider a system of polynomial equations

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \quad \vdots \\ f_s(x_1, \ldots, x_n) = 0, \end{cases}$$

where $f_1, \ldots, f_s$ are s polynomials in R.

The solutions in K^n of this system are the set of zeros of the ideal $I = (f_1, \ldots, f_s)$ in R, that is,

$$Z(I) = \{(p_1, \ldots, p_n) \in K^n \mid f(p_1, \ldots, p_n) = 0 \text{ for all } f \in I\}.$$

If this system has only a finite number of solutions, then the number of solutions can be bounded by Bézout's theorem (see [4, Theorem 2.10]):

$$|Z(I)| \leqslant \dim_K(R/I), \tag{1.1}$$

where $\dim_K(R/I)$ is the dimension of the vector space R/I over K. Moreover, if K is an algebraically closed field, the equality holds if and only if I is a radical ideal.

Thus, we can find the exact number of solutions if we know the radical of I because $Z(I) = Z(\sqrt{I})$. For a general ideal $I \subset R$, it is more difficult to find $\sqrt{I}$, though algorithms are known and have been implemented in some computer algebra systems

The third author is partially supported by NAFOSTED (Vietnam), grant number 101.04–2018.307.

(for example, *Macaulay2* [8]). Fortunately, when I is zero dimensional, computing the radical of I is much easier (see [4, Proposition 2.7] for more details). But, this computation requires that we know almost all solutions $Z(I)$. It means that in many cases, we cannot always consider radical ideals. Thus, the bound (1.1) is still very important in both theory and practice. This bound can be used to estimate and determine the minimum distance and generalised Hamming weights for a class of error-correcting codes obtained by evaluation of polynomials at points of an algebraic curve (see, for instance, [6, 7] and the references given there).

It is worth mentioning that when we count solutions with algebraic multiplicity, the bound (1.1) becomes equality if the field K is algebraically closed (see [4, Corollary 2.5]). We can compute the algebraic multiplicity using techniques from local rings, but the computation is quite complicated.

The aim of this paper is to introduce the combinatorial multiplicity for solutions of I in a combinatorial way. In practice, this invariant is easy to compute. Then we prove that the bound (1.1) still holds when the roots are counted with this multiplicity. Before stating our result, we need some terminology and notation.

For $f = \sum_{\boldsymbol{\beta}\in\mathbb{N}^n} a_{\boldsymbol{\beta}}x^{\boldsymbol{\beta}} \in R$ and $\boldsymbol{\alpha} \in \mathbb{N}^n$, we define the *Hasse derivative* $D^{\boldsymbol{\alpha}} f \in R$ by

$$D^{\boldsymbol{\alpha}} f = \sum_{\boldsymbol{\beta}\in\mathbb{N}^n} a_{\boldsymbol{\beta}} \binom{\beta_1}{\alpha_1} \cdots \binom{\beta_n}{\alpha_n} x_1^{\beta_1-\alpha_1} \cdots x_n^{\beta_n-\alpha_n}.$$

For simplicity of notation, we write a vector $\boldsymbol{\alpha} \in \mathbb{N}^n$ to mean $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and for $\mathbf{p} = (p_1, \ldots, p_n) \in K^n$ we let $(\mathbf{x} - \mathbf{p})^{\boldsymbol{\alpha}}$ stand for $(x_1 - p_1)^{\alpha_1} \cdots (x_n - p_n)^{\alpha_n}$. So, $\mathbf{x}^{\boldsymbol{\alpha}}$ is the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and the Taylor expansion of f at $\mathbf{p}$ is (see [11])

$$f = \sum_{\boldsymbol{\alpha}\in\mathbb{N}^n} D^{\boldsymbol{\alpha}} f(\mathbf{p})(\mathbf{x} - \mathbf{p})^{\boldsymbol{\alpha}}. \tag{1.2}$$

We say that f vanishes to order $\boldsymbol{\beta}$ at $\mathbf{p}$ if the Hasse derivatives $D^{\boldsymbol{\alpha}} f(\mathbf{p})$ vanish whenever $\boldsymbol{\alpha} \leqslant \boldsymbol{\beta}$, that is, $\alpha_i \leqslant \beta_i$ for $i = 1, \ldots, n$. Set

$$\mathrm{mv}_{\mathbf{p}}(f) = \{\boldsymbol{\beta} \in \mathbb{N}^n \mid f \text{ vanishes to order } \boldsymbol{\beta} \text{ at } \mathbf{p}\}$$

and, for an ideal $I \subseteq R$, set

$$\mathrm{mv}_{\mathbf{p}}(I) = \{\boldsymbol{\beta} \in \mathbb{N}^n \mid f \text{ vanishes to order } \boldsymbol{\beta} \text{ at } \mathbf{p} \text{ for all } f \in I\}.$$

By definition, if $I = (f_1, \ldots, f_s)$, then $\mathrm{mv}_{\mathbf{p}}(I) = \mathrm{mv}_{\mathbf{p}}(f_1) \cap \cdots \cap \mathrm{mv}_{\mathbf{p}}(f_s)$.

We now define the *combinatorial multiplicity* (or multiplicity if there is no confusion) of the ideal I of R at the point $\mathbf{p}$ by

$$\mathrm{mult}_{\mathbf{p}}(I) = |\mathrm{mv}_{\mathbf{p}}(I)|.$$

It is obvious by definition that $\mathrm{mult}_{\mathbf{p}}(I) \geq 1$ if and only if $\mathbf{p} \in Z(I)$.

The main result of the paper is the following version of Bézout's theorem with combinatorial multiplicity.

https://doi.org/10.1017/S0004972720001197 Published online by Cambridge University Press

THEOREM 1.1. *Let $I \subseteq R$ be an ideal of R such that $Z(I)$ is a finite set. Then*

$$\sum_{\mathbf{p}\in K^n} \mathrm{mult}_{\mathbf{p}}(I) \leqslant \dim_K(R/I).$$

As an application, we use this theorem to give a simple proof for Alon's Nullstellensatz for multisets (Theorem 3.3).

The paper is organised as follows. In Section 2 we prove Theorem 1.1. In Section 3 we apply this theorem to give a simple proof for the well-known theorem, usually called Alon's Nullstellensatz for multisets (Theorem 3.3), and we also give a slight generalisation of Alon's Nullstellensatz for multisets (Theorem 3.4).

2. The number of solutions

Let $\mathbf{p} = (p_1, \ldots, p_n) \in K^n$. The maximal ideal $\mathfrak{m}_{\mathbf{p}} = (x_1 - p_1, \ldots, x_n - p_n)$ of R is called the ideal of $\mathbf{p}$. For $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$, put

$$\mathfrak{m}_{\mathbf{p},\boldsymbol{\beta}} = ((x_1 - p_1)^{\beta_1}, \ldots, (x_n - p_n)^{\beta_n}).$$

On the set $\mathbb{N}^n$ we define the natural partial order:

$$(\alpha_1, \ldots, \alpha_n) \leqslant (\beta_1, \ldots, \beta_n) \text{ if and only if } \alpha_i \leqslant \beta_i \text{ for all } i$$

and we write $\boldsymbol{\alpha} < \boldsymbol{\beta}$ to mean $\alpha_i < \beta_i$ for all i.

For $f \in R = K[x_1, \ldots, x_n]$, from the Taylor expansion of f (see (1.2)), we deduce that $f \in \mathfrak{m}_{\mathbf{p},\boldsymbol{\beta}}$ if and only if

$$D^{\alpha} f(\mathbf{p}) = 0 \quad \text{for all } \boldsymbol{\alpha} < \boldsymbol{\beta}. \tag{2.1}$$

LEMMA 2.1. *Let $\mathfrak{m}, \mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be pairwise distinct maximal ideals of R. Assume that $Q, Q_1, Q_2, \ldots, Q_s$ are ideals of R such that $\sqrt{Q} = \mathfrak{m}$, $\sqrt{Q_1} = \mathfrak{m}_1, \ldots, \sqrt{Q_s} = \mathfrak{m}_s$. Then $Q_1 \cap \cdots \cap Q_s \nsubseteq Q$.*

PROOF. Assume on the contrary that $Q_1 \cap \cdots \cap Q_s \subseteq Q$. This would imply that

$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_s = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_s} = \sqrt{Q_1 \cap \cdots \cap Q_s} \subseteq \sqrt{Q} = \mathfrak{m}.$$

By [3, Proposition 1.11(ii)], we have $\mathfrak{m}_r \subseteq \mathfrak{m}$ for some $1 \leqslant r \leqslant s$. But $\mathfrak{m}$ and $\mathfrak{m}_r$ are two different maximal ideals of R, so that the inclusion $\mathfrak{m}_r \subseteq \mathfrak{m}$ is impossible. Thus, the lemma follows. □

We are now in the position to restate and prove the main result of this paper.

THEOREM 2.2 (= Theorem 1.1). *Let $I \subseteq R$ be an ideal of R such that $Z(I)$ is a finite set. Then*

$$\sum_{\mathbf{p}\in K^n} \mathrm{mult}_{\mathbf{p}}(I) \leqslant \dim_K(R/I).$$

PROOF. If $\mathbb{Z}(I) = \emptyset$ or $\dim_K(R/I) = \infty$, the theorem obviously holds. Therefore, we may assume that $Z(I) \neq \emptyset$ and $\dim_K(R/I) < \infty$.

https://doi.org/10.1017/S0004972720001197 Published online by Cambridge University Press

Let $Z(I) = \{\mathbf{p}_1, \dots, \mathbf{p}_s\}$ and let $m_i = \text{mult}_{\mathbf{p}_i}(I)$ for $i = 1, \dots, s$. Then

$$\sum_{\mathbf{p} \in K^n} \text{mult}_{\mathbf{p}}(I) = m_1 + \cdots + m_s.$$

Since $\dim_K(R/I) < \infty$, by [5, Theorem 6, page 234], there is a $g_i \in K[x_i] \cap I$ for each $i = 1, \dots, n$. Let $d_i = \deg(g_i)$ and $g_i = a_i x_i^{d_i} +$ (terms of lower orders), where each $a_i \in K$ and $a_i \neq 0$. It follows that $D^{d_i \mathbf{e}_i}(g_i) = a_i \neq 0$, where $\mathbf{e}_i \in \mathbb{N}^n$ has ith coordinate 1 and its other coordinates zero. Since $Z(I) \neq \emptyset$, we have $d_i > 0$ for every i. Let $\boldsymbol{\gamma} = (d_1, \dots, d_s)$. It follows that

$$\boldsymbol{\beta} < \boldsymbol{\gamma} \quad \text{and} \quad \boldsymbol{\beta} \in \text{mv}_{\mathbf{p}_i}(I) \quad \text{for } i = 1, \dots, s. \tag{2.2}$$

Let $\mathfrak{m}_1, \dots, \mathfrak{m}_s$ be the maximal ideals of $\mathbf{p}_1, \dots, \mathbf{p}_s$, respectively. For $i = 1, \dots, s$ and $\boldsymbol{\alpha} \in \mathbb{N}^n$, put

$$\mathfrak{m}_{i,\boldsymbol{\alpha}} = \mathfrak{m}_{\mathbf{p}_i,\boldsymbol{\alpha}} = ((x_1 - p_{i1})^{\alpha_1}, \dots, (x_r - p_{in})^{\alpha_n}),$$

where $\mathbf{p}_i = (p_{i1}, p_{i2}, \dots, p_{in})$. Obviously, $\sqrt{\mathfrak{m}_{i,\boldsymbol{\alpha}}} = \mathfrak{m}_i$ if $\alpha_i > 0$ for all i.

For each $i = 1, \dots, s$ and each $\boldsymbol{\alpha} \in \text{mv}_{\mathbf{p}_i}(I)$, we choose a polynomial $f_{i,\boldsymbol{\alpha}}$ as follows. By Lemma 2.1,

$$\mathfrak{m}_{1,\boldsymbol{\gamma}} \cap \cdots \cap \mathfrak{m}_{i-1,\boldsymbol{\gamma}} \cap \mathfrak{m}_{i+1,\boldsymbol{\gamma}} \cdots \cap \mathfrak{m}_{s,\boldsymbol{\gamma}} \not\subseteq \mathfrak{m}_i,$$

so we can take

$$g_{i,\boldsymbol{\alpha}} \in \mathfrak{m}_{1,\boldsymbol{\gamma}} \cap \cdots \cap \mathfrak{m}_{i-1,\boldsymbol{\gamma}} \cap \mathfrak{m}_{i+1,\boldsymbol{\gamma}} \cdots \cap \mathfrak{m}_{s,\boldsymbol{\gamma}} \setminus \mathfrak{m}_i.$$

Since $g_{i,\boldsymbol{\alpha}} \notin \mathfrak{m}_i = (x_1 - p_{i1}, \dots, x_n - p_{in})$, we can represent $g_{i,\boldsymbol{\alpha}}$ as

$$g_{i,\boldsymbol{\alpha}} = a_{\boldsymbol{\alpha}} + h_1 \cdot (x_1 - p_{i1}) + \cdots + h_n \cdot (x_n - p_{in}),$$

where $h_1, \dots, h_n \in R$, $a_{\boldsymbol{\alpha}} \in K$ with $a_{\boldsymbol{\alpha}} \neq 0$. Let $f_{i,\boldsymbol{\alpha}} = g_{i,\boldsymbol{\alpha}} \cdot (\mathbf{x} - \mathbf{p}_i)^{\boldsymbol{\alpha}}$. Then

$$f_{i,\boldsymbol{\alpha}} \in \mathfrak{m}_{1,\boldsymbol{\gamma}} \cap \cdots \cap \mathfrak{m}_{i-1,\boldsymbol{\gamma}} \cap \mathfrak{m}_{i,\boldsymbol{\alpha}} \cap \mathfrak{m}_{i+1,\boldsymbol{\gamma}} \cdots \cap \mathfrak{m}_{s,\boldsymbol{\gamma}} \tag{2.3}$$

and

$$f_{i,\boldsymbol{\alpha}} = a_{\boldsymbol{\alpha}}(\mathbf{x} - \mathbf{p}_i)^{\boldsymbol{\alpha}} + \sum_{j=1}^{n} h_j \cdot (x_j - p_{ij})(\mathbf{x} - \mathbf{p}_i)^{\boldsymbol{\alpha}}. \tag{2.4}$$

In particular,

$$D^{\boldsymbol{\alpha}} f_{i,\boldsymbol{\alpha}} = a_{\boldsymbol{\alpha}} \neq 0. \tag{2.5}$$

For $f \in R$, denote the image of f in the quotient ring R/I by $[f]$. Now we claim that the set $\{[f_{i,\boldsymbol{\alpha}}] \mid i = 1, \dots, s \text{ and } \boldsymbol{\alpha} \in \text{mv}_{\mathbf{p}_i}(I)\}$ is linearly independent in the K-space R/I. Indeed, assume that

$$\sum a_{i,\boldsymbol{\alpha}}[f_{i,\boldsymbol{\alpha}}] = 0$$

in R/I, where $a_{i,\boldsymbol{\alpha}} \in K$. Back in R, this means that $g = \sum_{i,\boldsymbol{\alpha}} a_{i,\boldsymbol{\alpha}} f_{i,\boldsymbol{\alpha}} \in I$. In particular,

$$D^{\boldsymbol{\beta}} g(\mathbf{p}_i) = 0 \quad \text{and} \quad \boldsymbol{\beta} \in \text{mv}_{\mathbf{p}_i}(I) \quad \text{for } i = 1, \dots, s. \tag{2.6}$$

We now prove that $a_{i,\boldsymbol{\alpha}} = 0$ for all $i, \boldsymbol{\alpha}$. By symmetry, it suffices to show that $a_{1,\boldsymbol{\alpha}} = 0$ for $\boldsymbol{\alpha} \in \text{mv}_{\mathbf{p}_1}(I)$.

https://doi.org/10.1017/S0004972720001197 Published online by Cambridge University Press

For $i \geqslant 2$,

$$D^{\boldsymbol{\beta}} f_{i,\boldsymbol{\rho}}(\mathbf{p}_1) = 0 \quad \text{for all } \boldsymbol{\rho} \in \mathrm{mv}_{\mathbf{p}_i}(I) \text{ and } \boldsymbol{\beta} \in \mathrm{mv}_{\mathbf{p}_1}(I) \tag{2.7}$$

because $f_{i,\boldsymbol{\rho}} \in \mathfrak{m}_{1,\boldsymbol{\gamma}}$ and $\boldsymbol{\beta} < \boldsymbol{\gamma}$ by (2.2). In the case $i = 1$,

$$D^{\boldsymbol{\beta}} f_{1,\boldsymbol{\alpha}}(\mathbf{p}_1) = 0 \quad \text{for all } \boldsymbol{\alpha} \in \mathrm{mv}_{\mathbf{p}_1}(I) \text{ and } \boldsymbol{\beta} < \boldsymbol{\alpha} \tag{2.8}$$

because $f_{1,\boldsymbol{\alpha}} \in \mathfrak{m}_{1,\boldsymbol{\alpha}}$.

Now we assume that $a_{1,\boldsymbol{\alpha}} \neq 0$ for some $\boldsymbol{\alpha} \in \mathrm{mv}_{\mathbf{p}_1}(I)$. Let $\boldsymbol{\alpha} \in \mathrm{mv}_{\mathbf{p}_1}(I)$ be such that $a_{1,\boldsymbol{\alpha}} \neq 0$ and $|\boldsymbol{\alpha}|$ is minimal. By (2.4), $D^{\boldsymbol{\alpha}} f_{1,\boldsymbol{\rho}}(\mathbf{p}_1) = 0$ if either $|\boldsymbol{\rho}| > |\boldsymbol{\alpha}|$ or $|\boldsymbol{\rho}| = |\boldsymbol{\alpha}|$ and $\boldsymbol{\rho} \neq \boldsymbol{\alpha}$. Together with (2.7) and (2.8) and the fact that $a_{1,\boldsymbol{\rho}} = 0$ for all $\boldsymbol{\rho} \in \mathrm{mv}_{\mathbf{p}_1}(I)$ with $|\boldsymbol{\rho}| < |\boldsymbol{\alpha}|$,

$$0 = D^{\boldsymbol{\alpha}} g(\mathbf{p}_1) = \sum_{i,\boldsymbol{\rho}} a_{i,\boldsymbol{\rho}} D^{\boldsymbol{\alpha}} f_{i,\boldsymbol{\rho}}(\mathbf{p}_1) = \sum_{\boldsymbol{\rho}} a_{1,\boldsymbol{\rho}} D^{\boldsymbol{\alpha}} f_{1,\boldsymbol{\rho}}(\mathbf{p}_1) = a_{1,\boldsymbol{\alpha}} D^{\boldsymbol{\alpha}} f_{1,\boldsymbol{\alpha}}(\mathbf{p}_1).$$

On the other hand, $D^{\boldsymbol{\alpha}} f_{1,\boldsymbol{\alpha}}(\mathbf{p}_1) \neq 0$ by (2.5). Thus, $a_{1,\boldsymbol{\alpha}} = 0$ and the claim follows.

By our claim, we have $m_1 + \cdots + m_s \leqslant \dim_K(R/I)$. The proof of the theorem is complete. □

For a polynomial $f \in R$ and a point $\mathbf{p} \in K^n$, we say that f vanishes to order at least m at $\mathbf{p}$ if the Hasse derivatives $D^{\boldsymbol{\alpha}} f(\mathbf{p})$ vanish whenever $|\boldsymbol{\alpha}| = \alpha_1 + \cdots + \alpha_n < m$. The largest m for which this occurs is called the *order* of f at $\mathbf{p}$ and will be denoted $\mathrm{ord}_p(f)$ (see [11] for the detail). Note that $\mathrm{ord}_{\mathbf{p}}(f) > 0$ if and only if $f(\mathbf{p}) = 0$. By convention, we set $\mathrm{ord}_{\mathbf{p}}(f) = \infty$ when f is the zero polynomial. It is obvious that $\mathrm{ord}_{\mathbf{p}}(f) \leqslant \deg(f)$ whenever f is a nonzero polynomial. We define the order of an ideal I of R at the point $\mathbf{p} \in K^n$ to be

$$\mathrm{ord}_{\mathbf{p}}(I) = \min\{\mathrm{ord}_{\mathbf{p}}(f) \mid f \in I\}.$$

This shows that $\mathrm{ord}_{\mathbf{p}}(I) = \min\{\mathrm{ord}_{\mathbf{p}}(f_1), \ldots, \mathrm{ord}_{\mathbf{p}}(f_s)\}$ if $I = (f_1, \ldots, f_s)$.

LEMMA 2.3. *Let I be a nonzero ideal of R and $\mathbf{p} \in K^n$. Then* $\mathrm{ord}_{\mathbf{p}}(I) \leqslant \mathrm{mult}_{\mathbf{p}}(I)$.

PROOF. We may assume that $\mathbf{p} \in Z(I)$. Let $m = \mathrm{ord}_{\mathbf{p}}(I)$. If $m = 0$, the lemma is obvious and so we assume that $m \geqslant 1$. Then there is a $\boldsymbol{\beta} \in \mathbb{N}^n$ such that $D^{\boldsymbol{\beta}} f(\mathbf{p}) \neq 0$ and $|\boldsymbol{\beta}| = m$. Moreover,

$$D^{\boldsymbol{\alpha}} g(\mathbf{p}) = 0 \quad \text{for all } g \in R \text{ and all } \boldsymbol{\alpha} \in \mathbb{N}^n \text{ with } |\boldsymbol{\alpha}| < m. \tag{2.9}$$

Since $m \geqslant 1$, we may assume that $\beta_1 \geqslant 1$. Let $\boldsymbol{\gamma} = (\beta_1 - 1, \beta_2, \ldots, \beta_n)$. By (2.9), we deduce that $\boldsymbol{\gamma} \in \mathrm{mv}_{\mathbf{p}}(I)$. Therefore,

$$\mathrm{mult}_{\mathbf{p}}(I) \geqslant (\gamma_1 + 1) \cdots (\gamma_n + 1) = \beta_1(\beta_2 + 1) \cdots (\beta_n + 1).$$

Together with $(\beta_2 + 1) \cdots (\beta_n + 1) \geqslant 1 + \beta_2 + \cdots + \beta_n$, this yields

$$\mathrm{mult}_{\mathbf{p}}(I) \geqslant \beta_1(1 + \beta_2 + \cdots + \beta_n) \geqslant \beta_1 + \beta_2 + \cdots + \beta_n = \mathrm{ord}_{\mathbf{p}}(I),$$

as required. □

In general, the inequality in Lemma 2.3 is strict.

https://doi.org/10.1017/S0004972720001197 Published online by Cambridge University Press

EXAMPLE 2.4. Let $n \geqslant 2$ and $I = (x^n, y^n) \subset R = \mathbb{Q}[x, y]$. Then

$$Z(I) = \{\mathbf{p} = (0, 0)\}, \quad \operatorname{mult}_{\mathbf{p}}(I) = n^2 \quad \text{and} \quad \operatorname{ord}_{\mathbf{p}}(I) = n.$$

Together, Theorem 2.2 and Lemma 2.3 yield the following result.

COROLLARY 2.5. *Let $I \subseteq R$ be an ideal of R such that $Z(I)$ is a finite set. Then*

$$\sum_{\mathbf{p} \in K^n} \operatorname{ord}_{\mathbf{p}}(I) \leqslant \dim_K(R/I).$$

3. Combinatorial Nullstellensatz

In this section we always assume that $S_1, \ldots, S_n$ are finite nonempty subsets of K with $s_i = |S_i|$ and $S = S_1 \times \cdots \times S_n \subseteq K^n$. For $f \in R = K[x_1, \ldots, x_n]$, we define

$$Z_S(f) = \{(p_1, \ldots, p_n) \in S \mid f(p_1, \ldots, p_n) = 0\}.$$

The following theorem of Alon, known as the *combinatorial Nullstellensatz*, has numerous applications in combinatorics, graph theory and additive number theory (see [1, 2, 11]). It gives a condition for $Z_S(f) \neq S$.

THEOREM 3.1 [1, Theorem 1.2]. *Let f be a polynomial in R. Suppose that the coefficient of $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ in f is nonzero and $\deg(f) = \alpha_1 + \cdots + \alpha_n$. Then, for any subsets $S_1, \ldots, S_n$ of K satisfying $|S_i| \geqslant \alpha_i + 1$, there is $\mathbf{p} = (p_1, \ldots, p_n) \in S_1 \times \cdots \times S_n$ so that $f(\mathbf{p}) \neq 0$.*

This theorem can be generalised in various ways. Kós and Rónyai [9, Theorem 6] formulated Alon's Nullstellensatz for *multisets*. For each $i = 1, \ldots, n$, suppose further that we have a (positive integer) *multiplicity* $m_i(s)$ attached to the elements of $s \in S_i$. We can view the pair (S_i, m_i) as a multiset which contains the element $s \in S_i$ precisely $m_i(s)$ times. We shall consider the sum $d_i = d(S_i) = \sum_{s \in S_i} m_i(s)$ as the size of the multiset (S_i, m_i). For an element $\mathbf{p} = (p_1, \ldots, p_n) \in S$, we set the multiplicity vector $m(\mathbf{p})$ as $(m_1(p_1), \ldots, m_n(p_n))$.

For each $\mathbf{p} \in S$ and $f \in R$, we define

$$\operatorname{mv}_{\mathbf{p}}(m, f) = \{\boldsymbol{\beta} \in \mathbb{N}^n \mid \boldsymbol{\beta} < m(\mathbf{p}) \text{ and } f \text{ vanishes to order } \boldsymbol{\beta}\}$$

and

$$\operatorname{mult}_{\mathbf{p}}(m, f) = |\operatorname{mv}_{\mathbf{p}}(m, f)|,$$

which we call the multiplicity of f at $\mathbf{p}$ with respect to multiplicity m.

By using Theorem 2.2, we obtain the following proposition.

PROPOSITION 3.2. *Consider an arbitrary, but fixed, monomial ordering on R. For a nonzero polynomial $f \in R$, let $\boldsymbol{x}^{\boldsymbol{\alpha}}$ be the leading monomial of f. Assume that $(S_1, m_1), (S_2, m_2), \ldots, (S_n, m_n)$ are multisets of K such that the size d_i of (S_i, m_i) satisfies $d_i > \alpha_i$ for every $i = 1, \ldots, n$. Then*

$$\sum_{\mathbf{p} \in S} \operatorname{mult}_{\mathbf{p}}(m, f) \leqslant d_1 \cdots d_n - (d_1 - \alpha_1) \cdots (d_n - \alpha_n). \tag{3.1}$$

https://doi.org/10.1017/S0004972720001197 Published online by Cambridge University Press

PROOF. For each $i = 1, \dots, n$, let

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s)^{m_i(s)}.$$

Then $\{g_1, \dots, g_n\}$ is a universal Groebner basis for the ideal $I = (g_1, \dots, g_n)$. For every $\mathbf{p} \in S$, it is obvious that $\mathrm{mv}_{\mathbf{p}}(I) = \{\boldsymbol{\beta} \in \mathbb{N}^n \mid \boldsymbol{\beta} < m(\mathbf{p})\}$, so $\mathrm{mv}_{\mathbf{p}}(I, f) = \mathrm{mv}_{\mathbf{p}}(m, f)$. By Theorem 2.2,

$$\sum_{\mathbf{p} \in S} \mathrm{mult}_{\mathbf{p}}(m, f) = \sum_{\mathbf{p} \in S} \mathrm{mult}_{\mathbf{p}}((I, f)) = \sum_{\mathbf{p} \in K^n} \mathrm{mult}_{\mathbf{p}}((I, f)) \leqslant \dim_K(R/(I, f)).$$

The leading term of f is of the form $\mathrm{lt}(f) = a\mathbf{x}^{\alpha}$ for some $a \in K$ with $a \neq 0$. Note that $\mathrm{lt}(g_i) = x_i^{d_i}$ for each i. By [5, Proposition 4, page 232],

$$\begin{aligned} \dim_K(R/(I, f)) = \dim_K(R/\,\mathrm{in}(I, f)) &\leqslant \dim_K(R/(x_1^{d_1}, \dots, x_n^{d_n}, \mathbf{x}^{\alpha}) \\ &= d_1 \cdots d_n - (d_1 - \alpha_1) \cdots (d_n - \alpha_n), \end{aligned}$$

where $\mathrm{in}(I)$ is the initial ideal of I with respect to the given order.

Thus,

$$\sum_{\mathbf{p} \in S} \mathrm{mult}_{\mathbf{p}}(m, f) \leqslant d_1 \cdots d_n - (d_1 - \alpha_1) \cdots (d_n - \alpha_n)$$

and the proposition follows. □

We now give a version of Alon's Nullstellensatz for multisets as formulated by Kós and Rónyai [9, Theorem 6]. We obtain Alon's result by setting $m_i(s) = 1$ identically. Here we give a proof by using Proposition 3.2.

THEOREM 3.3 [9, Theorem 6]. *Let $f \in R$ be a polynomial of degree $\sum_{i=1}^{n} \alpha_i$, where each α_i is a nonnegative integer. Assume that the coefficient in f of the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is nonzero. Suppose further that $(S_1, m_1), (S_2, m_2), \dots, (S_n, m_n)$ are multisets of K such that the size d_i of (S_i, m_i) satisfies $d_i > \alpha_i$ for $i = 1, \dots, n$. Then there exist a point $\mathbf{p} = (p_1, \dots, p_n) \in S_1 \times \cdots \times S_n$ and an exponent vector $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$ with $\beta_i < m_i(p_i)$ for each i such that $D^{\boldsymbol{\beta}} f(\mathbf{p}) \neq 0$.*

PROOF. Take any monomial order on R such that the leading monomial of f is x^{α}. By Proposition 3.2,

$$\sum_{\mathbf{p} \in S} \mathrm{mult}_{\mathbf{p}}(m, f) \leqslant d_1 \cdots d_n - (d_1 - \alpha_1) \cdots (d_n - \alpha_n).$$

On the other hand, if $\boldsymbol{\beta} \in \mathrm{mv}_{\mathbf{p}}(m, f)$ for every $\mathbf{p} \in S$ and $\boldsymbol{\beta} < m(\mathbf{p})$, then

$$\sum_{\mathbf{p} \in S} \mathrm{mult}_{\mathbf{p}}(m, f) = \sum_{\mathbf{p} = (p_1, \dots, p_n) \in S} m_1(p_1) \cdots m_n(p_n) = d_1 \cdots d_n,$$

which contradicts the inequality above. Thus, there are $\mathbf{p} \in S$ and $\boldsymbol{\beta} < m(\mathbf{p})$ such that $D^{\boldsymbol{\beta}} f(\mathbf{p}) \neq 0$, as required. □

https://doi.org/10.1017/S0004972720001197 Published online by Cambridge University Press

The next theorem is a slight generalisation of Theorem 3.3. The proof uses the theory of Groebner bases. Let f be a polynomial in R. We define the *support* of f by

$$\operatorname{supp}(f) = \{\boldsymbol{\alpha} \in \mathbb{N}^n \mid \text{ the coefficient of } \mathbf{x}^{\boldsymbol{\alpha}} \text{ is nonzero in } f\}.$$

An element of $\operatorname{supp}(f)$ is called maximal if it is maximal with respect to the natural order on $\mathbb{N}^n$.

THEOREM 3.4. *Let $f \in R$ be a polynomial. Suppose that $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n)$ is maximal in $\operatorname{supp}(f)$. Assume further that $(S_1, m_1), (S_2, m_2), \dots, (S_n, m_n)$ are multisets of K such that for the size d_i of (S_i, m_i), we have $d_i > \alpha_i$ for $i = 1, \dots, n$. Then there exist a point $\mathbf{p} = (p_1, \dots, p_n) \in S_1 \times \cdots \times S_n$ and an exponent vector $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$ with $\beta_i < m_i(p_i)$ for each i such that $D^{\boldsymbol{\beta}} f(\mathbf{p}) \neq 0$.*

PROOF. For a point $\mathbf{p} \in K^n$ and an exponent vector $\boldsymbol{\beta} \in \mathbb{N}^n$ with positive integer components, we put

$$I(\mathbf{p}, \boldsymbol{\beta}) = \{g \in R \mid D^{\boldsymbol{\gamma}} g(\mathbf{p}) = 0 \text{ for all } \boldsymbol{\gamma} < \boldsymbol{\beta}\},$$

where $\boldsymbol{\gamma} < \boldsymbol{\beta}$ means $\gamma_i < \beta_i$ for $i = 1, \dots, n$. This is actually an ideal in R.

Let

$$I = \bigcap_{\mathbf{p} \in S} I(\mathbf{p}, m(\mathbf{p})).$$

In order to find the generators of I, for each $i = 1, \dots, n$, we set

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s)^{m_i(s)}.$$

Then $\{g_1, \dots, g_n\}$ is a universal Groebner basis for I by [9, Corollary 3].

We now turn to the proof of the theorem. Assume on the contrary that for every $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$ with $\beta_i < m_i(p_i)$ for each i, we have $D^{\boldsymbol{\beta}} f(\mathbf{p}) = 0$. Then we would have $f \in I$. Take any monomial order on R. For a polynomial g in R, we denote the leading term of g by $\operatorname{lt}(g)$. Then $\operatorname{lt}(g_i) = x_i^{d_i}$ for each i.

Since $\{g_1, \dots, g_n\}$ is a Groebner basis for I, the remainder of f on division by $(g_1, \dots, g_n)$ by using the division algorithm (see [5, Theorem 3, page 64 and Corollary 2, page 82]) is zero. The division algorithm to find the remainder can be described as follows.

(1) Let $r := f$.
(2) If r has a term, say $a_{\boldsymbol{\beta}} \mathbf{x}^{\boldsymbol{\beta}}$, which is divisible by $\operatorname{lt}(g_i)$ for some i, then let

$$r := r - a_{\boldsymbol{\beta}} \frac{\mathbf{x}^{\boldsymbol{\beta}}}{\operatorname{lt}(g_i)} g_i$$

and repeat this procedure.
If r has no such terms, then r is the remainder.

We now claim that $\mathbf{x}^{\boldsymbol{\alpha}}$ is a maximal element in $\operatorname{supp}(r)$ in every step of the algorithm above. Indeed, at the start of the algorithm we have $r = f$, so the assertion holds.

https://doi.org/10.1017/S0004972720001197 Published online by Cambridge University Press

Assume that at some step $\mathbf{x}^{\alpha}$ is maximal in $\operatorname{supp}(r)$. At the next step,

$$r := r - \frac{a_{\beta}\mathbf{x}^{\beta}}{\operatorname{lt}(g_i)}g_i,$$

as in the algorithm above. Observe that $\mathbf{x}^{\beta}$ is divisible by $\operatorname{lt}(g_i)$ and $\mathbf{x}^{\alpha}$ is not since $\operatorname{lt}(g_i) = x_i^{d_i}$ and $\alpha_i < d_i$. Thus, $\mathbf{x}^{\beta} \neq \mathbf{x}^{\alpha}$. On the other hand, every term of $(a_{\beta}\mathbf{x}^{\beta}/\operatorname{lt}(g_i))g_i$ divides $\mathbf{x}^{\beta}$. Consequently, every term is not divisible by $\mathbf{x}^{\alpha}$ because of the maximality of $\mathbf{x}^{\alpha}$. This forces $\mathbf{x}^{\alpha}$ to be maximal in $\operatorname{supp}(r)$ after this step and the claim follows.

By this claim, we deduce that the remainder of f on division by $(g_1, \ldots, g_n)$ is nonzero, which is a contradiction. Therefore, $D^{\beta}f(\mathbf{p}) \neq 0$ for some $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ with $\beta_i < m_i(p_i)$ for each i and the proof is complete. □

A consequence of Theorem 3.4 is the following result of Lasoń [10], which is also a generalisation of Alon's Nullstellensatz.

THEOREM 3.5 [10, Theorem 2]. *Let f be a polynomial in R. Suppose that $(\alpha_1, \ldots, \alpha_n)$ is maximal in $\operatorname{supp}(f)$. Then, for any subsets $S_1, \ldots, S_n$ of K satisfying $|S_i| \geqslant \alpha_i + 1$, there are $p_1 \in S_1, \ldots, p_n \in S_n$ so that $f(p_1, \ldots, p_n) \neq 0$.*

REMARK 3.6. For each $i = 1, \ldots, n$, put

$$g_i(x_i) = \prod_{s \in S_i}(x_i - s).$$

For a nonzero polynomial f of R, let $I = (g_1, \ldots, g_n, f) \subseteq R$. Then $Z_S(f) = Z(I)$. Now take an arbitrary order on R and let $\mathbf{x}^{\alpha}$ be the leading monomial of f with respect to this order. Assume that $\alpha_i < s_i$ for all i. The inequality (3.1) in Proposition 3.2 becomes

$$|Z_S(f)| \leqslant s_1 \cdots s_n - (s_1 - \alpha_1) \cdots (s_n - \alpha_n), \tag{3.2}$$

which is called the *footprint bound* by some authors (see [7]), so we may consider (3.1) as the footprint bound for multisets.

By virtue of Theorem 3.5, it is natural to ask whether the footprint bound (3.2) holds whenever $\boldsymbol{\alpha}$ is maximal in $\operatorname{supp}(f)$ (that is, not necessarily a leading monomial of f). The following example shows that this is not the case.

EXAMPLE 3.7. Let $K = F_{64}$ be a finite field with 64 elements. Let $f = x^5 + y^{17} + xy$ and $S_1 = S_2 = K$, so that $s_1 = s_2 = 64$. Observe that the exponent $\boldsymbol{\alpha} = (1, 1)$ of xy is maximal in $\operatorname{supp}(f)$.

We have $s_1s_2 - (s_1 - \alpha_1)(s_2 - \alpha_2) = 127$. On the other hand, by using *Macaulay2* (see [8]), we can verify that

$$|Z_S(f)| = 316,$$

where $S = S_1 \times S_2$. Thus, $|Z_S(f)| > s_1s_2 - (s_1 - \alpha_1)(s_2 - \alpha_2)$.

https://doi.org/10.1017/S0004972720001197 Published online by Cambridge University Press

References

[1] N. Alon, 'Combinatorial Nullstellensatz', *Combin. Probab. Comput.* **8** (1999), 7–29.
[2] N. Alon, M. B. Nathanson and I. Z. Ruzsa, 'The polynomial method and restricted sums of congruence classes', *J. Number Theory* **56** (1996), 404–417.
[3] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra* (Addison-Wesley, Reading, MA, 1969).
[4] D. Cox, J. Little and D. O'Shea, *Using Algebraic Geometry* (Springer, New York–Berlin–Heidelberg, 1997).
[5] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 3rd edn (Springer, New York, 2006).
[6] G.-L. Feng, T. R. N. Rao, G. A. Berg and J. Zhu, 'Generalized Bezout's theorem in its applications in coding theory', *IEEE Trans. Inform. Theory* **43** (1997), 1799–1810.
[7] O. Geil and T. Høholdt, 'Footprints or generalized Bezout's theorem', *IEEE Trans. Inform. Theory* **46**(2) (2000), 635–641.
[8] D. R. Grayson and M. E. Stillman, *Macaulay2, a Software System for Research in Algebraic Geometry*, available at http://www.math.uiuc.edu/Macaulay2/.
[9] G. Kós and L. Rónyai, 'Alon's Nullstellensatz for multisets', *Combinatorica* **32**(5) (2012), 589–605.
[10] M. Lasoń, 'A generalization of combinatorial Nullstellensatz', *Electron. J. Combin.* **17**(1) (2010), Note 32, 6 pages.
[11] T. Tao, 'Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory', *EMS Surv. Math. Sci.* **1** (2014), 1–46.

NGUYEN CONG MINH, Department of Mathematics,
Hanoi National University of Education, 136 Xuan Thuy,
Hanoi, Vietnam
e-mail: minhnc@hnue.edu.vn

LUU BA THANG, Department of Mathematics,
Hanoi National University of Education, 136 Xuan Thuy,
Hanoi, Vietnam
e-mail: thanglb@hnue.edu.vn

TRAN NAM TRUNG, Institute of Mathematics,
VAST, 18 Hoang Quoc Viet, Hanoi, Vietnam
and
TIMAS, Thang Long University, Hanoi, Vietnam
e-mail: tntrung@math.ac.vn

https://doi.org/10.1017/S0004972720001197 Published online by Cambridge University Press