A Gröbner Basis Approach to Combinatorial Nullstellensatz

Yang Xu[1]   Haibin Kan[2]   Guangyue Han[3]

August 13, 2023

Abstract— In this paper, using some conditions that arise naturally in Alon's combinatorial Nullstellensatz as well as its various extensions and generalizations, we give characterizations of Gröbner bases consisting of monic polynomials, which help us to establish a Nullstellensatz from a Gröbner basis perspective. As corollaries of this general Nullstellensatz, we establish four special Nullstellensatz, which, among others, include a common generalization of the Nullstellensatz for multisets established in Kós, Rónyai and Mészáros [23, 24] and the Nullstellensatz with multiplicity established in Ball and Serra [9], and include a punctured Nullstellensatz, generalizing several existing results in the literature. As applications of our punctured Nullstellensatz, we extend some results on hyperplane covering in [9, 23, 24] to wider settings, and give an alternative proof of the generalized Alon-Füredi theorem established in Bishnoi, Clark, Potukuchi and Schmitt [12]. Unless specified otherwise, all our results are established over an arbitrary commutative ring R.

[1]Department of Mathematics, Faculty of Science, The University of Hong Kong, Pokfulam Road, Hong Kong, China. E-mail:12110180008@fudan.edu.cn

[2]Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China.
Shanghai Engineering Research Center of Blockchain, Shanghai 200433, China.
Yiwu Research Institute of Fudan University, Yiwu City, Zhejiang 322000, China. E-mail:hbkan@fudan.edu.cn

[3]Department of Mathematics, Faculty of Science, The University of Hong Kong, Pokfulam Road, Hong Kong, China. E-mail:ghan@hku.hk

1   Introduction

Throughout the paper, we let $\mathbb{Z}^+$ denote the set of all the positive integers, and let $\mathbb{N} = \mathbb{Z}^+ \cup \{0\}$.

Let $\mathbb{F}$ be a field, $n \in \mathbb{Z}^+$, $S_1, \ldots, S_n$ be nonempty finite subsets of $\mathbb{F}$, and set $g_i = \prod_{u \in S_i}(x_i - u) \in \mathbb{F}[x_1, \ldots, x_n]$ for $i = 1, \ldots, n$. The following two celebrated theorems, known as combinatorial Nullstellensatz, have been established in Alon [3].

Theorem 1.1. *([3, Theorem 1.1]) Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ with $f(a_1, \ldots, a_n) = 0$ for all $a \in \prod_{i=1}^n S_i$. Then, there exist $h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n]$ such that $f = \sum_{i=1}^n h_i \cdot g_i$ and*

$$\deg(h_i) + \deg(g_i) \leqslant \deg(f) \text{ for all } i = 1, \ldots, n. \tag{1.1}$$

Moreover, if $f, g_1, \ldots, g_n \in R[x_1, \ldots, x_n]$ for some subring R of $\mathbb{F}$, then $h_1, \ldots, h_n$ above can be chosen from $R[x_1, \ldots, x_n]$.

Theorem 1.2. *([3, Theorem 1.2]) Let $f \in \mathbb{F}[x_1, \ldots, x_n]$, and let $(t_1, \ldots, t_n) \in \mathbb{N}^n$ such that $\deg(f) = \sum_{i=1}^n t_i$, and the coefficient of $\prod_{i=1}^n x_i^{t_i}$ in f is nonzero. Suppose that $t_i \leqslant |S_i| - 1$ for all $i = 1, \ldots, n$. Then, there exists $a \in \prod_{i=1}^n S_i$ such that $f(a_1, \ldots, a_n) \neq 0$.*

Combinatorial Nullstellensatz is a very powerful algebraic tool, and has numerous applications in combinatorics, graph theory, combinatorial number theory and coding theory; see, among many others, the papers [2, 3, 5, 30, 32, 35] and the recent book [36] for more details.

As detailed below, Alon's combinatorial Nullstellensatz has been generalized and extended in a number of directions.

Ball and Serra prove in [9] a Nullstellensatz with multiplicity, which, with the multiplicities of zeros set to be 1, boils down to Alon's combinatorial Nullstellensatz. They also establish a punctured Nullstellensatz, which is used to recover the Alon-Füredi theorem on the number of zeros of a polynomial (see [4]), and to generalize many results in Alon and Füredi [4] and Bruen [15]. Kós and Rónyai prove in [24] a Nullstellensatz for multisets, which, with multisets assumed to be ordinary sets, boils down to Alon's combinatorial Nullstellensatz. As in [9], they establish a punctured Nullstellensatz, which is used to generalize many applications of Alon's combinatorial Nullstellensatz to multisets, including the theorem of Alon and Füredi on hyperplane covering (see [4]), the Cauchy-Davenport theorem, Sun's theorem on value sets (see [35]) and the Eliahou-Kervaire theorem (see [20]).

Mezei proves in [29] a more general Nullstellensatz which includes both the aforementioned Nullstellensatz as special cases.

Lasoń proves in [27] a generalization of Theorem 1.2 by weakening the assumption that $\deg(f) = \sum_{i=1}^{n} t_i$ to that $(t_1, \ldots, t_n)$ is maximal among all $(c_1, \ldots, c_n) \in \mathbb{N}^n$ where the coefficient of $\prod_{i=1}^{n} x_i^{c_i}$ in f is nonzero. Batzaya and Bayarmagnai further weaken the assumption for $(t_1, \ldots, t_n)$ and prove in [11] a common generalization of Lasoń's result and [24, Theorem 6].

Now, suppose that $\mathbb{F}$ is replaced by an arbitrary commutative ring R. Schauz proves in [34] that if for any $i = 1, \ldots, n$, S_i satisfies Condition (D), i.e., $v - u$ is not a zero divisor of R for all $u \neq v \in S_i$ (see [12, 17, 18, 34] or Definition 2.2 for more details), then the conclusion of Theorem 1.1 remains valid. Michałek proves in [30] that if all the S_i's satisfy Condition (D), then the conclusion of Theorem 1.2 remains valid. Clark proves in [17] that Condition (D) is in fact a necessary and sufficient condition for Theorem 1.1 to hold true. Clark proves in [18] a variant of the punctured Nullstellensatz in Ball and Serra [9] under the assumption that all the S_i's satisfy Condition (D). It is also observed in [18] that the Nullstellensatz in [9] and its punctured version can be generalized under Condition (D). Kulosman and Wang prove in [25] a Nullstellensatz for multisets under the assumption that R is an integral domain of characteristic zero. Kós, Mészáros and Rónyai prove in [23] a Nullstellensatz for multisets under Condition (D), which generalizes both Michałek's result in [30] and the Nullstellensatz for multisets in [24].

We refer the reader to [17, 28, 31] for other extensions and generalizations of Theorems 1.1 and 1.2.

As in [23, 24, 28, 29, 32], Gröbner bases (see [1, 16, 21]) arise naturally in Alon's combinatorial Nullstellensatz and its generalizations. In this paper, we re-examine Alon's combinatorial Nullstellensatz and some of its generalizations from a Gröbner basis perspective. Our starting point is the observation that each one of Theorem 1.1, Theorem 1.2 and Lasoń's generalization of Theorem 1.2 (see [27, Theorem 2]) is an equivalent formulation of the fact that $(g_1, \ldots, g_n)$ is a Gröbner basis; and moreover, this observation holds true for more general results including the Nullstellensatz with multiplicity and the Nullstellensatz for multisets.

In Section 2, we collect some notations, definitions and lemmas. In Section 3, we present alternative characterizations of Gröbner bases consisting of monic polynomials (Definition 2.1, Theorem 3.1). Three of these characterizations have appeared in Alon's combinatorial Nullstellensatz and its generalizations, yet there is also one characterization that seems to be new.

In Section 4, we apply Theorem 3.1 to derive a Nullstellensatz (Theorem 4.2), where Condition (D) plays a critical role (also see Theorem 4.1).

3

Theorems 4.1 and 4.2 are general in the sense that they can be used to derive more specific Nullstellensatz, as detailed in Section 5.

In Section 5.1, we apply Theorems 4.1 and 4.2 to establish an extension of Mezei's Nullstellensatz [29, Theorem 6.12] (Theorem 5.1). In Section 5.2, we further apply Theorem 5.1 to establish a common generalization of the Nullstellensatz with multiplicity in [9] and the Nullstellensatz for multisets in [23, 24] (Theorem 5.2). In Section 5.3, with the help of Theorem 5.2, we establish a punctured Nullstellensatz (Theorem 5.3), which includes the punctured Nullstellensatz in [9, 24] as special cases. In Section 5.4, we apply Theorems 4.1 and 4.2 to establish another Nullstellensatz (Theorem 5.4), which is further used to generalize a result in Sauermann and Wigderson [33] (Corollary 5.2). We note that in each of Theorems 5.1, 5.2 and 5.4, Condition (D) arises as a necessary and sufficient condition with some mild assumptions.

In Section 6.1, we apply our punctured Nullstellensatz to hyperplane covering (Theorem 6.1, Corollaries 6.1 and 6.2), generalizing some related results in [9, 23, 24]. In Section 6.2, following the spirit of [9, 18], we apply our punctured Nullstellensatz to give an alternative proof of the generalized Alon-Füredi theorem established in Bishnoi, Clark, Potukuchi and Schmitt [12], a result that has many applications in combinatorics and coding theory (see [12] for more details).

2 Preliminaries

First, we introduce some notations and terminologies that will be used throughout the remainder of the paper. Fix $n \in \mathbb{Z}^+$, and let

$$[1, n] = \{1, \ldots, n\}. \tag{2.1}$$

Let $\mathbf{0}$ denote the all-zero vector of $\mathbb{N}^n$. For any $\alpha \in \mathbb{N}^n$ and $i \in [1, n]$, we let α_i denote the i-th entry of α. For $\alpha, \beta \in \mathbb{N}^n$, we define $\alpha + \beta \in \mathbb{N}^n$ and $\alpha - \beta \in \mathbb{Z}^n$ as

$$(\alpha + \beta)_i = \alpha_i + \beta_i \text{ for all } i \in [1, n], \tag{2.2}$$

$$(\alpha - \beta)_i = \alpha_i - \beta_i \text{ for all } i \in [1, n], \tag{2.3}$$

and we write $\alpha \leqslant \beta$ if $\alpha_i \leqslant \beta_i$ for all $i \in [1, n]$. For any $A \subseteq \mathbb{N}^n$, we define

$$\Delta(A) = \{\beta \in \mathbb{N}^n \mid \exists\, \alpha \in A \ s.t.\ \beta \leqslant \alpha\}, \tag{2.4}$$

$$\nabla(A) = \{\beta \in \mathbb{N}^n \mid \exists\, \alpha \in A \ s.t.\ \alpha \leqslant \beta\}, \tag{2.5}$$

4

$$\max(A) = \{\beta \in A \mid \forall \; \alpha \in A : \beta \leqslant \alpha \Longrightarrow \beta = \alpha\}. \qquad (2.6)$$

For any $A \subseteq \mathbb{N}^n$ and $\theta \in A$, θ is referred to as *the greatest element* of A if $\gamma \leqslant \theta$ for all $\gamma \in A$. For any $A, B \subseteq \mathbb{N}^n$, we let

$$A + B = \{\alpha + \beta \mid \alpha \in A, \beta \in B\}. \qquad (2.7)$$

Let R be a commutative ring with multiplicative identity 1_R, and let

$$\Omega \triangleq R[x_1, \ldots, x_n] \qquad (2.8)$$

denote the polynomial ring over R in n variables $x_1, \ldots, x_n$. For $f \in \Omega$ and $\alpha \in \mathbb{N}^n$, we let $f_{[\alpha]}$ denote the coefficient of $\prod_{i=1}^n x_i^{\alpha_i}$ in f. For any $f \in \Omega$, we let

$$\mathrm{supp}\,(f) = \{\alpha \in \mathbb{N}^n \mid f_{[\alpha]} \neq 0\}. \qquad (2.9)$$

For any $A \subseteq \mathbb{N}^n$, let

$$\delta(A) = \{f \in \Omega \mid \mathrm{supp}\,(f) \subseteq A\}. \qquad (2.10)$$

We also define $\Phi : (R^n \times \mathbb{N}^n) \times \mathbb{N}^n \longrightarrow R$ as

$$\Phi((u, \alpha), \gamma) = \begin{cases} \left(\prod_{k=1}^n \binom{\gamma_k}{\alpha_k}\right) \left(\prod_{k=1}^n u_k^{\gamma_k - \alpha_k}\right), & \alpha \leqslant \gamma; \\ 0, & \alpha \nleqslant \gamma. \end{cases} \qquad (2.11)$$

Moreover, for any $f, g \in \Omega$, we write $g \mid f$ if there exists $h \in \Omega$ with $f = h \cdot g$; for any $U \subseteq \Omega$, we let $\langle U \rangle$ denote the ideal of Ω generated by U; and for any finitely generated R-module M, we let $\mathrm{rank}\,_R(M)$ denote the minimum number of generators of M.

Next, we give some definitions. We begin by introducing **monic polynomials**.

Definition 2.1. *For any $g \in \Omega$, g is said to be monic if there exists $\theta \in \mathrm{supp}\,(g)$ such that $g_{[\theta]} = 1_R$ and $\gamma \leqslant \theta$ for all $\gamma \in \mathrm{supp}\,(g)$, that is to say, θ is the greatest element of $\mathrm{supp}\,(g)$ and $g_{[\theta]} = 1_R$.*

Now following [17, Definition 1] and [34, Definition 2.8], we state the aforementioned Condition (D).

Definition 2.2. *For any $u \in R$, u is referred to as a multiplicative unit of R if there exists $v \in R$ with $uv = 1_R$, and u is referred to as a zero divisor of R if there exists $w \in R$ such that $w \neq 0$ and $uw = 0$. For $X \subseteq R$, we say that X satisfies Condition (F) in R if for any $a, b \in X$ with $a \neq b$, $b - a$ is a multiplicative unit of R; and we say that X satisfies Condition (D) in R if for any $a, b \in X$ with $a \neq b$, $b - a$ is **not** a zero divisor of R.*

Now we state our definition of Gröbner basis. **In this paper, we only consider Gröbner bases consisting of monic polynomials**. We refer the reader to [1, Definition 4.1.13] for the general definition of Gröbner basis.

Definition 2.3. *Let Λ be a finite set, and let $(g(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ be a family of monic polynomials. For any $\lambda \in \Lambda$, let $\theta(\lambda)$ be the greatest element of $\mathrm{supp}\,(g(\lambda))$. Let Q be an ideal of Ω with $\{g(\lambda) \mid \lambda \in \Lambda\} \subseteq Q$. Then, we say that $(g(\lambda) \mid \lambda \in \Lambda)$ is a Gröbner basis of Q if for any $\tau \in Q - \{0\}$, there exists $\alpha \in \mathrm{supp}\,(\tau)$ and $r \in \Lambda$ with $\theta(r) \leqslant \alpha$.*

We give some remarks on Definition 2.3.

Remark 2.1. *First, a Gröbner basis is usually defined as a set of polynomials instead of a tuple. In this paper, we find it convenient to handle a tuple since we do not assume that $g(\lambda) \neq g(\mu)$ for all $\lambda \neq \mu \in \Lambda$.*

Second, in general, a Gröbner basis is defined with respect to a fixed monomial order on $\mathbb{N}^n$, and the $g(\lambda)$'s do not need to be monic. Following [21, Sections 21.2 and 21.3], a monomial order on $\mathbb{N}^n$ is a total order $\preccurlyeq$ on $\mathbb{N}^n$ satisfying the following two conditions:

(i) For any $\alpha, \beta, \gamma \in \mathbb{N}^n$ with $\alpha \preccurlyeq \beta$, it holds that $\alpha + \gamma \preccurlyeq \beta + \gamma$;

(ii) For any $\alpha, \beta \in \mathbb{N}^n$ with $\alpha \leqslant \beta$, it holds that $\alpha \preccurlyeq \beta$.

Now let $g \in \Omega$ be monic, and let θ be the greatest element of $\mathrm{supp}\,(g)$. Then, for an arbitrary term order $\preccurlyeq$, it follows from (ii) that $\alpha \preccurlyeq \theta$ for all $\alpha \in \mathrm{supp}\,(g)$, that is to say, $\prod_{i=1}^n x_i^{\theta_i}$ is the leading monomial of g with respect to $\preccurlyeq$; and moreover, the leading coefficient of g with respect to $\preccurlyeq$ is equal to $g_{[\theta]} = 1_R$ (see [21, Definition 21.7]). Based on this observation, Definition 2.3 is indeed a special case of the general definition of Gröbner basis. Moreover, if R is a field, then Definition 2.3 becomes a special case of [1, Definition 1.6.1], [16, Section 2.8] and [21, Definition 21.25].

In the following example, we consider a class of Gröbner bases which will be used in Section 5.

Example 2.1. *Let $(g_1, \ldots, g_n) \in \Omega^n$ be a family of monic polynomials such that $g_k \in R[x_k]$ for all $k \in [1, n]$. Then, for any $\alpha \in \mathbb{N}^n$, $\prod_{k=1}^n g_k^{\alpha_k}$ is monic, and $(\deg(g_1)\alpha_1, \cdots, \deg(g_n)\alpha_n)$ is the greatest element of $\mathrm{supp}\,(\prod_{k=1}^n g_k^{\alpha_k})$.*

*Now let A be a finite subset of $\mathbb{N}^n$. Then, $(\prod_{k=1}^n g_k^{\alpha_k} \mid \alpha \in A)$ is a Gröbner basis of $\langle \{\prod_{k=1}^n g_k^{\alpha_k} \mid \alpha \in A\} \rangle$. This can be derived from the celebrated Buchberger's theorem (see [1, Theorem 1.7.4], [16, Section 2.10], [21, Theorem 21.31]) by examining **S**-polynomials (see [1, Definition 1.7.1],*

[16, Section 2.9], [21, Definition 21.29]). We note that though Buchberger's theorem is established for polynomials over a field, one can check that its proof remains valid in our setting.

Now we follow [23, 24] and introduce the notion of multiset, which will be used in Sections 5 and 6.

Definition 2.4. *A pair (X, ψ) is referred to as a multiset if X is a set, ψ is a function with $X \subseteq \mathrm{dom}\,(\psi)$, and $\psi(u) \in \mathbb{Z}^+$ for all $u \in X$.*

The following definition of r-hyperplane, which will be used in Section 6, extends that of hyperplane.

Definition 2.5. *For any $H \subseteq R^n$, $r \in \mathbb{N}$, H is referred to as an r-hyperplane of R^n if there exists $h \in \Omega$ such that $H = \{u \in R^n \mid h(u_1, \ldots, u_n) = 0\}$ and $\deg(h) = r$. A 1-hyperplane of R^n is referred to as a hyperplane of R^n.*

Now, we give some lemmas. The following lemma, whose proof is straightforward and hence omitted, collects some basic properties of monic polynomials that will be used frequently in our discussion.

Lemma 2.1. *Let $g \in \Omega$ be a monic polynomial, and let θ be the greatest element of $\mathrm{supp}\,(g)$. Also let $f \in \Omega$. Then, it holds that:*

(1) *For any $\gamma \in \max(\mathrm{supp}\,(f))$, we have $(f \cdot g)_{[\gamma + \theta]} = f_{[\gamma]}$;*

(2) $\max(\mathrm{supp}\,(f \cdot g)) = \max(\mathrm{supp}\,(f)) + \{\theta\}$;

(3) $\Delta(\mathrm{supp}\,(f \cdot g)) = \Delta(\mathrm{supp}\,(f)) + \Delta(\mathrm{supp}\,(g))$;

(4) $\deg(f \cdot g) = \deg(f) + \deg(g)$. *In particular, $f \neq 0 \implies f \cdot g \neq 0$.*

The following well known lemma, which will be used in Section 4, can be verified via some straightforward computation (see, e.g., [11, 23, 24]).

Lemma 2.2. *Let $f \in \Omega$. Then, for any $(u, \alpha) \in R^n \times \mathbb{N}^n$, it holds that*

$$f(x_1 + u_1, \ldots, x_n + u_n)_{[\alpha]} = \sum_{\gamma \in \mathrm{supp}\,(f)} \Phi((u, \alpha), \gamma) \cdot f_{[\gamma]}.$$

The following lemma, which will be used in Sections 4 and 5, is straightforward to verify.

Lemma 2.3. *Let $C \subseteq \mathbb{N}^n$. Then, $\mathbb{N}^n - \nabla(C)$ is finite if and only if for any $k \in [1, n]$, there exists $\beta \in C$ such that $(\forall\, l \in [1, n] - \{k\} : \beta_l = 0)$.*

The following three lemmas will be used in Section 5. Their proofs are included in Appendices A, B and C for completeness.

Lemma 2.4. *Let g be a monic polynomial, and let θ be the greatest element of $\operatorname{supp}(g)$. Also let $\rho \in \Omega$ such that for any $\gamma \in \operatorname{supp}(\rho)$, it holds that $0 \in \{\gamma_i, \theta_i\}$ for all $i \in [1, n]$. Let $\psi \in \Omega$ such that $\rho \mid \psi$, $g \mid \psi$. Then, we have $(\rho \cdot g) \mid \psi$.*

Lemma 2.5. *Let $\alpha \in \mathbb{N}^n$, $t \in \mathbb{N}$, and let*

$$B = \{(\alpha_1 \theta_1, \ldots, \alpha_n \theta_n) \mid \theta \in \mathbb{N}^n, \sum_{i=1}^n \theta_i = t\}.$$

Then, it holds that

$$|\mathbb{N}^n - \nabla(B)| = (\textstyle\prod_{i=1}^n \alpha_i) \binom{n+t-1}{n}. \tag{2.12}$$

Assume in addition that $\alpha \in (\mathbb{Z}^+)^n$. Then, it holds that

$$\mathbb{N}^n - \nabla(B) = \{\beta \in \mathbb{N}^n \mid \textstyle\sum_{i=1}^n \left\lfloor \frac{\beta_i}{\alpha_i} \right\rfloor \leqslant t - 1\}. \tag{2.13}$$

Lemma 2.6. *Let $\alpha \in \mathbb{N}^n$, $\gamma \in \mathbb{N}^n$ with $\gamma \leqslant \alpha$, and fix $t \in \mathbb{Z}^+$. Let*

$$B = \{(\alpha_1 \theta_1, \ldots, \alpha_n \theta_n) \mid \theta \in \mathbb{N}^n, \sum_{i=1}^n \theta_i = t\},$$

$$C = \{(\alpha_1 \theta_1, \ldots, \alpha_n \theta_n) + \alpha - \gamma \mid \theta \in \mathbb{N}^n, \sum_{i=1}^n \theta_i = t - 1\}.$$

Then, it holds that

$$|\mathbb{N}^n - \nabla(B \cup C)| = (\textstyle\prod_{i=1}^n \alpha_i) \binom{n+t-1}{n} - (\textstyle\prod_{i=1}^n \gamma_i) \binom{n+t-2}{n-1}.$$

3 Characterizations of Gröbner bases

Lemma 3.1. *Let Λ be a finite set, and let $(g(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ be a family of monic polynomials. For any $\lambda \in \Lambda$, let $\theta(\lambda)$ be the greatest element of $\operatorname{supp}(g(\lambda))$. Then, for any $f \in \Omega$, there exist $(p(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ and $\tau \in \Omega$ satisfying the following four conditions:*

(1) $f = (\sum_{\lambda \in \Lambda} p(\lambda) \cdot g(\lambda)) + \tau$;

(2) *For any $\lambda \in \Lambda$, it holds that $\operatorname{supp}(p(\lambda)) + \operatorname{supp}(g(\lambda)) \subseteq \Delta(\operatorname{supp}(f))$;*

(3) *For any $\lambda \in \Lambda$ and $\alpha \in \operatorname{supp}(\tau)$, it holds that $\theta(\lambda) \not\leqslant \alpha$;*

(4) $\operatorname{supp}(\tau) \subseteq \Delta(\operatorname{supp}(f))$.

Proof. Let $\Gamma \triangleq \{A \subseteq \mathbb{N}^n \mid A \text{ is finite}\}$, and let $\preccurlyeq$ be an order on Γ defined as follows: For any $A, B \in \Gamma$, $A \preccurlyeq B$ if and only if either $A = B$ or there exists $\beta \in B - A$ such that $\alpha \leqslant \beta$ for all $\alpha \in A - B$. One can check that $(\Gamma, \preccurlyeq)$ satisfies the minimal condition, i.e., for any $H \subseteq \Gamma$ with $H \neq \emptyset$, H contains a minimal element with respect to $\preccurlyeq$.

Now let $f \in \Omega$. If $\theta(\lambda) \not\leqslant \alpha$ for all $\lambda \in \Lambda$ and $\alpha \in \operatorname{supp}(f)$, then $(p(\lambda) \mid \lambda \in \Lambda)$ defined as $p(\lambda) = 0$ for all $\lambda \in \Lambda$ and $\tau = f$ satisfy Conditions (1)–(4). Therefore in the following, we assume that there exist $t \in \Lambda$, $\gamma \in \operatorname{supp}(f)$ such that $\theta(t) \leqslant \gamma$. Now let

$$h \triangleq f - f_{[\gamma]} \cdot \left(\prod_{i=1}^{n} x_i^{\gamma_i - \theta(t)_i}\right) \cdot g(t). \tag{3.1}$$

By (3.1) and the fact that $\theta(t)$ is the greatest element of $\operatorname{supp}(g(t))$, we have

$$\operatorname{supp}(h) - \operatorname{supp}(f) \subseteq \{\gamma - \theta(t)\} + \operatorname{supp}(g(t)) \subseteq \Delta(\{\gamma\}) \subseteq \Delta(\operatorname{supp}(f)). \tag{3.2}$$

From $g(t)_{[\theta(t)]} = 1_R$ and (3.1), we deduce that $h_{[\gamma]} = f_{[\gamma]} - f_{[\gamma]} = 0$, which implies that $\gamma \in \operatorname{supp}(f) - \operatorname{supp}(h)$. This, together with (3.2), implies that $\operatorname{supp}(h) \preccurlyeq \operatorname{supp}(f)$, $\operatorname{supp}(h) \neq \operatorname{supp}(f)$, $\operatorname{supp}(h) \subseteq \Delta(\operatorname{supp}(f))$, which further implies that $\Delta(\operatorname{supp}(h)) \subseteq \Delta(\operatorname{supp}(f))$.

Since $(\Gamma, \preccurlyeq)$ satisfies the minimal condition, applying an induction argument to h, we can choose $(q(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ and $\tau \in \Omega$ satisfying the following three conditions:

(i) $h = \left(\sum_{\lambda \in \Lambda} q(\lambda) \cdot g(\lambda)\right) + \tau$;

(ii) For any $\lambda \in \Lambda$, it holds that $\operatorname{supp}(q(\lambda)) + \operatorname{supp}(g(\lambda)) \subseteq \Delta(\operatorname{supp}(h))$;

(iii) For any $\lambda \in \Lambda$ and $\alpha \in \operatorname{supp}(\tau)$, it holds that $\theta(\lambda) \not\leqslant \alpha$.

Now define $(p(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ as $p(\lambda) = q(\lambda)$ for all $\lambda \in \Lambda - \{t\}$, and

$$p(t) = q(t) + f_{[\gamma]} \cdot \left(\prod_{i=1}^{n} x_i^{\gamma_i - \theta(t)_i}\right).$$

We claim that Conditions (1)–(4) hold true for f, $(p(\lambda) \mid \lambda \in \Lambda)$ and τ. Indeed, via some straightforward verification, (1) follows from (i) and (3.1), (2) follows from (ii), (3.2) and the fact that $\Delta(\operatorname{supp}(h)) \subseteq \Delta(\operatorname{supp}(f))$, (3) follows from (iii), and (4) follows from (1) and (2), as desired. $\qquad\square$

Now we are ready to prove the main result of this section.

Theorem 3.1. *Let Λ be a finite set, and let $(g(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ be a family of monic polynomials. For any $\lambda \in \Lambda$, let $\theta(\lambda)$ be the greatest element of*

supp $(g(\lambda))$. *Moreover, let Q be an ideal of Ω with $\{g(\lambda) \mid \lambda \in \Lambda\} \subseteq Q$.*
Then, the following six statements are equivalent to each other:

(1) $(g(\lambda) \mid \lambda \in \Lambda)$ *is a Gröbner basis of Q;*

(2) $Q \cap \delta(\mathbb{N}^n - \nabla(\{\theta(\lambda) \mid \lambda \in \Lambda\})) = \{0\}$;

(3) *For any $f \in Q$, there exists $(p(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ satisfying the following two conditions:*

    3.1) $f = \sum_{\lambda \in \Lambda} p(\lambda) \cdot g(\lambda)$;

    3.2) *For any $\lambda \in \Lambda$, it holds that* supp $(p(\lambda))$+supp $(g(\lambda)) \subseteq \Delta(\text{supp}\,(f))$;

(4) *For any $f \in Q$ and $\beta \in \max(\text{supp}\,(f))$, there exists $\xi \in \Lambda$ with $\theta(\xi) \leqslant \beta$;*

(5) *For any $f \in Q$, there exists $(p(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ satisfying the following two conditions:*

    5.1) $f = \sum_{\lambda \in \Lambda} p(\lambda) \cdot g(\lambda)$;

    5.2) *For any $\lambda \in \Lambda$, it holds that* $\deg(p(\lambda)) + \deg(g(\lambda)) \leqslant \deg(f)$;

(6) *For any $f \in Q - \{0\}$ and $\beta \in$ supp (f) with $\deg(f) = \sum_{i=1}^{n} \beta_i$, there exists $\xi \in \Lambda$ with $\theta(\xi) \leqslant \beta$.*

Proof. We begin by noting that $(1) \Longleftrightarrow (2)$ immediately follows from Definition 2.3, (2.5) and (2.10). Therefore in what follows, we will show that $(1) \Longrightarrow (3) \Longrightarrow (4) \Longrightarrow (6) \Longrightarrow (1)$ and $(3) \Longrightarrow (5) \Longrightarrow (6)$.

$(1) \Longrightarrow (3)$ Let $f \in Q$. By Lemma 3.1, we can choose $(p(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ and $\tau \in \Omega$ satisfying the following three conditions:

(i) $f = (\sum_{\lambda \in \Lambda} p(\lambda) \cdot g(\lambda)) + \tau$;

(ii) For any $\lambda \in \Lambda$, it holds that supp $(p(\lambda)) + $ supp $(g(\lambda)) \subseteq \Delta(\text{supp}\,(f))$;

(iii) For any $\lambda \in \Lambda$ and $\alpha \in$ supp (τ), it holds that $\theta(\lambda) \not\leqslant \alpha$.

By (i), we have $\tau \in Q$, which, together with (iii) and Definition 2.3, further implies that $\tau = 0$. Now (3) immediately follows from (i) and (ii).

$(3) \Longrightarrow (4)$ Let $f \in Q$. By (3), we can choose $(p(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ satisfying 3.1) and 3.2). Consider an arbitrary $\beta \in \max(\text{supp}\,(f))$. By 3.1), there exists $\xi \in \Lambda$ such that $\beta \in$ supp $(p(\xi) \cdot g(\xi))$. Hence we can choose $\alpha \in$ supp $(p(\xi))$, $\gamma \in$ supp $(g(\xi))$ with $\beta = \alpha + \gamma$. Since $\theta(\xi)$ is the greatest element of supp $(g(\xi))$, we have $\gamma \leqslant \theta(\xi)$, which further yields that $\beta \leqslant \alpha + \theta(\xi)$. By 3.2), we have $\alpha + \theta(\xi) \in \Delta(\text{supp}\,(f))$. Thus we can choose $\mu \in$ supp (f) with $\alpha + \theta(\xi) \leqslant \mu$. This, together with $\beta \leqslant \alpha + \theta(\xi)$, implies

that $\beta \leqslant \mu$. From $\beta \in \max(\mathrm{supp}\,(f))$, $\mu \in \mathrm{supp}\,(f)$, we deduce that $\beta = \mu$. It then follows that $\theta(\xi) \leqslant \alpha + \theta(\xi) = \beta$, as desired.

$(4) \implies (6)$ Let $f \in Q - \{0\}$ and $\beta \in \mathrm{supp}\,(f)$ with $\deg(f) = \sum_{i=1}^{n} \beta_i$. Then, we have $\beta \in \max(\mathrm{supp}\,(f))$, and the desired result follows from (4).

$(6) \implies (1)$ Consider an arbitrary $f \in Q - \{0\}$. Since $f \neq 0$, we can choose $\beta \in \mathrm{supp}\,(f)$ with $\deg(f) = \sum_{i=1}^{n} \beta_i$. By (6), we can further choose $\xi \in \Lambda$ with $\theta(\xi) \leqslant \beta$. Now (1) immediately follows from Definition 2.3.

$(3) \implies (5)$ This follows from the fact that 3.2) implies 5.2).

$(5) \implies (6)$ Let $f \in Q - \{0\}$. By (5), we can choose $(p(\lambda) \mid \lambda \in \Lambda) \in \Omega^{\Lambda}$ satisfying 5.1) and 5.2). Consider an arbitrary $\beta \in \mathrm{supp}\,(f)$ with $\deg(f) = \sum_{i=1}^{n} \beta_i$. By 5.1), there exists $\xi \in \Lambda$ with $\beta \in \mathrm{supp}\,(p(\xi) \cdot g(\xi))$. By 5.2), we have $\deg(p(\xi) \cdot g(\xi)) \leqslant \sum_{i=1}^{n} \beta_i$. It then follows that $\beta \in \max(\mathrm{supp}\,(p(\xi) \cdot g(\xi)))$, which, together with (2) of Lemma 2.1, implies that $\beta \in \max(\mathrm{supp}\,(p(\xi))) + \{\theta(\xi)\}$, and hence $\theta(\xi) \leqslant \beta$, as desired. $\qquad \square$

Remark 3.1. *In the study of combinatorial Nullstellensatz, conclusions of the form similar to (5), (6) of Theorem 3.1 have been established in various settings: in Alon's combinatorial Nullstellensatz Theorems 1.1 and 1.2, in the Nullstellensatz with multiplicity [9, Theorem 3.1, Corollary 3.2], in the Nullstellensatz for multisets [24, Theorems 1 and 6], in Mezei's Nullstellensatz [29, Theorem 6.12], and in Nullstellensatz over a commutative ring, including [34, Theorem 7.3], [30, Theorem 1], [17, Theorem 3.8 and c) of Theorem 3.9], [25, Theorems 2.1 and 2.2] and [23, Theorems 3 and 4]. Moreover, conclusions of the form similar to (4) of Theorem 3.1 have been established in [27, Theorem 2], which is a generalization of Theorem 1.2, and in [11, Corollary 1.6], which considers Nullstellensatz for multisets. In this sense, Theorem 3.1 reveals the essence of Alon's combinatorial Nullstellensatz and some of its generalizations from a Gröbner basis perspective. We also note that to the best of our knowledge, (3) of Theorem 3.1 seems to be a new characterization.*

As a first application of Theorem 3.1, in the following example, we recover Alon's combinatorial Nullstellensatz (Theorems 1.1 and 1.2) and Lasoń's generalization of Theorem 1.2 (see [27, Theorem 2]), and also derive an equivalent version of Theorem 1.1.

Example 3.1. *Suppose that R is an integral domain. Let $S_1, \ldots, S_n$ be nonempty finite subsets of R, $g_i = \prod_{u \in S_i}(x_i - u)$ for all $i \in [1, n]$, and let*

$$Q = \{f \in \Omega \mid f(a_1, \ldots, a_n) = 0 \text{ for all } a \in \prod_{i=1}^{n} S_i\}.$$

Apparently, $(g_1, \ldots, g_n)$ is a tuple of monic polynomials; for any $k \in [1, n]$, $\theta(k) \triangleq (\underbrace{0, \ldots, 0}_{k-1}, |S_k|, \underbrace{0, \ldots, 0}_{n-k})$ is the greatest element of $\mathrm{supp}\,(g_k)$; and more-over, Q is an ideal of Ω with $\{g_1, \ldots, g_n\} \subseteq Q$. By [3, Lemma 2.1], we have

$$Q \cap \delta(\mathbb{N}^n - \nabla(\{\theta(1), \ldots, \theta(n)\})) = \{0\}.$$

It then follows from Theorem 3.1 that $(g_1, \ldots, g_n)$ is a Gröbner basis of Q, as has been shown in [32, Section 6]. Moreover, (5) of Theorem 3.1 boils down to Theorem 1.1, (6) of Theorem 3.1 boils down to Theorem 1.2, (4) of Theorem 3.1 boils down to Lasoń's result [27, Theorem 2], and (3) of Theorem 3.1 boils down to an equivalent version of Theorem 1.1.

4   A Nullstellensatz derived from Theorem 3.1

Throughout this section, we let $S_1, \ldots, S_n$ be finite subsets of R, and let $(B_a \mid a \in \prod_{i=1}^n S_i)$ be a tuple of subsets of $\mathbb{N}^n$ such that for any $a \in \prod_{i=1}^n S_i$, $\mathbb{N}^n - \nabla(B_a)$ is finite. Moreover, we let

$$\zeta_1 \triangleq \sum_{a \in \prod_{i=1}^n S_i} |\mathbb{N}^n - \nabla(B_a)|, \tag{4.1}$$

and let Q denote the following ideal of Ω:

$$\{f \in \Omega \mid \forall\, a \in \textstyle\prod_{i=1}^n S_i : \mathrm{supp}\,(f(x_1 + a_1, \ldots, x_n + a_n)) \subseteq \nabla(B_a)\}. \tag{4.2}$$

Lemma 4.1. *Suppose that for any $i \in [1, n]$, S_i satisfies Condition (F) in R. Then, Ω/Q is a finitely generated free R-module with $\mathrm{rank}_R(\Omega/Q) = \zeta_1$.*

Proof. First, consider an arbitrary $a \in \prod_{i=1}^n S_i$. Let

$$J_a \triangleq \{f \in \Omega \mid \mathrm{supp}\,(f(x_1 + a_1, \ldots, x_n + a_n)) \subseteq \nabla(B_a)\}.$$

Apparently, J_a is an ideal of Ω. Moreover, since $\mathbb{N}^n - \nabla(B_a)$ is finite, it follows from Lemma 2.3 that for any $m \in [1, n]$, there exists $p \in \mathbb{N}$ with $(x_m - a_m)^p \in J_a$.

Next, let $b, d \in \prod_{i=1}^n S_i$ with $b \neq d$. We will show that

$$J_b + J_d = \Omega. \tag{4.3}$$

Indeed, fix $m \in [1, n]$ with $b_m \neq d_m$. Since S_m satisfies Condition (F) in R, by Definition 2.2, $d_m - b_m$ is a multiplicative unit of R. It then follows that $\langle\{x_m - b_m, x_m - d_m\}\rangle = \Omega$, which implies that $\langle\{(x_m - b_m)^p, (x_m - d_m)^q\}\rangle = \Omega$

12

for all $p, q \in \mathbb{N}$. By the previous paragraph, we can choose $p, q \in \mathbb{N}$ such that $(x_m - b_m)^p \in J_b$, $(x_m - d_m)^q \in J_d$, which further implies (4.3), as desired.

Note that if $\prod_{i=1}^n S_i = \emptyset$, then the desired result can be readily verified. Therefore in what follows, we assume $\prod_{i=1}^n S_i \neq \emptyset$. Then, we have $Q = \bigcap_{a \in \prod_{i=1}^n S_i} J_a$. For any $a \in \prod_{i=1}^n S_i$, it is straightforward to verify that Ω/J_a is a finitely generated free R-module with $\text{rank}\,_R(\Omega/J_a) = |\mathbb{N}^n - \nabla(B_a)|$. This, together with (4.3) and the Chinese remainder theorem (see [6, Proposition 1.10]), leads to the fact that Ω/Q is a finitely generated free R-module with

$$\text{rank}\,_R(\Omega/Q) = \textstyle\sum_{a \in \prod_{i=1}^n S_i} \text{rank}\,_R(\Omega/J_a) = \sum_{a \in \prod_{i=1}^n S_i} |\mathbb{N}^n - \nabla(B_a)| = \zeta_1,$$

as desired. $\qquad\square$

From now on, we let Λ be a finite set, and let $(g(\lambda) \mid \lambda \in \Lambda) \in Q^\Lambda$ be a family of monic polynomials. For any $\lambda \in \Lambda$, let $\theta(\lambda)$ be the greatest element of $\text{supp}\,(g(\lambda))$. Moreover, let $D = \{\theta(\lambda) \mid \lambda \in \Lambda\}$. Throughout the remainder of this section, we assume that $\mathbb{N}^n - \nabla(D)$ is finite, and let

$$\zeta_2 \triangleq |\mathbb{N}^n - \nabla(D)|. \tag{4.4}$$

Lemma 4.2. (1) *Suppose that for any $i \in [1, n]$, S_i satisfies Condition (F) in R. Then, we have $\zeta_1 \leqslant \zeta_2$. Moreover, if $\zeta_1 = \zeta_2$, then $(g(\lambda) \mid \lambda \in \Lambda)$ is a Gröbner basis of Q.*

(2) *Write $G = \bigcup_{a \in \prod_{i=1}^n S_i} \{a\} \times (\mathbb{N}^n - \nabla(B_a))$, and suppose that $(g(\lambda) \mid \lambda \in \Lambda)$ is a Gröbner basis of Q. Then, we have $\zeta_2 \leqslant \zeta_1$. Assume in addition that $\zeta_1 = \zeta_2$. Then, for any $\sigma \in R^G$, it holds that*

$$\left(\textstyle\sum_{(v,\alpha) \in G} \sigma_{(v,\alpha)} \cdot \Phi((v, \alpha), \gamma) = 0 \text{ for all } \gamma \in \mathbb{N}^n - \nabla(D)\right) \Longrightarrow \sigma = 0. \tag{4.5}$$

Proof. **(1)** We note that $\delta(\mathbb{N}^n - \nabla(D))$ is a finitely generated free R-module with $\text{rank}\,_R(\delta(\mathbb{N}^n - \nabla(D))) = \zeta_2$. Define the R-module homomorphism $\pi : \delta(\mathbb{N}^n - \nabla(D)) \longrightarrow \Omega/Q$ as $\pi(h) = h + Q$. It follows from Lemma 3.1 that π is surjective. This, together with Lemma 4.1, implies that $\zeta_1 = \text{rank}\,_R(\Omega/Q) \leqslant \zeta_2$, as desired. Now assume in addition that $\zeta_1 = \zeta_2$. Then, by Lemma 4.1, Ω/Q and $\delta(\mathbb{N}^n - \nabla(D))$ are finitely generated free R-modules with the same rank. This, together with the surjectivity of π and [14, Theorem 5.36], implies that π is injective, and hence $Q \cap \delta(\mathbb{N}^n - \nabla(D)) = \{0\}$. Now an application of Theorem 3.1 yields that $(g(\lambda) \mid \lambda \in \Lambda)$ is a Gröbner basis of Q, as desired.

(2) By Theorem 3.1, we have $Q \cap \delta(\mathbb{N}^n - \nabla(D)) = \{0\}$. Let $W \triangleq \Phi \mid_{G \times (\mathbb{N}^n - \nabla(D))}$. Then, W can be regarded as a matrix over R whose rows are indexed by G

13

and columns are indexed by $\mathbb{N}^n - \nabla(D)$. Consider the following homogeneous system of linear equations with unknowns $\rho \in R^{\mathbb{N}^n - \nabla(D)}$:

$$\sum_{\gamma \in \mathbb{N}^n - \nabla(D)} W((v, \alpha), \gamma) \cdot \rho_\gamma = 0 \text{ for all } (v, \alpha) \in G. \qquad (4.6)$$

Let $\rho \in R^{\mathbb{N}^n - \nabla(D)}$ be a solution to (4.6), and we will show that $\rho = 0$. Indeed, let $f = \sum_{\gamma \in \mathbb{N}^n - \nabla(D)} \rho_\gamma \cdot (\prod_{k=1}^n x_k{}^{\gamma_k})$. For any $(v, \alpha) \in G$, by Lemma 2.2 and $\text{supp}(f) \subseteq \mathbb{N}^n - \nabla(D)$, we have

$$f(x_1 + v_1, \ldots, x_n + v_n)_{[\alpha]} = \sum_{\gamma \in \mathbb{N}^n - \nabla(D)} W((v, \alpha), \gamma) \cdot \rho_\gamma = 0.$$

It follows that $f \in Q \cap \delta(\mathbb{N}^n - \nabla(D)) = \{0\}$, which further implies that $\rho = 0$, as desired. Therefore (4.6) only has trivial solution. Hence an application of McCoy's theorem [14, Theorem 5.3] yields that $|\mathbb{N}^n - \nabla(D)| \leqslant |G|$, and hence $\zeta_2 \leqslant \zeta_1$, as desired. Now, assume in addition that $\zeta_1 = \zeta_2$. Then, we have $|G| = |\mathbb{N}^n - \nabla(D)|$, and (4.6) only has trivial solution. It again follows from [14, Theorem 5.3] that (4.5) holds true, as desired. $\qquad\square$

Now we present some necessary and sufficient conditions for $(g(\lambda) \mid \lambda \in \Lambda)$ to be a Gröbner basis of Q.

Theorem 4.1. (1) *Suppose that for any $i \in [1, n]$, S_i satisfies Condition (D) in R. Then, it holds that $\zeta_1 \leqslant \zeta_2$. Moreover, $(g(\lambda) \mid \lambda \in \Lambda)$ is a Gröbner basis of Q if and only if $\zeta_1 = \zeta_2$.*

(2) *Suppose that $\prod_{i=1}^n S_i \neq \emptyset$, $\mathbf{0} \notin B_a$ for all $a \in \prod_{i=1}^n S_i$, $\zeta_1 \leqslant \zeta_2$, and $(g(\lambda) \mid \lambda \in \Lambda)$ is a Gröbner basis of Q. Then, it holds that $\zeta_1 = \zeta_2$, and for any $k \in [1, n]$, S_k satisfies Condition (D) in R.*

Proof. **(1)** Let $E = \{c \in R \mid c \text{ is not a zero divisor of } R\}$, and let T denote the ring of fractions of R with respect to E (see [6, Chapter 3]). Moreover, let $\Omega_1 \triangleq T[x_1, \ldots, x_n]$ denote the polynomial ring over T in n variables $x_1, \ldots, x_n$. For any $h \in \Omega_1$, we let $\text{supp}_1(h) = \{\alpha \in \mathbb{N}^n \mid h_{[\alpha]} \neq 0\}$, where for any $\alpha \in \mathbb{N}^n$, $h_{[\alpha]}$ denotes the coefficient of $\prod_{i=1}^n x_i{}^{\alpha_i}$ in h.

The following two facts are straightforward to verify.

Fact 1. $\varphi : R \longrightarrow T$ defined as $\varphi(a) = a/1_R$ is injective.

Fact 2. Let $X \subseteq R$ such that X satisfies Condition (D) in R, and let $Y = \{b/1_R \mid b \in X\}$. Then, for any $y_1, y_2 \in Y$ with $y_1 \neq y_2$, $y_2 - y_1$ is a multiplicative unit of T, that is to say, Y satisfies Condition (F) in T.

Based on Fact 1, we define $(P_1, \ldots, P_n)$, $(L_e \mid e \in \prod_{i=1}^n P_i)$ and Q_1 as follows:

$$\forall\, k \in [1, n] : P_k = \{u/1_R \mid u \in S_k\},$$

$$\forall\, a \in \prod_{i=1}^{n} S_i : L_{(a_1/1_R, \ldots, a_n/1_R)} = B_a; \tag{4.7}$$

$Q_1 \triangleq \{\eta \in \Omega_1 \mid \mathrm{supp}_1(\eta(x_1 + e_1, \ldots, x_n + e_n)) \subseteq \nabla(L_e) \text{ for all } e \in \prod_{i=1}^{n} P_i\}$.
By Fact 2, for any $k \in [1, n]$, P_k is a finite subset of T, and P_k satisfies
Condition (F) in T. By (4.7), for any $e \in \prod_{i=1}^{n} P_i$, it holds that $L_e \subseteq \mathbb{N}^n$,
$\mathbb{N}^n - \nabla(L_e)$ is finite. Moreover, it holds that

$$\sum_{e \in \prod_{i=1}^{n} P_i} |\mathbb{N}^n - \nabla(L_e)| = \sum_{a \in \prod_{i=1}^{n} S_i} |\mathbb{N}^n - \nabla(B_a)| = \zeta_1. \tag{4.8}$$

We also note that Q_1 is an ideal of Ω_1. Now define $(h(\lambda) \mid \lambda \in \Lambda) \in \Omega_1{}^{\Lambda}$ as

$$\forall\, \lambda \in \Lambda : h(\lambda)_{[\alpha]} = g(\lambda)_{[\alpha]}/1_R \text{ for all } \alpha \in \mathbb{N}^n.$$

Consider an arbitrary $\mu \in \Lambda$. From Fact 1, we deduce that $\mathrm{supp}_1(h(\mu)) =$
$\mathrm{supp}(g(\mu))$, $\theta(\mu)$ is the greatest element of $\mathrm{supp}_1(h(\mu))$, $h(\mu)_{[\theta(\mu)]} = 1_T$.
Moreover, $g(\mu) \in Q$ implies that $h(\mu) \in Q_1$. Now with (4.8), an application
of (1) of Lemma 4.2 to T and Ω_1 implies that $\zeta_1 \leqslant \zeta_2$, as desired.

Next, we prove the "moreover" assertion. Note that the "only if" part
follows from (2) of Lemma 4.2 and the proven fact that $\zeta_1 \leqslant \zeta_2$, it remains
to prove the "if" part. To this end, suppose that $\zeta_1 = \zeta_2$. Then, with (4.8),
an application of (1) of Lemma 4.2 to T and Ω_1 implies that in Ω_1, $(h(\lambda) \mid$
$\lambda \in \Lambda)$ is a Gröbner basis of Q_1. Now consider an arbitrary $\tau \in Q - \{0\}$.
Let $\eta \in \Omega_1$ be defined as $\eta_{[\alpha]} = \tau_{[\alpha]}/1_R$ for all $\alpha \in \mathbb{N}^n$. By Fact 1, we have
$\mathrm{supp}(\tau) = \mathrm{supp}_1(\eta)$. In particular, $\eta \neq 0$. Moreover, $\tau \in Q$ implies that
$\eta \in Q_1$. Since $(h(\lambda) \mid \lambda \in \Lambda)$ is a Gröbner basis of Q_1, by Definition 2.3,
we can choose $\alpha \in \mathrm{supp}_1(\eta)$ and $r \in \Lambda$ with $\theta(r) \leqslant \alpha$. Hence we have
$\alpha \in \mathrm{supp}(\tau)$, $r \in \Lambda$, $\theta(r) \leqslant \alpha$. It then follows from Definition 2.3 that
$(g(\lambda) \mid \lambda \in \Lambda)$ is a Gröbner basis of Q, as desired.

(2) Let $G = \bigcup_{a \in \prod_{i=1}^{n} S_i} \{a\} \times (\mathbb{N}^n - \nabla(B_a))$. First, it follows from (2) of
Lemma 4.2 that $\zeta_1 = \zeta_2$, as desired. Next, for any $a \in \prod_{i=1}^{n} S_i$, by $\mathbf{0} \notin B_a$,
we have $(a, \mathbf{0}) \in G$. Now let $k \in [1, n]$, and we will show that S_k satisfies
Condition (D) in R. Indeed, let $c, d \in S_k$ with $c \neq d$. Since $\prod_{i=1}^{n} S_i \neq \emptyset$,
we can choose $y, w \in \prod_{i=1}^{n} S_i$ such that $y_k = c$, $w_k = d$, and $y_j = w_j$ for all
$j \in [1, n] - \{k\}$. Consider an arbitrary $b \in R$ with $b \cdot (d - c) = 0$. Then, we
can choose $\sigma \in R^G$ such that $\sigma_{(y, \mathbf{0})} = -b$, $\sigma_{(w, \mathbf{0})} = b$, and $\sigma_{(a, \beta)} = 0$ for all
$(a, \beta) \in G - \{(y, \mathbf{0}), (w, \mathbf{0})\}$. Let $\gamma \in \mathbb{N}^n$ be arbitrary. By $b \cdot (d - c) = 0$, we
have $b \cdot (d^{\gamma_k} - c^{\gamma_k}) = 0$, which, together with (2.11) and the definitions of
σ, y, w, further implies that

$$\sum_{(v, \alpha) \in G} \sigma_{(v, \alpha)} \cdot \Phi((v, \alpha), \gamma) = b \cdot (\Phi((w, \mathbf{0}), \gamma) - \Phi((y, \mathbf{0}), \gamma))$$
$$= b \cdot (d^{\gamma_k} - c^{\gamma_k}) \cdot (\textstyle\prod_{i \in [1, n] - \{k\}} w_i{}^{\gamma_i})$$
$$= 0.$$

It then follows from (2) of Lemma 4.2 that $\sigma = 0$, which further implies that $b = \sigma_{(w,\mathbf{0})} = 0$. Therefore $d - c$ is not a zero divisor of R. Hence from Definition 2.2, we deduce that S_k satisfies Condition (D) in R, as desired. $\square$

Now we are ready to present the most general Nullstellensatz of this paper. The following theorem, which immediately follows from Theorems 3.1 and 4.1, will be used in Section 5 to derive several more explicit Nullstellensatz.

Theorem 4.2. *Suppose that $\zeta_1 = \zeta_2$, and for any $i \in [1, n]$, S_i satisfies Condition (D) in R. Consider an arbitrary $f \in Q$. Then, there exists $(p(\lambda) \mid \lambda \in \Lambda) \in \Omega^\Lambda$ such that $f = \sum_{\lambda \in \Lambda} p(\lambda) \cdot g(\lambda)$ and*

$$\forall \, \lambda \in \Lambda : \operatorname{supp}(p(\lambda)) + \operatorname{supp}(g(\lambda)) \subseteq \Delta(\operatorname{supp}(f)).$$

Moreover, for any $\beta \in \max(\operatorname{supp}(f))$, there exists $\lambda \in \Lambda$ with $\theta(\lambda) \leqslant \beta$.

Remark 4.1. *Theorem 4.1 implies that with some additional assumptions, Condition (D) is a necessary and sufficient condition for $(g(\lambda) \mid \lambda \in \Lambda)$ to be a Gröbner basis of Q. In fact, in Theorem 4.1, the assumption that all the $g(\lambda)$'s are monic can be weakened to that all the $g(\lambda)$'s have leading coefficient 1_R with respect to some fixed monomial order. Therefore Theorem 4.1 holds true in a more general setting. By contrast, our Nullstellensatz Theorem 4.2 relies heavily on the fact that all the $g(\lambda)$'s are monic.*

5   Some corollaries of Theorems 4.1 and 4.2

In this section, we will use Theorems 4.1 and 4.2 to derive several Nullstellensatz.

5.1   An extension of Mezei's Nullstellensatz

In [29, Theorem 6.12], Mezei establishes a general Nullstellensatz which includes both the Nullstellensatz for multisets in [24] and the Nullstellensatz with multiplicity in [9] as special cases. In this subsection, we further extend Mezei's result. Our extension will be an immediate corollary of Theorems 4.1 and 4.2.

Let $S_1, \ldots, S_n$ be finite subsets of R, Λ be a finite set, and let

$$(\varepsilon(i, u, \lambda) \mid i \in [1, n], u \in S_i, \lambda \in \Lambda)$$

be a tuple of natural numbers. Define $(g(\lambda) \mid \lambda \in \Lambda)$, $(\theta(\lambda) \mid \lambda \in \Lambda)$, D and $(B_a \mid a \in \prod_{i=1}^n S_i)$ as follows:

$$\forall \, \lambda \in \Lambda : g(\lambda) = \prod_{i=1}^n \prod_{u \in S_i} (x_i - u)^{\varepsilon(i,u,\lambda)} \in \Omega, \qquad (5.1)$$

$$\forall \, \lambda \in \Lambda : \theta(\lambda) = (\textstyle\sum_{u \in S_1} \varepsilon(1,u,\lambda), \ldots, \sum_{u \in S_n} \varepsilon(n,u,\lambda)) \in \mathbb{N}^n, \qquad (5.2)$$

$$D \triangleq \{\theta(\lambda) \mid \lambda \in \Lambda\} \subseteq \mathbb{N}^n, \qquad (5.3)$$

$$\forall \, a \in \textstyle\prod_{i=1}^n S_i : B_a \triangleq \{(\varepsilon(1,a_1,\lambda), \ldots, \varepsilon(n,a_n,\lambda)) \mid \lambda \in \Lambda\} \subseteq \mathbb{N}^n, \qquad (5.4)$$

and moreover, let Q denote the following ideal of Ω:

$$\{f \in \Omega \mid \forall \, a \in \textstyle\prod_{i=1}^n S_i : \mathrm{supp}\,(f(x_1 + a_1, \ldots, x_n + a_n)) \subseteq \nabla(B_a)\}. \qquad (5.5)$$

We assume in addition that $\mathbb{N}^n - \nabla(D)$ is finite, and let

$$\zeta_2 \triangleq |\mathbb{N}^n - \nabla(D)|.$$

By Lemma 2.3, one can check that for any $a \in \prod_{i=1}^n S_i$, $\mathbb{N}^n - \nabla(B_a)$ is finite. As in Section 4, we let

$$\zeta_1 \triangleq \textstyle\sum_{a \in \prod_{i=1}^n S_i} |\mathbb{N}^n - \nabla(B_a)|.$$

Via some straightforward verification, we deduce that $(g(\lambda) \mid \lambda \in \Lambda)$ is a family of monic polynomials with $\{g(\lambda) \mid \lambda \in \Lambda\} \subseteq Q$; moreover, for any $\lambda \in \Lambda$, $\theta(\lambda)$ is the greatest element of $\mathrm{supp}\,(g(\lambda))$.

Lemma 5.1. *It holds that $\zeta_1 \leqslant \zeta_2$.*

Proof. First, for the special case that all the S_i's satisfy Condition (F) in R, the desired result is an immediate corollary of (1) of Lemma 4.2.

Next, we consider the general case. To this end, let $P_1, \ldots, P_n$ be finite subsets of $\mathbb{C}$ with $|P_i| = |S_i|$ for all $i \in [1,n]$. For any $i \in [1,n]$, fix a bijective map $\omega_i : P_i \longrightarrow S_i$. Define a tuple $(\sigma(i,v,\lambda) \mid i \in [1,n], v \in P_i, \lambda \in \Lambda)$ as $\sigma(i,v,\lambda) = \varepsilon(i, \omega_i(v), \lambda)$. It can be readily verified that

$$\forall \, \lambda \in \Lambda : (\textstyle\sum_{v \in P_1} \sigma(1,v,\lambda), \ldots, \sum_{v \in P_n} \sigma(n,v,\lambda)) = \theta(\lambda),$$

$$\forall \, d \in \textstyle\prod_{i=1}^n P_i : \{(\sigma(1,d_1,\lambda), \ldots, \sigma(n,d_n,\lambda)) \mid \lambda \in \Lambda\} = B_{(\omega_1(d_1),\ldots,\omega_n(d_n))}.$$

Since $\mathbb{C}$ is a field, for any $i \in [1,n]$, P_i satisfies Condition (F) in $\mathbb{C}$. It then follows from the previous paragraph that

$$\zeta_1 = \textstyle\sum_{d \in \prod_{i=1}^n P_i} |\mathbb{N}^n - \nabla(B_{(\omega_1(d_1),\ldots,\omega_n(d_n))})| \leqslant |\mathbb{N}^n - \nabla(D)| = \zeta_2,$$

as desired. $\qquad\square$

Now we are ready to prove the main result of this subsection.

Theorem 5.1. (1) *Suppose that $\zeta_1 = \zeta_2$, and for any $k \in [1, n]$, S_k satisfies Condition (D) in R. Then, $(g(\lambda) \mid \lambda \in \Lambda)$ is a Gröbner basis of Q. Further consider an arbitrary $f \in Q$. Then, there exists $(p(\lambda) \mid \lambda \in \Lambda) \in \Omega^{\Lambda}$ such that $f = \sum_{\lambda \in \Lambda} p(\lambda) \cdot g(\lambda)$ and*

$$\forall \, \lambda \in \Lambda : \mathrm{supp}\,(p(\lambda)) + \mathrm{supp}\,(g(\lambda)) \subseteq \Delta(\mathrm{supp}\,(f)). \tag{5.6}$$

Moreover, for an arbitrary $\beta \in \max(\mathrm{supp}\,(f))$, there exists $\lambda \in \Lambda$ such that $\sum_{u \in S_k} \varepsilon(k, u, \lambda) \leqslant \beta_k$ for all $k \in [1, n]$.

(2) *Suppose that $\prod_{i=1}^{n} S_i \neq \emptyset$, and $\mathbf{0} \notin B_a$ for all $a \in \prod_{i=1}^{n} S_i$. Then, $(g(\lambda) \mid \lambda \in \Lambda)$ is a Gröbner basis of Q if and only if $\zeta_1 = \zeta_2$, and for any $k \in [1, n]$, S_k satisfies Condition (D) in R.*

Proof. We note that (1) follows from (1) of Theorem 4.1, Theorem 4.2 and (5.2), and (2) follows from Lemma 5.1 and Theorem 4.1. □

Remark 5.1. *In [29, Theorem 6.12], Mezei derives a Nullstellensatz by giving a sufficient condition for $\zeta_1 = \zeta_2$ to hold true (see [26, Lemma 6.11]). Therefore (1) of Theorem 5.1 extends Mezei's result from polynomials over a field to polynomials over a commutative ring; and from the conclusions of the form similar to (5) of Theorem 3.1 to the conclusions of the form similar to (3), (4) of Theorem 3.1; and to more general $g(\lambda)$'s. By contrast, we do not present explicit sufficient conditions for $\zeta_1 = \zeta_2$ to hold true.*

5.2 A common generalization of the Nullstellensatz in [23, 24] and [9]

In this subsection, we give a common generalization of the Nullstellensatz for multisets established in Kós, Rónyai and Mészáros [23, 24] and the Nullstellensatz with multiplicity established in Ball and Serra [9].

Notation 5.1. *Let $(g_1, \ldots, g_n) \in \Omega^n$ be a family of monic polynomials such that $g_k \in R[x_k]$ for all $k \in [1, n]$. Then, for any $t \in \mathbb{N}$, we let*

$$\mathcal{I}_t(g_1, \ldots, g_n) = \langle \{ \textstyle\prod_{k=1}^{n} g_k^{\alpha_k} \mid \alpha \in \mathbb{N}^n, \sum_{i=1}^{n} \alpha_i = t \} \rangle. \tag{5.7}$$

We collect some basic properties in the following proposition.

Proposition 5.1. *Let $(g_1, \ldots, g_n) \in \Omega^n$ be a family of monic polynomials such that $g_k \in R[x_k]$ for all $k \in [1, n]$. Also fix $t \in \mathbb{N}$. Then, the following two statements hold:*

(1) *$(\prod_{k=1}^{n} g_k{}^{\alpha_k} \mid \alpha \in \mathbb{N}^n, \sum_{i=1}^{n} \alpha_i = t)$ is a Gröbner basis of $\mathcal{I}_t(g_1, \ldots, g_n)$;*

(2) *Let $f \in \Omega$. Then, there uniquely exists $\psi \in \Omega$ such that $f - \psi \in \mathcal{I}_t(g_1, \ldots, g_n)$, and for any $\beta \in \mathrm{supp}\,(\psi)$ and $\alpha \in \mathbb{N}^n$ with $\sum_{i=1}^{n} \alpha_i = t$, there exists $s \in [1, n]$ with $\beta_s \leqslant \deg(g_s)\alpha_s - 1$. Moreover, such a ψ satisfies that $\mathrm{supp}\,(\psi) \subseteq \Delta(\mathrm{supp}\,(f))$.*

Proof. We note that (1) follows from Example 2.1, and so we only prove (2). To this end, let

$$D = \{(\deg(g_1)\alpha_1, \ldots, \deg(g_n)\alpha_n) \mid \alpha \in \mathbb{N}^n, \textstyle\sum_{i=1}^{n} \alpha_i = t\}.$$

From Example 2.1, Lemma 3.1, (1) and Theorem 3.1, we deduce that Ω is the direct sum of $\mathcal{I}_t(g_1, \ldots, g_n)$ and $\delta(\mathbb{N}^n - \nabla(D))$, which further implies the existence and uniqueness of ψ. Moreover, it follows from Lemma 3.1 that $\mathrm{supp}\,(\psi) \subseteq \Delta(\mathrm{supp}\,(f))$, as desired. $\qquad\square$

Now we state and prove the main result of this subsection. To this end, for any $k \in [1, n]$, we let S_k be a finite subset of R, and let (S_k, ψ_k) be a multiset. Define $(g_1, \ldots, g_n)$ as

$$\forall\, k \in [1, n] : g_k = \prod_{u \in S_k} (x_k - u)^{\psi_k(u)}. \tag{5.8}$$

Theorem 5.2. (1) *Suppose that for any $k \in [1, n]$, S_k satisfies Condition (D) in R. Fix $t \in \mathbb{N}$. Consider an arbitrary $f \in \Omega$. Then, $f \in \mathcal{I}_t(g_1, \ldots, g_n)$ if and only if for any $a \in \prod_{i=1}^{n} S_i$ and $\beta \in \mathbb{N}^n$ with $\sum_{i=1}^{n} \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t - 1$, it holds that $f(x_1 + a_1, \ldots, x_n + a_n)_{[\beta]} = 0$.*

(2) *Suppose that for any $k \in [1, n]$, S_k satisfies Condition (D) in R. Fix $t \in \mathbb{N}$. Let $f \in \Omega$ such that for any $a \in \prod_{i=1}^{n} S_i$ and $\beta \in \mathbb{N}^n$ with $\sum_{i=1}^{n} \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t - 1$, it holds that $f(x_1 + a_1, \ldots, x_n + a_n)_{[\beta]} = 0$. Then, there exists polynomials $(p(\alpha) \mid \alpha \in \mathbb{N}^n, \sum_{i=1}^{n} \alpha_i = t)$ such that*

$$f = \sum_{(\alpha \in \mathbb{N}^n, \sum_{i=1}^{n} \alpha_i = t)} p(\alpha) \cdot (\textstyle\prod_{k=1}^{n} g_k{}^{\alpha_k}),$$

and for any $\alpha \in \mathbb{N}^n$ with $\sum_{i=1}^{n} \alpha_i = t$, it holds that

$$\mathrm{supp}\,(p(\alpha)) + \mathrm{supp}\,(\textstyle\prod_{k=1}^{n} g_k{}^{\alpha_k}) \subseteq \Delta(\mathrm{supp}\,(f)).$$

19

Moreover, for any $\beta \in \max(\text{supp}\,(f))$, there exists $\gamma \in \mathbb{N}^n$, $\sum_{i=1}^n \gamma_i = t$ such that $(\sum_{u \in S_k} \psi_k(u)) \cdot \gamma_k \leqslant \beta_k$ for all $k \in [1, n]$.

(3) *Suppose that $\prod_{i=1}^n S_i \neq \emptyset$. Let $t \in \mathbb{Z}^+$. Further assume that for an arbitrary $f \in \Omega$ such that $f(x_1 + a_1, \ldots, x_n + a_n)_{[\beta]} = 0$ for all $a \in \prod_{i=1}^n S_i$ and $\beta \in \mathbb{N}^n$ with $\sum_{i=1}^n \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t - 1$, it holds that $f \in \mathcal{I}_t(g_1, \ldots, g_n)$. Then, for any $k \in [1, n]$, S_k satisfies Condition (D) in R.*

Proof. Throughout the proof, we fix $t \in \mathbb{N}$, and let

$$\Lambda = \{\theta \in \mathbb{N}^n \mid \textstyle\sum_{i=1}^n \theta_i = t\}.$$

Consider the tuple $(\psi_i(u)\theta_i \mid i \in [1, n], u \in S_i, \theta \in \Lambda)$. Then, we have

$$\forall\, \theta \in \Lambda : \prod_{i=1}^n \prod_{u \in S_i} (x_i - u)^{\psi_i(u)\theta_i} = \prod_{k=1}^n g_k{}^{\theta_k}. \tag{5.9}$$

Now we define D, $(B_a \mid a \in \prod_{i=1}^n S_i)$ and Q as follows:

$$D = \{((\textstyle\sum_{u \in S_1} \psi_1(u))\theta_1, \ldots, (\textstyle\sum_{u \in S_n} \psi_n(u))\theta_n) \mid \theta \in \Lambda\},$$

$$\forall\, a \in \prod_{i=1}^n S_i : B_a = \{(\psi_1(a_1)\theta_1, \ldots, \psi_n(a_n)\theta_n) \mid \theta \in \Lambda\},$$

$$Q = \{f \in \Omega \mid \forall\, a \in \textstyle\prod_{i=1}^n S_i : \text{supp}\,(f(x_1 + a_1, \ldots, x_n + a_n)) \subseteq \nabla(B_a)\}.$$

By Lemma 2.5, $\mathbb{N}^n - \nabla(D)$ is finite. From Section 5.1 and (5.9), we deduce that Q is an ideal of Ω with $\mathcal{I}_t(g_1, \ldots, g_n) \subseteq Q$. Moreover, for an arbitrary $f \in \Omega$, by Lemma 2.5, one can check that $f \in Q$ if and only if for any $a \in \prod_{i=1}^n S_i$ and $\beta \in \mathbb{N}^n$ with $\sum_{i=1}^n \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t - 1$, it holds that

$$f(x_1 + a_1, \ldots, x_n + a_n)_{[\beta]} = 0.$$

(1) and **(2)** By Lemma 2.5, we have

$$\begin{aligned}
\sum_{a \in \prod_{i=1}^n S_i} |\mathbb{N}^n - \nabla(B_a)| &= \sum_{a \in \prod_{i=1}^n S_i} \left(\prod_{i=1}^n \psi_i(a_i)\right) \binom{n+t-1}{n} \\
&= \left(\prod_{i=1}^n (\textstyle\sum_{u \in S_i} \psi_i(u))\right) \binom{n+t-1}{n} \\
&= |\mathbb{N}^n - \nabla(D)|.
\end{aligned}$$

Hence by (1) of Theorem 5.1 and (5.9), $(\prod_{k=1}^n g_k{}^{\theta_k} \mid \theta \in \Lambda)$ is a Gröbner basis of Q. It then follows from Theorem 3.1 that $Q = \mathcal{I}_t(g_1, \ldots, g_n)$, which further establishes (1). Moreover, (2) again follows from (1) of Theorem 5.1.

(3) Assume that $t \in \mathbb{Z}^+$ and $\prod_{i=1}^n S_i \neq \emptyset$. Then, one can check that $\mathbf{0} \notin B_a$ for all $a \in \prod_{i=1}^n S_i$. Moreover, we note that $Q = \mathcal{I}_t(g_1, \ldots, g_n)$. It then follows from (1) of Proposition 5.1 that $(\prod_{k=1}^n g_k{}^{\theta_k} \mid \theta \in \Lambda)$ is a Gröbner basis of Q. Hence an application of (2) of Theorem 5.1 completes the proof. $\qquad\square$

We note that by Theorem 5.2, Condition (D) is a necessary and sufficient condition for our Nullstellensatz to hold true under the relatively mild assumptions that $t \geqslant 1$ and $\prod_{i=1}^{n} S_i \neq \emptyset$. In the following remark, we show how Theorem 5.2 recovers some known results in the literature.

Remark 5.2. *First, if R is a field and $\psi_i(u) = 1$ for all $i \in [1, n]$ and $u \in S_i$, then (2) of Theorem 5.2 recovers the Nullstellensatz with multiplicity [9, Theorem 3.1], and enhances [9, Corollary 3.2]; if $t = 1$, then (2) of Theorem 5.2 enhances [23, Theorem 4], which further recovers [24, Theorem 6] when R is a field; moreover, if R is a field and $t = 1$, then (2) of Theorem 5.2, together with (2) of Proposition 5.1, recovers the Nullstellensatz for multisets [24, Theorem 1].*

Second, if $t = 1$ and $\psi_i(u) = 1$ for all $i \in [1, n]$ and $u \in S_i$, then Theorem 5.2 recovers the Chevalley-Alon-Tarsi-Schauz Lemma (see, [34, Equivalence and Definition 2.8], [12, Theorem 2.5], [17, Theorem 3.3], [18, Theorem 2.3]) and [17, Theorem 3.8]. Both of these two results have shown that Alon's combinatorial Nullstellensatz Theorem 1.1 remains valid with the field $\mathbb{F}$ replaced by R if and only if all the S_i's satisfy Condition (D) in R.

5.3 Punctured Nullstellensatz

In this subsection, we give a common generalization of the punctured Nullstellensatz established in Ball and Serra [9], and in Kós, Rónyai and Mészáros [24]. We begin with the following proposition, which is inspired by [9, Theorem 4.1] and [24, Theorem 7].

Proposition 5.2. *Let $(g_1, \ldots, g_n) \in \Omega^n$, $(h_1, \ldots, h_n) \in \Omega^n$ satisfy that $g_k, h_k \in R[x_k]$, g_k, h_k are monic, $h_k \mid g_k$ for all $k \in [1, n]$. Let $t \in \mathbb{N}$, and fix $f \in \bigcap_{m=1}^{n} \mathcal{I}_t(g_1, \ldots, g_{m-1}, g_m/h_m, g_{m+1}, \ldots, g_n)$. Moreover, let $\psi \in \Omega$ such that $f - \psi \in \mathcal{I}_t(g_1, \ldots, g_n)$, and for any $\beta \in \mathrm{supp}\,(\psi)$ and $\alpha \in \mathbb{N}^n$ with $\sum_{i=1}^{n} \alpha_i = t$, there exists $s \in [1, n]$ with $\beta_s \leqslant \deg(g_s)\alpha_s - 1$. Then, the following three statements hold:*

(1) $\psi \in \bigcap_{m=1}^{n} \mathcal{I}_t(g_1, \ldots, g_{m-1}, g_m/h_m, g_{m+1}, \ldots, g_n)$;

(2) $(\prod_{k=1}^{n} \frac{g_k}{h_k}) \mid \psi$;

(3) Suppose that $t \in \mathbb{Z}^+$. Let $\varphi \in \Omega$ with $\psi = \varphi \cdot (\prod_{k=1}^{n} \frac{g_k}{h_k})$, and let $(u_1, \ldots, u_n) \in R^n$ such that $g_k(u_1, \ldots, u_n) = 0$ for all $k \in [1, n]$. Moreover, fix $m \in [1, n]$, and let $a = \prod_{k \in [1,n]-\{m\}} (g_k/h_k)(u_1, \ldots, u_n)$. Then, we have

$$(g_m/h_m)^{t-1} \mid a \cdot \varphi(u_1, \ldots, u_{m-1}, x_m, u_{m+1}, \ldots, u_n). \qquad (5.10)$$

Assume in addition that $f(u_1, \ldots, u_n) \neq 0$, and $(g_k/h_k)(u_1, \ldots, u_n)$ is not a zero divisor of R for any $k \in [1, n]$. Then, it holds that

$$\deg(f) \geqslant \deg(\psi) \geqslant (t-1)\deg(g_m/h_m) + (\textstyle\sum_{k=1}^n \deg(g_k/h_k)). \qquad (5.11)$$

Proof. Throughout the proof, we let $\Lambda = \{\alpha \in \mathbb{N}^n \mid \sum_{i=1}^n \alpha_i = t\}$.

(1) This follows from the fact that

$$\mathcal{I}_t(g_1, \ldots, g_n) \subseteq \bigcap_{m=1}^n \mathcal{I}_t(g_1, \ldots, g_{m-1}, g_m/h_m, g_{m+1}, \ldots, g_n).$$

(2) Let $m \in [1, n]$, and let $(\zeta_1, \ldots, \zeta_n) = (g_1, \ldots, g_{m-1}, g_m/h_m, g_{m+1}, \ldots, g_n)$. By (1), (1) of Proposition 5.1 and Theorem 3.1, we can choose polynomials $(p(\alpha) \mid \alpha \in \Lambda)$ satisfying the following two conditions:

$$\psi = \textstyle\sum_{\alpha \in \Lambda} p(\alpha) \cdot (\prod_{k=1}^n \zeta_k^{\alpha_k}), \qquad (5.12)$$

$$\forall\, \alpha \in \Lambda : \mathrm{supp}\,(p(\alpha)) + \mathrm{supp}\,(\textstyle\prod_{k=1}^n \zeta_k^{\alpha_k}) \subseteq \Delta(\mathrm{supp}\,(\psi)). \qquad (5.13)$$

Consider an arbitrary $\alpha \in \Lambda$ with $p(\alpha) \neq 0$. By (5.13), we can choose $\beta \in \mathrm{supp}\,(\psi)$ with $(\deg(\zeta_1)\alpha_1, \ldots, \deg(\zeta_n)\alpha_n) \leqslant \beta$. Now we further choose $s \in [1, n]$ with $\beta_s \leqslant \deg(g_s)\alpha_s - 1$. It then follows that $\zeta_s \neq g_s$, and hence $s = m$, which further implies that $\alpha_m \geqslant 1$. It then follows from (5.12) that $(g_m/h_m) \mid \psi$. Now with the arbitrariness of m, (2) immediately follows from Lemma 2.4 and an induction argument.

(3) Let $(\zeta_1, \ldots, \zeta_n) = (g_1, \ldots, g_{m-1}, g_m/h_m, g_{m+1}, \ldots, g_n)$. By (1), we can choose polynomials $(p(\alpha) \mid \alpha \in \Lambda)$ satisfying (5.12). Let $\beta \in \mathbb{N}^n$ such that $\beta_m = t$ and $\beta_i = 0$ for all $i \in [1, n] - \{m\}$. Consider an arbitrary $\alpha \in \Lambda$ with $\alpha \neq \beta$. Then, there exists $s \in [1, n] - \{m\}$ with $\alpha_s \geqslant 1$. It follows that $g_s \mid (\prod_{k=1}^n \zeta_k^{\alpha_k})$. Since $g_s \in R[x_s]$, $s \neq m$, we have $g_s(u_1, \ldots, u_{m-1}, x_m, u_{m+1}, \ldots, u_n) = g_s(u_1, \ldots, u_n) = 0$, which further implies that $(\prod_{k=1}^n \zeta_k^{\alpha_k})(u_1, \ldots, u_{m-1}, x_m, u_{m+1}, \ldots, u_n) = 0$. Now set $\varpi \triangleq \psi(u_1, \ldots, u_{m-1}, x_m, u_{m+1}, \ldots, u_n)$. From the above discussion, we deduce that

$$\varpi = (p(\beta))(u_1, \ldots, u_{m-1}, x_m, u_{m+1}, \ldots, u_n) \cdot (g_m/h_m)^t.$$

On the other hand, it follows from $\psi = \varphi \cdot (\prod_{k=1}^n \frac{g_k}{h_k})$ that

$$\varpi = a \cdot \varphi(u_1, \ldots, u_{m-1}, x_m, u_{m+1}, \ldots, u_n) \cdot (g_m/h_m).$$

Combining the above two equations, (5.10) immediately follows from (4) of Lemma 2.1 and the fact that g_m/h_m is monic.

Now we prove (5.11). Noting that $(f - \psi)(u_1, \ldots, u_n) = 0$, we have $\psi(u_1, \ldots, u_n) = f(u_1, \ldots, u_n) \neq 0$. By $\varphi \mid \psi$, we have $\varphi(u_1, \ldots, u_n) \neq 0$, which, together with the fact that a is not a zero divisor of R, further implies that $a \cdot \varphi(u_1, \ldots, u_{m-1}, x_m, u_{m+1}, \ldots, u_n) \neq 0$. Noticing that $(g_m/h_m)^{t-1}$ is a monic polynomial with $\deg((g_m/h_m)^{t-1}) = (t-1)\deg(g_m/h_m)$, by (5.10) and (4) of Lemma 2.1, we have

$$(t-1)\deg(g_m/h_m) \leqslant \deg(a \cdot \varphi(u_1, \ldots, u_{m-1}, x_m, u_{m+1}, \ldots, u_n)) \leqslant \deg(\varphi).$$

Noticing that g_k/h_k is monic for all $k \in [1, n]$, by (4) of Lemma 2.1 and (2) of Proposition 5.1, we have

$$
\begin{aligned}
\deg(f) &\geqslant \deg(\psi) \\
&= \deg(\varphi) + \left(\sum_{k=1}^{n} \deg(g_k/h_k)\right) \\
&\geqslant (t-1)\deg(g_m/h_m) + \left(\sum_{k=1}^{n} \deg(g_k/h_k)\right),
\end{aligned}
$$

which further establishes (5.11), as desired. $\qquad\square$

Now we state and prove our punctured Nullstellensatz. Throughout the rest of this subsection, for any $k \in [1, n]$, we let S_k be a finite subset of R, (S_k, ψ_k) be a multiset, and fix $E_k \subseteq S_k$. Define $(g_1, \ldots, g_n)$ and $(h_1, \ldots, h_n)$ as follows:

$$\forall \, k \in [1, n] : g_k = \prod_{u \in S_k}(x_k - u)^{\psi_k(u)}, \; h_k = \prod_{u \in E_k}(x_k - u)^{\psi_k(u)}. \quad (5.14)$$

Theorem 5.3. *Suppose that for any $k \in [1, n]$, S_k satisfies Condition (D) in R. Let $t \in \mathbb{N}$, $f \in \Omega$. Then, it holds that:*

(1) $f \in \bigcap_{m=1}^{n} \mathcal{I}_t(g_1, \ldots, g_{m-1}, g_m/h_m, g_{m+1}, \ldots, g_n)$ *if and only if for any* $a \in (\prod_{i=1}^{n} S_i) - (\prod_{i=1}^{n} E_i)$ *and* $\beta \in \mathbb{N}^n$ *with* $\sum_{i=1}^{n} \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t - 1$, *it holds that* $f(x_1 + a_1, \ldots, x_n + a_n)_{[\beta]} = 0$;

(2) *Suppose that for any* $a \in (\prod_{i=1}^{n} S_i) - (\prod_{i=1}^{n} E_i)$ *and* $\beta \in \mathbb{N}^n$ *with* $\sum_{i=1}^{n} \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t - 1$, *it holds that*

$$f(x_1 + a_1, \ldots, x_n + a_n)_{[\beta]} = 0.$$

Then, there uniquely exists $\eta \in \Omega$ such that $f - \eta \in \mathcal{I}_t(g_1, \ldots, g_n)$, and for any $\beta \in \operatorname{supp}(\eta)$ and $\alpha \in \mathbb{N}^n$ with $\sum_{i=1}^{n} \alpha_i = t$, there exists $k \in [1, n]$ with $\beta_k \leqslant (\sum_{u \in S_k} \psi_k(u))\alpha_k - 1$. Moreover, we have $\operatorname{supp}(\eta) \subseteq \Delta(\operatorname{supp}(f))$, $(\prod_{k=1}^{n} \frac{g_k}{h_k}) \mid \eta$. Assume in addition that $t \geqslant 1$ and $f(w_1, \ldots, w_n) \neq 0$ for some $w \in \prod_{i=1}^{n} S_i$. Then, for any $m \in [1, n]$, it holds that

$$\deg(f) \geqslant \deg(\eta) \geqslant (t-1)(\sum_{u \in S_m - E_m} \psi_m(u)) + (\sum_{k=1}^{n} \sum_{u \in S_k - E_k} \psi_k(u)).$$

Proof. **(1)** First, let $m \in [1, n]$. Define $(P_1, \ldots, P_n)$ as $P_m = S_m - E_m$, and $P_k = S_k$ for all $k \in [1, n] - \{m\}$. Then, for any $k \in [1, n]$, P_k satisfies Condition (D) in R. An application of (1) of Theorem 5.2 to $(P_1, \psi_1), \ldots, (P_n, \psi_n)$ yields the following fact: $f \in \mathcal{I}_t(g_1, \ldots, g_{m-1}, g_m/h_m, g_{m+1}, \ldots, g_n)$ if and only if for any $a \in \prod_{i=1}^n P_i$ and $\beta \in \mathbb{N}^n$ with $\sum_{i=1}^n \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t - 1$, it holds that $f(x_1 + a_1, \ldots, x_n + a_n)_{[\beta]} = 0$. Now, with the above discussion, the desired result follows from the fact that

$$\left(\textstyle\prod_{i=1}^n S_i\right) - \left(\textstyle\prod_{i=1}^n E_i\right) = \textstyle\bigcup_{m=1}^n S_1 \times \cdots \times S_{m-1} \times (S_m - E_m) \times S_{m+1} \times \cdots \times S_n.$$

(2) By (1), $f \in \bigcap_{m=1}^n \mathcal{I}_t(g_1, \ldots, g_{m-1}, g_m/h_m, g_{m+1}, \ldots, g_n)$. Hence all the desired results except the last assertion follow from Propositions 5.1 and 5.2. Therefore in what follows, we assume that $t \geqslant 1$, and fix $w \in \prod_{i=1}^n S_i$ with $f(w_1, \ldots, w_n) \neq 0$. We note that $w \in \prod_{i=1}^n E_i$. Indeed, if $w \in (\prod_{i=1}^n S_i) - (\prod_{i=1}^n E_i)$, then by $\sum_{i=1}^n \left\lfloor \frac{\mathbf{0}_i}{\psi_i(w_i)} \right\rfloor = 0 \leqslant t - 1$, we have $f(w_1, \ldots, w_n) = f(x_1 + w_1, \ldots, x_n + w_n)_{[\mathbf{0}]} = 0$, a contradiction. For any $k \in [1, n]$, from $w_k \in E_k$ and S_k satisfies Condition (D) in R, one can check that $g_k(w_1, \ldots, w_n) = 0$, and $(g_k/h_k)(w_1, \ldots, w_n)$ is not a zero divisor of R. With these facts, the desired result follows from (3) of Proposition 5.2. $\qquad \square$

Remark 5.3. (1) *If $\prod_{i=1}^n E_i = \emptyset$, then (1) of Theorem 5.3 recovers (1) of Theorem 5.2.*

(2) *If R is a field and $\psi_i(u) = 1$ for all $i \in [1, n]$ and $u \in S_i$, then (2) of Theorem 5.3 recovers [9, Theorem 4.1]; if R is a field and $t = 1$, then (2) of Theorem 5.3 recovers [24, Theorem 7]; and if $t = 1$ and $\psi_i(u) = 1$ for all $i \in [1, n]$ and $u \in S_i$, then (2) of Theorem 5.3 recovers the punctured Nullstellensatz established in the proof of [18, Theorem 2.2].*

5.4 A generalization of [33, Theorem 1.5]

In this subsection, we use Theorems 4.1 and 4.2 to derive another Nullstellensatz. Our Nullstellensatz Theorem 5.4 is inspired by Sauermann and Wigderson [33], where the authors study the minimum possible degree of a polynomial that vanishes to high order on most of the hypercube $\{0, 1\}^n \subseteq \mathbb{R}^n$ (also see Clifton and Huang [19]). As an application of Theorem 5.4, we will derive a generalization of [33, Theorem 1.5].

For any $k \in [1, n]$, let S_k be a finite subset of R, (S_k, ψ_k) be a multiset, and fix $E_k \subseteq S_k$. Define $(g_1, \ldots, g_n)$ and $(h_1, \ldots, h_n)$ as follows:

$$\forall\, k \in [1, n]: g_k = \textstyle\prod_{u \in S_k}(x_k - u)^{\psi_k(u)}, \; h_k = \textstyle\prod_{u \in E_k}(x_k - u)^{\psi_k(u)}. \quad (5.15)$$

We fix $t \in \mathbb{Z}^+$, and let

$$\Lambda = \{\alpha \in \mathbb{N}^n \mid \textstyle\sum_{i=1}^n \alpha_i \in \{t-1, t\}\}. \tag{5.16}$$

Define $(\varphi(\alpha) \mid \alpha \in \Lambda) \in \Omega^\Lambda$ as follows:

$$\forall\ \alpha \in \mathbb{N}^n\ s.t.\ \textstyle\sum_{i=1}^n \alpha_i = t : \varphi(\alpha) = \prod_{i=1}^n g_i{}^{\alpha_i}, \tag{5.17}$$

$$\forall\ \alpha \in \mathbb{N}^n\ s.t.\ \textstyle\sum_{i=1}^n \alpha_i = t-1 : \varphi(\alpha) = (\prod_{i=1}^n g_i{}^{\alpha_i}) \cdot (\prod_{i=1}^n \frac{g_i}{h_i}). \tag{5.18}$$

Moreover, let $Q \subseteq \Omega$ such that for any $f \in \Omega$, $f \in Q$ if and only if the following two conditions hold:

(i) For any $a \in (\prod_{i=1}^n S_i) - (\prod_{i=1}^n E_i)$ and $\beta \in \mathbb{N}^n$ with $\sum_{i=1}^n \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t-1$, it holds that $f(x_1 + a_1, \ldots, x_n + a_n)_{[\beta]} = 0$;

(ii) For any $a \in \prod_{i=1}^n E_i$ and $\beta \in \mathbb{N}^n$ with $\sum_{i=1}^n \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t-2$, it holds that $f(x_1 + a_1, \ldots, x_n + a_n)_{[\beta]} = 0$.

Theorem 5.4. (1) Q *is an ideal of* Ω, *and* $(\varphi(\alpha) \mid \alpha \in \Lambda)$ *is a family of monic polynomials with* $\{\varphi(\alpha) \mid \alpha \in \Lambda\} \subseteq Q$.

(2) *Suppose that for any* $k \in [1, n]$, S_k *satisfies Condition (D) in R. Then,* $(\varphi(\alpha) \mid \alpha \in \Lambda)$ *is a Gröbner basis of* Q. *Moreover, for an arbitrary* $f \in Q$, *there exists* $(p(\alpha) \mid \alpha \in \Lambda) \in \Omega^\Lambda$ *such that* $f = \sum_{\alpha \in \Lambda} p(\alpha) \cdot \varphi(\alpha)$ *and*

$$\forall\ \alpha \in \Lambda : \operatorname{supp}(p(\alpha)) + \operatorname{supp}(\varphi(\alpha)) \subseteq \Delta(\operatorname{supp}(f)).$$

(3) *Suppose that* $\prod_{i=1}^n S_i \neq \emptyset$, $t \geqslant 2$, $(\varphi(\alpha) \mid \alpha \in \Lambda)$ *is a Gröbner basis of* Q. *Then, for any* $k \in [1, n]$, S_k *satisfies Condition (D) in R.*

Proof. Since (1) follows from some straightforward verification, in what follows, we only prove (2) and (3). For any $a \in (\prod_{i=1}^n S_i) - (\prod_{i=1}^n E_i)$, set

$$B_a \triangleq \{(\psi_1(a_1)\gamma_1, \ldots, \psi_n(a_n)\gamma_n) \mid \gamma \in \mathbb{N}^n, \textstyle\sum_{i=1}^n \gamma_i = t\},$$

and for any $a \in \prod_{i=1}^n E_i$, set

$$B_a \triangleq \{(\psi_1(a_1)\gamma_1, \ldots, \psi_n(a_n)\gamma_n) \mid \gamma \in \mathbb{N}^n, \textstyle\sum_{i=1}^n \gamma_i = t-1\}.$$

By Lemma 2.5, for any $a \in \prod_{i=1}^n S_i$, $\mathbb{N}^n - \nabla(B_a)$ is finite. Moreover, Lemma 2.5 implies that

$$Q = \{f \in \Omega \mid \forall\ a \in \textstyle\prod_{i=1}^n S_i : \operatorname{supp}(f(x_1 + a_1, \ldots, x_n + a_n)) \subseteq \nabla(B_a)\}.$$

25

Again by Lemma 2.5, we have

$$\sum_{a\in\prod_{i=1}^n S_i} |\mathbb{N}^n - \nabla(B_a)|$$

$$= (\sum_{a\in(\prod_{i=1}^n S_i)-(\prod_{i=1}^n E_i)} \prod_{i=1}^n \psi_i(a_i))\binom{n+t-1}{n} + (\sum_{a\in\prod_{i=1}^n E_i} \prod_{i=1}^n \psi_i(a_i))\binom{n+t-2}{n}$$

$$= (\sum_{a\in\prod_{i=1}^n S_i} \prod_{i=1}^n \psi_i(a_i))\binom{n+t-1}{n} - (\sum_{a\in\prod_{i=1}^n E_i} \prod_{i=1}^n \psi_i(a_i))(\binom{n+t-1}{n} - \binom{n+t-2}{n}))$$

$$= (\prod_{i=1}^n (\sum_{u\in S_i} \psi_i(u)))\binom{n+t-1}{n} - (\prod_{i=1}^n (\sum_{u\in E_i} \psi_i(u)))\binom{n+t-2}{n-1}$$

$$= (\prod_{i=1}^n \deg(g_i))\binom{n+t-1}{n} - (\prod_{i=1}^n \deg(h_i))\binom{n+t-2}{n-1}.$$

Now for any $\alpha \in \mathbb{N}^n$ with $\sum_{i=1}^n \alpha_i = t$, set

$$\theta(\alpha) \triangleq (\deg(g_1)\alpha_1, \ldots, \deg(g_n)\alpha_n),$$

and for any $\alpha \in \mathbb{N}^n$ with $\sum_{i=1}^n \alpha_i = t-1$, set

$$\theta(\alpha) \triangleq (\deg(g_1)\alpha_1 + \deg(g_1) - \deg(h_1), \ldots, \deg(g_n)\alpha_n + \deg(g_n) - \deg(h_n)).$$

Moreover, let $D = \{\theta(\alpha) \mid \alpha \in \Lambda\}$. Then, one can check that for any $\alpha \in \Lambda$, $\theta(\alpha)$ is the greatest element of $\mathrm{supp}(\varphi(\alpha))$. Furthermore, by Lemma 2.6, we have

$$|\mathbb{N}^n - \nabla(D)| = (\prod_{i=1}^n \deg(g_i))\binom{n+t-1}{n} - (\prod_{i=1}^n \deg(h_i))\binom{n+t-2}{n-1}$$

$$= \sum_{a\in\prod_{i=1}^n S_i} |\mathbb{N}^n - \nabla(B_a)|.$$

With the above discussion, (2) immediately follows from Theorems 4.1 and 4.2. Finally, noticing that if $t \geqslant 2$, then $\mathbf{0} \notin B_a$ for all $a \in \prod_{i=1}^n S_i$, (3) immediately follows from Theorem 4.1, as desired. $\qquad\square$

Theorem 5.4, together with Theorems 5.2 and 5.3, implies the following corollary.

Corollary 5.1. *Suppose that for any $k \in [1,n]$, S_k satisfies Condition (D) in R, and let $e = \min\{\sum_{u\in S_k} \psi_k(u) \mid k \in [1,n]\}$. Then, the following four statements hold:*

(1) $Q = (\bigcap_{m=1}^n \mathcal{I}_t(g_1, \ldots, g_{m-1}, g_m/h_m, g_{m+1}, \ldots, g_n)) \cap \mathcal{I}_{t-1}(h_1, \ldots, h_n)$;

(2) $Q = \mathcal{I}_t(g_1, \ldots, g_n) + \mathcal{I}_{t-1}(g_1, \ldots, g_n) \cdot (\prod_{i=1}^n \frac{g_i}{h_i})$;

(3) *For any $f \in Q$, $f \notin \mathcal{I}_t(g_1, \ldots, g_n)$ if and only if there exists $v \in \prod_{i=1}^n E_i$ and $\gamma \in \mathbb{N}^n$ such that $\sum_{i=1}^n \lfloor \frac{\gamma_i}{\psi_i(v_i)} \rfloor = t-1$, $f(x_1 + v_1, \ldots, x_n + v_n)_{[\gamma]} \neq 0$;*

(4) *Suppose that $\prod_{i=1}^n E_i \neq \emptyset$. Then, for any $\gamma \in \mathbb{N}^n$ with $\sum_{i=1}^n \gamma_i = t-1$, we have $\varphi(\gamma) \in Q - \mathcal{I}_t(g_1, \ldots, g_n)$. Moreover, it holds that*

$$\min\{\deg(f) \mid f \in Q - \mathcal{I}_t(g_1, \ldots, g_n)\} = (t-1)e + (\sum_{i=1}^n \sum_{u\in S_i - E_i} \psi_i(u)).$$

Proof. By the definition of Q, (1) follows from (1) of Theorem 5.3 and (1) of Theorem 5.2, (2) follows from (1), (2) of Theorem 5.4, and (3) follows from (1) of Theorem 5.2. Therefore it remains to establish (4). To this end, we first fix $\gamma \in \mathbb{N}^n$ with $\sum_{i=1}^n \gamma_i = t - 1$. Noticing that $\varphi(\gamma) \in Q$, it suffices to show that $\varphi(\gamma) \notin \mathcal{I}_t(g_1, \ldots, g_n)$. By way of contradiction, assume that $\varphi(\gamma) \in \mathcal{I}_t(g_1, \ldots, g_n)$. Since $(\deg(g_i)\gamma_i + \deg(g_i) - \deg(h_i) \mid i \in [1, n])$ is the greatest element of $\operatorname{supp}(\varphi(\gamma))$, by Theorem 5.2, there exists $\alpha \in \mathbb{N}^n$ such that $\sum_{i=1}^n \alpha_i = t$, and $\deg(g_i)\alpha_i \leqslant \deg(g_i)\gamma_i + \deg(g_i) - \deg(h_i)$ for all $i \in [1, n]$. Consider an arbitrary $k \in [1, n]$. Since $E_k \neq \emptyset$, we have $\deg(g_k) \geqslant \deg(h_k) \geqslant 1$. This, together with $\deg(g_k)\alpha_k \leqslant \deg(g_k)\gamma_k + \deg(g_k) - \deg(h_k)$, implies that $\alpha_k \leqslant \gamma_k$. It then follows that $\alpha \leqslant \gamma$, $\sum_{i=1}^n \alpha_i = t$, $\sum_{i=1}^n \gamma_i = t - 1$, a contradiction, as desired.

Next, choose $l \in [1, n]$ with $\deg(g_l) = e$. By the discussion in the previous paragraph, we have $g_l^{t-1}(\prod_{i=1}^n g_i/h_i) \in Q - \mathcal{I}_t(g_1, \ldots, g_n)$. Moreover, one can check that

$$\deg(g_l^{t-1}(\textstyle\prod_{i=1}^n g_i/h_i)) = (t - 1)e + (\textstyle\sum_{i=1}^n \sum_{u \in S_i - E_i} \psi_i(u)).$$

Finally, consider an arbitrary $f \in Q - \mathcal{I}_t(g_1, \ldots, g_n)$. By Theorem 5.4, there exists $(p(\alpha) \mid \alpha \in \Lambda) \in \Omega^\Lambda$ such that $f = \sum_{\alpha \in \Lambda} p(\alpha) \cdot \varphi(\alpha)$, and $\deg(p(\alpha)) + \deg(\varphi(\alpha)) \leqslant \deg(f)$ for all $\alpha \in \Lambda$. Since $f \notin \mathcal{I}_t(g_1, \ldots, g_n)$, we can choose $\beta \in \mathbb{N}^n$ such that $\sum_{i=1}^n \beta_i = t - 1$, $p(\beta) \neq 0$. It then follows that

$$\begin{aligned}
\deg(f) &\geqslant \deg(\varphi(\beta)) \\
&= (\textstyle\sum_{i=1}^n \deg(g_i)\beta_i) + (\textstyle\sum_{i=1}^n \sum_{u \in S_i - E_i} \psi_i(u)) \\
&\geqslant (t - 1)e + (\textstyle\sum_{i=1}^n \sum_{u \in S_i - E_i} \psi_i(u)),
\end{aligned}$$

which further completes the proof of (4). $\qquad\square$

Remark 5.4. **(1)** *If $\prod_{i=1}^n E_i = \emptyset$, then (1), (2) of Theorem 5.4 recover (1), (2) of Theorem 5.2.*

(2) *If R is a field, $S_i = \{0, 1_R\}$, $E_i = \{0\}$, $\psi_i(0) = \psi_i(1_R) = 1$ for all $i \in [1, n]$, then (3), (4) of Corollary 5.2 recover [33, Theorem 1.5].*

6 Applications of our punctured Nullstellensatz

6.1 Hyperplane covering

Throughout this subsection, for any $k \in [1, n]$, we let S_k be a finite subset of R, (S_k, ψ_k) be a multiset, and fix $E_k \subseteq S_k$.

Roughly speaking, given a family of r-hyperplanes (see Definition 2.5), we consider the case that every point of $(\prod_{i=1}^n S_i) - (\prod_{i=1}^n E_i)$ is covered by many r-hyperplanes, yet at least one point of $\prod_{i=1}^n S_i$ is not covered by any r-hyperplane. The following is the most general result of this section.

Theorem 6.1. *Suppose that for any $k \in [1, n]$, S_k satisfies Condition (D) in R. Let L be a finite set. For any $\lambda \in L$, let $e_\lambda \in \mathbb{N}$, H_λ be an e_λ-hyperplane of R^n, and fix $\rho_\lambda \in \Omega$ such that $\deg(\rho_\lambda) = e_\lambda$ and*

$$H_\lambda = \{u \in R^n \mid \rho_\lambda(u_1, \ldots, u_n) = 0\}.$$

Fix $t \in \mathbb{Z}^+$. Assume in addition that the following two conditions hold:

(i) *For any $a \in (\prod_{i=1}^n S_i) - (\prod_{i=1}^n E_i)$, it holds that*

$$|\{\lambda \in L \mid a \in H_\lambda\}| \geqslant \max\{\textstyle\sum_{i=1}^n \beta_i \mid \beta \in \mathbb{N}^n, \sum_{i=1}^n \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t - 1\} + 1;$$

(ii) *There exists $w \in \prod_{i=1}^n S_i$ such that $\prod_{\lambda \in L} \rho_\lambda(w_1, \ldots, w_n) \neq 0$.*

Then, for any $m \in [1, n]$, it holds that

$$\textstyle\sum_{\lambda \in L} e_\lambda \geqslant (t - 1)(\sum_{u \in S_m - E_m} \psi_m(u)) + (\sum_{k=1}^n \sum_{u \in S_k - E_k} \psi_k(u)).$$

Proof. Consider $a \in (\prod_{i=1}^n S_i) - (\prod_{i=1}^n E_i)$ and $\gamma \in \mathbb{N}^n$ with $\sum_{i=1}^n \left\lfloor \frac{\gamma_i}{\psi_i(a_i)} \right\rfloor \leqslant t - 1$. We claim that

$$(\textstyle\prod_{\lambda \in L} \rho_\lambda)(x_1 + a_1, \ldots, x_n + a_n)_{[\gamma]} = 0.$$

Indeed, suppose that this does not hold. Then, we can choose $(\theta(\lambda) \mid \lambda \in L)$ such that $\gamma = \sum_{\lambda \in L} \theta(\lambda)$, where $\theta(\lambda) \in \mathrm{supp}\,(\rho_\lambda(x_1 + a_1, \ldots, x_n + a_n))$ for all $\lambda \in L$. For any $\lambda \in L$ with $\rho_\lambda(a_1, \ldots, a_n) = 0$, noticing that $\rho_\lambda(x_1 + a_1, \ldots, x_n + a_n)_{[\mathbf{0}]} = 0$, we have $\theta(\lambda) \neq \mathbf{0}$. It then follows that

$$\textstyle\sum_{i=1}^n \gamma_i \geqslant |\{\lambda \in L \mid \rho_\lambda(a_1, \ldots, a_n) = 0)\}| = |\{\lambda \in L \mid a \in H_\lambda\}|,$$

a contradiction to (i), as desired. Now with (ii), an application of Theorem 5.3 to $\prod_{\lambda \in L} \rho_\lambda$ completes the proof. $\qquad\square$

Now we consider the special case that R is an integral domain.

Corollary 6.1. *Suppose that R is an integral domain. Let L be a finite set, and let $(H_\lambda \mid \lambda \in L)$ be a tuple of subsets of R^n with $\prod_{i=1}^n S_i \nsubseteq \bigcup_{\lambda \in L} H_\lambda$. Fix $t \in \mathbb{Z}^+$. Assume in addition that for any $a \in (\prod_{i=1}^n S_i) - (\prod_{i=1}^n E_i)$,*

$$|\{\lambda \in L \mid a \in H_\lambda\}| \geqslant \max\{\textstyle\sum_{i=1}^n \beta_i \mid \beta \in \mathbb{N}^n, \sum_{i=1}^n \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t - 1\} + 1.$$

Then, the following two statements hold true:

(1) *Let $(e_\lambda \mid \lambda \in L) \in \mathbb{N}^L$, and suppose that for any $\lambda \in L$, H_λ is an e_λ-hyperplane of R^n. Then, for any $m \in [1, n]$, it holds that*

$$\sum_{\lambda \in L} e_\lambda \geqslant (t-1)(\sum_{u \in S_m - E_m} \psi_m(u)) + (\sum_{k=1}^n \sum_{u \in S_k - E_k} \psi_k(u));$$

(2) *Suppose that for any $\lambda \in L$, H_λ is a hyperplane of R^n. Then, for any $m \in [1, n]$, it holds that*

$$|L| \geqslant (t-1)(\sum_{u \in S_m - E_m} \psi_m(u)) + (\sum_{k=1}^n \sum_{u \in S_k - E_k} \psi_k(u)).$$

Proof. **(1)** By Definition 2.5, for any $\lambda \in L$, we can choose $\rho_\lambda \in \Omega$ such that $\deg(\rho_\lambda) = e_\lambda$ and $H_\lambda = \{u \in R^n \mid \rho_\lambda(u_1, \ldots, u_n) = 0\}$. Now we choose $w \in \prod_{i=1}^n S_i$ with $w \notin \bigcup_{\lambda \in L} H_\lambda$. For any $\lambda \in L$, by $w \notin H_\lambda$, we have $\rho_\lambda(w_1, \ldots, w_n) \neq 0$. Noticing that R is an integral domain, we further derive that $\prod_{\lambda \in L} \rho_\lambda(w_1, \ldots, w_n) \neq 0$. Now the desired result immediately follows from Theorem 6.1.

(2) This immediately follows from (1). $\qquad\square$

If R is a field, then we have the following consequence of Corollary 6.1.

Corollary 6.2. *Suppose that R is a field. Let $\langle \ , \ \rangle : R^n \times R^n \longrightarrow R$ be a non-degenerate bilinear map. Let Y be a finite set, $(\eta_\lambda \mid \lambda \in Y) \in (R^n)^Y$, $(c_\lambda \mid \lambda \in Y) \in R^Y$. Fix $t \in \mathbb{Z}^+$. Assume in addition that the following two conditions hold:*

(i) *For any $a \in (\prod_{i=1}^n S_i) - (\prod_{i=1}^n E_i)$, it holds that*

$$|\{\lambda \in Y \mid \langle \eta_\lambda, a \rangle = c_\lambda\}| \geqslant \max\{\sum_{i=1}^n \beta_i \mid \beta \in \mathbb{N}^n, \sum_{i=1}^n \left\lfloor \frac{\beta_i}{\psi_i(a_i)} \right\rfloor \leqslant t-1\} + 1;$$

(ii) *There exists $w \in \prod_{i=1}^n S_i$ such that $\langle \eta_\lambda, w \rangle \neq c_\lambda$ for all $\lambda \in Y$.*

Then, for any $m \in [1, n]$, it holds that

$$|\{\lambda \in Y \mid \eta_\lambda \neq 0\}| \geqslant (t-1)(\sum_{u \in S_m - E_m} \psi_m(u)) + (\sum_{k=1}^n \sum_{u \in S_k - E_k} \psi_k(u)).$$

Proof. Let $L = \{\lambda \in Y \mid \eta_\lambda \neq 0\}$. Moreover, for any $\lambda \in L$, we let $H_\lambda = \{u \in R^n \mid \langle \eta_\lambda, u \rangle = c_\lambda\}$. Then, $(H_\lambda \mid \lambda \in L)$ is a tuple of hyperplanes of R^n. One can check from (ii) that $\prod_{i=1}^n S_i \not\subseteq \bigcup_{\lambda \in L} H_\lambda$; and moreover, for any $a \in R^n$, it holds that $\{\lambda \in Y \mid \langle \eta_\lambda, a \rangle = c_\lambda\} = \{\lambda \in L \mid a \in H_\lambda\}$. Hence an application of (2) of Corollary 6.1 yields the desired result. $\qquad\square$

Remark 6.1. (1) *In Theorem 6.1, we use the weaker assumption that all the S_i's satisfy Condition (D) instead of that R is an integral domain. This is inspired by [23, Theorem 10] which considers hyperplanes covering the Boolean cube $\{0, 1_R\}^n$. We note that Theorem 6.1 includes [23, Theorem 10] as a special case.*

(2) *Suppose that R is a field. If $\psi_i(u) = 1$ for all $i \in [1, n]$ and $u \in S_i$, then Corollary 6.1 recovers [9, Theorem 5.3]; and if $t = 1$ and $\prod_{i=1}^n E_i = \{0\}$, then Corollary 6.1 recovers [23, Theorem 9] and [24, Theorem 12].*

(3) *Suppose that R is a finite field with $|R| = q$. Fix $t \in \mathbb{Z}^+$. Let Y be a finite set, and let $(\eta_\lambda \mid \lambda \in Y) \in (R^n)^Y$ such that $|\{\lambda \in Y \mid \eta_\lambda \in H\}| \geqslant t$ for any hyperplane $H \subseteq R^n$. Then, Corollary 6.2 implies that*

$$|Y| \geqslant (n + t - 1)(q - 1) + 1, \tag{6.1}$$

which recovers Bruen's result [15, Theorem 2.1] (also see [9, Theorem 5.2]). (6.1) was first established for $t = 1$ by Jamison, and then independently by Brouwer and Schrijver via different methods (see [22, 13]). We also refer the reader to [7, 8, 26] for improvements and relevant work of (6.1).

6.2   The generalized Alon-Füredi theorem

In [4, Theorem 5], Alon and Füredi establish a general lower bound for the number of nonzero points of a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ in $\prod_{i=1}^n S_i$, where $\mathbb{F}$ is a field and the S_i's are finite subsets of $\mathbb{F}$. In [9, Corollary 4.3], Ball and Serra recover the Alon-Füredi theorem by using their punctured Nullstellensatz. In [18, Theorem 2.2], Clark generalizes the Alon-Füredi theorem to polynomials over a commutative ring by using a variant of Ball and Serra's punctured Nullstellensatz. In [12, Theorem 1.2], Bishnoi, Clark, Potukuchi and Schmitt further generalize [18, Theorem 2.2]. Their result is referred to as the generalized Alon-Füredi theorem, and has many applications in combinatorics and coding theory (see [12, Sections 4–6] for more details).

In this section, we give an alternative proof of the generalized Alon-Füredi theorem by using Theorems 5.2 and 5.3. Our proof closely follows the spirits in the proofs of [9, Corollary 4.3] and [18, Theorem 2.2].

Theorem 6.2. *(Generalized Alon-Füredi Theorem, [12, Theorem 1.2]) Let $S_1, \ldots, S_n$ be nonempty finite subsets of R such that for any $k \in [1, n]$, S_k satisfies Condition (D) in R. Let $\beta \in \mathbb{N}^n$ with $\beta \leqslant (|S_1| - 1, \ldots, |S_n| - 1)$,*

and let $f \in \Omega - \{0\}$ such that $\alpha \leqslant \beta$ for all $\alpha \in \operatorname{supp}(f)$. Then, there exists $\mu \in \mathbb{N}^n$ satisfying the following three conditions:

(1) $(|S_1| - \beta_1, \ldots, |S_n| - \beta_n) \leqslant \mu \leqslant (|S_1|, \ldots, |S_n|)$;

(2) $\sum_{k=1}^{n} \mu_k = (\sum_{k=1}^{n} |S_k|) - \deg(f)$;

(3) $|\{v \in \prod_{i=1}^{n} S_i \mid f(v_1, \ldots, v_n) \neq 0\}| \geqslant \prod_{k=1}^{n} \mu_k$.

Proof. Let $Q = \{v \in \prod_{i=1}^{n} S_i \mid f(v_1, \ldots, v_n) \neq 0\}$. Moreover, for any $k \in [1, n]$, let $E_k = \{v_k \mid v \in Q\}$, and let ψ_k denote the constant 1 map defined on S_k. Then, we have $f(w_1, \ldots, w_n) = 0$ for all $w \in (\prod_{i=1}^{n} S_i) - (\prod_{i=1}^{n} E_i)$. Since $f \neq 0$ and $\alpha \leqslant (|S_1| - 1, \ldots, |S_n| - 1)$ for all $\alpha \in \operatorname{supp}(f)$, an application of (2) of Theorem 5.2 and Theorem 5.3 to $(S_1, \psi_1), \ldots, (S_n, \psi_n)$ and $t = 1$ leads to the facts that $Q \neq \emptyset$ and

$$\prod_{k=1}^{n} \prod_{u \in S_k - E_k} (x_k - u) \mid f. \tag{6.2}$$

If $\beta = \mathbf{0}$, then $(|S_1|, \ldots, |S_n|)$ satisfies Conditions (1)–(3), as desired. Therefore in what follows, we assume that $\beta \neq \mathbf{0}$, which implies that we can choose $m \in [1, n]$ with $\beta_m \geqslant 1$. Since $Q \neq \emptyset$, we can choose $b \in E_m$ such that

$$|Q| \geqslant |E_m| \cdot |\{v \in Q \mid v_m = b\}|. \tag{6.3}$$

Let $g \triangleq f(x_1, \ldots, x_{m-1}, b, x_{m+1}, \ldots, x_n)$. It is straightforward to verify that

$$|\{v \in \prod_{i=1}^{n} S_i \mid g(v_1, \ldots, v_n) \neq 0\}| = |S_m| \cdot |\{v \in Q \mid v_m = b\}|. \tag{6.4}$$

By $b \in E_m$ and (6.4), we have $g \neq 0$. Moreover, (6.3) and (6.4) imply that

$$|Q| \geqslant \frac{|E_m|}{|S_m|} \cdot |\{v \in \prod_{i=1}^{n} S_i \mid g(v_1, \ldots, v_n) \neq 0\}|. \tag{6.5}$$

Let $\theta = (\beta_1, \ldots, \beta_{m-1}, 0, \beta_{m+1}, \ldots, \beta_n) \in \mathbb{N}^n$. Then, it is straightforward to verify that $\gamma \leqslant \theta$ for all $\gamma \in \operatorname{supp}(g)$. Since $\theta \leqslant \beta$, $\theta \neq \beta$, by induction, we can choose $\varepsilon \in \mathbb{N}^n$ satisfying the following three conditions:

(i) $(|S_1| - \theta_1, \ldots, |S_n| - \theta_n) \leqslant \varepsilon \leqslant (|S_1|, \ldots, |S_n|)$;

(ii) $\sum_{k=1}^{n} \varepsilon_k = (\sum_{k=1}^{n} |S_k|) - \deg(g)$;

(iii) $|\{v \in \prod_{i=1}^{n} S_i \mid g(v_1, \ldots, v_n) \neq 0\}| \geqslant \prod_{k=1}^{n} \varepsilon_k$.

We note that from $\theta_m = 0$ and *(i)*, we have $\varepsilon_m = |S_m|$. Now let

$$\lambda = (\varepsilon_1, \ldots, \varepsilon_{m-1}, |E_m|, \varepsilon_{m+1}, \ldots, \varepsilon_n) \in \mathbb{N}^n. \tag{6.6}$$

31

We will show that λ satisfies the following three conditions:

(iv) $(|S_1| - \beta_1, \ldots, |S_n| - \beta_n) \leqslant \lambda \leqslant (|S_1|, \ldots, |S_n|)$;

(v) $\sum_{k=1}^{n} \lambda_k \geqslant (\sum_{k=1}^{n} |S_k|) - \deg(f)$;

(vi) $|Q| \geqslant \prod_{k=1}^{n} \lambda_k$.

Indeed, for any $k \in [1, n] - \{m\}$, by $\beta_k = \theta_k$, $\lambda_k = \varepsilon_k$ and (i), we have $|S_k| - \beta_k \leqslant \lambda_k \leqslant |S_k|$. From (6.2), $f \neq 0$ and (2) of Lemma 2.1, we can choose $\alpha \in \mathrm{supp}\,(f)$ with $|S_m| - |E_m| \leqslant \alpha_m$. Since $\alpha \leqslant \beta$, we have $|S_m| - |E_m| \leqslant \beta_m$, which, together with $\lambda_m = |E_m|$, implies that $|S_m| - \beta_m \leqslant \lambda_m \leqslant |S_m|$, which further establishes (iv). Next, by (6.2), we can choose $h \in \Omega$ with $f = (\prod_{u \in S_m - E_m} (x_m - u)) \cdot h$. It then follows that

$$g = (\textstyle\prod_{u \in S_m - E_m} (b - u)) \cdot h(x_1, \ldots, x_{m-1}, b, x_{m+1}, \ldots, x_n),$$

which, together with (4) of Lemma 2.1, further implies that

$$\deg(g) \leqslant \deg(h) = \deg(f) - |S_m| + |E_m|. \tag{6.7}$$

With (6.6), $\varepsilon_m = |S_m|$ and some straightforward computation, (v) follows from (ii) and (6.7), and (vi) follows from (iii) and (6.5), as desired. Noticing that $\alpha \leqslant \beta$ for all $\alpha \in \mathrm{supp}\,(f)$, we have $\deg(f) \leqslant \sum_{k=1}^{n} \beta_k$, which, together with (v), implies that

$$\textstyle\sum_{k=1}^{n}(|S_k| - \beta_k) \leqslant (\sum_{k=1}^{n} |S_k|) - \deg(f) \leqslant \sum_{k=1}^{n} \lambda_k.$$

Since $(|S_1| - \beta_1, \ldots, |S_n| - \beta_n) \leqslant \lambda$ (see (iv)), we can choose $\mu \in \mathbb{N}^n$ with $(|S_1| - \beta_1, \ldots, |S_n| - \beta_n) \leqslant \mu \leqslant \lambda$ and $\sum_{k=1}^{n} \mu_k = (\sum_{k=1}^{n} |S_k|) - \deg(f)$. By (iv) and (vi), we conclude that μ satisfies Conditions (1)–(3), as desired. $\qquad \square$

Remark 6.2. *It has been proven in [12, Theorem 1.2] that the lower bound is sharp in all cases. We refer the reader to [12, Section 3.3] for more details.*

Appendices

A Proof of Lemma 2.4

Proof. Since $\rho \mid \psi$, we can choose $f \in \Omega$ with $\psi = f \cdot \rho$. By Lemma 3.1, we can choose $\tau \in \Omega$ such that $g \mid (f - \tau)$ and $\theta \not\leqslant \alpha$ for all $\alpha \in \mathrm{supp}\,(\tau)$. It then follows that $(\rho \cdot g) \mid (\psi - \rho \cdot \tau)$. We claim that $\theta \not\leqslant \beta$ for all $\beta \in \mathrm{supp}\,(\rho \cdot \tau)$.

Indeed, let $\beta \in \mathrm{supp}\,(\rho \cdot \tau)$. Then, we can choose $\alpha \in \mathrm{supp}\,(\tau)$, $\gamma \in \mathrm{supp}\,(\rho)$ with $\beta = \alpha + \gamma$. By $\alpha \in \mathrm{supp}\,(\tau)$, we have $\theta \not\leqslant \alpha$, and by $\gamma \in \mathrm{supp}\,(\rho)$, we have $0 \in \{\gamma_i, \theta_i\}$ for all $i \in [1, n]$. It then follows that $\theta \not\leqslant \alpha + \gamma = \beta$, as desired. Now by $g \mid \psi$, $g \mid (\psi - \rho \cdot \tau)$, we have $g \mid (\rho \cdot \tau)$. It then follows from (2) of Lemma 2.1 that $\max(\mathrm{supp}\,(\rho \cdot \tau)) = \emptyset$, and hence $\rho \cdot \tau = 0$. Therefore from $(\rho \cdot g) \mid (\psi - \rho \cdot \tau)$, we deduce that $(\rho \cdot g) \mid \psi$, as desired. $\qquad\square$

B   Proof of Lemma 2.5

Proof. If $\alpha \notin (\mathbb{Z}^+)^n$, then one can check that $\mathbf{0} \in B$, and hence $|\mathbb{N}^n - \nabla(B)| = 0 = (\prod_{i=1}^n \alpha_i) \cdot \binom{n+t-1}{n}$, as desired. Therefore in what follows, we assume that $\alpha \in (\mathbb{Z}^+)^n$. Then, for an arbitrary $\beta \in \mathbb{N}^n$, we have

$$\beta \in \mathbb{N}^n - \nabla(B) \Longleftrightarrow (\forall\, \theta \in \mathbb{N}^n \ s.t. \ \textstyle\sum_{i=1}^n \theta_i = t : (\alpha_1\theta_1, \ldots, \alpha_n\theta_n) \not\leqslant \beta)$$

$$\Longleftrightarrow (\forall\, \theta \in \mathbb{N}^n \ s.t. \ \textstyle\sum_{i=1}^n \theta_i = t : \theta \not\leqslant \left(\left\lfloor \frac{\beta_1}{\alpha_1} \right\rfloor, \ldots, \left\lfloor \frac{\beta_n}{\alpha_n} \right\rfloor\right))$$

$$\Longleftrightarrow \textstyle\sum_{i=1}^n \left\lfloor \frac{\beta_i}{\alpha_i} \right\rfloor \leqslant t - 1,$$

which establishes (2.13). Now, with the following two equations:

$$|\{\gamma \in \mathbb{N}^n \mid \textstyle\sum_{i=1}^n \gamma_i \leqslant t - 1\}| = \binom{n+t-1}{n},$$

$$\forall\, \gamma \in \mathbb{N}^n : |\{\beta \in \mathbb{N}^n \mid \left(\left\lfloor \frac{\beta_1}{\alpha_1} \right\rfloor, \ldots, \left\lfloor \frac{\beta_n}{\alpha_n} \right\rfloor\right) = \gamma\}| = \textstyle\prod_{i=1}^n \alpha_i,$$

(2.12) immediately follows from (2.13), as desired. $\qquad\square$

C   Proof of Lemma 2.6

Proof. Throughout the proof, we let $\mathbf{1} \in \mathbb{N}^n$ denote the all 1 vector, and let

$$\Lambda = \{\theta \in \mathbb{N}^n \mid \textstyle\sum_{i=1}^n \theta_i = t - 1\}.$$

Then, via some straightforward verification, we have

$$\nabla(C) - \nabla(B) = \{(\alpha_1\theta_1, \ldots, \alpha_n\theta_n) + \tau \mid \theta \in \Lambda, \tau \in \mathbb{N}^n, \alpha - \gamma \leqslant \tau \leqslant \alpha - \mathbf{1}\}.$$

Moreover, for any $\theta, \tau, \beta, \eta \in \mathbb{N}^n$ with $\tau \leqslant \alpha - \mathbf{1}$, $\eta \leqslant \alpha - \mathbf{1}$, it holds that

$$(\alpha_1\theta_1, \ldots, \alpha_n\theta_n) + \tau = (\alpha_1\beta_1, \ldots, \alpha_n\beta_n) + \eta \Longrightarrow \theta = \beta, \tau = \eta.$$

By the above discussion, we have

$$|\nabla(C) - \nabla(B)| = |\{\tau \in \mathbb{N}^n \mid \alpha - \gamma \leqslant \tau \leqslant \alpha - \mathbf{1}\}| \cdot |\Lambda| = (\textstyle\prod_{i=1}^n \gamma_i)\binom{n+t-2}{n-1}.$$

It then follows from Lemma 2.5 that

$$|\mathbb{N}^n - \nabla(B \cup C)| = |\mathbb{N}^n - \nabla(B)| - |\nabla(C) - \nabla(B)|$$
$$= (\textstyle\prod_{i=1}^n \alpha_i)\binom{n+t-1}{n} - (\textstyle\prod_{i=1}^n \gamma_i)\binom{n+t-2}{n-1},$$

as desired. $\qquad\square$

References

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

[2] G. N. Alfarano, M. Borello, A. Neri, A. Ravagnani, Three combinatorial perspectives on minimal codes, *SIAM Journal on Discrete Mathematics*, vol. 36, no. 1 (2022), 461-489.

[3] N, Alon, Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing*, vol. 8, no. 1-2 (1999), 7-29.

[4] N. Alon, Z. Füredi, Covering the cube by affine hyperplanes, *European Journal of Combinatorics*, vol. 14, no. 2 (1993), 79-83.

[5] N. Alon, M. Tarsi, Colorings and orientations of graphs, *Combinatorica*, vol. 12, no. 2 (1992), 125-134.

[6] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[7] S. Ball, On Nuclei and Blocking Sets in Desarguesian Spaces, *Journal of Combinatorial Theory, Series A*, vol. 85, no. 2 (1999), 232-236.

[8] S. Ball, On Intersection Sets in Desarguesian Affine Spaces, *European Journal of Combinatorics*, vol. 21, no. 4 (2000), 441-446.

[9] S. Ball, O. Serra, Punctured Combinatorial Nullstellensätze, *Combinatorica*, vol. 29, no. 5 (2009), 511-522.

[10] S. Ball, O. Serra, Erratum Punctured Combinatorial Nullstellensätze, *Combinatorica*, vol. 31, no. 3 (2011), 377-378.

[11] G. Batzaya, G. Bayarmagnai, A generalized Combinatorial Nullstellensatz for multisets, *European Journal of Combinatorics*, vol. 83 (2020), 5 pages.

[12] A. Bishnoi, P. L. Clark, A. Potukuchi, J. R. Schmitt, on zeros of a polynomial in a finite grid, *Combinatorics, Probability and Computing*, vol. 27, no. 3 (2018), 310-333.

[13] A. E. Brouwer, A. Schrijver, The blocking number of an affine space, *Journal of Combinatorial Theory, Series A*, vol. 24, no.2 (1978), 251-253.

[14] W. C. Brown, *Matrices over Commutative Rings*, Marcel Dekker, New York, 1992.

[15] A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *Journal of Combinatorial Theory, Series A*, vol. 60, no. 1 (1992), 19-33.

[16] B. Buchberger, Introduction to Gröbner bases, *Gröbner Bases and Applications*, Cambridge University Press (1998), 3-31.

[17] P. L. Clark, The Combinatorial Nullstellensätze revisited, *The Electronic Journal of Combinatorics*, vol. 21, no. 4 (2014), 17 pages.

[18] P. L. Clark, Warning's second theorem with relaxed outputs, *Journal of Algebraic Combinatorics*, vol. 48, no. 2 (2018), 325-349.

[19] A. Clifton, H. Huang, On almost k-covers of hypercubes, *Combinatorica*, vol. 40, no. 4 (2020), 511-526.

[20] S. Eliahou, M. Kervaire, Sumsets in vector spaces over finite fields, *Journal of Number Theory*, vol. 71, no. 1 (1998), 12-39.

[21] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra (Third edition)*, Cambridge University Press, New York, 2013.

[22] R. E. Jamison, Covering finite fields with cosets of subspaces, *Journal of Combinatorial Theory, Series A*, vol. 22, no. 3 (1977), 253-266.

[23] G. Kós, T. Mészáros, L. Rónyai, Some extensions of Alon's Nullstellensatz, *Publicationes Mathematicae Debrecen*, vol. 79, no. 3-4 (2011), 507-519.

[24] G. Kós, L. Rónyai, Alon's Nullstellensatz for multisets, *Combinatorica*, vol. 32, no. 5 (2012), 589-605.

[25] H. Kulosman, Minghu Wang, A generalization of Alon's Combinatorial Nullstellensatz, *JP Journal of Algebra, Number Theory and Applications*, vol. 20, no. 1 (2011), 61-75.

[26] I. Landjev, A. Rousseva, On the sharpness of Bruen's bound for intersection sets in Desarguesian affine spaces, *Design, Codes and Cryptography*, vol. 72, no. 3 (2014), 551-558.

[27] M. Lasoń, A generalization of Combinatorial Nullstellensatz, *The Electronic Journal of Combinatorics*, vol. 17, no. 1 (2010), 6 pages.

[28] T. Mészáros, L. Rónyai, A note on Alon's Combinatorial Nullstellensatz, *Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae Sectio Computatorica*, vol. 42 (2014), 249-260.

[29] T. R. Mezei, Combinatorial Nullstellensätze (in Hungarian), BSc thesis, ELTE, 2011.

[30] M. Michałek, A short proof of Combinatorial Nullstellensatz, *The American Mathematical Monthly*, vol. 117, no. 9 (2010), 821-823.

[31] B. Nica, Polynomials over structured grids, *Combinatorics, Probability and Computing*, 04 October, 2022, 1-15.

[32] L. Rónyai, T. Mészáros, Some combinatorial applications of Gröbner bases, *Algebraic Informatics 4th International Conference, CAI 2011*, Linz, Austria, June 21-24, 2011 Proceedings, Springer, 65-83.

[33] L. Sauermann, Y. Wigderson, Polynomials that vanish to high order on most of the hypercube, arXiv: 2010.00077v2 [math.CO] 28 Mar 2022.

[34] U. Schauz, Algebraically solvable problems: describing polynomials as equivalent to explicit solutions, *The Electronic Journal of Combinatorics*, vol. 15, no. 1 (2008), 35 pages.

[35] Z-W. Sun, On value sets of polynomials over a field, *Finite Fields and Their Applications*, vol. 14, no. 2 (2008), 470-481.

[36] Xuding Zhu, R. Balakrishnan, *Combinatorial Nullstellensatz with Applications to Graph Colouring*, CRC Press, Boca Raton & Oxon, 2022.