Publ. Math. Debrecen
79/3-4 (2011), 507–519
DOI: 10.5486/PMD.2011.5133

Some extensions of Alon's Nullstellensatz

By GÉZA KÓS (Budapest), TAMÁS MÉSZÁROS (Budapest)
and LAJOS RÓNYAI (Budapest)

This paper is dedicated to professors Kálmán Győry, Attila Pethő, János Pintz, and András Sárközy, on the occasion of their (round) birthdays

Abstract. Alon's combinatorial Nullstellensatz and in particular the resulting nonvanishing criterion is one of the most powerful algebraic tools in combinatorics, with many important applications. The nonvanishing theorem has been extended in two directions. The first and the third named authors proved a version allowing multiple points. Michałek established a variant which is valid over arbitrary commutative rings, not merely over subrings of fields. In this paper we give new proofs of the latter two results and provide a common generalization of them. As an application, we prove extensions of the theorem of Alon and Füredi on hyperplane coverings of discrete cubes.

1. Introduction

Alon's combinatorial Nullstellensatz (Theorem 1.1 from [2]) and the resulting nonvanishing criterion (Theorem 1.2 from [2]) is one of the most powerful algebraic tools in combinatorics. It has several beautiful and strong applications, see [7], [9], [10], [11], [12], [15], [17] for some recent examples.

Let $\mathbb{F}$ be a field, $S_1, S_2, \ldots, S_n$ be finite nonempty subsets of $\mathbb{F}$. Let $\mathbb{F}[\mathbf{x}] = \mathbb{F}[x_1, \ldots, x_n]$ stand for the ring of polynomials over $\mathbb{F}$ in variables $x_1, \ldots, x_n$.

Mathematics Subject Classification: 05-XX, 05E40, 12D10.
Key words and phrases: Combinatorial Nullstellensatz, polynomial method, interpolation, multiset, zero divisor, multiple point, covering by hyperplanes.
Research supported in part by OTKA grants NK 72845, K77476, and K77778.

Alon's theorem is a specialized, precise version of the Hilbertsche Nullstellensatz for the ideal $I(S)$ of all polynomial functions vanishing on the set $S = S_1 \times S_2 \times \cdots \times S_n \subseteq \mathbb{F}^n$, and for the basis $f_1, f_2, \ldots, f_n$ of $I(S)$, where

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

for $i = 1, \ldots, n$. From this a simple and widely applicable nonvanishing criterion (Theorem 1.2 in [2]) has been deduced. It provides a sufficient condition for a polynomial $f \in \mathbb{F}[\mathbf{x}]$ for not vanishing everywhere on S.

Herewith we consider extensions of the latter result in two directions. Before formulating these, we need first some notation and definitions. Let $\mathbb{N}$ denote the set of nonnegative integers, and let n be a fixed positive integer. Throughout the paper R will denote a commutative ring (with 1, as usual), and $\mathbb{F}$ stands for a field. Vectors of length n are denoted by boldface letters, for example $\mathbf{s} = (s_1, \ldots, s_n) \in R^n$ stands for points in the space R^n. For vectors $\mathbf{a}, \mathbf{b} \in \mathbb{N}^n$, the relation $\mathbf{a} \geq \mathbf{b}$ etc. means that the relation holds at every component. We use the same notation for constant vectors. e.g. $\mathbf{0} = (0, 0, \ldots, 0)$ or $\mathbf{1} = (1, 1, \ldots, 1)$.

For $\mathbf{w} \in \mathbb{N}^n$, we write $\mathbf{x}^{\mathbf{w}}$ for the monomial $x_1^{w_1} \ldots x_n^{w_n} \in R[x_1, \ldots, x_n]$. If $\mathbf{s} \in R^n$, then $(\mathbf{x} - \mathbf{s})^{\mathbf{w}}$ stands for the polynomial $(x_1 - s_1)^{w_1} \ldots (x_n - s_n)^{w_n}$.

It is well known that for an arbitrary $\mathbf{s} \in R^n$ we can express a polynomial $f(\mathbf{x}) \in R[x_1, \ldots, x_n]$ as

$$f(\mathbf{x}) = \sum_{\mathbf{u} \in \mathbb{N}^n} f_{\mathbf{u}}(\mathbf{s})(\mathbf{x} - \mathbf{s})^{\mathbf{u}}, \tag{1}$$

where the coefficients $f_{\mathbf{u}}(\mathbf{s}) \in R$ are uniquely determined by f, $\mathbf{u}$ and $\mathbf{s}$. In particular we have $f_{\mathbf{0}}(\mathbf{s}) = f(\mathbf{s})$ for all $\mathbf{s} \in R^n$. Observe that if $u_1 + \cdots + u_n \geq \deg f$, then $f_{\mathbf{u}} = f_{\mathbf{u}}(\mathbf{s})$ does not depend on $\mathbf{s}$.

Suppose now that $S_1, S_2, \ldots, S_n$ are nonempty finite subsets of R, and assume further that we have a positive integer *multiplicity* $m_i(s)$ attached to every element $s \in S_i$. This way we can view the pair (S_i, m_i) as a multiset which contains the element $s \in S_i$ precisely $m_i(s)$ times. We shall consider the sum $d_i = d(S_i) := \sum_{s \in S_i} m_i(s)$ as the size of the multiset (S_i, m_i). We put $S = S_1 \times S_2 \times \cdots S_n$. For an element $\mathbf{s} = (s_1, \ldots, s_n) \in S$ we set the multiplicity vector $m(\mathbf{s})$ as $(m_1(s_1), \ldots, m_n(s_n))$, and write $|m(\mathbf{s})| = m_1(s_1) + \cdots + m_n(s_n)$.

We formulate first a version of Alon's powerful nonvanishing theorem (Theorem 1.2 in [2]) for multiple points over fields. From this one can obtain Alon's result by setting $m_i(s) = 1$ identically.

Theorem 1. *Let $\mathbb{F}$ be a field, $f = f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial of degree $\sum_{i=1}^{n} t_i$, where each t_i is a nonnegative integer. Assume, that the coefficient in f of the monomial $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$ is nonzero. Suppose further that $(S_1, m_1), (S_2, m_2), \ldots, (S_n, m_n)$ are multisets of $\mathbb{F}$ such that for the size d_i of (S_i, m_i) we have $d_i > t_i$ $(i = 1, \ldots, n)$. Then there exists a point $\mathbf{s} = (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ and an exponent vector $\mathbf{u} = (u_1, \ldots, u_n)$ with $u_i < m_i(s_i)$ for each i, such that $f_{\mathbf{u}}(\mathbf{s}) \neq 0$.*

Theorem 1 was first proved in [13]. In another direction, over an arbitrary commutative ring R MICHAŁEK proved the following extension of the nonvanishing theorem:

Theorem 2. *Let R be a commutative ring, and let $f(\mathbf{x})$ be a polynomial in $R[x_1, \ldots, x_n]$. Suppose that the degree $\deg(g)$ of f is $\sum_{i=1}^{n} t_i$, where t_i is a nonnegative integer, and suppose that the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero. Suppose further that $S_1, \ldots, S_n$ are subsets of R with $|S_i| > t_i$, and with the property that if $s \neq s^* \in S_i$, then $s - s^*$ is a unit in R. Then there exists a vector $\mathbf{s} \in S = S_1 \times \cdots \times S_n$, such that*

$$f(\mathbf{s}) \neq 0.$$

In the case $R = \mathbb{F}$, when we work over a field, the above result specializes to Alon's nonvanishing theorem; note that if R is a field, then $s - s^*$ is always a unit, whenever s and s^* are different. We give two new proofs of Theorem 2. The first one will be on the basis of an identity obtained from an interpolation argument. The second proof follows closely the original line of reasoning by Alon. In fact, for a subset S of R^n let us denote the set of polynomials from $R[x_1, \ldots, x_n]$ vanishing at all $s \in S$ by $I(S)$. It is easy to see that $I(S)$ is an ideal of $R[x_1, \ldots, x_n]$. Now Theorem 2 will be a simple consequence of the following result, which can be considered as an extension of Alon's Nullstellensatz.

Theorem 3. *Let R be a commutative ring, and let $f(\mathbf{x})$ be a polynomial from $R[x_1, \ldots, x_n]$. Let $S_1, \ldots, S_n$ be nonempty finite subsets of R with the property that if $s \neq s^* \in S_i$, then $s - s^*$ is a unit in R, $S = S_1 \times \cdots \times S_n$ and define $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$. Then for every polynomial $f(\mathbf{x}) \in R[x_1, \ldots, x_n]$ there are polynomials $h_1, \ldots, h_n, r \in R[x_1, \ldots, x_n]$ such that $\deg h_i \leq \deg f - |S_i|$ for all i, the degree of r is less then $|S_i|$ in every x_i, for which*

$$f(\mathbf{x}) = r(\mathbf{x}) + \sum_{i=1}^{n} h_i(\mathbf{x}) g_i(x_i).$$

Moreover, $f \in I(S)$ if and only if r is identically zero, hence $g_1(x_1), \dots, g_n(x_n)$ is a basis of $I(S)$.

We have the following common generalization of Theorems 1 and 2:

Theorem 4. *Let R be a ring, $f = f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ be a polynomial of degree $\sum_{i=1}^n t_i$, where each t_i is a nonnegative integer. Assume, that the coefficient in f of the monomial $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$ is nonzero. Suppose further that $(S_1, m_1), (S_2, m_2), \dots, (S_n, m_n)$ are multisets of R such that for the size d_i of (S_i, m_i) we have $d_i > t_i$ $(i = 1, \dots, n)$, and for each i any nonzero element $s - s^*$ from $S_i - S_i$ is a unit in R. Then there exists a point $\mathbf{s} = (s_1, \dots, s_n) \in S_1 \times \cdots \times S_n$ and an exponent vector $\mathbf{u} = (u_1, \dots, u_n)$ with $u_i < m_i(s_i)$ for each i, such that $f_{\mathbf{u}}(\mathbf{s}) \neq 0$.*

In the next section we prove Theorem 4, which implies Theorems 1, and 2. The proof will be based on an argument extending univariate Hermite interpolation to our setting. In Section 3 we give an alternative proof for Theorem 2, which will follow from Theorem 3. This line of reasoning is an adaptation of Alon's original proofs from [2]. In Section 4 we give two applications. These will be extensions of a theorem of Alon and Füredi on almost covering a discrete hypercube by hyperplanes. In Section 5 some concluding remarks are given.

2. Proof of Theorem 4

Lemma 5. *Let (S, m) be a nonempty multiset in a commutative ring R such that all nonzero elements $s - s^*$ in $S - S$ are units, and let $g(x) = \prod_{s \in S} (x - s)^{m(s)}$. For all polynomials $f(x) \in R[x]$, the following statements are equivalent:*

(a) *$f_u(s) = 0$ for every $s \in S$ and $0 \leq u < m(s)$;*

(b) *the polynomial $(x - s)^{m(s)}$ divides $f(x)$ for every $s \in S$;*

(c) *$g(x)$ divides $f(x)$.*

Proof. The relations $(a) \Leftrightarrow (b)$ and $(c) \Rightarrow (b)$ are trivial. To prove $(a, b) \Rightarrow (c)$, apply an induction on $|S|$. The initial case $|S| = 1$ is trivial.

Let $n \geq 2$ and assume the statement of the Lemma for $|S| = n - 1$. Choose an $s_0 \in S$ arbitrarily. By (b), there is a polynomial $f^* \in R[x]$ such that $f(x) = (x - s_0)^{m(s_0)} f^*(x)$. Let $g^*(x) = \prod_{s \in S \setminus \{s_0\}} (x - s)^{m(s)}$. We have to prove that g^* divides f^*.

First we show that $f_u^*(s) = 0$ for every $s \in S \setminus \{s_0\}$ and $0 \leq u < m(s)$. Suppose the contrary, and take a pair (s, u) for which $f_u^*(s) \neq 0$ and u is minimal,

i.e. $f_0^*(s) = f_1^*(s) = \ldots = f_{u-1}^*(s) = 0$. Then

$$f_u(s) = \Big((x-s_0)^{m(s_0)} f^*(x)\Big)_u(s) = \sum_{v=0}^{u} \Big((x-s_0)^{m(s_0)}\Big)_v(s) \cdot f_{u-v}^*(s)$$
$$= (s-s_0)^{m(s)} f_u^*(s).$$

Since $s - s_0$ is a unit in R and $f_u^*(s) \neq 0$, this contradicts $f_u(s) = 0$.

So we have $f_u^*(s) = 0$ for every $s \in S \setminus \{s_0\}$ and $0 \leq u < m(s)$. By the induction hypothesis, f^* is divisible by g^*. □

Lemma 6. *Let (S, m) be a nonempty multiset in a commutative ring R such that all nonzero elements $s - s^*$ in $S - S$ are units, and let $s_0 \in S$ and $0 \leq u_0 < m(s_0)$. Then there exists a polynomial $h^{(s_0,u_0)}(x) \in R[x]$ with $\deg h^{(s_0,u_0)} < d(S)$ such that for every $s \in S$ and $0 \leq u < m(s)$ we have*

$$h_u^{(s_0,u_0)}(s) = \begin{cases} 1 & \text{if } s = s_0 \text{ and } u = u_0; \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For every $v = 0, 1, \ldots, m(s_0) - 1$ let

$$f^{(v)}(x) = (x-s_0)^v \prod_{s \in S \setminus \{s_0\}} \left(\frac{x-s}{s_0-s}\right)^{m(s)}.$$

These auxiliary polynomials have the following obvious properties:

- For every $s \in S \setminus \{s_0\}$ and every v, the polynomial $f^{(v)}(x)$ is divisible by $(x-s)^{m(s)}$, so $f_u^{(v)}(s) = 0$ for all $0 \leq u < m(s)$.
- For every $0 \leq u < v$, since $f^{(v)}(x)$ is divisible by $(x-s_0)^v$, we have $f_u^{(v)}(s_0) = 0$.
- For every v we have $f_v^{(v)}(s_0) = 1$.

Now we can construct $h_u^{(s_0,u_0)}(s)$ as a linear combination of the auxiliary polynomials, inductively: if $h^{(s_0,u_0+1)}, \ldots, h^{(s_0,m(s_0)-1)}$ are already defined then let

$$h^{(s_0,u_0)}(x) = f^{(u_0)}(x) - \sum_{u_0 < u < m(s_0)} f_u^{(u_0)}(s_0) \cdot h^{(s_0,u)}(x). \qquad \square$$

Lemma 7 (Hermite interpolation)**.** *Let (S, m) be a multiset in a commutative ring R such that all nonzero elements $s - s^*$ in $S - S$ are units. For each $s \in S$ and $0 \leq u < m(s)$, let $y_{s,u}$ be an arbitrary element in R. Then*

(a) *there exists a unique polynomial $f(s) \in R[x]$, with $\deg f < d(S)$, satisfying $f_u(s) = y_{s,u}$ for every pair (s, u);*

(b) *this polynomial can be constructed as*

$$f = \sum_{s\in S} \sum_{u<m(s)} y_{s,u} h^{(s,u)}.$$

PROOF. Let $f = \sum_{s\in S} \sum_{u<m(s)} y_{s,u} h^{(s,u)}$. For every $s \in S$ and $u < m(s)$ we have

$$f_u(s) = \sum_{r\in S} \sum_{v<m(r)} y_{r,v} h_u^{(r,v)}(s) = \sum_{r\in S} \sum_{v<m(r)} \begin{Bmatrix} 1 & \text{if } r = s \text{ and } v = u \\ 0 & \text{otherwise} \end{Bmatrix} y_{r,v} = y_{s,u}$$

so the polynomial f satisfies the requested property.

For the uniqueness, suppose that there exists another polynomial f^* with the same property. Then, for all $s \in S$ and $u < m(s)$ we have $(f - f^*)_u(s) = f_u(s) - f_u^*(s) = 0$. By Lemma 5, this implies that $f - f^*$ is divisible by $\prod_{s\in S}(x-s)^{m(s)}$. Since the degree of the latter polynomial is $d(S)$ and its leading coefficient is 1, this contradicts $\deg(f - f^*) < d(S)$. □

Lemma 8. *Let (S, m) be a multiset in a commutative ring R such that all nonzero elements $s - s^*$ in $S - S$ are units, and let $t = d(S) - 1$. Then there exist elements $\alpha(s, u) \in R$ for all $s \in S$ and $0 \le u < m(s)$ with the following property: for every $\ell \ge 0$,*

$$\sum_{s\in S} \sum_{0\le u<m(s)} \alpha(s,u) \binom{\ell}{u} s^{\ell-u} = \begin{cases} 0 & \text{if } \ell < t; \\ 1 & \text{if } \ell = t; \\ * & \text{if } \ell > t. \end{cases}$$

Here the symbol $*$ means "undetermined".)

PROOF. Take the polynomials $h^{(s,u)}(x)$ provided by Lemma 6, and let $\alpha(s, u)$ be the coefficient of x^t in the polynomial $h^{(s,u)}(x)$.

For every $s \in S$ we have

$$x^\ell = \big(s + (x-s)\big)^\ell = \sum_{u=0}^{\infty} \binom{\ell}{u} s^{\ell-u} (x-s)^u,$$

and therefore

$$\big(x^\ell\big)_u(s) = \binom{\ell}{u} s^{\ell-u}$$

for every $u \ge 0$. (For $u > \ell$ we have $\binom{\ell}{u} = 0$ and the negative exponent in $s^{\ell-u}$ does not matter.)

Now take an arbitrary $\ell < d(S)$, and apply Lemma 7 to the values $y_{s,u} = \binom{\ell}{u} s^{\ell-u}$. From these values, Lemma 7 reconstructs the polynomial x^ℓ:

$$\sum_{s\in S} \sum_{u<m(s)} \binom{\ell}{u} s^{\ell-u} h^{(s,u)}(x) = x^\ell.$$

Comparing the coefficients of x^t, we get

$$\sum_{s\in S} \sum_{u<m(s)} \alpha(s,u)\binom{\ell}{u} s^{\ell-u} \begin{cases} 0 & \text{if } \ell < t; \\ 1 & \text{if } \ell = t. \end{cases}$$ □

Proof of Theorem 4. Without loss of generality, we may assume that $t_i = d(S_i) - 1$ for every $i = 1, 2, \ldots, n$.

Expand f as $f(\mathbf{x}) = \sum_{\mathbf{k}} c_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}$. For every $\mathbf{s} \in S$, from

$$\begin{aligned} f(\mathbf{x}) &= \sum_{\mathbf{k}} c_{\mathbf{k}} \big(\mathbf{s} + (\mathbf{x}-\mathbf{s})\big)^{\mathbf{k}} = \sum_{\mathbf{k}} c_{\mathbf{k}} \sum_{\mathbf{u}} \left(\prod_{i=1}^n \binom{k_i}{u_i} s_i^{k_i-u_i} \right) (\mathbf{x}-\mathbf{s})^{\mathbf{u}} \\ &= \sum_{\mathbf{u}} \left(\sum_{\mathbf{k}} c_{\mathbf{k}} \prod_{i=1}^n \binom{k_i}{u_i} s_i^{k_i-u_i} \right) (\mathbf{x}-\mathbf{s})^{\mathbf{u}} \end{aligned}$$

we get

$$f_{\mathbf{u}}(\mathbf{s}) = \sum_{\mathbf{k}} c_{\mathbf{k}} \prod_{i=1}^n \binom{k_i}{u_i} s_i^{k_i-u_i}.$$

For each i, by Lemma 8, there exist elements $\alpha_i(s,u) \in R$ for all $s \in S_i$ and $0 \le u < m_i(s)$ such that

$$\sum_{s\in S_i} \sum_{0\le u<m_i(s)} \alpha_i(s,u)\binom{\ell}{u} s^{\ell-u} = \begin{cases} 0 & \text{if } \ell < t_i; \\ 1 & \text{if } \ell = t_i; \\ * & \text{if } \ell > t_i. \end{cases}$$

Now let $\alpha(\mathbf{s},\mathbf{u}) = \prod_{i=1}^n \alpha_i(s_i,u_i)$ and consider the following expression:

$$\begin{aligned} \sum_{\mathbf{s}\in S} \sum_{\mathbf{u}<m(\mathbf{s})} \alpha(\mathbf{s},\mathbf{u}) f_{\mathbf{u}}(\mathbf{s}) &= \sum_{\mathbf{s}\in S} \sum_{\mathbf{u}<m(\mathbf{s})} \left(\prod_{i=1}^n \alpha_i(s_i,u_i) \right) \sum_{\mathbf{k}} c_{\mathbf{k}} \prod_{i=1}^n \binom{k_i}{u_i} s_i^{k_i-u_i} \\ &= \sum_{\mathbf{k}} c_{\mathbf{k}} \sum_{s_1\in S_1} \sum_{u_1<m_1(s_1)} \cdots \sum_{s_n\in S_n} \sum_{u_n<m_n(s_n)} \prod_{i=1}^n \left(\alpha_i(s_i,u_i)\binom{k_i}{u_i} s_i^{k_i-u_i} \right) \end{aligned}$$

$$= \sum_{\mathbf{k}} c_{\mathbf{k}} \prod_{i=1}^{n} \left(\sum_{s_i \in S_i} \sum_{u_i < m_i(s_i)} \alpha_i(s_i, u_i) \binom{k_i}{u_i} s_i^{k_i - u_i} \right) = \sum_{\mathbf{k}} c_{\mathbf{k}} \prod_{i=1}^{n} \begin{Bmatrix} 0 & \text{if } k_i < t_i \\ 1 & \text{if } k_i = t_i \\ * & \text{if } k_i > t_i \end{Bmatrix}.$$

Since $\deg f = t_1 + \ldots + t_n$, the last product is zero except for $\mathbf{k} = \mathbf{t}$ (when every factor is 1). Therefore, we have

$$\sum_{\mathbf{s} \in S} \sum_{\mathbf{u} < m(\mathbf{s})} \alpha(\mathbf{s}, \mathbf{u}) f_{\mathbf{u}}(\mathbf{s}) = c_{\mathbf{t}}.$$

On the left-hand side, there stands a linear combination of the values $f_{\mathbf{u}}(\mathbf{s})$. Since $c_{\mathbf{t}} \neq 0$ on the right-hand side, there must be at least one nonzero among these values. □

3. An alternative proof for Theorem 2

Here we intend to give a proof of Theorem 2 which follows closely the original line of reasoning from Alon [2].

Proof of Theorem 3. We denote by V the R module of all functions from S to R. V is a free R module,

$$\operatorname{rank}_R V = |S| = \prod_{i=1}^{n} d_i,$$

where $|S_i| = \deg g_i = d_i$. In fact, for $\mathbf{s} \in S$ we denote by $f_{(\mathbf{s})}$ the $S \longrightarrow R$ function taking value 1 at $\mathbf{s}$ and 0 everywhere else in S. Then the set $F = \{f_{(\mathbf{s})} |\ \mathbf{s} \in S\}$ is a free generating set of V over R, and $|F| = \prod_{i=1}^{n} d_i = |S|$. Next we observe, that every $f_{(\mathbf{s})}$ can be written as a polynomial from $R[x_1, \ldots, x_n]$, using interpolation. For $\mathbf{s} = (s_1, \ldots, s_n) \in S$ we have

$$f_{(\mathbf{s})}(\mathbf{x}) = \prod_{i=1}^{n} \left(\prod_{\alpha \in S_i, \alpha \neq s_i} (x_i - \alpha)(s_i - \alpha)^{-1} \right).$$

Note that since $s_i \neq \alpha \in S_i$, the element $s_i - \alpha$ is a unit in R, hence the definition of $f_{(\mathbf{s})}(\mathbf{x})$ makes sense. Consider the following set of monomials

$$M = \{\mathbf{x}^{\mathbf{w}};\ w_i \leq d_i - 1,\ i = 1, \ldots, n\}.$$

Set $\mathcal{G} = \{g_1(x_1), \ldots, g_n(x_n)\}$. An arbitrary polynomial f from $R[x_1, \ldots, x_n]$ can be reduced with $\mathcal{G}$. This means that an occurrence of the monomial $x_i^{d_i}$ is

replaced by $-(g_i(x_i)-x_i^{d_i})$ as long as it is possible. Note that this reduction does not change f as a function on S. Clearly any f can be reduced into an R-linear combination of monomials from M. In particular, the elements of F are reduced this way into a collection of $|S|$ polynomials which are independent over R. Using also that $|M| = |S|$, we infer that M, as a set of functions from S to R, is also linearly independent over R.

Now consider an arbitrary polynomial f from $R[x_1,\dots,x_n]$, and reduce f with $\mathcal{G}$ as much as possible. Denote the resulting (reduced) polynomial by r, which is an R-linear combination of monomials from M. The fact that f reduces to r means that there are polynomials $h_1,\dots,h_n \in R[x_1,\dots,x_n]$ such that $\deg(h_i) \le \deg f - d_i$ for all i, the degree of r is less than d_i in every x_i, and

$$f(\mathbf{x}) = r(\mathbf{x}) + \sum_{i=1}^{n} h_i(\mathbf{x}) g_i(x_i).$$

Because of the linear independence of the monomial functions from M, we have that $f \in I(S)$ if and only if r is the all zero linear combination. This concludes the proof. □

We remark that the proof actually gives that $\mathcal{G}$ is a Gröbner basis of $I(S)$ with respect to an arbitrary term order on $R[x_1,\dots,x_n]$. For an introduction to Gröbner bases the reader is referred to [1].

From Theorem 3 the original argument of Alon gives Theorem 2 quite simply. Below we reproduce Alon's proof for the convenience of the reader.

An alternative proof of Theorem 2. Clearly we may assume that $|S_i| = t_i + 1$ for all i. Suppose that the result is false, i.e. $f \in I(S)$, and define $g_i(x_i) = \prod_{s\in S_i}(x_i - s)$. By Theorem 3 there are polynomials $h_1,\dots,h_n \in R[x_1,\dots,x_n]$ such that $\deg(h_j) \le \sum_{i=1}^n t_i - \deg(g_j)$ for all j, for which

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

Here the degree of $h_i g_i$ is at most $\deg(f)$, and if there are any monomials of degree $\deg(f)$ in it, then they are divisible by $x_i^{t_i+1}$. It follows that the coefficient of $\prod_{i=1}^n x_i^{t_i}$ on the right hand side is zero. However by our assumption the coefficient of $\prod_{i=1}^n x_i^{t_i}$ on the left hand side is nonzero, and this contradiction completes the proof. □

4. Two applications

We can extend a result of Alon and Füredi [4] on the covering of a discrete cube by hyperplanes in the following way. (The original result is the special case when every multiplicity is 1.)

Theorem 9. *Let $(S_1, m_1), \dots, (S_n, m_n)$ be finite multisets from the field $\mathbb{F}$. Suppose that $0 \in S_i$, with $m_i(0) = 1$ for every i, and $H_1, \dots, H_k$ are hyperplanes in $\mathbb{F}^n$ such that every point $\mathbf{s} \in S \setminus \{\mathbf{0}\}$ is covered by at least $|m(\mathbf{s})| - n + 1$ hyperplanes and the point $\mathbf{0}$ is not covered by any of the hyperplanes. Then $k \geq d(S_1) + d(S_2) + \cdots + d(S_n) - n$.*

Proof. Let $\ell_j(\mathbf{x})$ be a linear polynomial defining the hyperplane H_j, set $f(\mathbf{x}) = \prod_{j=1}^{k} \ell_j(\mathbf{x})$, and $t_i = d(S_i) - 1$.

Let

$$P(\mathbf{x}) = \prod_{i=1}^{n} \prod_{s \in S_i \setminus \{0\}} (x_i - s)^{m_i(s)}$$

and

$$F(\mathbf{x}) = P(\mathbf{x}) - \frac{P(\mathbf{0})}{f(\mathbf{0})} f(\mathbf{x}).$$

Note that we have $f(\mathbf{0}) \neq 0$, because the hyperplanes do not cover $\mathbf{0}$. If the statement is false, then the degree of F is $t_1 + t_2 + \cdots + t_n$ and the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is 1. Theorem 1 applies with $(S_1, m_1), \dots, (S_n, m_n)$ and $t_1, \dots, t_n$: there exists a vector $\mathbf{s} \in S$, and an exponent vector $\mathbf{u} < m(\mathbf{s})$ such that $F_{\mathbf{u}}(\mathbf{s}) \neq 0$. We observe that $\mathbf{s}$ cannot be $\mathbf{0}$, because $F(\mathbf{0}) = 0$. Thus $\mathbf{s}$ must have at least one nonzero coordinate, implying that $P_{\mathbf{u}}(\mathbf{s}) = 0$.

Moreover, as $\mathbf{s}$ is a nonzero vector, $f(\mathbf{x})$ must vanish at $\mathbf{s}$ at least $|m(\mathbf{s})| - n + 1$ times, implying that $f_{\mathbf{u}}(\mathbf{s}) = 0$ (expand the product at $\mathbf{s}$; for every term $(\mathbf{x} - \mathbf{s})^{\mathbf{v}}$ obtained there will be an index j such that $v_j \geq m_j(s_j)$). These facts imply that $F_{\mathbf{u}}(\mathbf{s}) = 0$, a contradiction. This finishes the proof. □

Next, as an application of Theorem 2, we present a generalization of Theorem 6.3. from [2] to the Boolean cube over a commutative ring R. By a hyperplane H in R^n we understand the set of zeros of a polynomial of the form $a_1 x_1 + \cdots + a_n x_n - b := (\mathbf{a}, \mathbf{x}) - b$, where $a_i, b \in R$.

Theorem 10. *Let R be a commutative ring, and let $H_1, \dots, H_m$ be hyperplanes in R^n such that $H_1, \dots, H_m$ cover all the vertices of the unit cube $\{0,1\}^n \subseteq R^n$, with the exception of $\mathbf{0}$. Let $(\mathbf{a}^i, \mathbf{x}) - b_i$ be the polynomial defining H_i. If $\prod_{i=1}^{m} b_i \neq 0$, then $m \geq n$.*

PROOF. The proof is essentially the same as the one in [2]. Assume that the assertion is false: $m < n$, and consider the polynomial

$$P(\mathbf{x}) = (-1)^{n+m+1} \prod_{j=1}^{m} b_j \prod_{i=1}^{n} (x_i - 1) - \prod_{i=1}^{m} [(\mathbf{a}^i, \mathbf{x}) - b_i].$$

The degree of this polynomial is clearly n, and the coefficient of $\prod_{i=1}^{n} x_i$ in P is $(-1)^{n+m+1} \prod_{j=1}^{m} b_j$, which is nonzero by our assumption. By applying Theorem 2 to $S_i = \{0, 1\}$, $t_i = 1$, we obtain a point $\mathbf{s} \in \{0, 1\}^n$ for which $P(\mathbf{s}) \neq 0$. This point is not the all zero vector, as P vanishes on $\mathbf{0}$. But otherwise $(\mathbf{a}_i, \mathbf{s}) - b_i = 0$ for some i (as $\mathbf{s}$ is covered by an H_i), implying that P does vanish on $\mathbf{s}$, a contradiction. □

Alon and Füredi have obtained the preceding statement for the case $R = \mathbb{F}$, using the original nonvanishing argument. If we put $R = \mathbb{Z}_n$ for some square free integer $n \in \mathbb{N}$, then an application of the original nonvanishing theorem for a suitable prime factor of n proves the statement. However, if n has square factors, then Theorem 10 appears to give a new result.

5. Concluding remarks

Our interest in developing a version of the nonvanishing theorem for multisets has grown out of an attempt to prove SNEVILY's conjecture [16] in a particular case.

Let G be a finite group of odd order and suppose that $a_1, \ldots, a_k \in G$ are pairwise distinct and $b_1, \ldots, b_k \in G$ are pairwise distinct. Snevily's Conjecture states that there is a permutation π of the indices $1, 2, \ldots, k$ for which $a_1 b_{\pi(1)}, a_2 b_{\pi(2)}, \ldots, a_k b_{\pi(k)}$ are pairwise distinct. The conjecture has been proved for cyclic groups of prime order by ALON [3], for cyclic groups by DASGUPTA, KÁROLYI, SERRA, and SZEGEDY [8] and recently for all commutative groups by ARSOVSKI [5]. Note that Alon's proof, which is based on the Combinatorial Nullstellensatz, allows one of the sequences $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ to contain repeated elements when $k < |G|$.

Our approach was the following. Let N be a normal subgroup of G. We look for the permutation to be applied to the factor group G/N first. Of course, in the factor group, some of the cosets $a_1 N, \ldots, a_n N$ and $b_1 N, \ldots, b_n N$ may coincide to each other; it is even possible that $a_1 N, \ldots, a_n N$ all coincide and $b_1 N, \ldots, b_n N$ all coincide. So we must allow $(a_i N)(b_{\pi(i)} N) = (a_j N)(b_{\pi(j)} N)$ in some cases.

The idea is to allow $(a_iN)(b_{\pi(i)}N) = (a_jN)(b_{\pi(j)}N)$ only in those cases, when $a_iN = a_jN$ and $b_{\pi(i)}N = b_{\pi(j)}N$ holds. Suppose that we found such a permutation π. If some classes $(a_{i_1}N)(b_{\pi(i_1)}N), (a_{i_2}N)(b_{\pi(i_2)}N), \ldots, (a_{i_\ell}N)(b_{\pi(i_\ell)}N)$ coincide, then the elements $a_{i_1}, \ldots, a_{i_\ell}$ are all in the same coset cN, and similarly $b_{\pi(i_1)}, \ldots, b_{\pi(i_\ell)}$ are in the same coset Nd. Then we could apply Snevily's Conjecture inductively to the sequences $c^{-1}a_{i_1}, \ldots, c^{-1}a_{i_\ell}$ and $b_{\pi(i_1)}d^{-1}, \ldots, b_{\pi(i_\ell)}d^{-1}$ which all lie in N. By the induction hypothesis, the values $\pi(j_1), \ldots, \pi(j_\ell)$ can be permuted in such a way, that $c^{-1}a_{i_1}b_{\pi(i_1)}d^{-1}, \ldots, c^{-1}a_{i_\ell}b_{\pi(i_\ell)}d^{-1}$ are pairwise distinct. Hence the elements $a_{i_1}b_{\pi(i_1)}, \ldots, a_{i_\ell}b_{\pi(i_\ell)}$ are all in the coset $(cd)N = cNd$, and they will be pairwise distinct.

If we choose N to be a maximal normal subgroup of G, then the order $|G/N| = p$ will be a prime (G is solvable, since $|G|$ is odd). In this case we can use the additive group of the prime field $\mathbb{F}_p$ and re-formulate the existence of the desired permutation.

Conjecture 11. *Suppose that $k \leq p$, and $a_1, \ldots, a_k \in \mathbb{F}_p$ and $b_1, \ldots, b_k \in \mathbb{F}_p$ are arbitrary elements. Then there is a permutation π of the indices $1, 2, \ldots, k$ with the following property: $a_i = a_j$ and $b_{\pi(i)} = b_{\pi(j)}$ holds whenever $a_i + b_{\pi(i)} = a_j + b_{\pi(j)}$.*

This conjecture would imply Snevily's conjecture for all cases when k is not greater than the smallest prime divisor of $|G|$.

To use the polynomial method to prove Conjecture 11 and similar statements, it appears that one is required to handle multiple values in the sequences $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$.

The requirements in Theorems 2 and 4 about the invertibility in R of the differences $s - s^*$ can be somewhat relaxed. The theorems still hold if we assume, instead of invertibility, that the multiplicative monoid $D \subset R$ generated by the differences $s - s^*$ and $f_{(t_1,\ldots,t_n)}$ does not contain 0. In this case the map from R to its ring of fractions $D^{-1}R$ lifts our proofs from $D^{-1}R$ to R (the reader is referred to [6] for basic facts on rings of fractions). Actually, it suffices to assume that a certain specific product from D is not zero.

References

[1] W. W. Adams and P. Loustaunau, An introduction to Gröbner bases, Graduate Studies in Mathematics, 3, *American Mathematical Society, Providence, RI*, 1994.

[2] N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.* **8** (1999), 7–29.

[3] N. Alon, Additive Latin transversals, *Israel J. Math.* **117** (2000), 125–130.

[4] N. Alon and Z. Füredi, Covering the cube by affine hyperplanes,, *European J. Combin.* **14** (1993), 79–83.

[5] B. Arsovski, A proof of Snevily's conjecture, *Israel J. Math.* **182** (2011), 505–508.

[6] M. F. Atiyah and I. G. Macdonald, Introduction to commutative algebra, *Addison—Wesley Publishing Co., Reading, Mass.–London–Don Mills, Ont., Amsterdam, Menlo Park–California, Sydney*, 1969.

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

[8] S. Dasgupta, Gy. Károlyi, O. Serra and B. Szegedy, Transversals of additive Latin squares, *Israel J. Math.* **126** (2001), 17–28.

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

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

[11] Gy. Károlyi, An inverse theorem for the restricted set addition in abelian groups, *J. Algebra* **290** (2005), 557–593.

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

[13] G. Kós and L. Rónyai, Alon's Nullstellensatz for multisets, *Combinatorica* (*to appear*).

[14] M. Michałek, A short proof of Combinatorial Nullstellensatz, *Amer. Math. Monthly* **117** (2010), 821–823.

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

[16] H. Snevily, Unsolved Problems: The Cayley Addition Table of $\mathbb{Z}_n$, *Amer. Math. Monthly* **106** (1999), 584–585.

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

GÉZA KÓS
COMPUTER AND AUTOMATION
RESEARCH INSTITUTE
HUNGARIAN ACAD. SCI
DEPARTMENT OF ANALYSIS
EÖTVÖS LORÁND UNIVERSITY
BUDAPEST
HUNGARY

E-mail: kosgeza@sztaki.hu

LAJOS RÓNYAI
COMPUTER AND AUTOMATION
RESEARCH INSTITUTE
HUNGARIAN ACAD. SCI.
DEPARTMENT OF ALGEBRA
BUDAPEST
UNIV. OF TECHNOLOGY AND ECONOMICS
BUDAPEST
HUNGARY

E-mail: lajos@ilab.sztaki.hu

TAMÁS MÉSZÁROS
DEPARTMENT OF MATHEMATICS
CENTRAL EUROPEAN UNIVERSITY
BUDAPEST
HUNGARY

E-mail: meszaros_tamas@ceu_budapest.edu

(Received February 7, 2011; revised September 23, 2011)