Alon’s Nullstellensatz for multisets

Géza Kós
Computer and Automation Research Institute, Hungarian Academy of Sciences;
Department of Analysis, Eötvös Loránd University, Budapest
kosgeza@sztaki.hu

Lajos Rónyai
Computer and Automation Research Institute, Hungarian Academy of Sciences;
Department of Algebra, Budapest University of Technology and Economics
ronyai@sztaki.hu

September 26, 2011

Abstract

Alon’s combinatorial Nullstellensatz (Theorem 1.1 from [2]) is one of the most powerful algebraic tools in combinatorics, with a diverse array of applications. Let $F$ be a field, $S_1, S_2, \ldots, S_n$ be finite nonempty subsets of $F$. Alon’s theorem is a specialized, precise version of the Hilbertsche Nullstellensatz for the ideal of all polynomial functions vanishing on the set $S = S_1 \times S_2 \times \cdots \times S_n \subseteq F^n$. From this Alon deduces a simple and amazingly widely applicable nonvanishing criterion (Theorem 1.2 in [2]). It provides a sufficient condition for a polynomial $f(x_1, \ldots, x_n)$ which guarantees that $f$ is not identically zero on the set $S$. In this paper we extend these two results from sets of points to multisets. We give two different proofs of the generalized nonvanishing theorem. We extend some of the known applications of the original nonvanishing theorem to a setting allowing multiplicities, including the theorem of Alon and Füredi on the hyperplane coverings of discrete cubes.

1 Introduction

Alon’s combinatorial Nullstellensatz (Theorem 1.1 from [2]) is one of the most powerful algebraic tools in combinatorics. It has dozens of beautiful and strong applications, see [8], [13], [14], [16], [17], [18] for some recent examples.

Let $F$ be a field, $S_1, S_2, \ldots, S_n$ be finite nonempty subsets of $F$. Let $F[x] = F[x_1, \ldots, x_n]$ stand for the ring of polynomials over $F$ in variables $x_1, \ldots, x_n$. Alon’s theorem is a specialized, precise version of the Hilbertsche Nullstellensatz for the ideal of all polynomial functions vanishing on the set $S = S_1 \times S_2 \times \cdots \times S_n \subseteq F^n$, and for the basis $f_1, f_2, \ldots, f_n$, where

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

Mathematics Subject Classification (MSC2010): 05-XX, 05E40, 12D10.
Key words and phrases: Combinatorial Nullstellensatz, polynomial method, Gröbner basis, divided differences, sumset, multiset, multiple point.
Research supported in part by OTKA grants NK 72845, K77476, and K77778.
for \( i = 1, \ldots, n \). From this Alon deduces a simple and amazingly widely applicable nonvanishing criterion (Theorem 1.2 in [2]). It provides a sufficient condition for a polynomial \( f \in \mathbb{F}[x] \) which guarantees that \( f \) is not identically zero on \( S \). Here we aim to extend these two results from sets of points to multisets.

To formulate our results, we need some more notation and definitions. Let \( \mathbb{N} \) denote the set of nonnegative integers, and let \( n \) be a fixed positive integer. Vectors of length \( n \) are denoted by boldface letters, for example \( \mathbf{s} = (s_1, \ldots, s_n) \in \mathbb{F}^n \) stands for points in the space \( \mathbb{F}^n \). 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 notations for constant vectors. e.g. \( 0 = (0,0,\ldots,0) \) or \( 1 = (1,1,\ldots,1) \).

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

It is well known that for an arbitrary \( \mathbf{s} \in \mathbb{F}^n \) we can express a polynomial \( f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}] \) as

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

where the coefficients \( f_\mathbf{u}(\mathbf{s}) \in \mathbb{F} \) are uniquely determined by \( f \), \( \mathbf{u} \) and \( \mathbf{s} \). In particular we have \( f_\mathbf{0}(\mathbf{s}) = f(\mathbf{s}) \) for all \( \mathbf{s} \in \mathbb{F}^n \). If \( u_i < \text{char} \mathbb{F} \) for all \( i \), then we have

\[
f_\mathbf{u}(\mathbf{s}) = \frac{1}{u_1! \cdots u_n!} \frac{\partial^{u_1+\cdots+u_n}}{\partial x_1^{u_1} \cdots \partial x_n^{u_n}} f(\mathbf{s}).
\]

Notice also that if \( u_1 + \cdots + u_n \geq \text{deg} f \), then \( f_\mathbf{u} = f_\mathbf{u}(\mathbf{s}) \) does not depend on \( \mathbf{s} \).

For a point \( \mathbf{s} \in \mathbb{F}^n \) and an exponent vector \( \mathbf{w} \in \mathbb{N}^n \) with positive integer components we write \( I(\mathbf{s},\mathbf{w}) \) for the set of polynomials \( f(x_1,\ldots,x_n) \) for which in the expansion (1) we have \( f_\mathbf{u}(\mathbf{s}) = 0 \) for all \( \mathbf{u} < \mathbf{w} \). It is a simple matter to check that \( I(\mathbf{s},\mathbf{w}) \) is actually an ideal in \( \mathbb{F}[\mathbf{x}] \). We have also that

\[
\dim_\mathbb{F} \mathbb{F}[\mathbf{x}] / I(\mathbf{s},\mathbf{w}) = w_1 w_2 \cdots w_n,
\]

because the monomials \( (\mathbf{x} - \mathbf{s})^\mathbf{u} \) with \( 0 \leq u_j < w_j \) form a basis of the factor \( \mathbb{F}[\mathbf{x}] / I(\mathbf{s},\mathbf{w}) \).

As before, suppose that \( S_1, S_2, \ldots, S_n \) are nonempty finite subsets of \( \mathbb{F} \). Suppose further that we have a positive integer multiplicity \( m_i(s) \) attached to the elements of \( s \in S_i \). 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 \( |m(\mathbf{s})| = m_1(s_1) + \cdots + m_n(s_n) \).

Our principal object of interest is the ideal

\[
I = I(S) = \bigcap_{\mathbf{s} \in S} I(\mathbf{s}, m(\mathbf{s})).
\]

For \( i = 1, \ldots, n \) we define the polynomials \( g_i(x_i) \in \mathbb{F}[\mathbf{x}] \) as

\[
g_i(x_i) = \prod_{s \in S_i} (x_i - s)^{m_i(s)}.
\]
We see that \( g_i \) is a monic polynomial of degree \( d_i \). Moreover, for the ideal generated by the \( g_i \) we have

\[
(g_1(x_1), g_2(x_2), \ldots, g_n(x_n)) \subseteq I. \tag{4}
\]

The following theorem is a generalization of Alon’s Nullstellensatz (Theorem 1.1 from [2]). We recover Alon’s result by setting \( m_i(s) = 1 \) everywhere.

**Theorem 1.** We have

\[
(g_1(x_1), \ldots, g_n(x_n)) = I.
\]

Moreover, for every polynomial \( f(x) \in \mathbb{F}[x] \) there are polynomials \( h_1, \ldots, h_n, r \in \mathbb{F}[x] \) such that \( \deg h_i \leq \deg f - d_i \), the degree of \( r \) is less than \( d_i \) in every \( x_i \), for which

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

In the above expansion \( r \) is uniquely determined by \( f \).

**Remark 2.** We have \( r(x) \equiv 0 \) in the expansion of the theorem if and only if \( f \in I \).

We can strengthen a little the part of Theorem 1 which states that \( \{g_1, \ldots, g_n\} \) is a nice generating set for \( I \). For the basics of the theory of Gröbner bases we refer to [9] and [1].

**Corollary 3.** The set of polynomials \( \{g_1, \ldots, g_n\} \) is a universal Gröbner basis for \( I \).

**Remark 4.** This will follow easily from the proof of Theorem 1. The Gröbner basis property of \( \{g_1, \ldots, g_n\} \) for the ideal it generates can also be proved by applying directly and very simply the \( S \)-polynomial test of Buchberger, (cf. [7], and Theorem 3.10 of Chapter 1 from [9]) to the pair of polynomials \( g_i(x_i), g_j(x_j) \).

**Remark 5.** As in the case of Alon’s theorem, we have that if the coefficients of \( f \) and \( g_i \) are from some subring \( R \) of \( \mathbb{F} \), then the polynomials \( h_i \) and \( r \) will be from \( R[x_1, \ldots, x_n] \) as well.

We can now formulate a version of Alon’s powerful nonvanishing theorem (Theorem 1.2 in [2]) for multiple points. Again, we obtain Alon’s result by setting \( m_i(s) = 1 \) identically.

**Theorem 6.** 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 \( f \) is not in the ideal \( I \) attached to the multisets \( (S_i, m_i) \).

In other words, there exists a point \( s = (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n \) and an exponent vector \( u = (u_1, \ldots, u_n) \) with \( u_i < m_i(s_i) \) for each \( i \), such that \( f_u(s) \neq 0 \) in the expansion of \( f \) as

\[
f(x_1, \ldots, x_n) = \sum f_u(s)(x - s)^u, \quad f_u(s) \in \mathbb{F}.
\]

For two multisets \( (H_1, m_1), (H_2, m_2) \) we write \( (H_1, m_1) \subseteq (H_2, m_2) \) if \( m_1(h) \leq m_2(h) \) holds whenever \( h \in H_1 \). We call the multisubset \( (H_1, m_1) \subseteq (H_2, m_2) \) a tight multisubset, if \( m_1(h) = m_2(h) \) holds for every \( h \in H_1 \).
In [5] Ball and Serra proved a punctured version of Alon’s Nullstellensatz. The result and the proof extend with slight modifications to a multiset case.

Let \((S_1, m_1), \ldots, (S_n, m_n)\) be multisets from the field \(F\). Suppose that \((D_i, m_i)\) is a nonempty tight multisubset of \((S_i, m_i)\) for \(i = 1, \ldots, n\). Write \(D = D_1 \times D_2 \times \cdots \times D_n\). Let \(g_i(x_i)\) be the polynomials from (3) and put

\[
\ell_i(x_i) = \prod_{s \in D_i} (x_i - s)^{m_i(s)} \text{ for } i = 1, \ldots, n.
\]

**Theorem 7.** Let \(f(x) \in F[x]\) be a polynomial such that for all \(s \in S\) with the exception of at least one \(s^* \in D\), for which \(f \not\in I(s^*, m(s^*))\), Then there are polynomials \(h_1, \ldots, h_n, r \in F[x]\) such that \(\deg h_i \leq \deg f - d_i\), the degree of \(r\) is less than \(d_i\) in every \(x_i\), for which

\[
f(x) = r(x) + \sum_{i=1}^{n} h_i(x) g_i(x),
\]

and

\[
r = h \prod_{i=1}^{n} \frac{g_i(x_i)}{\ell_i(x_i)}
\]

for some nonzero \(h \in F[x]\). As a consequence, \(\deg(f) \geq \sum_{i=1}^{n} (d(S_i) - d(D_i))\).

We mention here one more related result from [5] by Ball and Serra. They obtained a generalization of Alon’s Nullstellensatz to polynomials which vanish at least \(t\) times at every point of \(S\) (cf. Theorem 3.1 in [5]). This result is in turn related to the method of multiplicities (see the paper [10] by Dvir, Kopparty, Saraf and Sudan). To give a specific example, from Theorem 3.1 of [5] it follows immediately that if \(S\) is a subset of a field \(F\), \(f \in F[x_1, \ldots, x_n]\) is a polynomial of degree \(d\) which vanishes at least \(t\) times at every point of \(S^n\), then \(\deg f \geq t|S|\).

This Schwartz-Zippel type inequality is an important special case of Lemma 8 from [10].

In the next section we prove Theorems 1, 6, and 7. The proof of Theorem 1 uses some very simple facts from commutative algebra. For Theorem 6 we offer two different proofs. The first one is a direct application of Theorem 1 while the second proof involves a little more explicit relation among the expansion coefficients of \(f\), and is based on elementary calculations with divided differences (Theorem 9). We believe that Theorem 9 is of independent interest.

Section 3 is devoted to applications. We extend some known applications of the nonvanishing theorem to a setting allowing multiplicities. In most cases the original proofs are generalized to higher multiplicities.

## 2 Proofs of Theorems 1, 6, and 7

First we prove Theorem 1. We use Alon’s original argument together with dimension counting.

**Proof of Theorem 1.** We recall first that

\[
I = I(S) = \bigcap_{s \in S} I(s, m(s)).
\]
We show next that
\[ \dim_F F[x]/I = d_1 d_2 \cdots d_n. \] (6)

Indeed, the ideals \( I(s, m(s)) \) are pairwise relatively prime, as the radicals of \( I(s, m(s)) \) are the maximal ideals \( (x_1 - s_1, \ldots, x_n - s_n) \), which are clearly relatively prime (see Proposition 1.16 in [4]). Now the Chinese Remainder Theorem (Proposition 1.10 in [4]) gives that
\[
F[x]/I \cong \bigoplus_{s \in S} F[x]/I(s, m(s)).
\]

By taking dimensions and using (2) we obtain
\[
\dim_F F[x]/I = \sum_{s \in S} \dim_F F[x]/I(s, m(s)) = \sum_{s \in S} m_1(s_1) \cdots m_n(s_n) = d_1 d_2 \cdots d_n.
\]

To establish the Theorem, we focus first on the second statement. In the monomials occurring in \( f \) we repeatedly substitute \( x_i^{d_i} - g_i(x_i) \) for \( x_i^{d_i} \) as long as possible. As \( \deg(x_i^{d_i} - g_i(x_i)) < d_i \), this reduction process is guaranteed to terminate in finite steps with an \( r \) of the desired form.

Notice also, that the above reduction step means subtracting a multiple of degree at most \( \deg f - \deg g_i \) of \( g_i \) from \( f \). From the degree constraints for \( r \) we obtain the inequality
\[
\dim_F F[x]/(g_1(x_1), \ldots, g_n(x_n)) \leq d_1 d_2 \cdots d_n.
\]

Comparing this with (5) and (4), we see that there must be an equality in (4), proving the first claim.

The uniqueness of \( r \) also follows since two such polynomials \( r \) and \( r' \) satisfy \( r - r' \in I \), and then the degree constraints imply that \( r - r' = 0 \). \( \Box \)

**Remark 8.** Alternatively, one can prove \( \dim_F F[x]/(g_1(x_1), \ldots, g_n(x_n)) = d_1 d_2 \cdots d_n \) by a repeated application of the following simple fact: if \( A \) is a commutative ring and \( f(x) \in A[x] \) is a monic polynomial of positive degree, then \( A[x]/(f) \) is a free \( A \)-module of rank \( \deg f \).

**Proof of Corollary [3]** Let \( \prec \) be an arbitrary term order on the monomials of \( F[x] \). We observe that in the course of the reduction of a monomial \( y \), when we substitute \( x_i^{d_i} - g_i(x_i) \) for \( x_i^{d_i} \), we replace \( y \) by a linear combination of monomials which are all \( \prec \)-smaller than \( y \). This implies in particular, that if \( f \in I \) and \( 0 \neq y \) is the \( \prec \)-largest monomial of \( f \), then there exists an \( i \) such that \( x_i^{d_i} \leq y \). \( \Box \)

From the proof Theorem [1] it is apparent that if \( f, g_i \in R[x_1, \ldots, x_n] \) for some subring \( R \) of \( F \), then \( r, h_i \in R[x_1, \ldots, x_n] \) as well, proving the claim of Remark [5].

Theorem [6] now readily follows. The original argument of Alon is verbatim applicable, and is reproduced here for the reader’s convenience.

**Proof of Theorem [6]** Suppose for contradiction that \( f \in I = I(S) \). Then by Theorem [1] there are polynomials \( h_1, \ldots, h_n \in F[x] \) such that \( \deg h_i \leq \deg f - d_i \), for which
\[
f(x) = \sum_{i=1}^n h_i(x)g_i(x_i),
\]
where \( g_i \) are the polynomials from [3]. The coefficient of \( x_1^{d_1}x_2^{d_2} \cdots x_n^{d_n} \) on the left is nonzero. On the other hand, the degree of \( h_i g_i \) is at most the degree of \( f \), and any monomial of this degree must be divisible by \( x_i^{d_i} \) for some \( i \). It follows that the coefficient of \( x_1^{d_1}x_2^{d_2} \cdots x_n^{d_n} \) is 0 on the right hand side. This is a contradiction completing the proof. \( \Box \)
Next we adapt the argument of Ball and Serra from [5] to prove Theorem 7.

Proof of Theorem 7. By Theorem 1 we can write

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

with $h_1, \ldots, h_n, r \in \mathbb{F}[x]$, deg $h_i \leq \deg f - d_i$, and the degree of $r$ is less than $d_i$ in every $x_i$. For each $i$ the polynomial $r\ell_i$ is in $I$, hence it can be reduced to 0 by using the polynomials $g_1(x_1), \ldots, g_n(x_n)$. But if $j \neq i$ then $g_j(x_j)$ can not be used in the reduction of $r\ell_i$ (or of any reduct of $r\ell_i$ by $g_i(x_i)$) because the degree of $r\ell_i$ in $x_j$ is less than $d_j$. We infer, that $g_i$ divides $r\ell_i$: there is a polynomial $r_i \in \mathbb{F}[x]$ such that $r(x)\ell_i(x_i) = g_i(x_i)r_i(x)$. Using that $\ell_i$ divides $g_i$, we have that $\frac{g_i(x_i)}{\ell_i(x_i)}$ divides $r$. Knowing that $\mathbb{F}[x]$ is a UFD and $\frac{g_i(x_i)}{\ell_i(x_i)}$ and $\frac{g_j(x_j)}{\ell_j(x_j)}$ have no associate prime factors in $\mathbb{F}[x]$ for $i \neq j$, we obtain that

$$r = h\prod_{i=1}^{n} \frac{g_i(x_i)}{\ell_i(x_i)},$$

with some polynomial $h$. Here $h \neq 0$ because $f \not\in I$ and hence $r \neq 0$. The last statement follows from $\deg f \geq \deg r$.

\[\square\]

2.1 An alternative proof for Theorem 6

Our objective here is to give a more direct proof of Theorem 6. It is based on a linear relation among the expansion coefficients of $f$, which we develop in Theorem 9.

Throughout this subsection we keep our standard notation: $(S_1, m_1), (S_2, m_2), \ldots, (S_n, m_n)$ are nonempty finite multisets from $\mathbb{F}$, and $d_i$ denotes the size of the multiset $(S_i, m_i)$. We put $S = S_1 \times \cdots \times S_n \subset \mathbb{F}^n$. We set also $g_i(x_i) = \prod_{s \in S_i} (x_i - s)^{m_i(s)}$ for $i = 1, \ldots, n$, and $g(x) = \prod_{i=1}^{n} g_i(x_i)$.

Theorem 9. Let $t = d(S) - 1 = (d_1 - 1, \ldots, d_n - 1)$.

(a) Then there exist constants $\alpha^{(s)}_u \in \mathbb{F}$ for $s \in S$, $u < m(s)$, independent of $f$, such that

$$f_t = \sum_{s \in S} \sum_{u < m(s)} \alpha^{(s)}_uf_u(s) \quad (7)$$

holds for all polynomials $f \in \mathbb{F}[x]$ with $\deg f \leq t_1 + \cdots + t_n$.

(b) The coefficients $\alpha^{(s)}_u$ are uniquely determined by $(S, m)$, $s$, $t$ and $u$.

(c) If $s \in S$ and $u = m(s) - 1$, then $\alpha^{(s)}_u \neq 0$.

To prove Theorem 9, we apply some well-known properties of divided differences of univariate polynomials (see [6]). Our considerations include finite fields as well, where these facts must be handled with special care. In the statement above we allow multiplicities beyond the field characteristics, and many difficulties arise when one works with derivatives of order higher
We will use the notation \( h \) for the unique \( h \in \mathbb{F}[x] \) such that \( f - h \in (g_1, \ldots, g_n) \) and \( \deg_i h < d_i \) for every \( i \).

**Definition 10.** For \( f \in \mathbb{F}[x] \) we denote by \( f[S] \) the coefficient of \( x^{d(S)-1} = x_1^{d_1-1} \cdots x_n^{d_n-1} \) in the polynomial \( (f \mod (g_1, \ldots, g_n)) \).

**Lemma 11.** Let \( f \in \mathbb{F}[x] \) be a polynomial over \( \mathbb{F} \).

(a) If every \( S_i \) consists of a single element \( a_i \) with multiplicity \( t_i+1 \), then \( f[S] = f_t((a_1, \ldots, a_n)) \).

(b) Suppose that some \( S_i \) contains at least two different elements, say \( a \) and \( b \). Let \( S'_i = S_i \setminus \{a\} \) and \( S''_i = S_i \setminus \{b\} \) (these multisets contain \( a \) and \( b \) with multiplicity one less than \( S_i \)), and \( S' = S_1 \times \cdots \times S_{i-1} \times S'_i \times S_{i+1} \times \cdots \times S_n \) and \( S'' = S_1 \times \cdots \times S_{i-1} \times S''_i \times S_{i+1} \times \cdots \times S_n \). Then
\[
f[S] = \frac{f[S'] - f[S'']}{b - a}.
\]

**Proof.** To prove part (a), observe that
\[
(f(x) \mod ((x_1 - a_1)^{t_1+1}, \ldots, (x_n - a_n)^{t_n+1})) = \sum_{u \leq t} f_u(a)(x - a)^u.
\]
Then the coefficient of \( x^t \) is \( f[S] \) on the left-hand side, and it is \( f_t(a) \) on the right-hand side.

As for part (b), from the definition we see that
\[
\begin{align*}
(x_i - a) \left( f(x) \mod (g_1(x_1), \ldots, g_{i-1}(x_{i-1}), \frac{g_i(x_i)}{x_i - a}, g_{i+1}(x_{i+1}), \ldots, g_n(x_n)) \right) - \\
-(x_i - b) \left( f(x) \mod (g_1(x_1), \ldots, g_{i-1}(x_{i-1}), \frac{g_i(x_i)}{x_i - b}, g_{i+1}(x_{i+1}), \ldots, g_n(x_n)) \right) = \\
\left( (x_i - a)f(x) \mod (g_1(x_1), \ldots, g_n(x_n)) \right) - \left( (x_i - b)f(x) \mod (g_1(x_1), \ldots, g_n(x_n)) \right) = \\
\left( (b - a)f(x) \mod (g_1(x_1), \ldots, g_n(x_n)) \right).
\end{align*}
\]
Comparing the coefficients of \( x^t \), we obtain
\[
f[S'] - f[S''] = (b - a)f[S].
\]

**Proof of Theorem 12.** (a) By Definition 10, we have
\[
f_t = f[S].
\]
Apply Lemma 11(b) to the right-hand side repeatedly as long as possible. At the end, we arrive at a linear combination of some terms of the form \( f[M] \) where \( M = M_1 \times \cdots \times M_n \subset S \)
such that each $M_i$ consist of a single element $s_i$ with some multiplicity $u_i + 1 \leq m_i(s_i)$. By Lemma 11(a), we have $f[M] = f_u(s)$.

(b) Suppose that there exist two different systems of constants, $(\alpha_{u}^{(s)})$ and $(\alpha_{u}^{(s)})'$ which have the properties described in part (a). Taking the differences, $\delta_u^{(s)} = \alpha_u^{(s)} - \alpha_u^{(s)}'$ we have

$$\sum_{s \in S} \sum_{u < m(s)} \delta_u^{(s)} f_u(s) = 0$$

for all polynomials $f \in \mathbb{F}[x]$, with $\deg f \leq t_1 + \cdots + t_n$.

Since the systems $(\alpha_u^{(s)})$ and $(\alpha_u^{(s)})'$ are different, there exists some $\delta_u^{(s)}$ which is not 0. Take such a $\delta_u^{(s)}$ where the vector $u$ is maximal. Apply (8) to the polynomial

$$f(x) = \prod_{i=1}^{n} \left( (x_i - s_i)^{u_i} \prod_{r \in S \setminus \{s_i\}} (x_i - r)^{m_i(r)} \right).$$

Then, on the left-hand side of (8), since $f_{u'}(s) = 0$ unless $u' \geq u$, we see that $\delta_u^{(s)} f_u(s)$ is the only nonzero term, giving a contradiction.

(c) Fix $s$ and $u = m(s) - 1$. Again, apply Lemma 11(b) repeatedly to compute $f[S]$. Whenever we have some different $s_i$ and $b$ in $S_i$, apply Lemma 11(b) to that pair. This way the term $f_u(s)$ is obtained only once, and with a nonzero coefficient. In fact, we obtain that

$$\alpha_u^{(s)} = \prod_{i=1}^{n} \prod_{s \in S \setminus \{s_i\}} \frac{1}{(s - s_i)^{m(s)}}.$$

\[\square\]

Alternative proof of Theorem 6 If $d(S_i) > t_i + 1$ for some $i$, then we can remove an element from $S_i$ (or decrease its multiplicity). So we can assume that $d(S_i) = t_i + 1$ for every $i$.

Apply Theorem 6. On the left-hand side of (7), the coefficient $f_t$ is not zero. Hence, at least one of the values $f_u(s)$ is different from zero. \[\square\]

3 Applications

Some of the known applications of Alon’s nonvanishing theorem can be extended to multisets. Typically we found that the original argument can be modified to allow higher multiplicities.

3.1 Covering cubes

We can extend a result of Alon and Füredi [3] on the covering of a discrete cube by hyperplanes in the following way.

Theorem 12. Let $(S_1, m_1), \ldots, (S_n, m_n)$ be finite multisets from the field $\mathbb{F}$. Suppose that $0 \in S_i$, with $m_i(0) = 1$ for every $i$, and $H_1, \ldots, H_k$ are hyperplanes in $\mathbb{F}^n$ such that every point $s \in S \setminus \{0\}$ is covered by at least $|m(s)| - n + 1$ hyperplanes and the point 0 is not covered by any of the hyperplanes. Then $k \geq d(S_1) + d(S_2) + \cdots + d(S_n) - n$. 

We give three proofs. The first of them is essentially the original proof of Alon and Füredi (see [3, 2]), adapted to the multiple point setting. The second proof uses Theorem 9 directly. The last one is a quite straightforward application of the generalized Ball-Serra theorem.

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

Let
\[
P(x) = \prod_{i=1}^{n} \prod_{s \in S_i \setminus \{0\}} (x_i - s)^{m_i(s)}
\]
and
\[
F(x) = P(x) - \frac{P(0)}{f(0)} f(x).
\]

Note that we have \( f(0) \neq 0 \), because the hyperplanes do not cover 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 6 applies for \( (S_1, m_1), \ldots, (S_n, m_n) \) and \( t_1, \ldots, t_n \): there exists a vector \( s \in S \) such that \( F \notin I(s, m(s)) \). We observe that \( s \) cannot be 0, because \( F(0) = 0 \). Thus \( s \) must have at least one nonzero coordinate, implying that
\[
P(x) \in I(s, m(s)).
\]

Moreover, as \( s \) is a nonzero vector, \( f(x) \) must vanish at \( s \) at least \( |m(s)| - n + 1 \) times, implying that \( f(x) \in I(s, m(s)) \) (expand the product at \( s \); for every term \( (x - s)^u \) obtained there will be an index \( j \) such that \( u_j \geq m_j(s_j) \)). From \( P(x), f(x) \in I(s, m(s)) \) we infer that \( F(x) \in I(s, m(s)) \). This contradiction finishes the proof.

**Remark 13.** The polynomial \( \prod_{i=1}^{n} \prod_{s \in S_i \setminus \{0\}} (x_i - s)^{m_i(s)} \) used in the preceding argument shows that the bound of the theorem is sharp for any selection of \( (S_i, m_i) \). It gives \( d(S_1) + d(S_2) + \cdots + d(S_n) - n \) hyperplanes with the required covering multiplicities.

**Second proof.** We keep the notation \( t_i = d(S_i) - 1 \). We have
\[
d(S_1) + d(S_2) + \cdots + d(S_n) - n = t_1 + \cdots + t_n.
\]

As in the first proof, let \( \ell_j(x) \) be the linear polynomial defining the hyperplane \( H_j \), and \( f(x) = \prod_{j=1}^{k} \ell_j(x) \). Our goal is to prove \( \deg f \geq t_1 + \cdots + t_n \).

Suppose that \( k = \deg f < t_1 + \cdots + t_n \). By Theorem 9 we have
\[
f_t = \sum_{s \in S} \sum_{u < m(s)} \alpha_u^{(s)} f_u(s).
\]

On the right-hand side, we have \( f_u(s) = 0 \) for all \( s \in S \setminus \{0\} \) and \( u < m(s) \).

Since the point 0 is not covered, we have \( f(0) = f_0(0) \neq 0 \) and, by Theorem 9(c), \( \alpha_0^{(0)} \neq 0 \). Therefore,
\[
f_t = \alpha_0^{(0)} \cdot f_0(0) \neq 0.
\]

But \( f_t \neq 0 \) is possible only if \( \deg f \geq t_1 + \cdots + t_n \).
Third proof. We can apply Theorem \[7\] directly with \(D_i = \{0\}, m_i(0) = 1, s^* = 0,\) and \(f(x) = k \prod_{j=1}^{k} \ell_j(x).\)

\[3.2\] The Cauchy-Davenport theorem

Let \((A, m_1)\) and \((B, m_2)\) be finite multisets in an (additively written) Abelian group \(G.\) We define
\[m_3(c) = \max \{m_1(a) + m_2(b) - 1 : a \in A, b \in B, a + b = c\}\]
the multiplicity of an element \(c \in A + B.\) This way \((A + B, m_3)\) becomes a multiset.

**Theorem 14.** Let \((A, m_1)\) and \((B, m_2)\) are multisets from the finite prime field \(\mathbb{F}_p.\) Then we have
\[d(A + B) \geq \min \{p, d(A) + d(B) - 1\}.\]

**Proof.** We shall use essentially the same polynomial as given in \[2.\] Suppose for contradiction that there exists a multiset \(C = (C, m)\) such that \(A + B \subseteq C,\) \(p > d(C),\) and \(d(C) = d(A) - 1 + d(B) - 1.\) We define
\[f(x, y) = \prod_{c \in C} (x + y - c).\]
Here we take the factor \((x + y - c)\) precisely \(m(c)\) times. We have \(f(x, y) \in \mathbb{F}_p[x, y]\) and the coefficient of \(x^{d(A)-1}y^{d(B)-1}\) is the binomial coefficient \(\binom{d(A)-1+d(B)-1}{d(A)-2},\) which is nonzero in \(\mathbb{F}_p.\) We can apply Theorem \[6\] with \(t_1 = d(A) - 1, t_2 = d(B) - 1, (S_1, m_1) = (A, m_1)\) and \((S_2, m_2) = (B, m_2).\)

There exist \(a \in A, b \in B\) and natural numbers \(k < m_1(a), l < m_2(b)\) such that in the expansion of \(f(x, y)\) at \((a, b)\) the coefficient of \((x - a)^k(y - b)^l\) is nonzero. With the choice \(c^* = a + b\) we have
\[f(x, y) = f^*(x, y)(x + y - c^*)^r\]
where \(f^* \in \mathbb{F}_p[x, y]\) and \(r \geq m_1(a) + m_2(b) - 1.\) From
\[(x + y - c^*)^r = \sum_{i=0}^{r} \binom{r}{i}(x - a)^i(y - b)^{r-i}\]
we see that \(f(x, y)\) vanishes at least \(r > k + l\) times at \((a, b),\) a contradiction proving the claim.

**Remark 15.** The Cauchy Davenport theorem can be proved without the polynomial method. Our generalization can also be verified by combining the original Cauchy Davenport inequality with an elementary argument. In fact, it is possible to prove a bit more. For a multiset \((Y, m)\) from a group we set
\[\deg(Y, m) := \sum_{y \in Y} (m(y) - 1).\]
We can prove now that
\[\deg(A + B, m_3) \geq \deg(A, m_1) + \deg(B, m_2).\]  \(9\)
If \( p \geq |A| + |B| - 1 \), then we can add to (9) the Cauchy-Davenport inequality
\[
|A + B| \geq |A| + |B| - 1
\]
which gives the inequality of Theorem 14 under a slightly milder condition on \( p \).

To prove (9), we may assume without loss of generality that \( |A| \leq |B| \). Let \( a_0 \in A \) be an element for which \( m_1(a_0) \) is maximal. Then
\[
deg(A + B, m_3) \geq \deg (a_0 + B, m_3) = \sum_{b \in B} \left( m_3(a_0 + b) - 1 \right) \geq
\]
\[
\geq \sum_{b \in B} \left( m_1(a_0) + m_2(b) - 2 \right) = |B| \cdot (m_1(a_0) - 1) + \sum_{b \in B} (m_2(b) - 1) \geq
\]
\[
\geq |A| \cdot (m_1(a_0) - 1) + \deg(B, m_2) \geq \deg(A, m_1) + \deg(B, m_2).
\]

This multiplicity argument can be extended to non Abelian groups as well. From that one can obtain an extension of Theorem 14 by using the generalized Cauchy Davenport theorem of Károlyi [15].

### 3.3 Sun’s theorem on value sets of polynomials

In [18] Z-W. Sun obtained a common generalization of the Cauchy Davenport theorem, and the theorem of Felszeghy [13] on the solvability of diagonal equations over finite fields. Here we give a version of Sun’s result which involves multiplicities. As before, the original result is the special case when every multiplicity is 1.

Consider again some nonempty finite multisets \((S_1, m_1), (S_2, m_2), \ldots, (S_n, m_n)\) from a field \( \mathbb{F} \), write \( S = S_1 \times S_2 \times \cdots \times S_n \), and let \( f(x) \in \mathbb{F}[x] \) be a polynomial. The value set
\[
f(S_1, S_2, \ldots, S_n) := \{f(s_1, \ldots, s_n); \ s_1 \in S_1, \ldots, s_n \in S_n\}
\]
can be considered as a multiset in \( \mathbb{F} \). For a \( c \in f(S_1, S_2, \ldots, S_n) \) we set
\[
m(c) := \max\{m_1(s_1) + \cdots + m_n(s_n) - n + 1; \ s \in S, \ f(s) = c\}.
\]
Let \( p(\mathbb{F}) \) denote the characteristic of \( \mathbb{F} \) if it is positive, and set \( p(\mathbb{F}) = \infty \) otherwise.

**Theorem 16.** Let \( f(x) \in \mathbb{F}[x] \) be a polynomial of the form
\[
f(x) = a_1x_1^k + a_2x_2^k + \cdots + a_nx_n^k + g(x),
\]
where \( k \) is a positive integer, \( a_1, \ldots, a_n \) are nonzero elements of \( \mathbb{F} \), and \( g \in \mathbb{F}[x] \) with \( \deg g < k \). Also, let \((S_1, m_1), (S_2, m_2), \ldots, (S_n, m_n)\) be nonempty finite multisets from \( \mathbb{F} \). Then we have
\[
d(f(S_1, S_2, \ldots, S_n)) \geq \min \left\{ p(\mathbb{F}), \sum_{i=1}^{n} \left\lfloor \frac{d(S_i) - 1}{k} \right\rfloor + 1 \right\}.
\]

**Proof.** The argument is an adaptation of the one given by Felszeghy and Sun. As in [18], after possibly replacing some of the \( S_i \) by suitable multisubsets \( S_i' \subseteq S_i \), we can achieve that \( k \) divides \( d(S_i) - 1 \) for every \( i \), and that \( \sum_{i=1}^{n} (d(S_i) - 1) = k(N - 1) \) holds, where
\[
N = \min \left\{ p(\mathbb{F}), \sum_{i=1}^{n} \left\lfloor \frac{d(S_i) - 1}{k} \right\rfloor + 1 \right\}.
\]
Now put $C := f(S_1, S_2, \ldots, S_n)$, and suppose for contradiction, that $d(C) \leq N - 1$. Consider the polynomial

$$h(x) = f(x_1, \ldots, x_n)^{N-1-d(C)} \prod_{c \in C} (f(x_1, \ldots, x_n) - c).$$

Here on the right hand side the factor $f(x_1, \ldots, x_n) - c$ appears exactly $m(c)$ times. The degree of $h$ is $N - 1$, and the coefficient of the monomial $y = x_1^{d(S_1)-1} \cdots x_n^{d(S_n)-1}$ in $h(x)$ is the same as the coefficient of $y$ in

$$(a_1 x_1^k + a_2 x_2^k + \cdots + a_n x_n^k)^{N-1},$$

which is

$$\prod_{i=1}^n (f(S_i) - 1)! \cdot \frac{a_1^{(d(S_1)-1)/k} \cdots a_n^{(d(S_n)-1)/k} \neq 0.}

By Theorem 5 there exists an $s \in \mathbb{S}$ such that $h(x) \not\in I(s, m(s))$. Let $c^* = f(s_1, \ldots, s_n)$. Then $c^*$ appears in the multiset $C$ at least $m = m_1(s_1) + \cdots + m_n(s_n) - n + 1$ times, giving that the polynomial

$$h^*(x) = (f(x_1, \ldots, x_n) - c^*)^m$$

divides $h(x)$ in $\mathbb{F}[x]$. We expand $h^*(x)$ at $s$. As $f(x_1, \ldots, x_n) - c^*$ vanishes at $s$, we obtain that $h^*(x) = \sum c_j y_j$, where $c_j \in \mathbb{F}$ and the term $y_j$ is a product of at least $m$ linear factors from the set $\{x_1 - s_1, \ldots, x_n - s_n\}$. Thus, for each $j$ there exists an $i$ such that $(x_i - s_i)^{m(i)}$ divides $y_j$. We infer that $y_j \in I(s, m(s))$, hence $h^*(x) \in I(s, m(s))$ and $h(x) \in I(s, m(s))$ as well. This is a contradiction proving the claim $d(C) \geq N$.

3.4 The Eliahou-Kervaire theorem

Eliahou and Kervaire [11] proved an extension of the Cauchy-Davenport theorem to arbitrary vector spaces over finite prime fields $\mathbb{F}_p$.

A triple of integers $(r, s, n)$ satisfies the Hopf-Stiefel condition for the prime $p$ if $\binom{n}{k}$ is divisible by $p$ for every $k$ in the range $n - r < k < s$. Let $\beta_p(r, s)$ be the smallest $n$ for which $(r, s, n)$ satisfies the Hopf-Stiefel condition for $p$. We refer to Eliahou and Kervaire [12] for the properties of the generalized Hopf-Stiefel numbers $\beta_p(r, s)$.

We have the following extension of the Eliahou-Kervaire theorem to multisets. The proof follows closely the proof of Theorem 5.1 in [2].

**Theorem 17.** Let $(A, m_1)$ and $(B, m_2)$ be multisets from a (finite) vector space $V$ over the finite prime field $\mathbb{F}_p$, with $d(A) = r$ and $d(B) = s$. Then we have

$$d(A + B) \geq \beta_p(r, s).$$

**Proof.** We may identify $V$ with a finite field $\mathbb{F}$ of characteristic $p$, and view $A$ and $B$ as multisets from $\mathbb{F}$. Suppose for contradiction that $A + B$ is contained in a multiset $C = (C, m)$ such that $\beta_p(r, s) > d = d(C)$. As in the proof of Theorem 14, we define

$$f(x, y) = \prod_{c \in C} (x + y - c),$$

where the factor $(x + y - c)$ is taken $m(c)$ times.

From the definition of $\beta_p(r, s)$ it follows that there exists a $k$ with $d - r < k < s$ such that $\binom{d}{k}$ is not divisible by $p$. This implies, that the coefficient of $x^{d-k}y^k$ in $f$ is nonzero. Also,
we have \( d(A) = r > d - k \) and \( d(B) = s > k \). Theorem 6 implies that \( f \not\in I(A \times B) \). On the other hand, as in the proof of Theorem 14, from the choice of the multiset \( C \) we see that \( f \in I(A \times B) \). This contradiction proves the theorem.

References

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

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

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

[4] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[5] S. Ball, O. Serra, Punctured Combinatorial Nullstellensätze, *Combinatorica* **29** (2009), 511–522.

[6] C. de Boor, Divided differences, *Surveys in Approximation Theory* **1** (2005), 46–69.

[7] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Doctoral thesis, University of Innsbruck, 1965. *English Translation*: An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal. *Journal of Symbolic Computation* Special Issue on Logic, Mathematics, and Computer Science: Interactions. **41** (2006), 475–511.

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

[9] A. M. Cohen, H. Cuypers, H. Sterk, *Some Tapas of Computer Algebra*, Springer-Verlag, 1999.

[10] Z. Dvir, S. Kopparty, S. Saraf, M. Sudan: Extensions to the Method of Multiplicities, with applications to Kakeya Sets and Mergers, arXiv:0901.2529v2

[11] S. Eliahou, M. Kervaire, Sumsets in vector spaces over finite fields, *Journal of Number Theory* **71** (1988), 12–39.

[12] S. Eliahou, M. Kervaire, Old and new formulas for the Hopf-Stiefel and related functions, *Expositiones Mathematicae* **23** (2005), 127–145.

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

[14] B. Green, T. Tao, The distribution of polynomials over finite fields, with applications to the Gowers norms, *Contributions to Discrete Mathematics* **4** (2009), 1–36.
[15] Gy. Károlyi, Cauchy-Davenport theorem in group extensions, *L’Enseignement Mathématique* **51** (2005), 239–254.

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

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

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