

PUNCTURED COMBINATORIAL NULLSTELLENSÄTZE

SIMEON BALL^{*†}, ORIOL SERRA[†]

Received May 28, 2008

In this article we extend Alon’s Nullstellensatz to functions which have multiple zeros at the common zeros of some polynomials g_1, g_2, \dots, g_n , that are the product of linear factors. We then prove a punctured version which states, for simple zeros, that if f vanishes at nearly all, but not all, of the common zeros of $g_1(X_1), \dots, g_n(X_n)$ then every residue of f modulo the ideal generated by g_1, \dots, g_n , has a large degree.

This punctured Nullstellensatz is used to prove a blocking theorem for projective and affine geometries over an arbitrary field. This theorem has as corollaries a theorem of Alon and Füredi which gives a lower bound on the number of hyperplanes needed to cover all but one of the points of a hypercube and theorems of Bruen, Jamison and Brouwer and Schrijver which provides lower bounds on the number of points needed to block the hyperplanes of an affine space over a finite field.

1. Introduction

The Combinatorial Nullstellensatz proved by Alon in [1] has been used for a host of applications, some recent examples of which can be found in [6], [10], [11], [13] and [14]. In this article we prove two extensions of Alon’s Nullstellensatz. The first one, [Theorem 3.1](#) in [Section 3](#), is an extension which handles the multiplicities of zeros of multivariate polynomials. The

Mathematics Subject Classification (2000): 12E99, 51E21

* The first author acknowledges the support of the Ramon y Cajal programme of the Spanish Ministry of Science and Education.

† Both authors acknowledge the support of the projects MTM2005-08990-C02-01 and MTM2008-06620-C03-01 of the Spanish Ministry of Science and Education and the project 2005SGR00256 of the Catalan Research Council.

second one, [Theorem 4.1](#) in [Section 4](#), considers the punctured case in which a polynomial vanishes over almost all, but not all, of the common zeros of a family of univariate polynomials.

These two results allow us to prove a blocking theorem for projective and affine geometries over an arbitrary field, [Theorem 5.1](#) in [Section 5](#). It has as corollaries the classical result of Jamison [9] on the minimum number of points of a set blocking all hyperplanes in the affine geometry $\text{AG}(n, q)$, its extension to multiple incidences by Bruen [5] and results on almost blocking sets of the hypercube by Alon and Füredi [2]. Our blocking theorem can be illustrated by the following problem.

Consider two lines l_1 and l_2 of a projective plane over a field \mathbb{F} and finite non-intersecting subsets of points S_i of l_i . Let A be a set of points with the property that every line joining a point of S_1 to a point of S_2 is incident with a point of A . If we asked ourselves how small can A be then obviously we could simply choose A to be the smaller of the S_i and clearly we can do no better. If, however, we impose the restriction that one of the lines joining a point P_1 of S_1 to a point P_2 of S_2 is not incident with any point of A then it is not so obvious how small A can be. According to [Theorem 5.1](#) we need at least $|S_1| + |S_2| - 2$ points, which is clearly an attainable bound, for example take A to be $(S_1 \cup S_2) \setminus \{P_1, P_2\}$. [Theorem 5.1](#) generalises this bound to arbitrary dimension and to sets that have not just one point incident with the lines joining a point of S_1 to a point of S_2 , but a fixed number t of points.

2. Combinatorial Nullstellensatz

Let \mathbb{F} be a field and let f be a non-zero polynomial in $\mathbb{F}[X_1, X_2, \dots, X_n]$. Suppose that S_1, S_2, \dots, S_n are arbitrary non-empty finite subsets of \mathbb{F} and define

$$g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i).$$

Alon's Combinatorial Nullstellensatz [1, Theorem 1.1] is the following, which differs from the classical Nullstellensatz of Hilbert, see for example [7, pp. 21], in that the polynomials in Alon's version are univariate and the field is arbitrary, whereas in the classical version the polynomials are arbitrary and the field is algebraically closed.

Theorem 2.1. *If f vanishes over all the common zeros of g_1, g_2, \dots, g_n , in other words $f(s_1, s_2, \dots, s_n) = 0$ for all $s_i \in S_i$, then there are polynomials*

h_1, h_2, \dots, h_n , elements of $\mathbb{F}[X_1, X_2, \dots, X_n]$, satisfying $\deg(h_i) \leq \deg(f) - \deg(g_i)$ with the property that

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

Although not explicitly stated in his article, the following generalisation of Theorem 2.2 in [1] is easily proven. Note that under the hypothesis, there is always at least one point of the grid where f does not vanish. This corollary also incorporates Theorem 5 from Alon and Füredi [2].

Corollary 2.2. *If f has a term of maximum degree $X_1^{r_1} \cdots X_n^{r_n}$, where $r_i = |S_i| - t_i$ and $t_i \geq 1$ for all i , then a grid which contains the points of $S_1 \times \cdots \times S_n$ where f does not vanish, has size at least $t_1 \times \cdots \times t_n$.*

Proof. Suppose that there is a grid $M_1 \times \cdots \times M_n$, where $n_j = |M_j| < t_j$ for some j , containing all the points of $S_1 \times \cdots \times S_n$ where f does not vanish. Let

$$e_j(X_j) = \prod_{m \in M_j} (X_j - m).$$

The polynomial $f e_j$ is zero at all points of $S_1 \times \cdots \times S_n$ and has a term of maximum degree $X_1^{r_1} \cdots X_{j-1}^{r_{j-1}} X_j^{r_j+n_j} X_{j+1}^{r_{j+1}} \cdots X_n^{r_n}$. Note that $r_j + n_j < |S_j|$ and $r_i < |S_i|$ for $i \neq j$. By Theorem 2.1 the polynomial $f e_j = \sum_{i=1}^n g_i h_i$ for some polynomials h_i of degree at most $\deg(f) - \deg(g_i) + n_j$. Since f is not zero, the terms of maximum degree in $f e_j$ have degree in X_i at least $|S_i|$ for some i , a contradiction. ■

3. Combinatorial Nullstellensätze with multiplicity

In this section we take into account the multiplicities of the zeros of the polynomial f . The following proof of Theorem 3.1 is based on the proof of Theorem 1.3 in [5].

If $a \in \mathbb{F}^n$ is a zero of the polynomial $f \in \mathbb{F}[X_1, \dots, X_n]$ then the expansion of the polynomial $f_a(X_1, \dots, X_n) = f(X_1 + a_1, \dots, X_n + a_n)$ has no monomials of degree zero. Following Fulton [7, pp. 66] and Bruen [5], an element $a \in \mathbb{F}^n$ is a zero of multiplicity t of a non-zero polynomial $f \in \mathbb{F}[X_1, X_2, \dots, X_n]$, where t is defined to be the minimum degree of the terms that occur in $f(X_1 + a_1, X_2 + a_2, \dots, X_n + a_n)$. By convention the zero polynomial has a zero of multiplicity t at every point and for every positive integer t .

Let $T(n, t)$ be the set of all non-decreasing sequences of length t on the set $\{1, 2, \dots, n\}$. For any $\tau \in T(n, t)$, let $\tau(i)$ denote the i -th element in the sequence τ , and we write $j \in \tau$ if and only if j appears in the sequence τ .

Let \mathbb{F} be a field and let f be a polynomial in $\mathbb{F}[X_1, X_2, \dots, X_n]$. Suppose that S_1, S_2, \dots, S_n are arbitrary non-empty finite subsets of \mathbb{F} and define

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

Theorem 3.1. *If f has a zero of multiplicity t at all the common zeros of g_1, g_2, \dots, g_n then there are polynomials h_τ in $\mathbb{F}[X_1, X_2, \dots, X_n]$, satisfying $\deg(h_\tau) \leq \deg(f) - \sum_{i \in \tau} \deg(g_i)$, such that*

$$f = \sum_{\tau \in T(n, t)} g_{\tau(1)} \cdots g_{\tau(t)} h_\tau.$$

Proof. We shall prove this by double induction on n and t . If $n = 1$ and f has a zero of degree t for all $s_1 \in S_1$ then $f = g(X_1)^t h(X_1)$ for some polynomial h . If $t = 1$ then the theorem is Alon’s Nullstellensatz, [Theorem 2.1](#).

Assume that the theorem holds whenever $m < n$ and $u \leq t$ or whenever $m \leq n$ and $u < t$.

Let $\alpha \in S_n$. Write $f = (X_n - \alpha)A_\alpha + B_\alpha$, where $A_\alpha \in \mathbb{F}[X_1, X_2, \dots, X_n]$ and $B_\alpha \in \mathbb{F}[X_1, X_2, \dots, X_{n-1}]$. The polynomial B_α has a zero of multiplicity t at all elements of $S_1 \times S_2 \times \cdots \times S_{n-1}$, so by induction with $m = n - 1$

$$B_\alpha = \sum_{\tau \in T(n-1, t)} g_{\tau(1)} \cdots g_{\tau(t)} h_\tau,$$

where $\deg(h_\tau)$ is at most $\deg(f) - \sum_{i \in \tau} \deg(g_i)$.

We will show that we can write $f = g_n(X_n)A + B$ where A has degree at most $\deg(f) - \deg(g_n)$ and

$$B = \sum_{\tau \in T(n-1, t)} g_{\tau(1)} \cdots g_{\tau(t)} o_\tau,$$

where o_τ has degree at most $\deg(f) - \sum_{i \in \tau} \deg(g_i)$.

If $|S_n| = 1$ then we are done. If not then there is a $\beta \in S_n$ with $\beta \neq \alpha$. Write $A_\alpha = (X_n - \beta)A_\beta + B_\beta$, where $A_\beta \in \mathbb{F}[X_1, X_2, \dots, X_n]$ and $B_\beta \in \mathbb{F}_q[X_1, X_2, \dots, X_{n-1}]$. Again by induction with $m = n - 1$, the polynomial

$$B_\beta = \sum_{\tau \in T(n-1, t)} g_{\tau(1)}, \dots, g_{\tau(t)} l_\tau,$$

for some polynomials l_τ , where $\deg(l_\tau) \leq \deg(B_\beta) - \sum_{i \in \tau} \deg(g_i) \leq \deg(f) - 1 - \sum_{i \in \tau} \deg(g_i)$.

Thus we can write $f = (X_n - \alpha)(X_n - \beta)A_\beta + U_{\alpha\beta}$ for some

$$U_{\alpha\beta} = \sum_{\tau \in T(n-1,t)} g_{\tau(1)}, \dots, g_{\tau(t)} m_\tau,$$

where m_τ has degree at most $\deg(f) - \sum_{i \in \tau} \deg(g_i)$.

Continuing in this way for all elements of S_n we are able to write $f = g_n(X_n)A + B$ where A has degree at most $\deg(f) - \deg(g_n)$ and

$$B = \sum_{\tau \in T(n-1,t)} g_{\tau(1)}, \dots, g_{\tau(t)} o_\tau,$$

where o_τ has degree at most $\deg(f) - \sum_{i \in \tau} \deg(g_i)$.

The polynomial $g_n(X_n)A$ has a zero of multiplicity t at all points of $S_1 \times S_2 \times \dots \times S_n$ and so A has a zero of multiplicity $t - 1$ at all points of $S_1 \times S_2 \times \dots \times S_n$. By induction, with $u = t - 1$,

$$A = \sum_{\tau \in T(n,t-1)} g_{\tau(1)}, \dots, g_{\tau(t-1)} p_\tau,$$

where p_τ has degree at most $\deg(A) - \sum_{i \in \tau} \deg(g_i)$.

Therefore, f can be written in the desired way. ■

Theorem 3.1 has the following corollary.

Corollary 3.2. *Let \mathbb{F} be a field and let f be a non-zero polynomial in $\mathbb{F}[X_1, X_2, \dots, X_n]$. Let $X_1^{r_1} X_2^{r_2} \dots X_n^{r_n}$ be a term of f of maximum degree. If S_1, S_2, \dots, S_n are non-empty subsets of \mathbb{F} with the property that for all non-negative integers $\alpha_1, \dots, \alpha_n$ satisfying $\sum_{i=1}^n \alpha_i = t$, one has*

$$r_i < \alpha_i |S_i|,$$

for some i , then there is a point $a = (a_1, a_2, \dots, a_n)$, with $a_i \in S_i$, where f has a zero of multiplicity at most $t - 1$.

Proof. Suppose that f has a zero of degree at least t at all elements of $S_1 \times S_2 \times \dots \times S_n$. By **Theorem 3.1**, there are polynomials $h_\tau \in \mathbb{F}[X_1, X_2, \dots, X_n]$ with the property that

$$f = \sum_{\tau \in T} g_{\tau(1)}, \dots, g_{\tau(t)} h_\tau,$$

and h_τ has degree at most $\deg(f) - \sum_{i \in \tau} \deg(g_i)$. On the right hand side of this equality the terms of highest degree are divisible by $\prod_{i \in \tau} X_i^{|S_i|}$ for some τ . Therefore, there is a τ for which $r_i \geq \sum_{i \in \tau} |S_i|$ for all $i \in \tau$. Let α_i be the number of times i occurs in the sequence τ . The sum $\sum_{i=1}^n \alpha_i = t$ and $r_i \geq \alpha_i |S_i|$ for all i , a contradiction. ■

Note that the above corollary with $t=1$ is the original corollary to Alon’s Nullstellensatz that has proven so useful. Specifically, if $r_i < |S_i|$ for all i then there is a point (a_1, a_2, \dots, a_n) , with $a_i \in S_i$, where f does not vanish.

4. Punctured Combinatorial Nullstellensatz

In Alon’s Combinatorial Nullstellensatz, [Theorem 2.1](#), the function f was assumed to have zeros at all points of the grid $S_1 \times S_2 \times \dots \times S_n$. In the case that there is a point in $S_1 \times S_2 \times \dots \times S_n$ where f does not vanish a slightly different conclusion holds. The following can be thought of as a punctured version of Alon’s Combinatorial Nullstellensatz.

Let \mathbb{F} be a field and let f be a polynomial in $\mathbb{F}[X_1, X_2, \dots, X_n]$. For $i = 1, \dots, n$, let D_i and S_i be finite non-empty subsets of \mathbb{F} , where $D_i \subset S_i$, and define

$$g_i(X_i) = \prod_{s \in S_i} (X_i - s), \quad \text{and} \quad l_i(X_i) = \prod_{d \in D_i} (X_i - d).$$

Theorem 4.1. *If f has a zero of multiplicity at least t at all the common zeros of g_1, g_2, \dots, g_n , except at least one point of $D_1 \times D_2 \times \dots \times D_n$ where it has a zero of multiplicity less than t , then there are polynomials h_τ in $\mathbb{F}[X_1, X_2, \dots, X_n]$, satisfying $\deg(h_i) \leq \deg(f) - \sum_{i \in \tau} \deg(g_i)$, and a non-zero polynomial u satisfying $\deg(u) \leq \deg(f) - \sum_{i=1}^n (\deg(g_i) - \deg(l_i))$, such that*

$$f = \sum_{\tau \in T(n,t)} g_{\tau(1)} \cdots g_{\tau(t)} h_\tau + u \prod_{i=1}^n \frac{g_i}{l_i}.$$

Moreover, if there is a point of $D_1 \times D_2 \times \dots \times D_n$ where f is non-zero, then,

$$\deg(f) \geq (t - 1) \max_j (|S_j| - |D_j|) + \sum_{i=1}^n (|S_i| - |D_i|).$$

Proof. Let $I(n, t)$ be the ideal generated by the polynomials $\{g_{\tau(1)} \cdots g_{\tau(t)} \mid \tau \in T(n, t)\}$. We can write

$$f = \sum_{\tau \in T(n,t)} g_{\tau(1)} \cdots g_{\tau(t)} h_\tau + w,$$

where w , a polynomial in the same equivalence class as f modulo $I(n, t)$, has no terms $X_1^{r_1} \cdots X_n^{r_n}$ for which there is a $\tau \in T(n, t)$ with $r_j \geq \sum_{j \in \tau} |S_j|$ for all j .

By hypothesis, for all i , fl_i^t has zeros of multiplicity t at all common zeros of g_1, g_2, \dots, g_n and hence, so does wl_i^t . By [Theorem 3.1](#) there are polynomials v_τ with the property that

$$(4.1) \quad wl_i^t = \sum_{\tau \in T(n, t)} g_{\tau(1)} \cdots g_{\tau(t)} v_\tau.$$

However wl_i^t has no terms $X_1^{r_1} \cdots X_n^{r_n}$ for which there is a $\tau \in T(t, n)$ with $r_j \geq \sum_{j \in \tau} |S_j|$ for all j , unless $i \in \tau$. Thus

$$wl_i^t = g_i(X_i) \sum_{\tau \in T(n, t-1)} g_{\tau(1)} \cdots g_{\tau(t-1)} o_\tau,$$

for some polynomials o_τ , from which it follows that g_i divides wl_i^t for each i . However l_i divides g_i and $(g_i/l_i, l_i) = 1$, from which we deduce that g_i/l_i divides w . Thus we can write

$$f = \sum_{\tau \in T(n, t)} g_{\tau(1)} \cdots g_{\tau(t)} h_\tau + u \prod_{i=1}^n \frac{g_i}{l_i},$$

for some polynomial u , where $u \neq 0$ since f does not belong to the ideal $I(n, t)$.

To prove the lower bound on the degree of f , we will prove a lower bound on the degree of u .

Suppose that, after a suitable relabelling of the subscripts, the maximum value of $|S_j| - |D_j|$ occurs when $j = 1$.

Let (d_1, \dots, d_n) be a point of $D_1 \times \cdots \times D_n$ where f is not zero. [Equation 4.1](#) with $i = 1$ gives

$$u(X_1, d_2, \dots, d_n) l_1^t \frac{g_1}{l_1} = g_1^t v_1,$$

for some polynomial v_1 , and hence $(g_1/l_1)^{t-1}$ divides $u(X_1, d_2, \dots, d_n)$.

It only remains to show that $u(X_1, d_2, \dots, d_n)$ is not zero. This follows immediately since $f(X_1, \dots, d_n)$ is not zero at $X_1 = d_1$, it follows that $u(X_1, d_2, \dots, d_n) g_1/l_1$ is not zero and hence neither is $u(X_1, d_2, \dots, d_n)$. ■

The following corollary is a converse of the corollary to Alon's Nullstellensatz, [Corollary 2.2](#).

Corollary 4.2. *If $D_1 \times \dots \times D_n$ is a grid containing all the points of the grid $S_1 \times \dots \times S_n$ where f does not vanish and $D_i \subset S_i$ for all i , then f has a term $X_1^{r_1} \dots X_n^{r_n}$, where $|S_i| - 1 \geq r_i \geq |S_i| - |D_i|$.*

Proof. Let

$$g_i(X_i) = \prod_{s \in S_i} (X_i - s), \quad \text{and} \quad l_i(X_i) = \prod_{d \in D_i} (X_i - d).$$

By [Theorem 4.1](#) we can write

$$f = \sum_{i=1}^n h_i g_i + w,$$

and

$$w = u \prod_{i=1}^n \frac{g_i}{l_i},$$

for some non-zero polynomial u , where the degree in X_i of u is less than $|D_i|$. Therefore the degree in X_i of w is less than $|S_i|$ and at least $|S_i| - |D_i|$. ■

Note that [Corollary 4.2](#) is not the exact converse of [Corollary 2.2](#) since we cannot conclude that the term $X_1^{r_1} \dots X_n^{r_n}$ will be of maximum degree. Indeed it is easy to construct examples where f does not have such a term of maximum degree. For $i = 1, 2$ let $D_i = \{0\}$ and $S_i = \{0, 1\}$ and therefore $g_i(X_i) = X_i(X_i - 1)$. The polynomial

$$f(X_1, X_2) = X_1^2(X_1 - 1) + (X_1 - 1)(X_2 - 1)$$

is zero at all points of the grid $S_1 \times S_2$ except at the origin which is the unique point in $D_1 \times D_2$. According to [Corollary 4.2](#), the polynomial f has a term $X_1 X_2$, which is the case, but it is not a term of maximum degree.

The following corollary to [Theorem 4.1](#) is [Theorem 5](#) from [\[2\]](#).

Corollary 4.3. *Let S_1, \dots, S_n be finite non-empty subsets of \mathbb{F} and let f be a polynomial in $\mathbb{F}[X_1, \dots, X_n]$. If there is a point of $S_1 \times \dots \times S_n$ where f is not zero then there are at least $\min \prod_{i=1}^n y_i$ points of $S_1 \times \dots \times S_n$ where f is not zero, where the minimum is taken over all positive integers $y_i \leq |S_i|$ the sum of which are at least $\sum_{i=1}^n |S_i| - \deg(f)$.*

Proof. The proof is by induction on n . The result holds for $n = 1$ since a polynomial of degree m has at most m zeros.

Let D_n be the subset of S_n for which $x \in D_n$ implies $f(X_1, \dots, X_{n-1}, x) \neq 0$. Since there is a point of $S_1 \times \dots \times S_n$ where f is not zero, it follows that D_n is non-empty.

Let $x \in D_n$. By [Theorem 4.1](#) there is a polynomial w of degree at most $\deg(f) - |S_n| + |D_n|$ where $w(s_1, \dots, s_{n-1}) = f(s_1, \dots, s_{n-1}, x)$ for all $(s_1, \dots, s_{n-1}) \in S_1 \times \dots \times S_{n-1}$.

By induction there are at least $\min \prod_{i=1}^{n-1} y_i$ points of $S_1 \times \dots \times S_{n-1}$ where w is not zero, where the minimum is taken over all positive integers y_i where $y_1 + \dots + y_{n-1} \geq \sum_{i=1}^{n-1} |S_i| - \deg(w)$.

Put $y_n = |D_n|$ and use $-\deg(w) \geq |S_n| - y_n - \deg(f)$ to complete the induction. ■

5. Applications to geometry

Let \mathbb{F} be an arbitrary field and let $\text{PG}(n, \mathbb{F})$ denote the n -dimensional projective geometry over \mathbb{F} . The following theorem solves, in a more general setting, the geometrical problem mentioned in the introduction.

Theorem 5.1. *Let t be a positive integer and let l_1, l_2, \dots, l_n be n concurrent lines, all incident with the point x , spanning $\text{PG}(n, \mathbb{F})$. Let S_i be a subset of points of $l_i \setminus \{x\}$ and let D_i be a proper non-empty subset of S_i . Suppose that there is a set A of points with the property that every hyperplane $\langle s_1, s_2, \dots, s_n \rangle$ where $(s_1, \dots, s_n) \in (S_1 \times \dots \times S_n) \setminus (D_1 \times \dots \times D_n)$ is incident with at least t points of A . If there is a hyperplane $\langle d_1, d_2, \dots, d_n \rangle$, where $(d_1, \dots, d_n) \in D_1 \times \dots \times D_n$, which is incident with no point of A , then*

$$|A| \geq (t - 1) \max_j (|S_j| - |D_j|) + \sum_{i=1}^n (|S_i| - |D_i|).$$

Proof. Let H be a hyperplane that meets the lines l_i in a point of S_i but is not incident with any point of A . Apply a collineation of $\text{PG}(n, \mathbb{F})$ that takes l_1, l_2, \dots, l_n to the axes of $\text{AG}(n, \mathbb{F})$, the affine space obtained from $\text{PG}(n, \mathbb{F})$ by removing the hyperplane H , and takes the point $H \cap l_i$ to the point $\langle e_i \rangle$, where e_i is the canonical basis vector with a 1 in the i -th coordinate and zero in the others.

Thus we can then assume that H is the hyperplane defined by the equation $X_{n+1} = 0$, that A is a subset of $\text{AG}(n, \mathbb{F})$, the affine space obtained from $\text{PG}(n, \mathbb{F})$ by removing the hyperplane H , and that l_i is the line $\langle e_i, e_{n+1} \rangle$.

Let T_i be the subset of \mathbb{F} containing 0 with the property that $s^{-1} \in T_i \setminus \{0\}$ if and only if $\langle se_i + e_{n+1} \rangle$ is a point of S_i . Similarly, let E_i be the subset of \mathbb{F} containing 0 with the property that $d^{-1} \in E_i \setminus \{0\}$ if and only if $\langle de_i + e_{n+1} \rangle$

is a point of D_i . Note that $|T_i|=|S_i|$ and $|E_i|=|D_i|$. Define

$$f(X_1, X_2, \dots, X_n) = \prod_{a \in A} \left(\left(\sum_{i=1}^n a_i X_i \right) - 1 \right).$$

The affine hyperplanes $\sum_{i=1}^n t_i X_i = 1$, where $t_i \in T_i$ are not all zero, are the affine hyperplanes spanned by points s_1, s_2, \dots, s_n , where $s_i \in S_i$. By hypothesis there are t points of A incident with these hyperplanes, unless $t_i \in E_i$ for all i , and so f has a zero of multiplicity t at each point of $(T_1 \times \dots \times T_n) \setminus (E_1 \times \dots \times E_n)$. Moreover, f is not zero at the origin, which is a point of $E_1 \times \dots \times E_n$.

Theorem 4.1 implies that

$$|A| = \deg(f) \geq (t - 1) \max_j (|T_j| - |E_j|) + \sum_{i=1}^n (|T_i| - |E_i|). \quad \blacksquare$$

Note that the above proof also shows that the theorem holds for any multi-set A .

The condition that there is a hyperplane that is not incident with a point of A is essential. If we do not impose this condition then there is always an appropriate choice of τ , a sequence of length t whose elements come from $\{1, 2, \dots, n\}$, so that if we put $A = \cup_{i=1}^n S_{\tau(i)}$ then A would satisfy the hypothesis of the theorem with $D_i = \emptyset$ for all i , but

$$|A| = |S_{\tau(1)}| + \dots + |S_{\tau(t)}| < (t - 1) \max_j |S_j| + \sum_{i=1}^n |S_i|,$$

contradicting the conclusion.

For $t=1$ the bound is tight, take

$$A = \bigcup_{i=1}^n (S_i \setminus D_i).$$

Theorem 5.1 has some corollaries. The following theorem is due to Bruen [5] and together with Alon’s Nullstellensatz was the inspiration for this article. It was initially proven for $t=1$ by Jamison [9] but more pertinent here is the independent proof found by Brouwer and Schrijver [4].

If \mathbb{F} is a finite field \mathbb{F}_q we usually write $\text{PG}(n, q)$ instead of $\text{PG}(n, \mathbb{F}_q)$ and $\text{AG}(n, q)$ instead of $\text{AG}(n, \mathbb{F}_q)$.

Theorem 5.2. *If every hyperplane of $\text{AG}(n, q)$ is incident with at least t points of a set of points A , then A has at least $(n+t-1)(q-1)+1$ points.*

Proof. Let l_1, l_2, \dots, l_n be n lines of $\text{PG}(n, q)$ incident with the same point x of A and spanning $\text{PG}(n, q)$. Let H be the hyperplane of $\text{PG}(n, q)$ which is incident with no point of A and set $S_i = l_i \setminus \{x\}$ and $D_i = l_i \cap H$. [Theorem 5.1](#) implies $|A| - 1 \geq (t - 1)(q - 1) + n(q - 1)$. ■

The bound in [Theorem 5.2](#) can be improved slightly in many cases when $t \leq q$, as was proven in [3].

The following theorem is almost the dual of [Theorem 5.1](#). It is slightly easier to prove since here we fix a coordinate system.

Theorem 5.3. *Let A be a set of hyperplanes of $\text{AG}(n, \mathbb{F})$ and let D_i be a non-empty proper subset of S_i , $1 \leq i \leq n$, a finite subset of \mathbb{F} . If every point (s_1, s_2, \dots, s_n) , where $s_i \in S_i$, is incident with at least t hyperplanes of A except at least one point of $D_1 \times D_2 \times \dots \times D_n$, which is incident with no hyperplane of A , then*

$$|A| \geq (t - 1) \max_j (|S_j| - |D_j|) + \sum_{i=1}^n (|S_i| - |D_i|).$$

Proof. Define

$$f(X_1, X_2, \dots, X_n) = \prod \left(\left(\sum_{i=1}^n a_i X_i \right) - a_{n+1} \right),$$

where each factor in the product corresponds to a hyperplane, defined by the equation $\sum_{i=1}^n a_i X_i = a_{n+1}$, in A . By hypothesis the polynomial f has a zero of multiplicity t at all the points of $S_1 \times S_2 \times \dots \times S_n$ except at least one point of $D_1 \times D_2 \times \dots \times D_n$ where it is not zero. By [Theorem 4.1](#) the bound follows. ■

If $S_i = \mathbb{F}_q$ and $D_i = \{0\}$ then [Theorem 5.3](#) implies that a set of hyperplanes A with the property that every point of $\text{AG}(n, q)$, different from the origin, is incident with at least t hyperplanes of A has cardinality at least $(n + t - 1)(q - 1)$. This is the dual of [Theorem 5.2](#).

[Theorem 5.3](#) has the following immediate corollary for $t = 1$, which is due to Alon and Füredi [2].

Theorem 5.4. *Let h_1, h_2, \dots, h_n be positive integers and let G be the set whose points are (y_1, \dots, y_n) , where $y_i \in \mathbb{Z}$ and $0 \leq y_i \leq h_i$. A set of hyperplanes of $\text{AG}(n, \mathbb{R})$ which covers all but one point of G has cardinality at least $h_1 + h_2 + \dots + h_n$.*

The following is [Theorem 4](#) from [2] and follows directly from [Corollary 4.3](#).

Theorem 5.5. *Let S_1, \dots, S_n be finite non-empty subsets of \mathbb{F} . If m hyperplanes of $\text{AG}(n, \mathbb{F})$ do not cover $S_1 \times \dots \times S_n$, then they do not cover at least $\min \prod_{i=1}^n y_i$, where the minimum is taken over positive integers $y_i \leq |S_n|$ whose sum is at least $\sum_{i=1}^n |S_i| - m$.*

6. Acknowledgements

The authors would like to thank the anonymous referee for his/her careful reading of the manuscript and his/her suggestions.

References

- [1] N. ALON: Combinatorial Nullstellensatz, *Combin. Probab. Comput.* **8** (1999), 7–29.
- [2] N. ALON and Z. FÜREDI: Covering the cube by affine hyperplanes, *European J. Combin.* **14** (1993), 79–83.
- [3] S. BALL: On intersection sets in Desarguesian affine spaces, *European J. Combin.* **21** (2000), 441–446.
- [4] A. E. BROUWER and A. SCHRIJVER: The blocking number of an affine space, *J. Combin. Theory Ser. A* **24** (1978), 251–253.
- [5] A. A. BRUEN: Polynomial multiplicities over finite fields and intersection sets, *J. Combin. Theory Ser. A* **60** (1992), 19–33.
- [6] M. CÁMARA, J. MORAGAS and A. LLADÓ: On a Häggkavist’s conjecture with the polynomial method, *Electr. Notes in Discrete Math.* **29** (2007), 559–563.
- [7] W. FULTON: *Algebraic Curves*, Benjamin, 1969.
- [8] D. HEFETZ: Anti-magic graphs via the combinatorial Nullstellensatz, *J. Graph Theory* **50** (2005), 263–272.
- [9] R. JAMISON: Covering finite fields with cosets of subspaces, *J. Combin. Theory Ser. A* **22** (1977), 253–266.
- [10] GY. KÁROLYI: A compactness argument in the additive theory and the polynomial method, *Discrete Math.* **302** (2005), 124–144.
- [11] A. KÉZDY: ρ -valuations for some stunted trees, *Discrete Math.* **306** (2006), 2786–2789.
- [12] T. G. OSTROM and F. A. SHERK: Finite projective planes with affine subplanes, *Canad. Math. Bull.* **7** (1964), 549–559.
- [13] U. SCHAUZ: Colorings and orientations of matrices and graphs, *Electron. J. Combin.* **13** (2006), 12 pp.
- [14] Z-W. SUN and Y-N. YEH: On various restricted sumsets, *J. Number Theory* **114** (2005), 209–220.

Simeon Ball, Oriol Serra

Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya, Jordi Girona 1–3
Mòdul C3, Campus Nord
08034 Barcelona, Spain

simeon@ma4.upc.edu, oserra@ma4.upc.edu