PUNCTURED COMBINATORIAL NULLSTELLENSÄTZE

SIMEON BALL AND ORIOL SERRA

Abstract. In this article we present a punctured version of Alon's Nullstellensatz which states that if f vanishes at nearly all, but not all, of the common zeros of some polynomials $g_1(X_1), \ldots, g_n(X_n)$ then every I-residue of f, where the ideal $I = \langle g_1, \ldots, g_n \rangle$, has a large degree.

Furthermore, we extend Alon's Nullstellensatz to functions which have multiple zeros at the common zeros of $g_1, g_2, \ldots, g_n$ and prove a punctured version of this generalised version.

Some applications of these punctured Nullstellensätze to projective and affine geometries over an arbitrary field are considered which, in the case that the field is finite, will lead to some bounds related to linear codes containing the all one vector.

1. Introduction

The Combinatorial Nullstellensatz proved by Alon in [2] has been used for a host of applications, some recent examples of which can be found in [9], [13], [14], [16] and [17]. In this article some extensions of Alon's Nullstellensatz are proven, related to zeros of multiplicity and punctured cases in which a polynomial vanishes over almost all, but not all, of the common zeros of some uni-variate polynomials $g_1, g_2, \ldots, g_n$.

Before proving these extensions we consider a geometrical application which will be proven in a more general setting in Theorem 5.1.

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 can 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.

Date: 19 November 2007.

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 project MTM2005-08990-C02-01 of the Spanish Ministry of Science and Education and the project 2005SGR00256 of the Catalan Research Council.

Let $\mathbb{F}$ be a field and let f be a polynomial in $\mathbb{F}[X_1, X_2, \ldots, X_n]$. Suppose that $S_1, S_2, \ldots, S_n$ 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 [2, Theorem 1.1] is the following, which differs from the classical Nullstellensatz of Hilbert [10, 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 1.1. *If f vanishes over all the common zeros of $g_1, g_2, \ldots, g_n$, in other words $f(s_1, s_2, \ldots, s_n) = 0$ for all $s_i \in S_i$, then there are polynomials $h_1, h_2, \ldots, h_n \in \mathbb{F}[X_1, X_2, \ldots, X_n]$ 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 corollary 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 incorporates Theorem 5 from Alon and Füredi [3].

COROLLARY 1.2. *If $f \in \mathbb{F}[X_1, X_2, \ldots, X_n]$ has a term of maximum degree $X_1^{r_1} \ldots X_n^{r_n}$, where $r_i = |S_i| - t_i$ and $t_i \geq 1$ for all i, then a grid which contains the points of $S_1 \times \ldots \times S_n$ where f does not vanish, has size at least $t_1 \times \ldots \times t_n$.*

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

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

The polynomial fe_j is zero at all points of $S_1 \times \ldots \times S_n$ and has a term of maximum degree $X_1^{r_1} \ldots X_{j-1}^{r_{j-1}} X_j^{r_j + n_j} X_{j+1}^{r_{j+1}} \ldots X_n^{r_n}$. Note that $r_j + n_j < |S_j|$ and $r_i < |S_i|$ for $i \neq j$. By Theorem 1.1 the polynomial $fe_j = \sum_{i=1}^{n} g_i h_i$ for some polynomials h_i of degree at most $deg(f) - deg(g_i) + n_j$. The terms of maximum degree in fe_j have degree in X_i at least $|S_i|$ for some i, a contradiction. $\square$

2. PUNCTURED COMBINATORIAL NULLSTELLENSATZ

In Alon's Combinatorial Nullstellensatz, Theorem 1.1, the function f was assumed to have zeros at all points of the grid $S_1 \times S_2 \times \ldots \times S_n$. In the case that there is a point in $S_1 \times S_2 \times \ldots \times S_n$ 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 $\mathbb{F}[X_1, X_2, \ldots, X_n]$. For $i = 1, \ldots, n$, let D_i and S_i be finite non-empty subsets of $\mathbb{F}$, where $D_i \subset S_i$, and define

$$g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i), \text{ and } l_i(X_i) = \prod_{d_i \in D_i} (X_i - d_i).$$

Theorem 2.1. *If f vanishes over all the common zeros of $g_1, g_2, \dots, g_n$ except at least one element of $D_1 \times D_2 \times \dots \times D_n$, where it is not zero, then there are polynomials $h_1, h_2, \dots, h_n \in \mathbb{F}[X_1, X_2, \dots, X_n]$ satisfying $deg(h_i) \le deg(f) - deg(g_i)$ and a non-zero polynomial w, whose degree in X_i is less than $|S_i|$ and whose overall degree is at most the degree of f, with the property that*

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

and

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

for some non-zero polynomial u. In particular, $deg(f) \ge \sum_{i=1}^{n}(|S_i| - |D_i|)$.

Proof. We can write

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

for some polynomials h_i of degree at most $deg(f) - deg(g_i)$, and a polynomial w, where the degree of w in X_i is less than the degree of g_i and the overall degree of w is at most the degree of f. For each i the polynomial fl_i has zeros on all common zeros of $g_1, g_2, \dots, g_n$, by assumption, and hence so does wl_i. By Alon's Nullstellensatz there are polynomials v_i with the property that

$$wl_i = \sum_{i=1}^{n} g_i v_i.$$

However the degree of X_j in wl_i, for $j \neq i$, is less than the degree of $g_j(X_j)$ and so $wl_i = g_i v_i$. Thus g_i divides wl_i. Note that l_i divides g_i, so this divisibility implies g_i/l_i divides w. Hence

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

for some polynomial u and u is not zero since $0 \neq f(d_1, d_2, \dots, d_n) = w(d_1, d_2, \dots, d_n)$ for some $d_i \in D_i$.

Since $w \neq 0$ and $deg(f) \ge deg(w)$ we conclude that $deg(f) \ge \sum_{i=1}^{n}(|S_i| - |D_i|)$. □

The following corollary is a converse of the corollary to Alon's Nullstellensatz, Corollary 1.2.

Corollary 2.2. *If $D_1 \times \dots \times D_n$ is a grid containg all the points of the grid $S_1 \times \dots \times S_n$ where f does not vanish, then f has a term $X_1^{r_1} \dots X_n^{r_n}$, where $|S_i| - 1 \ge r_i \ge |S_i| - |D_i|$.*

Proof. Let

$$g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i), \text{ and } l_i(X_i) = \prod_{d_i \in D_i} (X_i - d_i).$$

By Theorem 2.1 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, and the degree in X_i of w is less than $|S_i|$. □

Note that Corollary 2.2 is not the exact converse of Corollary 1.2 since we cannot conlude 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 $g_i(X_1) = X_i(X_i - 1)$. 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 2.2 f has a term X_1X_2, which is the case, but it is not a term of maximum degree.

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 [8].

In the following theorem we use the term $a \in \mathbb{F}^n$ *is a zero of multiplicity* t *of a polynomial* $f \in \mathbb{F}[X_1, X_2, \dots, X_n]$. This is defined to be the maximum non-negative integer t with the property that for every term $X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ which occurs in $f(X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$ the sum $t_1 + t_2 + \dots + t_n$ is at least t.

Let T be the set of all non-decreasing sequences of length t on the set $\{1, 2, \dots, n\}$. For any $\tau \in T$, let $\tau(i)$ denote the i-th element 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

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

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*

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

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 1.1.

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 $A_\alpha \in \mathbb{F}_q[X_1, X_2, \dots, X_n]$ and $B_\alpha \in \mathbb{F}_q[X_1, X_2, \dots, X_{n-1}]$. The polynomial B_α has a zero of multilplicity of t at all elements of $S_1 \times S_2 \times \dots \times S_{n-1}$, so by induction

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

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

Let $\beta \in S_n$ with $\beta \neq \alpha$. Write $A_\alpha = (X_n - \beta)A_\beta + B_\beta$, where $A_\beta \in \mathbb{F}_q[X_1, X_2, \dots, X_n]$ and $B_\beta \in \mathbb{F}_q[X_1, X_2, \dots, X_{n-1}]$. Again by induction, 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 we can write $f = g_n(X_n)A + B$ where A has degree at most $deg(f) - deg(g_n)$ and

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

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 $S_1 \times S_2 \times \ldots \times S_n$ and so A has a zero of multiplicity $t-1$ at all points of $S_1 \times S_2 \times \ldots \times S_n$. By induction

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

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 polynomial in $\mathbb{F}[X_1, X_2, \dots, X_n]$ and suppose that f has a term $X_1^{r_1}X_2^{r_2}\dots X_n^{r_n}$ 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 $S_1 \times S_2 \times \ldots \times S_n$. 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 $(a_1, a_2, \ldots, a_n)$, with $a_i \in S_i$, where f does not vanish.

The following is a version of the punctured Nullstellensatz, Theorem 2.1, taking into account the multiplicity of the zeros of f.

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

$$g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i), \text{ and } l_i(X_i) = \prod_{d_i \in D_i} (X_i - d_i).$$

Theorem 3.3. *If f has a zero of multiplicity at least t at all the common zeros of $g_1, g_2, \ldots, g_n$, except at at least one point of $D_1 \times D_2 \times \ldots \times D_n$ where it has a zero of multiplicity less than t, then there are polynomials h_τ in $\mathbb{F}[X_1, X_2, \ldots, X_n]$, 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*

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

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

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

Proof. We can write

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

where w has no terms $X_1^{r_1} \ldots X_n^{r_n}$ for which there is a $\tau \in T$ 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 $g_1, g_2, \ldots, g_n$ and hence, so does wl_i^t. By Theorem 3.1 there are polynomials v_τ with the property that

$$wl_i^t = \sum_{\tau \in T_{t,n}} g_{\tau(1)} \ldots g_{\tau(t)} v_\tau. \tag{3.1}$$

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

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

for some polynomials o_τ, from which it follows that $g_i l_i$ divides w for each i. Thus we can write

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

for some polynomial u, where $u \not\equiv 0$ since $f \notin \langle g_{\tau(1)}, \ldots, g_{\tau(t)} \mid \tau \in T_{n,t} \rangle$.

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

Let $(d_1, \ldots, d_n)$ be a point of $D_1 \times \ldots \times D_n$ where f is not zero. Equation 3.1 with $i = 1$ gives

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

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

It only remains to show that $u(X_1, d_2, \ldots, d_n)$ is not zero. This follows immediately since $f(X_1, \ldots, d_n)$ is not zero at $X_1 = d_1$, $u(X_1, d_2, \ldots, d_n) g_1/l_1$ isn't either and hence neither is $u(X_1, d_2, \ldots, d_n)$. □

4. Applications to finite fields

The following Chevalley-Warning type theorem follows directly from Theorem 2.1.

Let $\mathbb{F}_q$ be the finite field with q elements.

Theorem 4.1. *Let $f_1, f_2, \ldots, f_m$ be polynomials of $\mathbb{F}_q[X_1, X_2, \ldots, X_n]$ and let $d = |D_1| + \ldots + |D_n|$, where D_i is the set of elements a of $\mathbb{F}_q$ where there is common zero of $f_1, f_2, \ldots, f_m$ with i-th coordinate a. If $d \neq 0$, in other words if the polynomials $f_1, f_2, \ldots, f_m$ have a common zero, then*

$$\sum_{i=1}^{m} deg(f_i) \geq \frac{nq - d}{q - 1}.$$

Proof. Define

$$f = \prod_{i=1}^{m} (1 - f_i(X_1, X_2 \ldots, X_n)^{q-1}).$$

and note that f is non-zero only when evaluated at a common zero of $f_1, f_2, \ldots, f_m$. If there is a common zero then Theorem 2.1 implies that the degree of f,

$$(q-1) \sum_{i=1}^{m} deg(f_i) \geq nq - \sum_{i=1}^{n} |D_i|.$$

□

If $d \neq 0$ then $d \geq n$ and when $d = n$ there are examples of m polynomials f_i with $\sum_{i=1}^{m} f_i = n$ with exactly one common zero. For example, take η to be non-square in $\mathbb{F}$, let $f_1 = X_1^2 - \eta X_2^2$, and for $i = 2, \ldots, n-1$ let $f_i = X_i - X_{i+1}$. The only common zero of the f_i is the origin.

5. Applications to geometry

Let $\mathbb{F}$ be an arbitrary field and let $\mathrm{PG}(n, \mathbb{F})$ denote the n-dimensional projective geometry over $\mathbb{F}$.

Theorem 5.1. *Let t be a positive integer and let $l_1, l_2, \ldots, l_n$ be n concurrent lines, all incident with the point x, spanning $PG(n, \mathbb{F})$. 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 $\langle s_1, s_2, \ldots, s_n \rangle$ where $(s_1, \ldots, s_n) \in (S_1 \times \ldots \times S_n) \setminus (D_1 \times$*

$\ldots \times D_n)$ is incident with at least t points of A. If there is a hyperplane $\langle d_1, d_2, \ldots, d_n\rangle$, where $(d_1, \ldots, d_n) \in D_1 \times \ldots \times D_n$, which is incident with no point of A, then for all j

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

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 $\mathrm{PG}(n, \mathbb{F})$ that takes $l_1, l_2, \ldots, l_n$ to the axes of $\mathrm{AG}(n, \mathbb{F})$, the affine space obtained from $\mathrm{PG}(n, \mathbb{F})$ 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.

We can then assume that A is a subset of $\mathrm{AG}(n, \mathbb{F})$, the affine space obtained from $\mathrm{PG}(n, \mathbb{F})$ by removing the hyperplane H. The hyperplane H is defined by the equation $X_{n+1} = 0$.

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. Note that the line l_i, after applying the collineation, is $\langle e_i, e_{n+1}\rangle$ and $|T_i| = |S_i|$. 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. Define

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

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 $s_1, s_2, \ldots, s_n$, 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 $(t_1, t_2, \ldots, t_n)$, unless $t_i \in E_i$ for all i.

However $0 \in E_i$ for all i and $F(0, 0, \ldots, 0) = (-1)^{|A|}$, so there is an element of $T_1 \times T_2 \times \ldots \times T_n$ where f does not vanish. Theorem 3.3 implies that for all j

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

□

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 $\{1, 2, \ldots, n\}$, so that if we put $A = \cup_{i=1}^{n} S_{\tau(i)}$ then A satisfies the hypothesis of the theorem, but

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

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 [8] and together with Alon's Nullstellensatz was the inspiration for this article. It was initially proven for $t = 1$ by Jamison [12] but more pertinent here is the independent proof found by Brouwer and Schrijver [7].

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

THEOREM 5.2. *If every hyperplane of $AG(n, q)$ 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 $\mathrm{PG}(n, q)$ incident with the same point x of A and spanning $\mathrm{PG}(n, q)$. Let H be the hyperplane 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 this theorem can be improved slightly in many cases when $t \leq q$ as was proven in [5]. In Theorem 5.7 we shall investigate when this improvement applies to the more general Theorem 5.4 below.

Firstly let us look at a consequence of Theorem 5.1 for projections.

THEOREM 5.3. *If there are $m - 1$ points $x_1, x_2, \dots, x_{m-1}$ of $PG(n, \mathbb{F})$ that project m collinear points S_1 onto m collinear points S_2 then there is a further point x_m which also projects S_1 onto S_2.*

Proof. Suppose that there is no such point x_m which also projects S_1 onto S_2. Thus there are m lines $l_1, \dots, l_m$ that join a point of S_1 to a point of S_2 but are not incident with any of the points $x_1, x_2, \dots, x_{m-1}$. The points of S_1 and S_2 are all contained in the same plane and so any two lines l_i and l_j are incident. If they are not all incident with a common point x_m then we can choose $m - 2$ points $y_1, \dots, y_{m-2}$ such that y_i is incident with l_i but is not incident with l_m and y_{m-2} is the intersection of the lines l_{m-2} and l_{m-1}. Note we may have to relabel the lines to ensure that l_m is not incident with the intersection of the lines l_{m-2} and l_{m-1}. The set $A = \{x_1, x_2, \dots, x_{m-1}, y_1, \dots, y_{m-2}\}$ has the property that every line that joins a point of S_1 to a point of S_2 is incident with a point of A except l_m, which contradicts Theorem 5.1, which says that A should have at least $|S_1| - 1 + |S_2| - 1 = 2m - 2$ points. □

In the case when $m = 3$ the nine points $S_1 \cup S_2 \cup \{x_1, x_2, x_3\}$ form an affine plane of order 3 embedded in $\mathrm{PG}(2, \mathbb{F})$. This can be proven again applying Theorem 5.1 to the dual structure. The 8 point structure, i.e. not including x_3, is referred to as the 8_3 configuration, so the above theorem says that an 8_3 configuration embedded in $\mathrm{PG}(n, \mathbb{F})$ extends to an affine plane of order three $\mathrm{AG}(2, 3)$ embedded in $\mathrm{PG}(n, \mathbb{F})$, see [1] and [15]. One can readily check with coordinates when the 8 point structure is embedded in $\mathrm{PG}(n, \mathbb{F})$, where the condition appears that this indeed occurs if and only if -3 is a square in $\mathbb{F}$ and the characteristic is not 2 or the characteristic is 2 and $\mathbb{F}$ contains a primitive third root of unity.

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

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

Proof. Define

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

where each factor in the product corresponds to a hyperplane, defined by the equation $\sum_{i=1}^{n} a_iX_i = a_{n+1}$, in A. By hypothesis the polynomial f has a zero of mutiplicity t at all the points of $S_1 \times S_2 \times \ldots \times S_n$ except at least one point of $D_1 \times D_2 \times \ldots \times D_n$ where it is not zero. By Theorem 3.3 the bound follows. □

If $S_i = \mathbb{F}_q$ and $D_i = \{0\}$ then Theorem 5.4 implies that a set of hyperplanes A with the property that every point of $\mathrm{AG}(n,q)$, different from the origin, is incident with at least t hyperplanes of A has cardinality at least $(n+t-1)(q-1)$, which dualising gives Bruen's Theorem, Theorem 5.2 again.

Theorem 5.4 has the following immediate corollaries for $t=1$, which are due to Alon and Füredi [3].

Theorem 5.5. *Let $h_1,h_2,\ldots,h_n$ be positive integers and let G be the set of points $(y_1,\ldots,y_n)$, with $0 \leq y_i \leq h_i$. A set of hyperplanes which covers all but one point of G has cardinality at least $h_1+h_2+\ldots+h_n$.*

Theorem 5.6. *Let A be a set of hyperplanes of $AG(n,\mathbb{F})$. If every point of $S_1 \times \ldots \times S_n$ is incident with a hyperplane of A, except at least one point, then there are at least $min(|\{y_1y_2\ldots y_n \mid \sum_{i=1}^{n} y_i \leq -|A|+\sum_{i=1}^{n}|S_i|, y_i < |S_i|\}|)$ points of $S_1 \times \ldots \times S_n$ incident with no hyperplane of A.*

We end this section by proving the following theorem which is similar to Theorem 5.4 but in which there are translations of the set of hyperplanes of $\mathrm{AG}(n,q)$, not incident with the origin, which also cover most, but not all, of the points of the grid $S_1 \times \ldots \times S_n$.

For any $\lambda \in \mathbb{F}^n$ and A, a finite subset of $\mathbb{F}^n$, define $A+\lambda=\{a+\lambda \mid a \in A\}$.

In the following a *punctured grid* is a set of points $(S_1\times\ldots\times S_n)\setminus(D_1\times\ldots\times D_n)$, where D_i is a proper non-empty subset of S_i, a finite subset of $\mathbb{F}$. If $(0,\ldots,0) \in D_1 \times \ldots \times D_n$ then we say that the grid is punctured at the origin. We define the *weight* of the punctured grid to be $\sum_{i=1}^{n}(|S_i|-|D_i|)$.

Theorem 5.7. *Let $\{G^\lambda \mid \lambda \in \Lambda\}$ be a set of grids, punctured at the origin, which all have the same width c and for which $c_1 = |S_1|-|D_1|$ does not depend on λ. Let A be a set of vectors with the property that every point of G^λ is incident with at least t hyperplanes defined by equations of the form*

$$b_1X_1+\ldots+b_nX_n=1,$$

for some $b \in A+\lambda$.

Let m *be minimal such that for all* $\lambda \in \Lambda$

$$\prod_{s \in S_1^\lambda \setminus D_1^\lambda} (X-s) = 1 + X^m r_\lambda(X)$$

for some polynomial r_λ*, where* G^λ *is the punctured grid* $(S_1^\lambda \times \ldots \times S_n^\lambda) \setminus (D_1^\lambda \times \ldots \times D_n^\lambda)$*.*

Let $\mu = |\{\lambda_1 \mid (\lambda_1, \ldots, \lambda_n) \in \Lambda\}|$ *and let* $\mu_A = |\{\lambda_1 \mid (\lambda_1, \ldots, \lambda_n) \in \Lambda \cap (-A)\}|$*.*

Suppose there are non-negative integers j *and* k *with the property that either*

$$k \leq j \leq \min\{t-1, m-1, \mu_A - 1\}$$

or

$$k+1 \leq j \leq \min\{t-1, m-1, \mu - 1\}.$$

If

$$\binom{c+(t-1)c_1+k}{j} \neq 0$$

then

$$|A| \geq c + (t-1)c_1 + k + 1.$$

Note that applying Theorem 5.4 to A for any of the punctured grids G^λ gives the lower bound $c+(t-1)c_1$.

Proof. Suppose that $|A| = c+(t-1)c_1+k$. Let

$$f_\lambda(X_1, X_2, \ldots, X_n) = \prod_{a \in A} \left(\left(\sum_{i=1}^n (a_i + \lambda_i) X_i \right) - 1 \right).$$

The degree of f_λ is $|A|-1+\epsilon$, where $\epsilon = 0$ if $\lambda = -a$ for some $a \in A$ and $\epsilon = 1$ if not. By hypothesis the polynomial f has a zero of mutiplicity t at all the points of $S_1 \times S_2 \times \ldots \times S_n$ except at least one point of $D_1 \times D_2 \times \ldots \times D_n$ where it is non-zero. Let

$$g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i) \text{ and } l_i(X_i) = \prod_{d_i \in D_i} (X_i - d_i).$$

By Theorem 3.3

$$f_\lambda(X_1, \ldots, X_n) = \sum_{\tau \in T} g_{\tau(1)} \ldots g_{\tau(t)} h_\tau + u_1 \prod_{i=1}^n \frac{g_i}{l_i},$$

for some polynomial u_1 of degree at most $(t-1)(|S_1|-|D_1|)+k-1+\epsilon$. Since there is a point, the origin, of $D_1 \times D_2 \times \ldots \times D_n$ where f_λ is non-zero, the polynomial u_1 is non-zero at this point. The polynomial in one variable

$$f_\lambda(X, 0, \ldots, 0) = g_1^t h + u_2 \frac{g_1}{l_1},$$

for some polynomial h and polynomial u_2 of degree at most the degree of u_1.

By hypothesis f_λ has a zero of multiplicity t at all the points $(s_1, 0, \dots, 0)$, where $s_1 \in S_1 \setminus D_1$. Therefore $f_\lambda(X, 0, \dots, 0)$ is divisible by

$$\left(\frac{g_1}{l_1}\right)^t = (1 + X^m r_\lambda(X))^t.$$

Let A_1 be the multiset where a_1 appears as an element of A_1 the number of times it appears as the first coordinate of an element of A. Thus

$$f_\lambda(X, 0, \dots, 0) = g_1^t h + u_2 \frac{g_1}{l_1},$$

can be written as

$$\prod_{a_1 \in A_1} ((a_1 + \lambda_1)X - 1) = (1 + X^m r_\lambda)^t (u_3 + h l_1^t),$$

for some polynomial u_3 of degree at most the degree of u_2 minus $(t-1)(|S_1| - |D_1|)$, which is at most $k - 1 + \epsilon$. Since $0 \in D_1$ we can write $hl_1^t = X^t h_2$ for some polynomial h_2. Thus, the coefficient of X^j in the right hand side of the equation above is zero for all j for which $k + \epsilon \leq j \leq \min\{m-1, t-1\}$. On the left-hand side of the equation above the coefficient of X^j is a polynomial in λ_1 of degree at most j where the term λ_1^j, if it appears in the polynomial, has coefficient

$$\binom{|A|}{j}.$$

If the number of λ_1 which appear as first coordinate in the vectors in Λ is more than j, then the coefficient of X^j, which is a polynomial in λ_1 of degree at most j, must be identically zero, and therefore the binomial coefficient is zero. $\square$

The following corollary is a slight generalisation of Theorem 2.2 from [5].

Corollary 5.8. *A set A of points of $AG(n, q)$ with the property that every hyperplane is incident with at least t points of A has size at least*

$$(n + t - 1)(q - 1) + k + 1$$

provided that there exists a j with the property that $k \leq j \leq \min\{t-1, q-2\}$ and

$$\binom{-n - t + k + 1}{j} \neq 0.$$

Proof. Apply Theorem 5.7 with $\Lambda = -A$, $S_i = \mathbb{F}_q$ and $D_i = \{0\}$ for all $i = 1, 2, \dots, n$. Note that for all i

$$\prod_{s \in S_i \setminus D_i} (X - s) = X^{q-1} - 1,$$

so $m = q - 1$ and that $|\{\lambda_1 \mid (\lambda_1, \dots, \lambda_n) \in \Lambda \cap (-A)\}| = |\{-a_1 \mid (a_1, \dots, a_n) \in A\}| = q$.

We conclude that if there are non-negative integers j and k with the property that $k \leq j \leq \min\{t-1, q-2\}$ and

$$\binom{(n + t - 1)(q - 1) + k}{j} = \binom{-n - t + k + 1}{j} \neq 0,$$

then

$$|A| \geq (n + t - 1)(q - 1) + k + 1.$$

□

The following corollary is from Blokhuis [6] for $(t, q) = 1$ and [4] in general.

COROLLARY 5.9. *A set of points of $AG(2, q)$ with the property that every line is incident with at least t points of A has size at least $(t + 1)q - (t, q)$.*

Proof. The binomial coefficient in the previous corollary with $n = 2$ and $j = k = t-(t, q)$ is

$$\binom{-1-(t,q)}{t-(t,q)},$$

which is non-zero by Lucas' Theorem. □

6. Applications to linear codes

The set of columns of a generator matrix of a k-dimensional linear code of length n containing the all-one vector, is a set S of n points of $\mathrm{AG}(k-1, q)$. The minimum weight of any non-zero codeword is the minimum distance d of the code. This implies that every hyperplane of $\mathrm{AG}(k - 1, q)$ is incident with at most $n - d$ points of S. Therefore the set A of points which is the complement of S is a set of $q^{k-1} - n$ points with the property that every hyperplane is incident with at least $t = q^{k-2} - (n - d)$ points of A. Thus the bounds we have proved in Corollary 5.8 and Corollary 5.9 give bounds on the length of such linear codes. For example, Corollary 5.9 has the following consequence.

Let $e = n - k + 1 - d$ be the *Singleton defect* of a k-dimensional linear code of length n and minimum distance d.

COROLLARY 6.1. *A three-dimensional linear code containing the all-one vector with Singleton defect e has length at most*

$$(e + 1)q + (e + 2, q).$$

Proof. By the comments immediately preceeding, Corollary 5.9 for $k = 3$ implies

$$q^2 - n \geq (q - n + d + 1)q - (n - d, q)$$

and hence

$$n \leq (e + 1)q + (e + 2, q).$$

□

References

[1] M. S. Abdul-Elah, M. W. Al-Dhahir and D. Jungnickel, 8_3 in $\mathrm{PG}(2, q)$, *Archiv der Mathematik*, **49** (1987), 141–150.
[2] N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.*, **8** (1999) 7–29.
[3] N. Alon and Z. Füredi, Covering the cube by affine hyperplanes, *European J. Combin.*, **14** (1993) 79–83.
[4] S. Ball, On nuclei and blocking sets in Desarguesian spaces, *J. Combin. Theory Ser. A*, **85** (1999) 232–237.
[5] S. Ball, On intersection sets in Desarguesian affine spaces, *European J. Combin.*, **21** (2000) 441–446.
[6] A. Blokhuis, On multiple nuclei and a conjecture of Lunelli and Sce, *Bull. Belg. Math. Soc. Simon Stevin*, **3** (1994) 349–353.

[7] A. E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combin. Theory Ser. A*, **24** (1978) 251–253.

[8] A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *J. Combin. Theory Ser. A*, **60** (1992) 19–33.

[9] 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.

[10] W. Fulton, *Algebraic Curves*, Benjamin, 1969.

[11] D. Hefetz, Anti-magic graphs via the combinatorial nullstellensatz, *J. Graph Theory*, **50** (2005) 263–272.

[12] R. Jamison, Covering finite fields with cosets of subspaces, *J. Combin. Theory Ser. A*, **22** (1977) 253–266.

[13] G. Károlyi, A compactness argument in the additive theory and the polynomial method, *Discrete Math.*, **302** (2005) 124–144.

[14] A. Kézdy, ρ-valuations for some stunted trees, *Discrete Math.*, **306** (2006) 2786–2789.

[15] T. G. Ostrom, F. A. Sherk, Finite projective planes with affine subplanes, *Canad. Math. Bull.*, **7** (1964) 549–559.

[16] U, Schauz, Colorings and orientations of matrices and graphs, *Electron. J. Combin.*, **13** (2006), 12pp.

[17] Z-W. Sun and Y-N. Yeh, On various restricted sumsets, *J. Number Theory*, **114** (2005) 209–220.

Simeon Ball and 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