ON ZEROS OF A POLYNOMIAL IN A FINITE GRID

ANURAG BISHNOI

Department Mathematics, Ghent University, Belgium

PETE L. CLARK

Department of Mathematics, University of Georgia, Athens, GA, USA

ADITYA POTUKUCHI[‡]

Chennai Mathematical Institute, Chennai, India

JOHN R. SCHMITT

Department of Mathematics, Middlebury College, Middlebury, VT, USA

Abstract. A 1993 result of Alon and Füredi gives a sharp upper bound on the number of zeros of a multivariate polynomial over an integral domain in a finite grid in terms of the degree of the polynomial. This result was recently generalized to polynomials over an arbitrary commutative ring, assuming a certain "Condition (D)" on the grid which holds vacuously when the ring is a domain. In the first half of this paper we give a further Generalized Alon-Füredi Theorem, which provides a sharp upper bound when the degrees of the polynomial in each variable are also taken into account. This yields in particular a new proof of Alon-Füredi. We then discuss the relationship between Alon-Füredi and results of DeMillo-Lipton, Schwartz and Zippel. A direct coding theoretic interpretation of Alon-Füredi theorem and its generalization in terms of Reed-Muller type affine variety codes is shown which gives us the minimum Hamming distance of these codes. Then we apply the Alon-Füredi Theorem to quickly recover – and sometimes strengthen – old and new results in finite geometry, including the Jamison/Brouwer-Schrijver bound on affine blocking sets. We end with a discussion of multiplicity enhancements.

E-mail addresses: anurag.2357@gmail.com, plclark@gmail.com, apotu.57@gmail.com, jschmitt@middlebury.edu.

[‡]*Present Address*: Department of Computer Science, Rutgers University, NJ, USA.

Contents

1. Introduction

1.1. **Notation.** For $n \in \mathbb{Z}^+$ we put $[n] = \{1, 2, \ldots, n\}$.

For us, rings are commutative with multiplicative identity. Throughout this paper R denotes a ring and F denotes a field, each arbitrary unless otherwise specified.

Following [Sc08] and [Cl14], a nonempty subset $S \subset R$ is said to satisfy **Condition (D)** if for all $x \neq y \in S$, the element $x - y \in R$ is not a zero divisor. A **finite grid** is a subset $A = \prod_{i=1}^n A_i$ of R^n (for some $n \in \mathbb{Z}^+$) with each A_i a finite, nonempty subset of R. We say that A satisfies Condition (D) if each A_i does.

For $N, a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}^+$, we denote by $\mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; N)$ a certain combinatorial quantity which will be defined in §2.1. When $b_1 = \cdots = b_n = 1$ we denote this quantity by $\mathfrak{m}(a_1, \ldots, a_n; N)$.

For $A \subset R^n$ and $f \in R[\underline{t}] = R[t_1, \ldots, t_n]$, we put

$$Z_A(f) = \{x \in A \mid f(x) = 0\} \text{ and } \mathcal{U}_A(f) = \{x \in A \mid f(x) \neq 0\}.$$

1.2. **The Alon-Füredi Theorem.** In [AF93] N. Alon and Z. Füredi solved a problem posed by I. Bárány (based on a result of Komjath) of finding the minimum number of hyperplanes required to cover all points of the hypercube $\{0,1\}^n \subseteq F^n$ *except one*. One such covering is given by n hyperplanes defined by the zeros of the polynomials $t_1 - 1$, $t_2 - 1$, ..., $t_n - 1$. Alon and Füredi proved that n is in fact the minimum number. They then generalised this result to all finite grids $A = \prod_{i=1}^n A_i \subset F^n$, showing that the minimum number of hyperplanes required to cover all points of A except one is $\sum_{i=1}^n (\#A_i - 1)$.

There is also a quantitative refinement: as we vary over families of d hyperplanes which do not cover all points of A, what is the minimum number of points which are missed? To answer this, Alon and Füredi proved the following result.

Theorem 1.1 (Alon-Füredi Theorem [AF93, Thm. 5])**.** *Let F be a field, let $A = \prod_{i=1}^n A_i \subset F^n$ be a finite grid, and let $f \in F[\underline{t}] = F[t_1, \ldots, t_n]$ be a polynomial which does not vanish identically on A. Then $f(x) \neq 0$ for at least $\min \prod y_i$ elements $x \in A$, where the minimum is taken over all positive integers $y_i \leq \#A_i$ with $\sum_{i=1}^n y_i = \sum_{i=1}^n \#A_i - \deg f$. More concisely (cf. §2.1)*

$$\mathcal{U}_A(f) \geq \mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - \deg f).$$

The minimum referred to in Theorem 1.1 is known in all cases – see Lemma 2.1a) – leading to an explicit form of the bound.

Several proofs of Theorem 1.1 have been given. The original argument in [AF93] involves the construction of auxiliary polynomial functions of low degree via linear algebra. A second proof was given by Ball and Serra as an application of their Punctured Combinatorial Nullstellensatz [BS09], [BS11]. Recently, López, Renterá-Márquez and Villarreal gave a proof of Alon-Füredi [LRMV14], in its coding theoretic formulation (cf. §5). Carvalho has given another proof of this result in the finite field case using results from Gröbner basis theory [Ca13, Prop. 2.3]. In [Cl15], P. L. Clark generalized the Alon-Füredi Theorem by replacing the field F by an arbitrary ring R, under the assumption that the finite grid A satisfies Condition (D). This is a modest generalization in that Condition (D) is exactly what is needed for polynomial functions on A to behave as they do in the case of a field, and the proof adapts that of Ball-Serra.

P. L. Clark, A. Forrow and J. R. Schmitt [CFS14] used Alon-Füredi to obtain a restricted variable generalization of a theorem of Warning [Wa35] giving a lower bound on the number of zeros of a system of polynomials over a finite field. (Alon-Füredi gives a lower bound on *non-zeros*, but over a finite field $\mathbb{F}_q$, we have Chevalley's trick: $f(x) = 0 \iff 1 - f(x)^{q-1} \neq 0$.) This work also gave several combinatorial applications of this lower bound on restricted variable zero sets.

One of the main goals of this paper is to revisit the Alon-Füredi Theorem and give direct combinatorial applications (i.e., not of Chevalley-Warning type). We begin by giving the following generalization of the Alon-Füredi Theorem:

Theorem 1.2 (Generalized Alon-Füredi Theorem)**.** *Let R be a ring and let $A_1, \ldots, A_n$ be non-empty finite subsets of R that satisfy Condition (D). For $i \in [n]$, let b_i be*

an integer such that $1 \leq b_i \leq \#A_i$. *Let* $f \in R[t_1, \ldots, t_n]$ *be a non-zero polynomial such that* $\deg_{t_i} f \leq \#A_i - b_i$ *for all* $i \in [n]$. *Let* $\mathcal{U}_A = \{x \in A : f(x) \neq 0\}$ *where* $A = A_1 \times \cdots \times A_n \subseteq R^n$. *Then we have (see §2.1 for the notation)*

$$\#\mathcal{U}_A \geq \mathfrak{m}(\#A_1, \ldots, \#A_n; b_1, \ldots b_n; \sum_{i=1}^{n} \#A_i - \deg f).$$

Moreover, this bound is sharp in all cases.

As we shall explain in §2.3, one recovers Theorem 1.1 from Theorem 1.2 by taking $b_1 = \ldots = b_n = 1$. Our argument specializes to give a new proof of Alon-Füredi.

In §4 we relate the Generalized Alon-Füredi Theorem to work of DeMillo-Lipton, Schwartz and Zippel. We find in particular that Alon-Füredi implies the result which has become known as the "Schwartz-Zippel Lemma". In fact, the original result of Zippel (and earlier, DeMillo-Lipton) is a bit different and not implied by Alon-Füredi (cf. Example 4.7). However, it is implied by Generalized Alon-Füredi, and this was one of our motivations for strengthening Alon-Füredi as we have.

The Alon-Füredi Theorem has a natural coding theoretic interpretation (see §5) as it computes the minimum Hamming distance of the affine grid code $\mathrm{AGC}_d(A)$, an F-linear code of length $\#A$. In this way Alon-Füredi turns out to be the restricted variable generalization of a much older result in the case $A_i = F = \mathbb{F}_q$, the Kasami-Lin-Peterson Theorem, which computes the minimum Hamming distance of generalized Reed-Muller codes. We will show that the Generalized Alon-Füredi Theorem is equivalent to the computation of the minimum Hamming distance of a more general class of R-linear codes. These generalized affine grid codes have larger distance (though also smaller dimension) than the standard ones, so they may turn out to be useful.

In §6, we pursue applications to finite geometry. We begin by revisiting and slightly sharpening the original result of Alon-Füredi on hyperplane coverings. This naturally leads us to partial covers and blocking sets in affine and projective geometries over $\mathbb{F}_q$. Applying Alon-Füredi and projective duality we get a new upper bound, Theorem 6.7, on the number of hyperplanes which do not meet a k-element subset of $AG(n, q)$. From this result the classical theorems of Jamison-Brouwer-Schrijver on affine blocking sets and Blokhuis-Brouwer on essential points of projective blocking sets follow as corollaries. We are also able to strengthen a recent result of Dodunekov, Storme and Van de Voorde.

Finally, in §7 we discuss multiplicity enhancements in the sense of [DKSS13]. The material here is most closely related to that of §4, but we have placed it at the end because it has a somewhat more technical character than the rest of the paper.

2. Preliminaries

2.1. **Balls in Prefilled Bins.** Let $a_1, \ldots, a_n \in \mathbb{Z}^+$. Consider n bins $A_1, \ldots, A_n$ such that A_i can hold up to a_i balls. For $N \in \mathbb{Z}^+$ with $n \leq N \leq \sum_{i=1}^n a_i$, we define a distribution of N balls in these n bins to be an n-tuple $y = (y_1, \ldots, y_n) \in (\mathbb{Z}^+)^n$ with $y_i \leq a_i$ for all $i \in [n]$ and $\sum_{i=1}^n y_i = N$. For a distribution y of N balls in n bins, we put $P(y) = \prod_{i=1}^n y_i$. For $n \leq N \leq \sum_{i=1}^n a_i$ we define $\mathfrak{m}(a_1, \ldots, a_n; N)$ to

be the minimum value of $P(y)$ as y ranges over all such distributions of N balls in n bins. For $N < n$ we define $\mathfrak{m}(a_1, \dots, a_n; N) = 1$.

Without loss of generality we may – and shall – assume $a_1 \geq \cdots \geq a_n$. We define the **greedy distribution** $y_G = (y_1, \dots, y_n)$ as follows: first place one ball in each bin; then place the remaining balls into bins from left to right, filling each bin completely before moving on to the next bin, until we run out of balls.

Lemma 2.1. *Let $n \in \mathbb{Z}^+$, and let $a_1 \geq \cdots \geq a_n$ be positive integers. Let $N \in \mathbb{Z}$ with $n \leq N \leq a_1 + \cdots + a_n$.*
a) We have

$$\mathfrak{m}(a_1, \dots, a_n; N) = P(y_G) = y_1 \cdots y_n.$$

b) Suppose $a_1 = \cdots = a_n = a \geq 2$. Then

$$\mathfrak{m}(a, \dots, a; N) = (r+1)a^{\lfloor \frac{N-n}{a-1} \rfloor},$$

where $r \equiv N - n \pmod{a-1}$ and $0 \leq r < a-1$.
c) For all non-negative integers k, we have

$$\mathfrak{m}(2, \dots, 2; 2n-k) = 2^{n-k}.$$

d) Let $n, a_1, \dots, a_n \in \mathbb{Z}^+$ with $a_1 \geq \cdots \geq a_n$. Let $N \in \mathbb{Z}$ be such that $N - n = \sum_{i=1}^{j}(a_i - 1) + r$ for some $j \in \{0, \dots, n\}$ and some r satisfying $0 \leq r < a_{j+1}$. Then $\mathfrak{m}(a_1, \dots, a_n; N) = (r+1)\prod_{i=1}^{j} a_i$.

Proof. Parts a) through c) are [CFS14, Lemma 2.2]. d) After placing one ball in each bin we are left with $N - n$ balls. The greedy distribution is achieved by filling the first j bins entirely and then putting r balls in bin $j+1$. □

In every distribution $y = (y_1, \dots, y_n)$ we need $y_i \geq 1$ for all $i \in [n]$; i.e., we must place at least one ball in each bin. So it is reasonable to think of the bins coming **prefilled** with one ball each, and then our task is to distribute the $N - n$ remaining balls so as to minimize $P(y)$. The concept of prefilled bins makes sense more generally: given any $b_1, \dots, b_n \in \mathbb{Z}$ with $1 \leq b_i \leq a_i$, we may consider the scenario in which the i-th bin comes prefilled with b_i balls. If $\sum_{i=1}^{n} b_i \leq N \leq \sum_{i=1}^{n} a_i$, we may restrict to distributions $y = (y_1, \dots, y_n)$ of N balls into bins of sizes $a_1, \dots, a_n$ such that $b_i \leq y_i \leq a_i$ for all $i \in [n]$ and put

$$\mathfrak{m}(a_1, \dots, a_n; b_1, \dots, b_n; N) = \min P(y),$$

where the minimum ranges over this restricted set of distributions. For $N < \sum_{i=1}^{n} b_i$ we define $\mathfrak{m}(a_1, \dots, a_n; b_1, \dots, b_n; N) := \prod_{i=1}^{n} b_i$.

Lemma 2.2. *We have $\mathfrak{m}(a_1, \dots, a_n; b_1, \dots, b_n; N) = \prod_{i=1}^{n} b_i \iff N \leq \sum_{i=1}^{n} b_i$.*

Proof. If $N \leq \sum_{i=1}^{n} b_i$ then $\mathfrak{m}(a_1, \dots, a_n; b_1, \dots, b_n; N) = \prod_{i=1}^{n} b_i$ by definition unless $N = \sum_{i=1}^{n} b_i$, and this case is immediate: we have exactly enough balls to perform the prefilling. If $N > \sum_{i=1}^{n} b_i$, then $\mathfrak{m}(a_1, \dots, a_n; b_1, \dots, b_n; N)$ is the minimum over a set of integers each of which is strictly greater than $\prod_{i=1}^{n} b_i$. □

In this prefilled context, the greedy distribution y_G is defined by starting with the bins prefilled with $b_1, \dots, b_n$ balls and then distribute the remaining balls from left to right, filling each bin completely before moving on to the next bin. One sees, e.g. by adapting the argument of [CFS14, Lemma 2.2], that

$$\mathfrak{m}(a_1, \dots, a_n; b_1, \dots, b_n; N) = P(y_G)$$

when we also have $b_1 \geq \cdots \geq b_n$. But this may not hold in general, as the following example shows.

Example 2.3. *Let $n = 2$, $a_1 = 4$, $a_2 = 3$, $b_1 = 1$, $b_2 = 2$, $N = 4$. Then $P(y_G) = 4$ but $\mathfrak{m}(4, 3; 1, 2; 4) = 3$ achieved by the distribution $(1, 3)$.*

In general, we do not know a simple description of $\mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; N)$. In practice, it can be computed using dynamic programming.

Lemma 2.4. *Let $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}^+$ with $1 \leq b_i \leq a_i$ for all $i \in [n]$. Let $k \in \mathbb{Z}$ such that $b_n \leq k \leq a_n$. If*

$$b_1 + \cdots + b_{n-1} \leq N - k \leq a_1 + \cdots + a_{n-1}$$

for some $N \in \mathbb{Z}$, then

$$k \cdot \mathfrak{m}(a_1, \ldots, a_{n-1}; b_1, \ldots, b_{n-1}; N - k) \geq \mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; N).$$

Proof. Let $y' = (y_1, \ldots, y_{n-1})$ be a distribution of $N - k$ balls in the first $n - 1$ bins. Then $y = (y_1, \ldots, y_{n-1}, k)$ is a distribution of N balls in n bins with the last bin getting k balls. Therefore,

$$\mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; N) \leq P(y) = k \cdot P(y').$$

Since this holds for all such distributions y', we get

$$\mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; N) \leq k \cdot \mathfrak{m}(a_1, \ldots, a_{n-1}; b_1, \ldots, b_{n-1}; N - k). \qquad \square$$

2.2. **Grid Reduction and Condition (D).** For any finite grid $A \subset R^n$, evaluation of a polynomial $f \in R[\underline{t}] = R[t_1, \ldots, t_n]$ at elements of A gives a ring homomorphism

$$E_A : R[\underline{t}] \to R^A, \ f \mapsto (x \in A \mapsto f(x)).$$

Let $I(A)$ be the kernel of E_A, i.e., the set of polynomials which vanish identically on A. There are some "obvious" elements of $I(A)$, namely

$$\forall i \in [n], \ \varphi_i = \prod_{x_i \in A_i} (t_i - x_i).$$

Let $\Phi = \langle \varphi_1, \ldots, \varphi_n \rangle$ be the ideal generated by these elements. Then $\Phi \subset I(A)$.

We say a polynomial $f \in R[\underline{t}]$ is **A-reduced** if $\deg_{t_i}(f) < \#A_i$ for all $i \in [n]$. The A-reduced polynomials form an R-submodule $\mathcal{R}_A$ of $R[\underline{t}]$ which is free of rank $\#A$, and the composite map

$$\mathcal{R}_A \hookrightarrow R[\underline{t}] \to R[\underline{t}]/\Phi$$

is an R-module isomorphism [Cl14, Prop. 10], i.e., every polynomial $f \in R[\underline{t}]$ differs from a unique A-reduced polynomial $r_A(f)$ by an element of Φ, and we have $E_A(f) = E_A(r_A(f))$. The polynomial $r_A(f)$ can be computed from f by dividing by φ_1, then dividing the remainder by φ_2, and so on. It follows that $\deg r_A(f) \leq \deg f$ and $\deg_{t_i} r_A(f) \leq \deg_{t_i} f$ for all $i \in [n]$.

Theorem 2.5 (CATS[1] Lemma [Ch35], [AT92], [Sc08], [Cl14, Thm. 12])**.** *The following are equivalent:*
(i) The finite grid A satisfies Condition (D).
(ii) If $f \in \mathcal{R}_A$ and $f(x) = 0$ for all $x \in A$, then $f = 0$.
(iii) We have $\Phi = I(A)$.

[1]CATS = Chevalley-Alon-Tarsi-Schauz.

Remark 2.6. *These results can be directly used to solve the main problem studied by Alon and Füredi. Let f be a polynomial that vanishes on all points of A except the point $x = (x_1, \ldots, x_n)$. Since the polynomial $\prod_{i=1}^{n} \prod_{\lambda \in A_i \setminus \{x_i\}} (t_i - \lambda)$ is A-reduced and it vanishes everywhere on A except at x, it must be equal to $r_A(f)$. Thus,*

$$\deg f \geq \deg r_A(f) = \sum_{i=1}^{n} (\#A_i - 1).$$

Now associate the set of hyperplanes that cover all points of A except one by the product of their corresponding linear polynomials.

2.3. **Generalized Alon-Füredi Implies Alon-Füredi.** Let $A = \prod_{i=1}^{n} A_i \subset R^n$ be a finite grid satisfying Condition (D), and for $i \in [n]$ put $a_i = \#A_i$. Suppose $f \in R[\underline{t}]$ does not vanish identically on A. Let

$$\mathcal{U}_A(f) = \{x \in A \mid f(x) \neq 0\}.$$

Then the Alon-Füredi Theorem is the assertion that

$$\#\mathcal{U}_A(f) \geq \mathfrak{m}(a_1, \ldots, a_n; \sum_{i=1}^{n} a_i - \deg f).$$

The nonvanishing hypothesis on f is equivalent to $r_A(f) \neq 0$. Then $r_A(f)$ satisfies the hypotheses of Theorem 1.2 with $b_1 = \cdots = b_n = 1$. Since $E_A(f) = E_A(r_A(f))$, we have $\mathcal{U}_A(f) = \mathcal{U}_A(r_A(f))$, and thus

$$\#\mathcal{U}_A(f) \geq \mathfrak{m}(a_1, \ldots, a_n; 1, \ldots, 1; \sum_{i=1}^{n} a_i - \deg r_A(f))$$

$$= \mathfrak{m}(a_1, \ldots, a_n; \sum_{i=1}^{n} a_i - \deg r_A(f)) \geq \mathfrak{m}(a_1, \ldots, a_n; \sum_{i=1}^{n} a_i - \deg f).$$

3. Proof of the Generalized Alon-Füredi Theorem

3.1. **A Preliminary Remark.** If f satisfies the hypotheses of the Generalized Alon-Füredi Theorem, then

$$\deg f \leq \sum_{i=1}^{n} \deg_{t_i} f \leq \sum_{i=1}^{n} (a_i - b_i),$$

so

$$\sum_{i=1}^{n} b_i \leq \sum_{i=1}^{n} a_i - \deg f \leq \sum_{i=1}^{n} a_i.$$

Thus, whereas the conventional Alon-Füredi setup allows the case in which we have too few balls to fill the bins – in which case the result gives the trivial (but sharp!) bound $\#\mathcal{U}_A(f) \geq 1$ –, in our setup we do not need to consider this case.

3.2. **Proof of the Generalized Alon-Füredi Bound.** For $i \in [n]$, put $a_i = \#A_i$. We go by induction on n.

Base Case: Let $f \in R[t_1]$ be a nonzero polynomial. Suppose f vanishes precisely at the distinct elements $x_1, \ldots, x_k$ of A_1. Dividing f by $t_1 - x_1$ shows $f = (t_1 - x_1) f_1(t_1)$, and – since A_1 satisfies Condition (D) – $f_1(x_i) = 0$ for $2 \leq i \leq k$. Continuing in this way we get $f = \prod_{i=1}^{k} (t_1 - x_i) f_k(t_1)$, and thus $\deg f \geq k$. So

$$\#\mathcal{U}_A(f) = a_1 - k \geq a_1 - \deg f,$$

which is the conclusion of the Generalized Alon-Füredi Theorem in this case.
Induction Step: Suppose $n \geq 2$ and the result holds for $n-1$. Write

$$f(t_1, \ldots, t_n) = \sum_{i=0}^{d_n} f_i(t_1, \ldots, t_{n-1}) t_n^i,$$

so that $d_n = \deg_{t_n} f$ is the largest index i such that $f_i \neq 0$. Moreover we have $\deg f_{d_n} \leq \deg f - d_n$ and for all $i \in [n-1], \deg_{t_i} f_{d_n} \leq \deg_{t_i} f \leq a_i - b_i$.
Put $A' = \prod_{i=1}^{n-1} A_i$. By the induction hypothesis, we have

$$\#\mathcal{U}_{A'}(f_{d_n}) \geq \mathfrak{m}(a_1, \ldots, a_{n-1}; b_1, \ldots, b_{n-1}; \sum_{i=1}^{n-1} a_i - \deg f_{d_n})$$

$$\geq \mathfrak{m}(a_1, \ldots, a_{n-1}; b_1, \ldots, b_{n-1}; \sum_{i=1}^{n-1} a_i - \deg f + d_n).$$

Let $x' = (x_1, \ldots, x_{n-1}) \in \mathcal{U}_{A'}(f_{d_n})$. Then $f(x', t_n) \in R[t_n]$ has degree $d_n \geq 0$. Since A_n satisfies Condition (D), $f(x', t_n)$ vanishes at no more than d_n points of A_n, so there are at least $a_n - d_n$ elements $x_n \in A_n$ such that $(x', x_n) \in \mathcal{U}_A$. Thus

$$\#\mathcal{U}_A \geq (a_n - d_n)\mathfrak{m}(a_1, \ldots, a_{n-1}; b_1, \ldots, b_{n-1}; \sum_{i=1}^{n-1} a_i - \deg f + d_n).$$

Since

$$\deg f \leq \sum_{i=1}^{n} \deg_{t_i} f = \sum_{i=1}^{n-1} \deg_{t_i} f + d_n$$

and thus

$$\sum_{i=1}^{n-1} b_i \leq \sum_{i=1}^{n-1} (a_i - \deg_{t_i} f) \leq \sum_{i=1}^{n-1} a_i - \deg f + d_n \leq \sum_{i=1}^{n-1} a_i,$$

we may apply Lemma 2.4 with $N = \sum_{i=1}^{n} a_i - \deg f$ and $k = a_n - d_n$, getting

$$(a_n - d_n)\mathfrak{m}(a_1, \ldots, a_{n-1}; b_1, \ldots, b_{n-1}; \sum_{i=1}^{n-1} a_i - \deg f + d_n) \geq$$

$$\mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; \sum_{i=1}^{n} a_i - \deg f).$$

We deduce that

$$\#\mathcal{U}_A \geq \mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; \sum_{i=1}^{n} a_i - \deg f).$$

3.3. **Sharpness of the Generalized Alon-Füredi Bound.** For $i \in [n]$, put $a_i = \#A_i$, and let d be an integer such that $0 \leq d \leq \sum_{i=1}^{n}(a_i - b_i)$ (cf. §3.1). For any distribution $y = (y_1, \ldots, y_n)$ of $\sum_{i=1}^{n} a_i - d$ balls in n bins with $b_i \leq y_i \leq a_i$, for all $i \in [n]$ choose a subset $S_i \subset A_i$ of cardinality $a_i - y_i$, and put[2]

$$f(t) = \prod_{i=1}^{n} \prod_{x_i \in S_i} (t_i - x_i).$$

[2]An empty product is understood to take the value 1.

Then

$$\deg f = \sum_{i=1}^{n} (a_i - y_i) = d,$$

$$\forall i \in [n],\ \deg_{t_i} f = a_i - y_i \leq a_i - b_i$$

and

$$\mathcal{U}_A(f) = P(y) = \prod_{i=1}^{n} y_i.$$

Thus, for all finite grids $A = \prod_{i=1}^{n} A_i$ satisfying Condition (D) and all permissible values of $\deg_{t_1} f, \ldots, \deg_{t_n} f$ and $\deg f$, there are instances of equality in the Generalized Alon-Füredi Bound. The case $b_1 = \cdots = b_n = 1$ yields the (known) sharpness of the Alon-Füredi Bound.

3.4. **An equivalent formulation.** Let us say that a polynomial $f \in R[\underline{t}]$ is **polylinear** (resp. **simple polylinear**) if it is a product of factors (resp. distinct factors) of the form $t_i - x$ for $x \in R$. F. Petrov has observed that the Generalized Alon-Füredi Theorem is equivalent to the statement that for any nonzero A-reduced polynomial $f \in R[\underline{t}]$, there is a simple polylinear polynomial $g \in R[\underline{t}]$ with $\deg_{t_i} f = \deg_{t_i} g$ for all $i \in [n]$, $\deg f = \deg g$ and such that $\#Z_A(f) \leq \#Z_A(g)$. Thus it is possible to formulate the result without reference to balls in prefilled bins. However, as we will see, having the result in this form is useful for applications.

4. Connections with the Schwartz-Zippel Lemma

4.1. **Schwartz-Zippel Lemma.** The material in this section is motivated by a blog post of R. Lipton [Li09] which discusses the history of the "Schwartz-Zippel Lemma". We will further weigh in on the history of this circle of results, discuss various improvements and give the connection to the Alon-Füredi Theorem.

Theorem 4.1 (Schwartz-Zippel Lemma)**.** *Let R be a domain and let $S \subset R$ be finite and nonempty. Let $f \in R[\underline{t}] = R[t_1, \ldots, t_n]$ be a nonzero polynomial. Then*

$$\#Z_{S^n}(f) \leq (\deg f)(\#S)^{n-1}. \tag{1}$$

Proof. Let $s = \#S$. The statement is equivalent to

$$\#\mathcal{U}_{S^n}(f) \geq s^{n-1}(s - \deg f).$$

If $\deg f \geq s$, then (1) asserts that f has no more zeros in S^n than the size of S^n: true. So the nontrivial case is $\deg f < s$. Then f is S^n-reduced, so

$$\#\mathcal{U}_{S^n}(f) \geq \mathfrak{m}(s, \ldots, s; ns - \deg f) = s^{n-1}(s - \deg f)$$

by Alon-Füredi and because the greedy distribution is $(s, \ldots, s, s - \deg f)$. □

The case of the Schwartz-Zippel Lemma in which $R = S = \mathbb{F}_q$ is due to O. Ore [Or22]. Thus the Schwartz-Zippel Lemma may be viewed as a "Restricted Variable Ore Theorem", although it is not the most general result along those lines. In fact, the same argument establishes the following.

Theorem 4.2 (Generalized Schwartz-Zippel Lemma)**.** *Let $A = \prod_{i=1}^n A_i \subset R^n$ be a finite grid satisfying Condition (D), and suppose $\#A_1 \geq \cdots \geq \#A_n$. Let $f \in R[\underline{t}] = R[t_1, \ldots, t_n]$ be a nonzero polynomial. Then*

$$\#Z_A(f) \leq (\deg f) \prod_{i=1}^{n-1} \#A_i.$$

Indeed, the nontrivial case of this result is precisely the case $\#A_1 \geq \cdots \geq \#A_n > \deg f$ of Alon-Füredi, and the greedy distribution is $(\#A_1, \ldots, \#A_{n-1}, \#A_n - \deg f)$.

4.2. **Schwartz's Theorem.** The Schwartz-Zippel Lemma appears in J. Schwartz's 1980 paper as a corollary of a more general upper bound on zeros of a polynomial over a domain [Sc80, Cor. 1]. We give a version over an arbitrary ring.

Theorem 4.3 (Schwartz Theorem [Sc80, Lemma 1])**.** *Let $f = f_n \in R[t_1, \ldots, t_n]$ be a nonzero polynomial and let $d_n = \deg_{t_n} f_n$. Let $f_{n-1} \in R[t_1, \ldots, t_{n-1}]$ be the coefficient of $t_n^{d_n}$ in f_n. Let $d_{n-1} = \deg_{t_{n-1}} f_{n-1}$, and let $f_{n-2} \in R[t_1, \ldots, t_{n-2}]$ be the coefficient of $t_{n-1}^{d_{n-1}}$ in f_{n-1}. Continuing in this manner we define for all $1 \leq i \leq n$ a polynomial $f_i \in R[t_1, \ldots, t_i]$ with $\deg_{t_i} f_i = d_i$. Let $A = \prod_{i=1}^n A_i$ be a finite grid satisfying Condition (D). Then*

$$\#Z_A(f) \leq \#A \sum_{i=1}^n \frac{d_i}{\#A_i}.$$

Proof. For $i \in [n]$, put $a_i = \#A_i$. We go by induction on n. The base case is the same as that of Theorem 1.2: essentially the root-factor phenomenon of high school algebra, used with some care because R need not be a domain. Inductively we suppose the result holds for polynomials in $n-1$ variables and in particular for $f_{n-1} \in R[t_1, \ldots, t_{n-1}]$ and $A' = \prod_{i=1}^{n-1} A_i$. Let $x' = (x_1, \ldots, x_{n-1}) \in A'$. If $f_{n-1}(x') = 0$, it may be the case that $f_n(x', x_n) = 0$ for all $x_n \in A_n$. But if not, then $f_n(x', t_n) \in R[t_n]$ has at most d_n zeros in A_n. Thus the number of zeros of $f = f_n$ in A is at most

$$\#A_n \cdot \#A' \left(\sum_{i=1}^{n-1} \frac{d_i}{a_i} \right) + d_n \#A' = \#A \sum_{i=1}^n \frac{d_i}{a_i}. \qquad \square$$

Proposition 4.4. *Theorem 4.3 implies Theorem 4.2.*

Proof. The coefficient of $t_1^{d_1} \cdots t_n^{d_n}$ in f is nonzero, so $\sum_{i=1}^n d_i \leq \deg f$, and thus

$$\#Z_A(f) \leq \#A \sum_{i=1}^n \frac{d_i}{\#A_i} \leq (\#A_1 \cdots \#A_{n-1}) \sum_{i=1}^n d_i \leq (\deg f) \prod_{i=1}^{n-1} \#A_i. \qquad \square$$

4.3. **DeMillo-Lipton and Zippel.** The following result was proved by R. A. DeMillo and R. Lipton in [DeML78] and then independently by R. Zippel [Zip79].

Theorem 4.5 (DeMillo-Lipton-Zippel Theorem)**.** *Let R be a domain, let $f \in R[\underline{t}] = R[t_1, \ldots, t_n]$ be a nonzero polynomial, and let $d \in \mathbb{Z}^+$ be such that $\deg_{t_i} f \leq d$ for all $i \in [n]$. Let $S \subset R$ be a nonempty set with more than d elements. Then*

$$\#Z_{S^n}(f) \leq (\#S)^n - (\#S - d)^n.$$

Proof. Put $s = \#S$. We go by induction on n, and $n = 1$ case is by now familiar. Assume the result for $n-1$. Since $\deg_{t_n} f \leq d$, we have

$$\#\{x_n \in S \mid f(t_1, \ldots, t_{n-1}, x_n) = 0\} \leq d,$$

so there are at least $s-d$ values of x_n such that $g = f(t_1, \ldots, t_{n-1}, x_n)$ is a nonzero polynomial. By induction, g has at most $s^{n-1} - (s-d)^{n-1}$ zeros on S^{n-1}. So

$$\begin{aligned}\#Z_{S^n}(f) &\leq ds^{n-1} + (s-d)(s^{n-1} - (s-d)^{n-1}) \\ &= ds^{n-1} + s^n - ds^{n-1} - (s-d)^n = s^n - (s-d)^n.\end{aligned}$$

□

Just like the Schwartz-Zippel Lemma, a stronger version of the DeMillo-Lipton-Zippel Theorem can be proved with essentially the same argument. We leave the proof – or rather this proof – to the reader.

Theorem 4.6 (Generalized DeMillo-Lipton-Zippel Theorem)**.** *Let R be a ring, $f \in R[t_1, \ldots, t_n]$ a nonzero polynomial, and for $i \in [n]$ put $d_i = \deg_{t_i} f$. Let $A = \prod_{i=1}^n A_i$ be a finite grid satisfying Condition (D). We suppose that $1 \leq d_i < a_i$ for all $i \in [n]$. Then*

$$\#\mathcal{U}_A(f) \geq \prod_{i=1}^n (\#A_i - d_i).$$

Now for a somewhat unsettling remark: the DeMillo-Lipton-Zippel Theorem does not imply the Schwartz-Zippel Lemma nor is it implied by any of Schwartz's results!

Example 4.7. *Let S be a finite subset of R containing 0, satisfying Condition (D), and of size $s \geq 3$. Let $f = t_1 t_2 \in R[t_1, t_2]$. Then we have*

$$\#Z_{S^2}(f) = 2s - 1.$$

DeMillo-Lipton-Zippel gives

$$\#Z_{S^2}(f) \leq s^2 - (s-1)^2 = 2s - 1.$$

Schwartz's Theorem gives

$$\#Z_{S^2}(f) \leq s^2 \left(\frac{1}{s} + \frac{1}{s}\right) = 2s.$$

The Alon-Füredi Theorem gives

$$\#Z_{S^2}(f) \leq s^2 - \mathfrak{m}(s, s; 2s-2) = s^2 - s(s-2) = 2s.$$

Thus neither Alon-Füredi nor Schwartz implies DeMillo-Lipton-Zippel. For the other direction, take $f = t_1 + t_2$. DeMillo-Lipton-Zippel gives $\#Z_{S^2}(f) \leq s^2 - (s-1)^2 = 2s - 1$, while the other results give $\#Z_{S^2}(f) \leq s$.

But we can still relate Schwartz-Zippel and DeMillo-Lipton-Zippel as follows.

Proposition 4.8. *The Generalized Alon-Füredi Theorem implies the Generalized DeMillo-Lipton-Zippel Theorem.*

Proof. For $i \in [n]$, put $a_i = \#A_i$ and $b_i = a_i - d_i$, so $1 \leq b_i \leq a_i$ for all $i \in [n]$. Moreover $\deg f \leq \sum_{i=1}^n d_i$, so the Generalized-Alon-Füredi Theorem gives

$$\#\mathcal{U}_A \geq \mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; \sum_{i=1}^n a_i - \deg f) \geq \mathfrak{m}(a_1 \ldots, a_n; b_1, \ldots, b_n; \sum_{i=1}^n (a_i - d_i))$$

$$= \mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; \sum_{i=1}^{n} b_i) = \prod_{i=1}^{n} b_i = \prod_{i=1}^{n} (a_i - d_i). \qquad \square$$

Generalized DeMillo-Lipton-Zippel is equivalent to the case $\deg f = \sum_{i=1}^{n} \deg_{t_i} f$ of Generalized Alon-Füredi. In particular, the bound is sharp in every case.

5. Connections with Coding Theory

In this section we make use of some terminology (only) from coding theory. Definitions can be found in e.g. [vL99, Ch. 3].

Consider the polynomial ring $\mathbb{F}_q[\underline{t}] = \mathbb{F}_q[t_1, \ldots, t_n]$. Since $\mathbb{F}_q$ is finite, we can take $\mathbb{F}_q^n$ itself as a finite grid, and in fact many aspects of the theory presented here were worked out in this case in the early part of the 20th century. In particular, we say a polynomial is **reduced** if it is $\mathbb{F}_q^n$-reduced, and this notion was introduced by Chevalley in his seminal work [Ch35] on polynomial systems of low degree. We denote the the set of reduced polynomials by $\mathcal{P}(n, q)$; it is an $\mathbb{F}_q$-vector space of dimension q^n. The evaluation map gives an $\mathbb{F}_q$-linear isomorphism

$$E : \mathcal{P}(n, q) \to \mathbb{F}_q^{\mathbb{F}_q^n}, \ f \mapsto (x \in \mathbb{F}_q^n \mapsto f(x)).$$

Fixing an ordering $\alpha_1, \ldots, \alpha_{q^n}$ of $\mathbb{F}_q^n$, this isomorphism allows us to identify each $f \in \mathcal{P}(n, q)$ with its **value table** $(f(\alpha_1), \ldots, f(\alpha_{q^n}))$. For $d \in \mathbb{N}$ we denote by $\mathcal{P}_d(n, q)$ the set of all reduced polynomials of degree at most d.

Definition The set of all value tables of all polynomials in $\mathcal{P}_d(n, q)$ is called the d-th order generalized Reed-Muller code of length q^n, denoted by $\mathrm{GRM}_d(n, q)$.

For $q = 2$, these codes were introduced and studied by D. Muller [Mu54] and I. S. Reed [Re54]. An explicit formula for minimum distance of the generalized Reed-Muller codes was given by T. Kasami, S. Lin and W. W. Peterson [KLP68], which we will recover using Alon-Füredi. A systematic study of these codes in terms of the polynomial formulation was conducted by P. Delsarte, J. M. Goethals and F. J. MacWilliams in [DGM70].

Theorem 5.1 (Kasami-Lin-Peterson)**.** *The minimum weight of the d-th order Generalized Reed-Muller code* $\mathrm{GRM}_d(n, q)$ *is equal to* $(q-b)q^{n-a-1}$ *where* $d = a(q-1)+b$ *with* $0 < b \leq q-1$.

Proof. The minimum weight of $\mathrm{GRM}_d(n, q)$ is equal to the least number of nonzero values taken by a nonzero reduced polynomial of degree at most d, which by Alon-Füredi is $\mathfrak{m}(q, \ldots, q; nq - d)$. Moreover we have

$$(nq - d) - n = n(q-1) - a(q-1) - b = (n - a - 1)(q-1) + q - 1 - b,$$

and

$$0 \leq q - 1 - b < q - 1,$$

so by Lemma 2.1 we have

$$\mathfrak{m}(q, \ldots, q; nq - d) = (q - b)q^{n-a-1}. \qquad \square$$

The Generalized Alon-Füredi Theorem can also be stated in terms of coding theory. Let $A = \prod_{i=1}^n A_i$ be a finite grid in a ring R^n satisfying Condition (D), with $a_i = \#A_i$ for $i \in [n]$. Given positive integers $b_i \leq a_i$ for all $i \in [n]$, and a natural number $d \leq \sum_{i=1}^n (a_i - b_i)$, we define the **generalized affine grid code** $\mathrm{GAGC}_d(A; b_1, \ldots, b_n)$ as the set of value tables of all polynomials $f \in R[\underline{t}]$ with $\deg_{t_i} f \leq a_i - b_i$ for all $i \in [n]$ and $\deg f \leq d$ evaluated on A. We put

$$\mathrm{AGC}_d(A) = \mathrm{GAGC}_d(A; 1, \ldots, 1)$$

and speak of **affine grid codes**. Then:

Theorem 5.2. *The minimum weight of* $\mathrm{GAGC}_d(A; b_1, \ldots, b_n)$ *is* $\mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; \sum_{i=1}^n a_i - d)$.

Affine grid codes were studied in [LRMV14] (under the name of Affine Cartesian Codes) where they proved the following:

Theorem 5.3 ([LRMV14, Thm. 3.8])**.** *Let F be a field and $A = \prod_{i=1}^n A_i \subset F^n$ a finite grid with $\#A_1 \geq \cdots \geq \#A_n \geq 1$. Then the minimum weight of* $\mathrm{AGC}_d(A)$ *is*

$$\begin{cases} \#A_1 \cdots \#A_{k-1}(\#A_k - \ell) & \text{if } d \leq \sum_{i=1}^n (\#A_i - 1) - 1 \\ 1 & \text{if } d \geq \sum_{i=1}^n (\#A_i - 1) \end{cases},$$

where $k, \ell \in \mathbb{Z}$ are such that $d = \sum_{i=k+1}^n (\#A_i - 1) + \ell$, $k \in [n]$ and $\ell \in [\#A_k - 1]$.

Proof. The minimum weight of $\mathrm{AGC}_d(A)$ is $\mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - d)$. So the result follows from Lemma 2.1, as the greedy distribution of

$$\sum_{i=1}^n \#A_i - d = \sum_{i=1}^{k-1} (\#A_i - 1) + (\#A_k - 1 - \ell) + n$$

balls is $(\#A_1, \ldots, \#A_{k-1}, \#A_k - \ell, 1, \ldots, 1)$. □

Remark 5.4. *a) The paper* [LRMV14] *makes no mention of Alon-Füredi. Their proof of Theorem 5.3 is self-contained and thus gives a proof of Alon-Füredi with the balls in bins constant replaced by its explicit value $P(y_G)$. On the other hand it is longer than the other proofs of Alon-Füredi appearing in the literature.*
b) Our proof of Theorem 5.3 works for a grid $A \subset R^n$ satisfying Condition (D).
c) When $b_1 \geq \cdots \geq b_n$, the greedy algorithm computes $\mathfrak{m}(a_1, \ldots, a_n; b_1, \ldots, b_n; N)$ and we could give a similarly explicit description of $\mathrm{GAGC}_d(A_1; b_1, \ldots, b_n)$.

6. Applications to Finite Geometry

6.1. **Partial Coverings of Grids by Hyperplanes.** By a **hyperplane** in R^n we mean a polynomial $H = c_1 t_1 + \cdots + c_n t_n + r \in R[\underline{t}]$ for which at least one c_i is not a zero-divisor. (Referring to the polynomial itself rather than its zero locus in R^n will make the discussion cleaner.) A family $\mathcal{H} = \{H_i\}_{i=1}^d$ **covers** $x \in R^n$ if $H_i(x) = 0$ for some $i \in [n]$; $\mathcal{H}$ **covers** a subset $S \subset R^n$ if it covers every point of S, and $\mathcal{H}$ **partially covers** S otherwise. For a family $\mathcal{H} = \{H_i\}_{i=1}^d$ of hyperplane in R^n, put

$$f_{\mathcal{H}} = \prod_{i=1}^d H_i.$$

Thus $f_{\mathcal{H}}$ is a polynomial of degree d. If $\mathcal{H}$ covers A, then f vanishes identically on A. If R is a domain the converse holds, and thus $\mathcal{H}$ covers A iff $f_{\mathcal{H}} \in \langle \varphi_1, \ldots, \varphi_n \rangle$. We now revisit the original combinatorial problem studied by Alon and Füredi,

which is part c) of the following theorem. However, our proof is via Theorem 1.1 instead of the approach used in [AF93].

Theorem 6.1. *Let R be a domain, let $A = \prod_{i=1}^n A_i \subset R^n$ be a finite grid, and let $\mathcal{H} = \{H_i\}_{i=1}^d$ be family of hyperplanes in R^n.*
a) If $\mathcal{H}$ partially covers A, then $\mathcal{H}$ fails to cover at least
$\mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - d)$ points of A.
b) For all $d \in \mathbb{Z}^+$, there is a family of hyperplane $\{H_i = t_{j_i} - x_i\}_{i=1}^d$ with $j_i \in [n]$ and $x_i \in A_i$ which covers all but exactly
$\mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - d)$ points of A.
c) If $\mathcal{H}$ covers all but exactly one point of A, then $d \geq \sum_{i=1}^n (\#A_i - 1)$.

Proof. a) As above, $\mathcal{H}$ covers $x \in R^n$ iff $f_{\mathcal{H}}(x) = 0$. Apply Alon-Füredi.
b) The sharpness construction of §3.3 is precisely of this form.
c) If $\mathcal{H}$ covers all points of A except one, then

$$1 = \mathcal{U}_A(H_1 \ldots H_d) \geq \mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - d),$$

so Lemma 2.2 gives $\sum_{i=1}^n \#A_i - d \leq n$, i.e. $d \geq \sum_{i=1}^n (\#A_i - 1)$. □

We complement Theorem 6.1 by computing the minimum cardinality of a hyperplane covering of a finite grid (not necessarily specifying Condition (D)) over a ring R.

Theorem 6.2. *Let $A = \prod_{i=1}^n A_i \subset R^n$ be a finite grid, and let $\mathcal{H} = \{H_i\}_{i=1}^d$ be a hyperplane covering of A. Then $d \geq \min \#A_i$.*

Proof. First we observe that if A satisfies Condition (D) then the result is almost immediate: going by contraposition, if $d \leq \#A_i - 1$ for all $i \in [n]$ then $f_{\mathcal{H}}$ is nonzero and A-reduced, so it cannot vanish identically on A.

Now we give a non-polynomial method proof in the general case. Without loss of generality assume $\#A_1 \geq \cdots \geq \cdots \geq \#A_n$. We CLAIM that any hyperplane $H = \sum_{i=1}^n c_i t_i + g$ covers at most $\prod_{i=1}^{n-1} \#A_i$ points of A: this suffices, for then $d \geq \#A_n$.
PROOF OF CLAIM: Fix $i \in [n]$ such that c_i is not a zero-divisor in R. Let $\pi : R^n \to R^{n-1}$ be the projection $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. Then

$$A = \coprod_{x' = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in \pi(A)} \{x_1\} \times \cdots \times \{x_{i-1}\} \times A_i \times \{x_{i+1}\} \times \ldots \{x_n\}$$

is a partition of A into $\#\pi(A) = \prod_{j \neq i} \#A_j$ nonempty subsets, each one of which meets H in at most one point. So

$$\#\left(Z(H) \cap A\right) \leq \prod_{j \neq i} \#A_j \leq \prod_{i=1}^{n-1} \#A_i. \qquad \square$$

Conjecture 6.3. *Let R be a ring, and let $A_1, \ldots, A_n \subset R$ be nonempty (but possibly infinite). Let $\mathcal{H} = \{H_j\}_{j \in J}$ be a covering of the grid $A = \prod_{i=1}^n A_i$ by hyperplanes. Then $\#J \geq \min_{i=1}^n \#A_i$.*

Remark 6.4. *a) For $i \in [n]$, let $B_i \subset A_i \subset R$. Then we need at least as many hyperplanes to cover $\prod_{i=1}^n A_i$ as we do to cover $\prod_{i=1}^n B_i$. Together with Theorem 6.2 it follows that in the setting of Conjecture 6.3 we need at least* $\min(\#A_i, \aleph_0)$

hyperplanes. Thus Conjecture 6.3 holds when R is countable.
b) When R is a field and $A = R^n$, Conjecture 6.3 is a case of [Cl12, Thm. 3].

6.2. **Partial Covers and Blocking Sets in Finite Geometries.** The same ideas can be used to prove old and new results about Desarguesian projective and affine spaces over finite fields.

Let $PG(n,q)$ denote the n-dimensional projective space over $\mathbb{F}_q$ (the same object would in some other circles be denoted by $\mathbb{P}^n(\mathbb{F}_q)$) and let $AG(n,q)$ denote the n-dimensional affine space over $\mathbb{F}_q$ (resp. $\mathbb{A}^n(\mathbb{F}_q)$). The set $AG(n,q)$ comes equipped with a sharply transitive action of the additive group of $\mathbb{F}_q^n$ and thus a choice of a point $x \in AG(n,q)$ induces an isomorphism $AG(n,q) \cong \mathbb{F}_q^n$. We will make such identifications without further comment.

A **partial cover** of $PG(n,q)$ is a set of hyperplanes that do not cover all the points. The points missed by a partial cover are called **holes**.

Theorem 6.5. *Let $\mathcal{H}$ be a partial cover of $PG(n,q)$ of size $k \in \mathbb{Z}^+$. Then $\mathcal{H}$ has at least $\mathfrak{m}(q,\dots,q;nq-k+1)$ holes.*

Proof. Let $H \in \mathcal{H}$. Then $PG(n,q) \setminus H \cong AG(n,q)$ so $\mathcal{H} \setminus H$ is a partial cover of $\mathbb{F}_q^n$ by $k-1$ hyperplanes. As above, there are at least $\mathfrak{m}(q,\dots,q;nq-(k-1))$ points not covered by $\mathcal{H}$. □

Corollary 6.6. *If $0 \le a < q$, a partial cover of $PG(n,q)$ of size $q+a$ has at least $q^{n-1} - aq^{n-2}$ holes.*

Proof. By Theorem 6.5 there are at least $\mathfrak{m}(q,\dots,q;(n-1)q-a+1)$ holes. Since $0 \le a < q$, the greedy distribution is $(q,\dots,q,q-a,1)$, and the result follows. □

S. Dodunekov, L. Storme and G. Van de Voorde have shown that a partial cover of $PG(n,q)$ of size $q+a$ has at least $q^{n-1} - aq^{n-2}$ holes if $0 \le a < \frac{q-2}{3}$ [DSV10, Thm. 17]. Corollary 6.6 gives an improvement in that the restriction on a is relaxed. They also show that if $a < \frac{q-2}{3}$ and the number of holes are at most q^{n-1}, then they are all contained in a single hyperplane. We cannot make any such conclusions from our arguments.

Projective duality yields a dual form of Theorem 6.5: k points in $PG(n,q)$ which do not meet all hyperplanes must miss at least $\mathfrak{m}(q,\dots,q;nq-k+1)$ of them. Thus:

Theorem 6.7. *Let S be a set of k points in $AG(n,q)$. Then there are at least $\mathfrak{m}(q,\dots,q;nq-k+1)-1$ hyperplanes of $AG(n,q)$ which do not meet S.*

Proof. Add a hyperplane at infinity to get to the setting of $PG(n,q)$ and then apply the dual form of Theorem 6.5. □

The general problem of the number of linear subspaces missed by a given set of points in $PG(n,q)$ is studied by K. Metsch in [Me06]. We wish to note that Theorem 6.7 gives the same bounds as Part a) of [Me06, Theorem 1.2] for the specific case when the linear subspaces are hyperplanes.

A **blocking set** in $AG(n,q)$ or $PG(n,q)$ is a set of points that meets every hyperplane. The union of the coordinate axes in $\mathbb{F}_q^n$ yields a blocking set in $AG(n,q)$

of size $n(q-1)+1$. J. Doyen conjectured in a 1976 Oberwolfach lecture that $n(q-1)+1$ is the least possible size of a blocking set in $AG(n,q)$. A year later two independent proofs appeared, by R. E. Jamison [Jam77], and then a (simpler) proof by A. E. Brouwer and A. Schrijver [BS78]. We are in a position to give another proof.

Corollary 6.8 (Jamison-Brouwer-Schrijver)**.** *The minimum size of a blocking set in $AG(n,q)$ is $n(q-1)+1$.*

Proof. Let $B \subset AG(n,q)$ be a blocking set of cardinality at most $n(q-1)$. By Theorem 6.7 and Lemma 2.2 there are at least

$$\mathfrak{m}(q,\dots,q;nq-n(q-1)+1)-1=\mathfrak{m}(q,\dots,q;n+1)-1\geq 1$$

hyperplanes which do not meet B. □

Turning now to $PG(n,q)$, every line is a blocking set. But classifying blocking sets that do not contain any line is one of the major open problems in finite geometry. For a survey on blocking sets in finite projective spaces, see [DBS11, Chapter 3].

If $B \subset PG(n,q)$, $x \in B$ and H is a hyperplane in $PG(n,q)$, then H **is a tangent to B through x** if $H \cap B = \{x\}$. An **essential point** of a blocking set B in $PG(n,q)$ is a point x such that $B \setminus \{x\}$ is not a blocking set. A point x of B is essential if and only if there is a tangent hyperplane to B through x.

Theorem 6.9. *Let B be a blocking set in $PG(n,q)$ and x an essential point of B. There are at least $\mathfrak{m}(q,\dots,q;nq-\#B+2)$ tangent hyperplanes to B through x.*

Proof. Let H be a tangent hyperplane to B through x. Then $B' = B \setminus \{x\} \subset PG(n,q) \setminus H \cong AG(n,q)$. By Theorem 6.7 there are at least $\mathfrak{m}(q,\dots,q;nq-\#B+2)-1$ hyperplanes in $AG(n,q)$ that do not meet B'. Since B is a blocking set all of these hyperplanes, when seen in $PG(n,q)$, must meet x. Thus there are at least $\mathfrak{m}(q,\dots,q;nq-\#B+2)$ tangent hyperplanes to B through x. □

Corollary 6.10 (Blokhuis-Brouwer [BB86])**.** *Let B be a blocking set in $PG(2,q)$ of size $2q-s$. There are at least $s+1$ tangent lines through each essential point of B.*

Proof. By Theorem 6.9, each essential point of B has at least

$$\mathfrak{m}(q,q;2q-(2q-s)+2)=\mathfrak{m}(q,q;s+2)$$

tangent lines. Since $\#B = 2q-s < q^2+q+1 = \#PG(2,q)$, there is $x \in PG(2,q)\setminus B$. There are $q+1$ lines through x, so $2q-s=\#B \geq q+1$. Thus $s+1 \leq q$, so the greedy distribution is $(s+1,1)$ and $\mathfrak{m}(q,q;s+2)=s+1$. □

Corollary 6.11. [DSV10, Theorem 7] *If $0 \leq a < q$, there are at least $q^{n-1}-aq^{n-2}$ tangent hyperplanes through each essential point of a blocking set of size $q+a+1$ in $PG(n,q)$.*

Proof. By Theorem 6.9 and the proof of Corollary 6.6, each essential point of B has at least $\mathfrak{m}(q,\dots,q;nq-(q+a+1)+2)=q^{n-1}-aq^{n-2}$ tangent hyperplanes. □

7. Multiplicity Enhancements

That one can assign to a zero of a polynomial a positive integer called **multiplicity** is a familiar concept in the univariate case. The definition of the multiplicity $m(f,x)$ of a multivariate polynomial $f \in R[\underline{t}]$ at a point $x \in R^n$ (see §7.2) may be less familiar, but the concept is no less useful. All of the main results considered thus far are upper bounds on $\#Z_A(f)$, the number of zeros of a polynomial f on a finite grid. By a **multiplicity enhancement** we mean the replacement of $\#Z_A(f)$ by $\sum_{x\in A} m(f,x)$ in such an upper bound. The prototypical example: for a nonzero univariate polynomial f over a field F we have $\sum_{x\in F} m(f,x) \leq \deg f$.

Recently, multiplicity enhancements have become part of the polynomial method toolkit. In [DKSS13] Dvir, Kopparty, Saraf and Sudan gave a multiplicity enhancement of the Schwartz-Zippel Lemma. This was a true breakthrough with important applications in both combinatorics and theoretical computer science. In §4 we saw that the original work of Schwartz, DeMillo-Lipton and Zippel consists of more than the Schwartz-Zippel Lemma and gave some extensions of this work, in particular working over an arbitrary ring. So it is natural to consider multiplicity enhancements of these results. We do so here, giving a multiplicity enhancement of Theorem 4.3 and thus also of Theorem 4.2. On the other hand the Alon-Füredi Theorem does not allow for a multiplicity enhancement (at least not in the precise sense described above), as we will see in Example 7.13.

This is a situation where working over a ring under Condition (D) makes things harder: even the univariate case is nontrivial! Lemma 7.7, which pushes through the root-factor phenomenon under Condition (D), is one of our main contributions.

In places our treatment closely follows that of [DKSS13]. We need to set things up over a ring, whereas they work over a field. Nevertheless, their work carries over verbatim much of the time, and when this is the case we state the result in the form we need it, cite the analogous result in [DKSS13] and omit the proof.

7.1. **Hasse Derivatives.** Let $R[\underline{t}] = R[t_1,\ldots,t_n]$. For $I = (i_1,\ldots,i_n) \in \mathbb{N}^n$, put

$$\underline{t}^I = t_1^{i_1}\cdots t_n^{i_n}$$

and $|I| = \sum_{j=1}^n i_j = \deg \underline{t}^I$. Thus, $\{\underline{t}^I\}_{I\in\mathbb{N}^n}$ is an R-basis for $R[\underline{t}]$. We put

$$\binom{I}{J} = \prod_{k=1}^n \binom{i_k}{j_k},$$

taking $\binom{i}{j} = 0$ if $j > i$.

For $J \in \mathbb{N}^n$, let $D^J : R[\underline{t}] \to R[\underline{t}]$ be the unique R-linear map such that

$$D^J(\underline{t}^I) = \binom{I}{J}\underline{t}^{I-J}.$$

We have $D^J(\underline{t}^I) = 0$, unless $J \leq I$. Repeated application of the identity

$$t^n = (t-x+x)^n = \sum_{j=0}^n \binom{n}{j} x^{n-j}(t-x)^j$$

leads to the Taylor expansion: for $f \in R[\underline{t}]$ and $x \in R^n$,

$$f(\underline{t}) = \sum_J D^J(f)(x)(\underline{t} - x)^J. \tag{2}$$

Applying the automorphism $\underline{t} \mapsto \underline{t} + x$ gives the alternate form

$$f(\underline{t} + x) = \sum_J D^J(f)(x)\underline{t}^J.$$

These $D^J(f)$ were defined in [Ha36] and are now called **Hasse derivatives**.

Proposition 7.1 ([DKSS13, Prop. 4]). *Let $f \in R[\underline{t}]$, and let $I, J \in \mathbb{N}^n$.*
a) If f is homogeneous of degree d, then $D^I(f)$ is homogeneous of degree $d - |I|$.
b) We have

$$D^J(D^I(f)) = \binom{I+J}{I} D^{I+J}(f).$$

7.2. **Multiplicities.**

Let $f \in R[\underline{t}]$ be nonzero and $x \in R^n$. The **multiplicity of f at x**, denoted $m(f, x)$, is the natural number m such that $D^J(f)(x) = 0$ for all J with $|J| < m$ and $D^J(f)(x) \neq 0$ for some J with $|J| = m$. We put $m(0, x) = \infty$ for all $x \in R^n$.

Lemma 7.2 ([DKSS13, Lemma 5]). *For $f \in R[\underline{t}]$, $x \in R^n$ and $I \in \mathbb{N}^n$, we have*

$$m(D^I f, x) \geq m(f, x) - |I|.$$

Given a vector $\underline{f} = (f_1, \ldots, f_k) \in R[\underline{t}]^k$, we put $m(\underline{f}, x) = \min_{1 \leq j \leq k} m(f_j, a)$.

Proposition 7.3 ([DKSS13, Prop. 6]). *Let $X_1, \ldots, X_n, Y_1, \ldots, Y_\ell$ be independent indeterminates. Let $\underline{f} = (f_1, \ldots, f_k) \in R[X_1, \ldots, X_n]^k$ and let $\underline{g} = (g_1, \ldots, g_n) \in R[Y_1, \ldots, Y_\ell]^n$. We define $\underline{f} \circ \underline{g} \in R[Y_1, \ldots, Y_\ell]^k$ to be $\underline{f}(g_1, \ldots, g_n)$.*
a) For any $a \in R^\ell$ we have

$$m(\underline{f} \circ \underline{g}, a) \geq m(\underline{f}, \underline{g}(a)) m(\underline{g} - \underline{g}(a), a).$$

b) We have

$$m(\underline{f} \circ \underline{g}, a) \geq m(\underline{f}, \underline{g}(a)).$$

Corollary 7.4 ([DKSS13, Cor. 7]). *Let $f \in R[\underline{t}]$ and let $a, b \in R^n$. Then for all $c \in R$ we have*

$$m(f(a + tb), c) \geq m(f, a + cb).$$

Lemma 7.5. *Let R be a ring, let $m, n \in \mathbb{Z}^+$, and let $f = \prod_{i=1}^m (t - x_i)$, $g = \prod_{j=1}^n (t - y_j) \in R[t]$. Suppose $x_i - y_j \in R^\times$ for all $i \neq j$. Then $\langle f, g \rangle = R[t]$.*

Proof. We have an injection of R-modules $\iota : \langle f, g \rangle \hookrightarrow R[t]$, and our task is to show that ι is surjective. By [CA, Prop. 7.12], it is enough to show that for all maximal ideals $\mathfrak{m}$ of R, $\iota_{\mathfrak{m}} : \langle f, g \rangle \otimes_R R_{\mathfrak{m}} \to R[t] \otimes_R R_{\mathfrak{m}}$ is surjective.

Thus we may assume that $(R, \mathfrak{m})$ is a local ring and $x_i - y_j \notin \mathfrak{m}$ for all $i \neq j$. Write $\overline{f}$ and $\overline{g}$ for the images of f and g in $(R/\mathfrak{m})[t]$. Since $\mathfrak{m}$ is maximal, $R/\mathfrak{m}$ is a field and $(R/\mathfrak{m})[t]$ is a PID. The condition on x_i and y_j ensures that none of the prime factors of $\overline{g}$ are associate to any of the prime factors of $\overline{f}$, so $\overline{f}$ and $\overline{g}$ are relatively prime and thus $\langle \overline{f}, \overline{g} \rangle = (R/\mathfrak{m})[t]$. Let $M = R[t]/\langle f, g \rangle$. Then M is finitely generated over the local ring R and $M/\mathfrak{m}M = (R/\mathfrak{m})[t]/\langle \overline{f}, \overline{g} \rangle = 0$. By Nakayama's Lemma (e.g. [CA, Theorem 3.38]), $M = 0$. □

Lemma 7.6. *Let R be a ring.*
a) Let $a, b, c \in R$. Suppose $a \mid bc$ and $\langle a, b\rangle = R$. Then $a \mid c$.
b) Let $a, b \in R$. If $\langle a, b\rangle = R$, then $\langle a^m, b^n\rangle = R$ for all $m, n \in \mathbb{Z}^+$.

Proof. a) Choose $x, A, B \in R$ such that $ax = bc$ and $Aa + Bb = 1$. Then

$$Bax = Bbc = (1 - Aa)c = c - Aac,$$

so

$$a(Bx + Ac) = c.$$

b) This is a special case of a standard result in ring theory [CA, Prop. 4.16]. □

Lemma 7.7. *Let R be a ring, and let $f \in R[t]$ be a polynomial of degree $d \geq 1$. Let $A = \{x_1, \ldots, x_n\} \subset R$ be a finite set satisfying Condition (D). Then*

$$\sum_{x \in A} m(f, x) \leq d.$$

Proof. We have $(t - x_i)^{m(f,x_i)} \mid f$ for all $i \in [n]$. In particular we may write

$$f(t) = (t - x_1)^{m(f,x_1)} g_1(t),$$

so $\deg f \geq m(f, x_1)$ and we are done if $n = 1$. So suppose $n \geq 2$. We may replace R by its total fraction ring and thus assume that for all $x \neq y \in A$, $x - y \in R^\times$. Lemmas 7.5 and 7.6b) then give that for all $2 \leq k \leq n$,

$$\langle \prod_{i=1}^{k-1} (t - x_i)^{m(f,x_i)},\ (t - x_k)^{m(f,x_k)} \rangle = R[t].$$

Then

$$(t - x_2)^{m(f,x_2)} \mid f(t) = (t - x_1)^{m(f,x_1)} f_1(t),$$

so by Lemma 7.6a) we may write $f_1(t) = (t - x_2)^{m(f,x_2)} f_2(t)$ and thus

$$f(t) = (t - x_1)^{m(f,x_1)} (t - x_2)^{m(f,x_2)} f_2(t),$$

so $\deg f \geq m(f, x_1) + m(f, x_2)$. Continuing in this manner we eventually get

$$\deg(f) \geq m(f, x_1) + \cdots + m(f, x_n).$$ □

Lemma 7.8 (DKSS Lemma)**.** *Let $A = \prod_{i=1}^n A_i \subset R^n$ be a finite subset satisfying Condition (D). Let $f \in R[t]$, and write*

$$f = \sum_{j=0}^{d_n} f_j(t_1, \ldots, t_{n-1}) t_n^j$$

with $f_{d_n} \neq 0$. Put $A' = \prod_{i=1}^{n-1} A_i$. For all $x' = (x_1, \ldots, x_{n-1}) \in A'$, we have

$$\sum_{x \in A_n} m(f, (x', x)) \leq (\#A_n) m(f_{d_n}, x') + d_n.$$

Proof. Choose $I' \in \mathbb{N}^{n-1}$ such that $|I'| = m(f_{d_n}, x')$ and $(D^I f_{d_n})(x') \neq 0$. Put $I = I' \times \{0\} \in \mathbb{N}^n$. Then

$$D^I f = \sum_{j=0}^{d_n} D^{I'} f_j t_n^j,$$

so $D^I f \neq 0$. By Lemma 7.2, we have

$$m(f, (x', x)) \leq |I| + m(D^I f, (x', x)) = m(f_{d_n}, x') + m(D^I f, (x', x)).$$

Apply Corollary 7.4 to $D^I f$ with $a = (x', 0)$, $b = (0, 1)$ and $c = x$: we get

$$m(D^I f, (x', x)) \leq m((D^I f)(x', t_n), x).$$

Summing over $x \in A_n$ gives

$$\sum_{x \in A_n} m(f, (x', x)) \leq (\#A_n) m(f_{d_n}, x') + \sum_{x \in A_n} m((D^I f)(x', t_n), x).$$

Since $I = I' \times \{0\}$, $(D^I f)(x', t_n)$ has degree d_n and thus Lemma 7.7 gives

$$\sum_{x \in A_n} m((D^I f)(x', t_n), x) \leq d_n.$$

The result follows. □

Remark 7.9. *The case of Lemma 7.8 in which R is a field and $A_1 = \cdots = A_n$ is due to Dvir, Kopparty, Saraf and Sudan* [DKSS13, pp. 8-9]. *Our proof follows theirs very closely, but uses Lemma 7.7 in place of the root-factor phenomenon.*

7.3. **Multiplicity Enhanced Schwartz Theorem.**

Theorem 7.10 (Multiplicity Enhanced Schwartz Theorem)**.** *Let R be a ring, let $A = \prod_{i=1}^n A_i \subset R^n$ be finite, nonempty and satisfy Condition (D), and let $f = f_n \in F[t_1, \ldots, t_n]$ be a nonzero polynomial. Let $d_n = \deg_{t_n} f$, and let $f_{n-1} \in R[t_1, \ldots, t_{n-1}]$ be the coefficient of $t_n^{d_n}$ in f_n. Let $d_{n-1} = \deg_{t_{n-1}} f_{n-1}$, and let $f_{n-2} \in R[t_1, \ldots, t_{n-2}]$ be the coefficient of $t_{n-2}^{d_{n-2}}$ in f_{n-2}. Continuing in this manner we define for all $1 \leq i \leq n$ a polynomial $f_i \in R[t_i, \ldots, t_n]$ with $\deg_{t_i} f_i = d_i$. Then*

$$\sum_{x \in A} m(f, x) \leq \#A \sum_{i=1}^n \frac{d_i}{\#A_i}.$$

Proof. By induction on n. The case $n = 1$ is Lemma 7.7. Suppose the result holds for polynomials in $n - 1$ variables. Let $A' = \prod_{i=1}^{n-1} A_i$. Applying Lemma 7.8 and then the induction hypothesis, we get

$$\sum_{x \in A} m(f, x) = \sum_{x' \in A'} \sum_{x \in A_n} m(f, (x', x)) \leq \#A_n \sum_{x' \in A'} m(f_{n-1}, x') + \#A' d_n$$

$$\leq \#A_n \#A' \sum_{i=1}^{n-1} \frac{d_i}{\#A_i} + \#A \frac{d_n}{\#A_n} = \#A \sum_{i=1}^n \frac{d_i}{\#A_i}.$$ □

Theorem 7.11 (Multiplicity Enhanced Generalized Schwartz-Zippel Lemma)**.** *Let $A = \prod_{i=1}^n A_i \subset R^n$ be a finite grid satisfying Condition (D), and suppose $\#A_1 \geq \cdots \geq \#A_n$. Let $f \in R[\underline{t}] = R[t_1, \ldots, t_n]$ be a nonzero polynomial. Then*

$$\sum_{x \in A} m(f, x) \leq \deg f \prod_{i=1}^{n-1} \#A_i.$$

Proof. This follows from Theorem 7.10 as Theorem 4.2 does from Theorem 4.3. □

Remark 7.12. *a) When R is a field, Theorem 7.10 was proved by Geil and Thomsen* [GT13, Thm. 5]. *They also build closely on* [DKSS13].
b) Unlike most of the other results presented here, Theorem 7.10 is not *claimed to be sharp in all cases. In fact, it is not always sharp, and Geil and Thomsen give significant discussion of this point including an algorithm which sometimes leads to an improved bound* [GT13, Thm. 6] *and further numerical exploration.*

7.4. **A Counterexample.** It is natural to ask whether Alon-Füredi holds in multiplicity enhanced form, i.e., whether the bound

$$\#Z_A(f) \leq \#A - \mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^{n} \#A_i - \deg f)$$

could be improved to

$$\sum_{x \in A} m(f,x) \leq \#A - \mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^{n} \#A_i - \deg f).$$

The following example shows that such an improvement does not always hold.

Example 7.13. *Let $n = 2$ and $R = A_1 = A_2 = \mathbb{F}_q$. Let $d_1, d_2 \in \mathbb{Z}^+$ be such that $d_1, d_2 < q \leq d_1 + d_2 + 1$. Then $f = t_1^{d_1} t_2^{d_2}$ is A-reduced, and we have*

$$\sum_{x \in A} m(f,x) = qd_1 + qd_2 > q^2 - 2q + d_1 + d_2 + 1 = q^2 - \mathfrak{m}(q, q; 2q - d_1 - d_2).$$

Notice that the polynomial $f = t_1^{d_1} t_2^{d_2}$ is polylinear (cf. §3.4). So far as we know it may be true that $\sum_{x \in A} m(f,x)$ is maximized among all polynomials of fixed degree when f is a polylinear polynomial. We leave this as an open problem.

References

[AF93] N. Alon and Z. Füredi, *Covering the cube by affine hyperplanes*. Eur. J. Comb. 14 (1993), 79–83.

[AT92] N. Alon and M. Tarsi *Colorings and orientations of graphs*. Combinatorica 12 (1992), 125–134.

[BS09] S. Ball and O. Serra, *Punctured combinatorial Nullstellensätze*. Combinatorica 29 (2009), 511–522.

[BS11] S. Ball and O. Serra, *Erratum: Punctured combinatorial Nullstellensätze*. Combinatorica 31 (2011), 377–378.

[BB86] A. Blokhuis and A.E. Brouwer. *Blocking sets in Desarguesian projective planes*. Bull. London Math. Soc. 18 (1986), 132–134.

[BS78] A. E. Brouwer and A. Schrijver, *The blocking number of an affine space*. J. Comb. Theory Ser. A 24 (1978), 251–253.

[Ca13] C. Carvalho, *On the second Hamming weight of some Reed-Muller type codes*. Finite Fields Appl. 24 (2013), 88–94.

[Ch35] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*. Abh. Math. Sem. Univ. Hamburg 11 (1935), 73–75.

[CA] P. L. Clark, *Commutative Algebra*, `http://math.uga.edu/~pete/integral.pdf`.

[Cl12] P. L. Clark, *Covering numbers in linear algebra* . Amer. Math. Monthly 119 (2012), 65-–67.

[Cl14] P. L. Clark, *The Combinatorial Nullstellensätze revisited*. Electronic Journal of Combinatorics. Volume 21, Issue 4 (2014). Paper #P4.15

[Cl15] P. L. Clark, *Fattening up Warning's Second Theorem*. Preprint.

[CFS14] P. L. Clark, A. Forrow and J. R. Schmitt, *Warning's Second Theorem With Restricted Variables*. To appear in Combinatorica, (2014) `http://arxiv.org/abs/1404.7793`.

[DBS11] J. De Beule, L. Storme (Eds.), *Current Research Topics in Galois Geometry*, Nova Science Publishers, 2011.

[DGM70] P. Delsarte, J.-M. Goethals, and F. J. MacWilliams, *On generalized Reed-Muller codes and their relatives*. Information and Control 16 (1970), 403–442.

[DeML78] R. A. DeMillo and R. Lipton, *A probabilistic remark on algebraic program testing*. Information Processing Letters 7 (1978), 193–195.

[DSV10] S. Dodunekov, L. Storme and G. Van de Voorde, *Partial Covers of $PG(n,q)$*. Eur. J. Comb. 31 (2010), 1611–1616.

[DKSS13] Z. Dvir, S. Kopparty, S. Saraf and M. Sudan, *Extensions to the Method of Multiplicities, with Applications to Kakeya Sets and Mergers*. SIAM J. Comput. 42 (2013), 2305–2328.

[GT13] O. Geil and C. Thomsen, *Weighted Reed-Muller codes revisited*. Des. Codes Cryptogr. 66 (2013), 195-–220.

[Ha36] H. Hasse, *Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik*. J. Reine Angew. Math. 175 (1936), 50-–54.

[Jam77] R. E. Jamison, *Covering finite fields with cosets of subspaces*. J. Comb. Theory Ser. A 22 (1977), 253–266.

[KLP68] T. Kasami, S. Lin, and W. W. Peterson, *Generalized Reed-Muller codes*. Electron. Commun. Japan 51(3) (1968), 96–104.

[Li09] R. Lipton, *The curious history of the Schwartz-Zippel Lemma*. `https://rjlipton.wordpress.com/2009/11/30`

[LRMV14] H. H. López, C. Renterá-Márquez, and R. H. Villarreal, *Affine Cartesian codes*. Des. Codes Cryptogr. 71 (1) (2014), 5-–19.

[Me06] K. Metsch, *How many s-subspaces must miss a point set in $PG(d, q)$*. J. Geom. 86 (2006) 154-164.

[Mu54] D. Muller, *Application of boolean algebra to switching circuit design and to error detection*. IRE Tran. on Electronic Computers EC-3 #3 (1954), 6–12.

[Or22] Ö. Ore, *Über höhere Kongruenzen*. Norsk Mat. Forenings Skrifter Ser. I (1922), no. 7, 15 pages.

[Re54] I. S. Reed, *A class of multiple-error-correcting codes and the decoding scheme*. IRE Trans. Information Theory PGIT-4 (1954), 38–49.

[Sc08] U. Schauz, *Algebraically solvable problems: describing polynomials as equivalent to explicit solutions*. Electron. J. Combin. 15 (2008), no. 1, Research Paper 10, 35 pp.

[Sc80] J.T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities.* J. Assoc. Comput. Mach. 27 (1980), no. 4, 701–717.

[vL99] J. H. van Lint. *Introduction to coding theory*, volume 86 of Graduate Texts in Mathematics. Springer-Verlag, Berlin, third edition, 1999.

[Wa35] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*. Abh. Math. Sem. Hamburg 11 (1935), 76–83.

[Zip79] R. Zippel, *An explicit separation of relativised random polynomial time and relativised deterministic polynomial time*. Inform. Process. Lett. 33 (1979), no. 4, 207–212.