On Zeros of a Polynomial in a Finite Grid: the Alon-Füredi Bound

John R. Schmitt

Middlebury College, Vermont, USA

joint work with Anurag Bishnoi (Ghent), Pete L. Clark (U. Georgia), Aditya Potukuchi (Rutgers)

"The strategy [of the polynomial method] is to capture the arbitrary sets of objects (viewed as points in some configuration space) in the zero set of a polynomial whose degree (or other measure of complexity) is under control...One then uses tools from algebraic geometry to understand the structure of this zero set, and thence to control the original sets of objects."

Terence Tao, *EMS Surveys*, 2014

A one variable non-zero polynomial over a field $\mathbb{F}$ can have at most as many zeroes as its degree.

A one variable non-zero polynomial over a field $\mathbb{F}$ can have at most as many zeroes as its degree.

Lemma

Let $\mathbb{F}$ be an arbitrary field, and let $f = f(x)$ be a polynomial in $\mathbb{F}[x]$. Suppose the degree of f is t (thus the x^t coefficient of f is nonzero). Then, if A is a subset of $\mathbb{F}$ with $|A| > t$, there is an $a \in A$ so that

$$f(a) \neq 0.$$

Example: $f(x) = x^2 - 1 \in \mathbb{R}[x]$ and $A = \{1, -1, 7\}$. $f(7) \neq 0$.

Theorem (Non-vanishing corollary to the Combinatorial Nullstellensatz, Noga Alon, 1999)

Let $\mathbb{F}$ be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. Suppose the degree $\deg(f)$ of f is $\sum_{i=1}^{n} t_i$, where each t_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero. Then, if $A_1, \ldots, A_n$ are subsets of $\mathbb{F}$ with $|A_i| > t_i$, there are $a_1 \in A_1, \ldots, a_n \in A_n$ so that

$$f(a_1, \ldots, a_n) \neq 0.$$

Theorem

(Chevalley-Warning Theorem) Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ *with* $d = d_1 + \ldots + d_r < n$. *For* $1 \leq i \leq r$, *let* $P_i(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ *be a polynomial of degree* d_i. *Let*

$$Z = Z(P_1, \ldots, P_r) = \{a \in \mathbb{F}_q^n \mid P_1(a) = \ldots = P_r(a) = 0\}$$

be the common zero set in $\mathbb{F}_q^n$ *of the* P_i*'s, and let* $\mathbf{z} = |Z|$. *Then:*
a) (Chevalley's Theorem, 1935) We have $\mathbf{z} = 0$ *or* $\mathbf{z} \geq 2$.
b) (Warning's Theorem, 1935) We have $\mathbf{z} \equiv 0 \pmod{p}$.

Theorem

(Chevalley-Warning Theorem) Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ with $d = d_1 + \ldots + d_r < n$. For $1 \le i \le r$, let $P_i(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial of degree d_i. Let

$$Z = Z(P_1, \ldots, P_r) = \{a \in \mathbb{F}_q^n \mid P_1(a) = \ldots = P_r(a) = 0\}$$

be the common zero set in $\mathbb{F}_q^n$ of the P_i's, and let $\mathbf{z} = |Z|$. Then:
a) (Chevalley's Theorem, 1935) We have $\mathbf{z} = 0$ or $\mathbf{z} \ge 2$.
b) (Warning's Theorem, 1935) We have $\mathbf{z} \equiv 0 \pmod{p}$.

- Alon proved (a) using Non-vanishing corollary.
- Chevalley's Theorem is useful in zero-sum theory.
- Schauz ('08) proved (b) using a generalization of Alon's statement.

A one variable non-zero polynomial over a field $\mathbb{F}$ can have at most as many zeroes as its degree.

Lemma

Let $\mathbb{F}$ be an arbitrary field, and let $f = f(x)$ be a polynomial in $\mathbb{F}[x]$. Suppose the degree of f is t (thus the x^t coefficient of f is nonzero). Then, if A is a subset of $\mathbb{F}$ with $|A| > t$, there is an $a \in A$ so that

$$f(a) \neq 0.$$

Example: $f(x) = x^2 - 1 \in \mathbb{R}[x]$ and $A = \{1, -1, 7, 9, 5\}$.

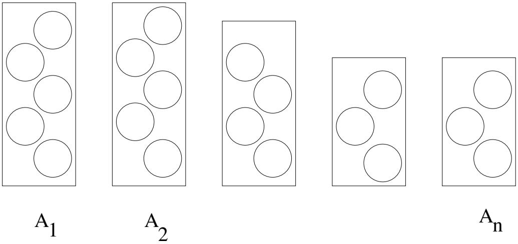
Theorem

(Alon-Füredi Theorem, 1993) Let $\mathbb{F}$ be a field, let $A_1, \ldots, A_n$ be nonempty finite subsets of $\mathbb{F}$. Put $A = \prod_{i=1}^{n} A_i$ for all $1 \leq i \leq n$. Let $f \in \mathbb{F}[x] = \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial. Let

$$\mathcal{U}_A = \{a \in A \mid f(a) \neq 0\}, \ \mathbf{u}_A = |\mathcal{U}_A|.$$

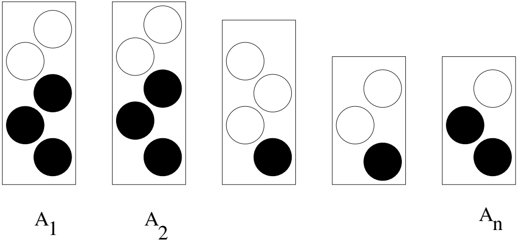
Then $\mathbf{u}_A = 0$ or $\mathbf{u}_A \geq \mathfrak{m}(|A_1|, \ldots, |A_n|; |A_1| + \ldots + |A_n| - \deg f)$.

Balls in bins lemma



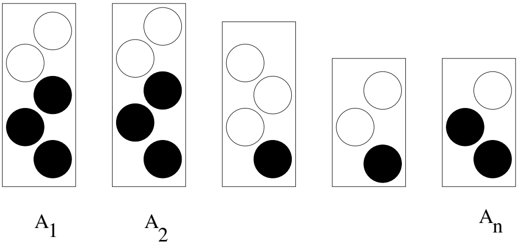
Bin A_i holds at most $|A_i|$ balls.

Balls in bins lemma



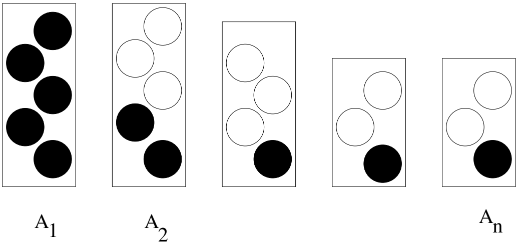
Bin A_i holds at most $|A_i|$ balls. Distribution of N balls is an n-tuple $y = (y_1, \ldots, y_n)$ with $y_1 + \ldots + y_n = N$ and $1 \leq y_i \leq |A_i|$ for all i.

Balls in bins lemma



Let $\Pi(y) = y_1 \cdots y_n$. If $n \le N \le |A_1| + \ldots + |A_n|$, let $\mathfrak{m}(|A_1|, \ldots, |A_n|; N)$ be the minimum value of $\Pi(y)$ as y ranges over all distributions of N balls into bins $A_1, \ldots, A_n$.

Balls in bins lemma



Let $\Pi(y) = y_1 \cdots y_n$. If $n \leq N \leq |A_1| + \ldots + |A_n|$, let $\mathfrak{m}(|A_1|, \ldots, |A_n|; N)$ be the minimum value of $\Pi(y)$ as y ranges over all distributions of N balls into bins $A_1, \ldots, A_n$. To minimize the product: serve the largest bins first.

Theorem

(Chevalley-Warning Theorem) Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ *with* $d = d_1 + \ldots + d_r < n$. *For* $1 \leq i \leq r$, *let* $P_i(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ *be a polynomial of degree* d_i. *Let*

$$Z = Z(P_1, \ldots, P_r) = \{a \in \mathbb{F}_q^n \mid P_1(a) = \ldots = P_r(a) = 0\}$$

be the common zero set in $\mathbb{F}_q^n$ *of the* P_i*'s, and let* $\mathbf{z} = |Z|$. *Then:*
a) (Chevalley's Theorem, 1935) We have $\mathbf{z} = 0$ *or* $\mathbf{z} \geq 2$.
b) (Warning's Theorem, 1935) We have $\mathbf{z} \equiv 0 \pmod{p}$.

Theorem

(Warning's Second Theorem) With same hypotheses,

$$\mathbf{z} = 0 \text{ or } \mathbf{z} \geq q^{n-d}.$$

Encode combinatorial/number-theoretic/incidence-geometry problems via a polynomial so that non-zeros of polynomial correspond to solutions of the given problem.

PROOF OF WARNING'S SECOND THEOREM: (Clark, Forrow, S. - 2014+) Let $x = (x_1, \ldots, x_n)$ and

$$P(x) = \prod_{i=1}^{r}(1 - P_i(x)^{q-1})$$

- $P(x)$ is zero whenever any P_i is nonzero.
- $P(x)$ is nonzero only when each P_i is zero.

Apply the Alon-Füredi Theorem.□

Clark, Forrow, S. (14+) showed applications of this to:

- weighted Davenport constants,
- generalizations of Erdős-Ginzburg-Ziv Theorem, and
- graph theory;

  and Clark (15+) gave strengthenings of these and a further application to:

- polynomial interpolation.

Theorem (Schwartz-Zippel Lemma, 1979)

Let R be a domain and let $S \subset R$ be finite and nonempty, with $|S| := s$. Let $f \in R[x_1, \ldots, x_n]$ be a nonzero polynomial. Then

$$\mathbf{z}_{S^n}(f) \leq (\deg f) s^{n-1}. \tag{1}$$

Theorem (Schwartz-Zippel Lemma, 1979)

Let R be a domain and let $S \subset R$ be finite and nonempty, with $|S| := s$. Let $f \in R[x_1, \ldots, x_n]$ be a nonzero polynomial. Then

$$\mathbf{z}_{S^n}(f) \leq (\deg f)s^{n-1}. \tag{1}$$

Proof.

The conclusion is equivalent to

$$\mathbf{u}_{S^n}(f) \geq s^{n-1}(s - \deg f).$$

Theorem (Schwartz-Zippel Lemma, 1979)

Let R be a domain and let $S \subset R$ be finite and nonempty, with $|S| := s$. Let $f \in R[x_1, \ldots, x_n]$ be a nonzero polynomial. Then

$$\mathbf{z}_{S^n}(f) \leq (\deg f)s^{n-1}. \tag{1}$$

Proof.

The conclusion is equivalent to

$$\mathbf{u}_{S^n}(f) \geq s^{n-1}(s - \deg f).$$

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

Theorem (Schwartz-Zippel Lemma, 1979)

Let R be a domain and let $S \subset R$ be finite and nonempty, with $|S| := s$. Let $f \in R[x_1, \ldots, x_n]$ be a nonzero polynomial. Then

$$\mathbf{z}_{S^n}(f) \leq (\deg f)s^{n-1}. \quad (1)$$

Proof.

The conclusion is equivalent to

$$\mathbf{u}_{S^n}(f) \geq s^{n-1}(s - \deg f).$$

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

$$\mathbf{u}_{S^n}(f) \geq \mathfrak{m}(s, \ldots, s; ns - \deg f) = s^{n-1}(s - \deg f).$$

□

Theorem

(DeMillo-Lipton-Zippel Theorem, 1978) Let R be a domain, let $f \in R[x_1, \dots, x_n]$ be a nonzero polynomial, and let $d \in \mathbb{Z}^+$ be such that $\deg_{x_i} f \leq d$ for all $i \in [n]$. Let $S \subset R$ be a nonempty set with $|S| := s > d$ elements. Then

$$\mathbf{z}_{S^n}(f) \leq s^n - (s-d)^n.$$

Example

Let S be a finite subset of R containing 0 and of size $s \geq 3$. Let $f = x_1 x_2 \in R[x_1, x_2]$. Then we have

$$\mathbf{z}_{S^2}(f) = 2s - 1.$$

DeMillo-Lipton-Zippel gives

$$\mathbf{z}_{S^2}(f) \leq s^2 - (s-1)^2 = 2s - 1.$$

Schwartz-Zippel gives

$$\mathbf{z}_{S^2}(f) \leq 2s.$$

The Alon-Füredi Theorem gives

$$\mathbf{z}_{S^2}(f) \leq s^2 - \mathfrak{m}(s, s; 2s-2) = s^2 - s(s-2) = 2s.$$

Thus neither Alon-Füredi nor Schwartz-Zippel implies DeMillo-Lipton-Zippel.

Example

For the other direction, take $f = x_1 + x_2$.

DeMillo-Lipton-Zippel gives
$\mathbf{z}_{S^2}(f) \leq s^2 - (s-1)^2 = 2s - 1$.

Schwartz-Zippel and Alon-Füredi give
$\mathbf{z}_{S^2}(f) \leq s$.

Thus DeMillo-Lipton-Zippel does not imply Schwartz-Zippel or Alon-Füredi.

Theorem (Generalized Alon-Füredi Theorem; A. Bishnoi, P.L. Clark, A. Potukuchi, S (15+))

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* $f \in R[x_1, \ldots, x_n]$ *be a non-zero polynomial such that* $\deg_{x_i} f \leq |A_i| - b_i$ *for all* $i \in [n]$*. Let* $\mathcal{U}_A = \{a \in A : f(a) \neq 0\}$ *where* $A = A_1 \times \cdots \times A_n \subseteq R^n$*. Then we have*

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

Moreover, this bound is sharp in all cases.

Theorem (Generalized Alon-Füredi Theorem; A. Bishnoi, P.L. Clark, A. Potukuchi, S (15+))

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 $f \in R[x_1, \ldots, x_n]$ be a non-zero polynomial such that $\deg_{x_i} f \leq |A_i| - b_i$ for all $i \in [n]$. Let $\mathcal{U}_A = \{a \in A : f(a) \neq 0\}$ where $A = A_1 \times \cdots \times A_n \subseteq R^n$. Then we have

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

Moreover, this bound is sharp in all cases.

- Generalized Alon-Füredi does imply DeMillo-Lipton-Zippel.

Theorem (Generalized Alon-Füredi Theorem; A. Bishnoi, P.L. Clark, A. Potukuchi, S (15+))

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 $f \in R[x_1, \ldots, x_n]$ be a non-zero polynomial such that $\deg_{x_i} f \leq |A_i| - b_i$ for all $i \in [n]$. Let $\mathcal{U}_A = \{a \in A : f(a) \neq 0\}$ where $A = A_1 \times \cdots \times A_n \subseteq R^n$. Then we have

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

Moreover, this bound is sharp in all cases.

- Generalized Alon-Füredi does imply DeMillo-Lipton-Zippel.
- (Generalized) Alon-Füredi has other applications to coding theory and finite geometry.

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.

Given any $b_1, \ldots, b_n \in \mathbb{Z}$ 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 $y = (y_1, \ldots, y_n)$ of N balls into bins of sizes $a_1, \ldots, a_n$ such that $b_i \leq y_i \leq a_i$ for all $i \in [n]$ and put

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

where the minimum ranges over this restricted set of distributions.

- Alon, Noga Combinatorial Nullstellensatz. Recent trends in combinatorics (Mátraháza, 1995). *Combin. Probab. Comput.* **8** (1999), no. 1-2, 7–29.
- P. L. Clark, A. Forrow and J.R.S., *Warning's Second Theorem With Restricted Variables*. To appear in Combinatorica, (2014) `http://arxiv.org/abs/1404.7793`.
- R. Lipton, *The curious history of the Schwartz-Zippel Lemma*. `https://rjlipton.wordpress.com/2009/11/30`
- Tao, Terence Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory. *EMS Surv. Math. Sci.* **1** (2014), no. 1, 1–46.

Vielen Dank!