Counting zero-sum subsequences with the polynomial method

John Schmitt

Middlebury College
Vermont, USA

Joint work with Pete L. Clark (U. Georgia) and Aden Forrow (now at Oxford)

The Erdős-Ginzburg-Ziv Theorem

Theorem (Erdős-Ginzburg-Ziv - 1961)

Every sequence of length $2m-1$ in $\mathbb{Z}/m\mathbb{Z}$ has a zero-sum subsequence of length m.

PROOF FOR PRIME CASE (BAILEY-RICHTER - 1989): Let us consider a sequence $(b_1, \dots, b_n) \in \mathbb{F}_p^n$.
Let

$$P_1(t_1, \dots, t_n) = \sum_{i=1}^{n} b_i t_i^{p-1} \in \mathbb{F}_p[t_1, \dots, t_n]$$

and

$$P_2(t_1, \dots, t_n) = \sum_{i=1}^{n} t_i^{p-1} \in \mathbb{F}_p[t_1, \dots, t_n].$$

PROOF FOR PRIME CASE (BAILEY-RICHTER - 1989): Let us consider a sequence $(b_1, \ldots, b_n) \in \mathbb{F}_p^n$.
Let

$$P_1(t_1, \ldots, t_n) = \sum_{i=1}^{n} b_i t_i^{p-1} \in \mathbb{F}_p[t_1, \ldots, t_n]$$

and

$$P_2(t_1, \ldots, t_n) = \sum_{i=1}^{n} t_i^{p-1} \in \mathbb{F}_p[t_1, \ldots, t_n].$$

Recall Fermat's Little Theorem. P_1 encodes divisibility condition on sum. P_2 encodes number of terms in subsequence. Seek common zeros other than $\mathbf{0}$, for a shared zero $\mathbf{0} \neq (x_1, \ldots, x_n) \in \mathbb{F}_p^n$ will provide $I = \{1 \leq i \leq n | x_i \neq 0\}$, the set we seek.

Theorem (Chevalley-Warning - 1935)

Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ *with* $d_1 + \ldots + d_r < n$. *For* $1 \leq i \leq r$, *let* $P_i(t_1, \ldots, t_n) \in \mathbb{F}_q[t_1, \ldots, t_n]$ *be a polynomial of degree* d_i. *Let*

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

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 - 1935)

Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ with $d_1 + \ldots + d_r < n$. For $1 \leq i \leq r$, let $P_i(t_1, \ldots, t_n) \in \mathbb{F}_q[t_1, \ldots, t_n]$ be a polynomial of degree d_i. Let

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

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 $\mathbf{z} \equiv 0 \pmod{p}$.

Proof of EGZ continued: With $n = 2p - 1 > p - 1 + p - 1$, we can apply Chevalley's Theorem.□

Theorem (Combinatorial Nullstellensatz (Part 2), N. Alon 1999)

Let $\mathbb{F}$ be an arbitrary field, and let $f = f(t_1, \ldots, t_n)$ be a polynomial in $\mathbb{F}[t_1, \ldots, t_n]$. Suppose the degree $\deg(f)$ of f is $\sum_{i=1}^{n} \alpha_i$, where each α_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{n} t_i^{\alpha_i}$ in f is nonzero. Then, if $A_1, \ldots, A_n$ are subsets of $\mathbb{F}$ with $|A_i| > \alpha_i$, there are $a_1 \in A_1, \ldots, a_n \in A_n$ so that $f(a_1, \ldots, a_n) \neq 0$.

Theorem (Combinatorial Nullstellensatz (Part 2), N. Alon 1999)

Let $\mathbb{F}$ be an arbitrary field, and let $f = f(t_1, \ldots, t_n)$ be a polynomial in $\mathbb{F}[t_1, \ldots, t_n]$. Suppose the degree $\deg(f)$ of f is $\sum_{i=1}^{n} \alpha_i$, where each α_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{n} t_i^{\alpha_i}$ in f is nonzero. Then, if $A_1, \ldots, A_n$ are subsets of $\mathbb{F}$ with $|A_i| > \alpha_i$, there are $a_1 \in A_1, \ldots, a_n \in A_n$ so that $f(a_1, \ldots, a_n) \neq 0$.

Combinatorial Nullstellensatz $\Rightarrow$ Chevalley's Theorem $\Rightarrow$ EGZ.

Theorem (Combinatorial Nullstellensatz (Part 2), N. Alon 1999)

Let $\mathbb{F}$ be an arbitrary field, and let $f = f(t_1, \ldots, t_n)$ be a polynomial in $\mathbb{F}[t_1, \ldots, t_n]$. Suppose the degree $\deg(f)$ of f is $\sum_{i=1}^{n} \alpha_i$, where each α_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{n} t_i^{\alpha_i}$ in f is nonzero. Then, if $A_1, \ldots, A_n$ are subsets of $\mathbb{F}$ with $|A_i| > \alpha_i$, there are $a_1 \in A_1, \ldots, a_n \in A_n$ so that $f(a_1, \ldots, a_n) \neq 0$.

Combinatorial Nullstellensatz $\Rightarrow$ Chevalley's Theorem $\Rightarrow$ EGZ.

These are existence theorems.

GOAL FOR THIS TALK: Show how to refine combinatorial existence theorems into theorems which give explicit (and sometimes sharp) lower bounds on the *number* of combinatorial objects asserted to exist.

Theorem (Chevalley-Warning - 1935)

Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ with $d_1 + \ldots + d_r < n$. For $1 \leq i \leq r$, let $P_i(t_1, \ldots, t_n) \in \mathbb{F}_q[t_1, \ldots, t_n]$ be a polynomial of degree d_i. Let

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

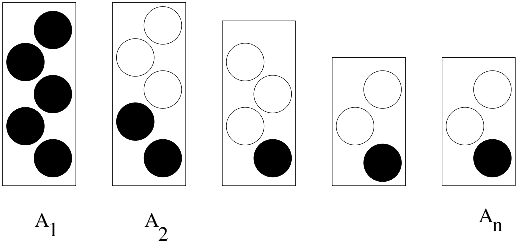
be the common zero set in $\mathbb{F}_q^n$ of the P_i's, and let $\mathbf{z} = \#Z$. Then:
a) (Chevalley's Theorem, 1935) We have $\mathbf{z} = 0$ or $\mathbf{z} \geq 2$.
b) (Warning's Theorem, 1935) We have $\mathbf{z} \equiv 0 \pmod{p}$.

Theorem (Warning's Second Theorem)

With same hypotheses,

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

Balls in bins



Let $P(y) = y_1 \cdots y_n$. If $n \leq N \leq a_1 + \ldots + a_n$, let $\mathfrak{m}(a_1, \ldots, a_n; N)$ be the minimum value of $P(y)$ as y ranges over all distributions of N balls into bins $A_1, \ldots, A_n$, where $|A_i| = a_i$ and where each bin must have at least one ball. To minimize the product: greedily serve the largest bins first.

Alon-Füredi Theorem

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 $A = \prod_{i=1}^{n} A_i$ and $a_i = \# A_i$ for all $1 \leq i \leq n$. Let $P \in \mathbb{F}[t] = \mathbb{F}[t_1, \ldots, t_n]$ be a polynomial. Let

$$\mathcal{U}_A = \{x \in A \mid P(x) \neq 0\}, \ \mathfrak{u}_A = \#\mathcal{U}_A.$$

Then $\mathfrak{u}_A = 0$ or $\mathfrak{u}_A \geq \mathfrak{m}(a_1, \ldots, a_n; a_1 + \ldots + a_n - \deg P)$.

Proof.

Induction on n. □

Theorem (Warning's Second Theorem)

Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ *with* $d_1 + \ldots + d_r < n$*. For* $1 \leq i \leq r$*, let* $P_i(t_1, \ldots, t_n) \in \mathbb{F}_q[t_1, \ldots, t_n]$ *be a polynomial of degree* d_i*. Let*

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

be the common zero set in $\mathbb{F}_q^n$ *of the* P_i*'s, and let* $\mathbf{z} = \#Z$*. Then,*

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

Theorem (Warning's Second Theorem)

Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ with $d_1 + \ldots + d_r < n$. For $1 \leq i \leq r$, let $P_i(t_1, \ldots, t_n) \in \mathbb{F}_q[t_1, \ldots, t_n]$ be a polynomial of degree d_i. Let

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

be the common zero set in $\mathbb{F}_q^n$ of the P_i's, and let $\mathbf{z} = \#Z$. Then,

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

PROOF (CLARK-FORROW-S. - 2017): Apply Alon-Füredi to

$$\prod_{i=1}^{r} (1 - P_i(t)^{q-1}).$$

Theorem (Clark, Forrow, S. - 2017)

Let p be a prime, let $n, r, v \in \mathbb{Z}^+$, and for $1 \leq i \leq r$, let $1 \leq v_j \leq v$. Let $A_1, \ldots, A_n \subset \mathbb{Z}$ be nonempty subsets each having the property that no two distinct elements are congruent modulo p. Let $P_1, \ldots, P_r \in \mathbb{Z}[t_1, \ldots, t_n]$. Put

$$Z_{\mathbf{A}} := \{x \in \prod_{i=1}^{n} A_i \mid \forall 1 \leq j \leq r,\ P_j(x) \equiv 0 \pmod{p^{v_j}}\}.$$

Then $\# Z_{\mathbf{A}} = 0$ or

$$\# Z_{\mathbf{A}} \geq \mathfrak{m}\left(\# A_1, \ldots, \# A_n; \sum_{i=1}^{n} \# A_i - \sum_{j=1}^{r} (p^{v_j} - 1) \deg P_j\right).$$

Use this generalization of Warning's Second Theorem to prove a generalization of EGZ.

Theorem (Clark-Forrow-S. - 2017)

Let $k, r, v_1 \leq \ldots \leq v_r$ *be positive integers, and let* $G = \bigoplus_{i=1}^r \mathbb{Z}/p^{v_i}\mathbb{Z}$. *Let* $A_1, \ldots, A_n$ *be nonempty subsets of* $\mathbb{Z}$*, each containing* 0*, such that for each* i *the elements of* A_i *are pairwise incongruent modulo* p. *Put*

$$A = \prod_{i=1}^n A_i, \ a_M = \max \# A_i.$$

For $g \in G$*, let* $\mathrm{EGZ}_{A,k}(g)$ *be the number of* $(a_1, \ldots, a_n) \in A$ *such that* $a_1 g_1 + \ldots + a_n g_n = g$ *and* $p^k \mid \#\{1 \leq i \leq n \mid a_i \neq 0\}$. *Then either* $\mathrm{EGZ}_{A,k}(g) = 0$ *or*

$$\mathrm{EGZ}_{A,k}(g) \geq \mathfrak{m}(\#A_1, \ldots, \#A_n; \sum_{i=1}^n \#A_i - \sum_{i=1}^r (p^{v_i} - 1) - (a_M - 1)(p^k - 1)). \tag{1}$$

Lemma

Let $\{0\} \subset A \subset \mathbb{Z}$ be a finite subset, no two of whose elements are congruent modulo p. There is $C_A \in \mathbb{Z}_{(p)}[t]$ of degree $\#A - 1$ such that for $a \in A$,

$$C_A(a) = \begin{cases} 0 & a = 0 \\ 1 & a \neq 0 \end{cases}.$$

Proof.

We may take $C_A(t) = 1 - \prod_{a \in A \setminus \{0\}} \frac{a-t}{a}$. □

PROOF OF THEOREM: Represent elements of G by r-tuples of integers $(b_1, \ldots, b_r)$. For $1 \leq i \leq n$ and $1 \leq j \leq r$, let

$$g_i = (b_1^{(i)}, \ldots, b_r^{(i)})$$

and

$$P_j(t_1, \ldots, t_n) = \sum_{i=1}^{n} b_j^{(i)} t_i.$$

If there is an element $x \in \prod_{i=1}^{n} A_i$ such that

$$\sum_{i=1}^{n} b_j^{(i)} x_i \equiv g^j \pmod{p^{v_j}} \ \forall 1 \leq j \leq r,$$

then we get a zero-sum generalized subsequence from $I = \{1 \leq i \leq n \mid x_i = 1\}$.

The extra condition that the number of nonzero terms in the zero-sum generalized subsequence is a multiple of p^k is enforced via the polynomial congruence

$$C_{A_1}(t_1) + \ldots + C_{A_n}(t_n) \equiv 0 \pmod{p^k},$$

which has degree $a_M - 1$. □

Corollary

In the preceding theorem, let $0 \in A_1 = \ldots = A_n$, $k = v_r$. *Put* $a = \#A_1$.

a) Suppose

$$n \geq \exp G - 1 + \frac{D(G)}{a-1}.$$

Let R *be such that* $R \equiv -\sum_{i=1}^{r}(p^{v_i} - 1) \pmod{a-1}$ *and* $0 \leq R < a - 1$. *Then*

$$\mathrm{EGZ}_{A,v_r}(0) \geq (R+1)a^{n+1-\exp G + \lfloor \frac{1-D(G)}{a-1} \rfloor}. \tag{2}$$

b) (Das Adhikari, Grynkiewicz, Sun - '12) Every sequence of length n *in* G *has a nonempty zero-sum generalized subsequence of length divisible by* $\exp G$ *when*

$$n \geq \exp G - 1 + \frac{D(G)}{a-1}. \tag{3}$$

Relaxed outputs

Theorem (P.L. Clark - 2018)

Let p be a prime, let $n, r, v \in \mathbb{Z}^+$, and for $1 \leq i \leq r$, let $1 \leq v_j \leq v$. Let $A_1, \ldots, A_n, B_1, \ldots, B_r \subset \mathbb{Z}$ be nonempty subsets each having the property that no two distinct elements are congruent modulo p. Let $P_1, \ldots, P_r \in \mathbb{Z}[t_1, \ldots, t_n]$. Put

$$Z_{\mathbf{A}}^{\mathbf{B}} := \{x \in \prod_{i=1}^{n} A_i \mid \forall 1 \leq j \leq r,\ P_j(x) \in B_j \pmod{p^{v_j}}\}.$$

Then $\# Z_{\mathbf{A}}^{\mathbf{B}} = 0$ or

$$\# Z_{\mathbf{A}}^{\mathbf{B}} \geq \mathfrak{m}\left(\# A_1, \ldots, \# A_n; \sum_{i=1}^{n} \# A_i - \sum_{j=1}^{r} (p^{v_j} - \# B_j) \deg P_j\right).$$

Thank you!