Zero-Sums in p-groups via a Generalization of the Ax-Katz Theorem

David Grynkiewicz

University of Memphis

July 12, 2023

Combinatorial Sequences

- Let G be a finite abelian group

Combinatorial Sequences

- Let G be a finite abelian group
- Let

$$S = g_1 \cdot \ldots \cdot g_\ell$$

  be a finite (unordered) sequence of terms $g_i \in G$ written as a multiplicative string.

Combinatorial Sequences

- Let G be a finite abelian group
- Let
$$S = g_1 \cdot \ldots \cdot g_\ell$$
be a finite (unordered) sequence of terms $g_i \in G$ written as a multiplicative string.
- $|S| = \ell$ is the length of S

Combinatorial Sequences

- Let G be a finite abelian group
- Let
$$S = g_1 \cdot \ldots \cdot g_\ell$$
be a finite (unordered) sequence of terms $g_i \in G$ written as a multiplicative string.
- $|S| = \ell$ is the length of S

$$\Sigma(S) = \{g \in G : \; g = \sum_{i \in I} g_i \text{ for some nonempty } I \subseteq [1, \ell]\}$$
$$\Sigma_k(S) = \{g \in G : \; g = \sum_{i \in I} g_i \text{ for some } I \subseteq [1, \ell] \text{ with } |I| = k\}$$

Combinatorial Sequences

- Let G be a finite abelian group
- Let
$$S = g_1 \cdot \ldots \cdot g_\ell$$
be a finite (unordered) sequence of terms $g_i \in G$ written as a multiplicative string.
- $|S| = \ell$ is the length of S

$$\Sigma(S) = \{g \in G : \ g = \sum_{i \in I} g_i \text{ for some nonempty } I \subseteq [1, \ell]\}$$
$$\Sigma_k(S) = \{g \in G : \ g = \sum_{i \in I} g_i \text{ for some } I \subseteq [1, \ell] \text{ with } |I| = k\}$$

Example

$S = (-1) \cdot 1^2 \cdot 4 = (-1) \cdot 1 \cdot 1 \cdot 4, \quad |S| = 4,$

$$\Sigma_2(S) = \{-1 + 1, \quad -1 + 4, \quad 1 + 1, \quad 1 + 4\} = \{0, 3, 2, 5\}$$

Zero-Sum Questions

G finite abelian group, S a sequence of terms from G.

Zero-Sum Questions

G finite abelian group, S a sequence of terms from G.

Definition

The **Davenport Constant** $\mathrm{D}(G)$ is the minimal integer such that $|S| \geq \mathrm{D}(G)$ implies $0 \in \Sigma(S)$.

Zero-Sum Questions

G finite abelian group, S a sequence of terms from G.

Definition

The **Davenport Constant** $\mathsf{D}(G)$ is the minimal integer such that $|S| \geq \mathsf{D}(G)$ implies $0 \in \Sigma(S)$.

- If $G = \langle e_1 \rangle \oplus \ldots \oplus \langle e_r \rangle = C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $n_1 \mid \ldots \mid n_r$, then

$$S = e_1^{n_1 - 1} \cdot \ldots \cdot e_r^{n_r - 1}$$

  shows

$$\mathsf{D}(G) \geq \mathsf{D}^*(G) := 1 + \sum_{i=1}^{r} (n_i - 1)$$

Zero-Sum Questions

G finite abelian group, S a sequence of terms from G.

Definition

The **Davenport Constant** $\mathsf{D}(G)$ is the minimal integer such that $|S| \geq \mathsf{D}(G)$ implies $0 \in \Sigma(S)$.

- If $G = \langle e_1 \rangle \oplus \ldots \oplus \langle e_r \rangle = C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $n_1 \mid \ldots \mid n_r$, then

$$S = e_1^{n_1 - 1} \cdot \ldots \cdot e_r^{n_r - 1}$$

  shows

$$\mathsf{D}(G) \geq \mathsf{D}^*(G) := 1 + \sum_{i=1}^{r} (n_i - 1)$$

- (Olson 1969 or Kruyswijk 1968) If G is a p-group, then

$$\mathsf{D}(G) = \mathsf{D}^*(G).$$

k-term Zero-Sums

G finite abelian group with exponent $\exp(G) = n$,
S a sequence of terms from G.

k-term Zero-Sums

G finite abelian group with exponent $\exp(G) = n$,
S a sequence of terms from G.

Definition

For $k \geq 0$, let $\mathsf{s}_{kn}(G)$ be the minimal integer such that $|S| \geq \mathsf{s}_{kn}(G)$ implies $0 \in \Sigma_{kn}(S)$.

k-term Zero-Sums

G finite abelian group with exponent $\exp(G) = n$,
S a sequence of terms from G.

Definition

For $k \geq 0$, let $\mathsf{s}_{kn}(G)$ be the minimal integer such that $|S| \geq \mathsf{s}_{kn}(G)$ implies $0 \in \Sigma_{kn}(S)$.

- Why a multiple of n? Answer: $S = e^N$ with $\mathrm{ord}(e) = n$

k-term Zero-Sums

G finite abelian group with exponent $\exp(G) = n$,
S a sequence of terms from G.

Definition

For $k \geq 0$, let $\mathsf{s}_{kn}(G)$ be the minimal integer such that $|S| \geq \mathsf{s}_{kn}(G)$ implies $0 \in \Sigma_{kn}(S)$.

- Why a multiple of n? Answer: $S = e^N$ with $\mathrm{ord}(e) = n$
- Lower bound:

$$S = 0^{kn-1} \cdot T,$$

with T a zero-sum free sequence with maximal length $|T| = \mathsf{D}(G) - 1$, shows

$$\mathsf{s}_{kn}(G) \geq kn + \mathsf{D}(G) - 1.$$

The case $k = 1$

- (Erdős-Ginzburg-Ziv Theorem 1961) Via combinatorial methods:

$$\mathsf{s}_n(C_n) = 2n - 1$$

The case $k = 1$

- (Erdős-Ginzburg-Ziv Theorem 1961) Via combinatorial methods:

$$\mathsf{s}_n(C_n) = 2n - 1$$

- (Alon and Dubiner 1995) Via spectral graph theory:

$$\mathsf{s}_n(C_n^d) \leq c_d(n-1) + 1$$

with $c_d = 2(2^{10} d \log d)^d$

The case $k = 1$

- (Erdős-Ginzburg-Ziv Theorem 1961) Via combinatorial methods:

$$\mathsf{s}_n(C_n) = 2n - 1$$

- (Alon and Dubiner 1995) Via spectral graph theory:

$$\mathsf{s}_n(C_n^d) \leq c_d(n-1) + 1$$

with $c_d = 2(2^{10} d \log d)^d$

- (Alon and Dubiner 1993) Via the Chevalley-Warning Theorem:

$$\mathsf{s}_n(C_p^2) \leq 6p - 5$$

The case $k = 1$

- (Erdős-Ginzburg-Ziv Theorem 1961) Via combinatorial methods:

$$s_n(C_n) = 2n - 1$$

- (Alon and Dubiner 1995) Via spectral graph theory:

$$s_n(C_n^d) \leq c_d(n-1) + 1$$

  with $c_d = 2(2^{10} d \log d)^d$

- (Alon and Dubiner 1993) Via the Chevalley-Warning Theorem:

$$s_n(C_p^2) \leq 6p - 5$$

- (Ronyai 2000) Via the Linear Algebra of multilinear polynomials:

$$s_p(C_p^2) \leq 4p - 2$$

The case $k = 1$

- (Erdős-Ginzburg-Ziv Theorem 1961) Via combinatorial methods:

$$s_n(C_n) = 2n - 1$$

- (Alon and Dubiner 1995) Via spectral graph theory:

$$s_n(C_n^d) \leq c_d(n-1) + 1$$

with $c_d = 2(2^{10} d \log d)^d$

- (Alon and Dubiner 1993) Via the Chevalley-Warning Theorem:

$$s_n(C_p^2) \leq 6p - 5$$

- (Ronyai 2000) Via the Linear Algebra of multilinear polynomials:

$$s_p(C_p^2) \leq 4p - 2$$

- (Reiher 2007) Via the Chevalley-Warning Theorem:

$$s_n(C_n^2) = 4n - 3$$

The case $k = 1$

- (Erdős-Ginzburg-Ziv Theorem 1961) Via combinatorial methods:
$$s_n(C_n) = 2n - 1$$
- (Alon and Dubiner 1995) Via spectral graph theory:
$$s_n(C_n^d) \leq c_d(n-1) + 1$$
with $c_d = 2(2^{10} d \log d)^d$
- (Alon and Dubiner 1993) Via the Chevalley-Warning Theorem:
$$s_n(C_p^2) \leq 6p - 5$$
- (Ronyai 2000) Via the Linear Algebra of multilinear polynomials:
$$s_p(C_p^2) \leq 4p - 2$$
- (Reiher 2007) Via the Chevalley-Warning Theorem:
$$s_n(C_n^2) = 4n - 3$$
- (Ellenberg and Gijswijt 2017) Via the Croot-Lev-Pach Polynomial Method
$$s_3(C_3^d) < 2c^d + 1$$
for some $c < 3$

Larger k?

- (Gao 1995) $\mathsf{s}_{|G|}(G) = |G| + \mathsf{D}(G) - 1$

Larger k?

- (Gao 1995) $\mathsf{s}_{|G|}(G) = |G| + \mathsf{D}(G) - 1$
- (Gao 1995) $\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq \frac{|G|}{n}$.

Larger k?

- (Gao 1995) $\mathsf{s}_{|G|}(G) = |G| + \mathsf{D}(G) - 1$
- (Gao 1995) $\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq \frac{|G|}{n}$.
- In particular,

$$\mathsf{s}_{kp}(C_p^d) = kp + d(p-1) \quad \text{for } k \geq p^{d-1}.$$

Larger k?

- (Gao 1995) $\mathsf{s}_{|G|}(G) = |G| + \mathsf{D}(G) - 1$
- (Gao 1995) $\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq \frac{|G|}{n}$.
- In particular,

$$\mathsf{s}_{kp}(C_p^d) = kp + d(p-1) \quad \text{for } k \geq p^{d-1}.$$

- A basic construction shows

$$\mathsf{s}_p(C_p^d) \geq 2^d(p-1) + 1 \quad \text{for } k = 1.$$

Larger k?

- (Gao 1995) $\mathsf{s}_{|G|}(G) = |G| + \mathsf{D}(G) - 1$
- (Gao 1995) $\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad$ for all $k \geq \frac{|G|}{n}$.
- In particular,

$$\mathsf{s}_{kp}(C_p^d) = kp + d(p-1) \quad \text{for } k \geq p^{d-1}.$$

- A basic construction shows

$$\mathsf{s}_p(C_p^d) \geq 2^d(p-1) + 1 \quad \text{for } k = 1.$$

- As $k \to \infty$, $s_p(C_p^d)$ goes from exponential to linear (in d).

Larger k?

- (Gao 1995) $\mathsf{s}_{|G|}(G) = |G| + \mathsf{D}(G) - 1$
- (Gao 1995) $\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq \frac{|G|}{n}$.
- In particular,

$$\mathsf{s}_{kp}(C_p^d) = kp + d(p-1) \quad \text{for } k \geq p^{d-1}.$$

- A basic construction shows

$$\mathsf{s}_p(C_p^d) \geq 2^d(p-1) + 1 \quad \text{for } k = 1.$$

- As $k \to \infty$, $s_p(C_p^d)$ goes from exponential to linear (in d).
- Question: What is minimal $\ell(G)$ such that

$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq \ell(G).$$

Larger k?

- (Gao 1995) $\mathsf{s}_{|G|}(G) = |G| + \mathsf{D}(G) - 1$
- (Gao 1995) $\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq \frac{|G|}{n}$.
- In particular,

$$\mathsf{s}_{kp}(C_p^d) = kp + d(p-1) \quad \text{for } k \geq p^{d-1}.$$

- A basic construction shows

$$\mathsf{s}_p(C_p^d) \geq 2^d(p-1) + 1 \quad \text{for } k = 1.$$

- As $k \to \infty$, $s_p(C_p^d)$ goes from exponential to linear (in d).
- Question: What is minimal $\ell(G)$ such that

$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq \ell(G).$$

- (Kubertin 2005, Gao and Han 2014) Conjecture:

$$\ell(G) = d := \left\lceil \frac{\mathsf{D}(G)}{n} \right\rceil.$$

Note $\left\lceil \frac{\mathsf{D}(C_p^d)}{p} \right\rceil = d$ for $p \geq d$.

Partial Progress

G finite abelian group with $n = \exp(G)$ and $d = \lceil \frac{\mathsf{D}(G)}{n} \rceil$.

- (Dongchun and Han 2018) If G is a p-group, $p \geq 2d - 1$ and $d \leq 4$, then
$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq d$$

Partial Progress

G finite abelian group with $n = \exp(G)$ and $d = \lceil \frac{\mathsf{D}(G)}{n} \rceil$.

- (Dongchun and Han 2018) If G is a p-group, $p \geq 2d - 1$ and $d \leq 4$, then
$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq d$$
- (Xiaoyu He 2016) If G is a p-group and $p \geq \frac{7}{2}d - \frac{3}{2}$, then
$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq p + d$$

Partial Progress

G finite abelian group with $n = \exp(G)$ and $d = \lceil \frac{\mathsf{D}(G)}{n} \rceil$.

- (Dongchun and Han 2018) If G is a p-group, $p \geq 2d-1$ and $d \leq 4$, then

$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq d$$

- (Xiaoyu He 2016) If G is a p-group and $p \geq \frac{7}{2}d - \frac{3}{2}$, then

$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq p + d$$

- Above improves bound $k \geq p^{d-1}$ to $k \geq p+d$ (for $G = C_p^d$)

Partial Progress

G finite abelian group with $n = \exp(G)$ and $d = \lceil \frac{\mathsf{D}(G)}{n} \rceil$.

- (Dongchun and Han 2018) If G is a p-group, $p \geq 2d - 1$ and $d \leq 4$, then

$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq d$$

- (Xiaoyu He 2016) If G is a p-group and $p \geq \frac{7}{2}d - \frac{3}{2}$, then

$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k \geq p + d$$

- Above improves bound $k \geq p^{d-1}$ to $k \geq p + d$ (for $G = C_p^d$)
- Can all dependence on p be eliminated?

Eliminating the dependence on p

Theorem (G. 2023)

Let G be a finite abelian p-group with exponent n and let $d = \lceil \frac{\mathsf{D}(G)}{n} \rceil$. If $p > d(d-1)$, then

$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \text{for all } k > \frac{d(d-1)}{2}.$$

Chevalley-Warning Theorem

Theorem (Chevalley-Warning Theorem 1936)

Let $\mathbb{F}_q$ *be a finite field of characteristic* p*, let* $f_1, \dots, f_s \in \mathbb{F}_q[X_1, \dots, X_\ell]$ *be nonzero polynomials, where* $s \geq 1$*, and let*

$$V = \{\mathbf{x} \in \mathbb{F}_q^\ell : \; f_1(\mathbf{x}) = 0, \dots, f_s(\mathbf{x}) = 0\}.$$

If $\ell > \sum_{i=1}^{s} \deg f_i$*, then* $|V| \equiv 0 \mod p$*.*

Chevalley-Warning Theorem

Theorem (Chevalley-Warning Theorem 1936)

Let $\mathbb{F}_q$ be a finite field of characteristic p, let $f_1, \ldots, f_s \in \mathbb{F}_q[X_1, \ldots, X_\ell]$ be nonzero polynomials, where $s \geq 1$, and let

$$V = \{\mathbf{x} \in \mathbb{F}_q^\ell : \ f_1(\mathbf{x}) = 0, \ldots, f_s(\mathbf{x}) = 0\}.$$

If $\ell > \sum_{i=1}^{s} \deg f_i$, then $|V| \equiv 0 \mod p$.

Theorem (Ax-Katz Theorem 1971)

Let $\mathbb{F}_q$ be a finite field of characteristic p and order q, let $f_1, \ldots, f_s \in \mathbb{F}_q[X_1, \ldots, X_\ell]$ be nonzero polynomials, where $s \geq 1$, and let

$$V = \{\mathbf{x} \in \mathbb{F}_q^\ell : \ f_1(\mathbf{x}) = 0, \ldots, f_s(\mathbf{x}) = 0\}.$$

If $\ell > (m-1)\max_{i \in [1,s]}\{\deg f_i\} + \sum_{i=1}^{s} \deg f_i$, where $m \geq 1$, then

$$|V| \equiv 0 \mod q^m.$$

A Weighted Generalization

Theorem (2023)

Let $p \geq 2$ *be prime, let* $n \geq 1$ *and* $\mathcal{B} = \mathcal{I}_1 \times \ldots \times \mathcal{I}_n$ *with each* $\mathcal{I}_j \subseteq \mathbb{Z}$ *for* $j \in [1, n]$ *a complete system of residues modulo* p*, let* $s \geq 1$ *and* $m_1, \ldots, m_s \geq 0$ *be integers, let* $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$ *be nonzero polynomials, let* $w_1, \ldots, w_s \in \mathbb{Q}[X]$ *be integer–valued polynomials with respective degrees* $t_1, \ldots, t_s \geq 0$*, and let*

$$V = \{\mathbf{x} \in \mathcal{B} : \ f_i(\mathbf{x}) \equiv 0 \mod p^{m_i} \text{ for all } i \in [1, s]\} \qquad \text{and}$$

$$N = \sum_{\mathbf{a} \in V} \prod_{i=1}^{s} w_i\Big(\frac{f_i(\mathbf{a})}{p^{m_i}}\Big).$$

If $n > (m-1)\max_{i\in[1,s]}\left\{1, \ \frac{\varphi(p^{m_i})}{p-1}\deg f_i\right\} + \sum_{i=1}^{s} \frac{(t_i+1)p^{m_i}-1}{p-1}\deg f_i$*, where* $m \geq 0$ *and* φ *denotes the Euler totient function, then*

$$N \equiv 0 \mod p^m.$$

The Importance of the Box $\mathcal{B}$

- Hensel's lemma can be used to choose the I_j so that behavior modulo p is simulated modulo p^m for all $x \in I_j$

The Importance of the Box $\mathcal{B}$

- Hensel's lemma can be used to choose the I_j so that behavior modulo p is simulated modulo p^m for all $x \in I_j$
- Fermat's Litte Theorem:

$$x^{p-1} \equiv \begin{cases} 1 \mod p & \text{if } x \not\equiv 0 \mod p \\ 0 \mod p & \text{if } x \equiv 0 \mod p. \end{cases}$$

The Importance of the Box $\mathcal{B}$

- Hensel's lemma can be used to choose the I_j so that behavior modulo p is simulated modulo p^m for all $x \in I_j$
- Fermat's Litte Theorem:

$$x^{p-1} \equiv \begin{cases} 1 \mod p & \text{if } x \not\equiv 0 \mod p \\ 0 \mod p & \text{if } x \equiv 0 \mod p. \end{cases}$$

- There exists a complete system I of residues modulo p such that

$$x^{p-1} \equiv \begin{cases} 1 \mod p^m & \text{if } x \not\equiv 0 \mod p \\ 0 \mod p^m & \text{if } x \equiv 0 \mod p, \end{cases} \qquad \text{for every } x \in \mathcal{I}.$$

Using the Ax-Katz Generalization

$$G = \langle e_1 \rangle \oplus \ldots \oplus \langle e_s \rangle = C_{p^{m_1}} \oplus \ldots \oplus C_{p^{m_s}}, \qquad S = g_1 \cdot \ldots \cdot g_\ell,$$

$$g_i = a_i^{(1)} e_1 + \ldots + a_i^{(s)} e_s \quad \text{for } i \in [1, \ell]$$

Define

$$f_j = \sum_{i=1}^{\ell} a_i^{(j)} X_i^{p-1} \in \mathbb{Z}[X_1, \ldots, X_\ell], \quad \text{for } j \in [1, s].$$

and define

$$f_{s+1} = \sum_{i=1}^{\ell} X_i^{p-1} \in \mathbb{Z}[X_1, \ldots, X_\ell].$$

$$V = \Big\{ \mathbf{x} \in \underbrace{I \times \ldots \times I}_{\ell} \ : \ f_j(\mathbf{x}) \equiv 0 \mod p^{m_j} \text{ for } j \in [1, s] \\ f_{s+1}(\mathbf{x}) \equiv 0 \mod p^{m_s} = n \Big\}$$

$$\mathbf{x} = (x_1, \ldots, x_\ell) \leftrightarrow T_{\mathbf{x}}, \quad g_i \text{ term of } T_{\mathbf{x}} \text{ when } x_i \neq 0.$$

The Main Tool

Theorem (G. 2023)

Let G be a finite abelian p-group with exponent $n > 1$, let $d = \left\lceil \frac{\mathsf{D}(G)}{n} \right\rceil$, let $m \geq 0$, let $X \subseteq \mathbb{N}$ be a subset of positive integers with $|X| \geq d + m$, and let $\{x_1, \ldots, x_s\} = [1, \max X] \setminus X$ with the x_i distinct. Suppose

$$\prod_{i=1}^{s} x_i \prod_{1 \leq i < j \leq s} (x_j - x_i) \not\equiv 0 \mod p^{m+1}. \tag{1}$$

Then

$$\begin{aligned} \mathsf{s}_{X \cdot n}(G) &\leq \Big(\max X - |X| + \frac{m(p-1)}{p} + 1 \Big) n + \mathsf{D}(G) - 1 \\ &\leq \Big(\max X + 1 - \frac{m}{p} \Big) n - r, \end{aligned}$$

where $r \in [1, n]$ is the integer such that $d = \frac{\mathsf{D}(G) + r - 1}{n}$.

The Proof

- Main Step: Show $\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1$ whenever

$$\frac{d(d-1)}{2} < k \leq p$$

The Proof

- Main Step: Show $\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1$ whenever

$$\frac{d(d-1)}{2} < k \leq p$$

- Transfer Step: Combine above with the following lemma to remove upper bound constraint on k.

Lemma

Let G be a finite abelian p-group with exponent m, let $d = \left\lceil \frac{\mathsf{D}(G)}{n} \right\rceil$, and let $k_0 \geq 1$. Suppose $\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1$ for all $k \in [k_0, 2k_0 - 1]$. Then

$$\mathsf{s}_{kn}(G) = kn + \mathsf{D}(G) - 1 \quad \textit{for all } k \geq k_0.$$

Thanks!