AN IMPROVED EXPONENTIAL UPPER BOUND FOR THE ERDŐS-GINZBURG-ZIV CONSTANT

Gábor Hegedűs
Óbuda University, Budapest, Hungary
hegedus.gabor@nik.uni-obuda.hu

Received: 2/28/19, Accepted: 2/27/20, Published: 3/6/20

Abstract

Tao introduces in his blog a new polynomial method, the slice rank bounding method. Naslund gave Tao's slice rank bounding method new exponential upper bounds for the Erdős–Ginzburg-Ziv constant of finite Abelian groups of high rank. He based his proofs on Tao's method. In our short manuscript we slightly improve Naslund's upper bounds. We extend Naslund's results and prove new exponential upper bounds for the Erdős–Ginzburg-Ziv constant of arbitrary finite Abelian groups. Our main results depend on a conjecture about Property D.

1. Introduction

Let A denote an additive finite Abelian group. Let $\exp(A)$ denote the exponent of A. We denote by $s(A)$ the smallest integer $\ell \in \mathbb{N}$ such that every sequence S over G of length $|S| \geq \ell$ has a zero-sum subsequence of length $|T| = \exp(A)$. Then $s(A)$ is the *Erdős-Ginzburg-Ziv* constant of A.

Harborth determined the Erdős-Ginzburg-Ziv constant $s(A)$ in the following special case in [8].

Theorem 1.1. *Let $a \geq 1$, $n \geq 1$ be arbitrary integers. Let $k := 2^a$. Let $A := (\mathbb{Z}_k)^n$. Then*

$$s(A) = (k-1)2^n + 1.$$

We frequently use the following result (see [1], Proposition 3.1).

Theorem 1.2. *Let G be a finite Abelian group and let $H \leq G$ be a subgroup such that $\exp(G) = \exp(H)\exp(G/H)$. Then*

$$s(G) \leq \exp(G/H)(s(H) - 1) + s(G/H).$$

The following lemma will be useful in our proofs (see [5], Lemma 3.5).

Lemma 1. *Let A be a finite Abelian group. Let us write A as*

$$A \cong A(p_1) \times \ldots \times A(p_m)$$

where each $A_i := A(p_i)$ is a p_i-group. Then each A_i can be written as a product of cyclic groups whose orders are power of p_i. Let n_i denote the number of these cyclic factors. Then

$$s(A) < \exp(A)\Big(\sum_{j=1}^{m} \frac{s(\mathbb{Z}_{p_j}^{n_j})}{p_j - 1}\Big).$$

Let $A := (\mathbb{Z}_k)^n$ with $k, n \in \mathbb{N}$ and $k \geq 2$. We can ask for the structure of sequences of length $s(A) - 1$ that do not have a zero-sum subsequence of length k. We now consider what is known as Property D (see [7], Section 7).

Property D: Every sequence S over A of length $|S| = s(A) - 1$ that has no zero-sum subsequence of length k has the form $S = T^{k-1}$ for some subset T over A.

Gao introduced Property D in [6]. The following statement is a well–known conjecture (see [7], Conjecture 7.2): every group $A := (\mathbb{Z}_k)^n$ satisfies Property D.

One of our main results is a better bound for $s(A)$, where $A = (\mathbb{Z}_p)^r$ and p is a prime. We also give new exponential upper bounds for the numbers $s((\mathbb{Z}_k)^r)$, where k is an arbitrary integer. We use Tao's slice rank method in our proof (see the blog post [10]). This method is a symmetric reformulation of the original Croot-Lev-Pach polynomial method (see [2]). This proof technique simplified the previous proof of Ellenberg and Gijswijt's breakthrough about the upper bounds for the size of subsets A in $(\mathbb{Z}_p)^n$ without three-term arithmetic progressions (see [4]).

Naslund achieved the following breakthrough (see [9], Theorem 2). He used Tao's rank bounding method in his proofs.

Theorem 1.3. *Let q denote an arbitrary prime power. Suppose that $A := (\mathbb{Z}_q)^n$ satisfies Property D. Then*

$$s(A) \leq (q-1)\gamma_q^n + 1,$$

where

$$\gamma_q = \inf_{0<x<1} \frac{1-x^q}{1-x} x^{-\frac{q-1}{q}}.$$

Consequently

$$s(A) \leq (q-1)4^n + 1.$$

Finally we use the following well-known statement in the proofs of our main results (for a simple proof see [3] Chapter 9).

Lemma 2. *Consider the set of monomials*

$$B(n,k) := \{x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} : \sum_i \alpha_i \leq k\}.$$

Then

$$|B(n,k)| = \binom{n+k}{n}.$$

We now state our main results.

Theorem 1.4. *Let p be a prime. Let $n \geq 1$ be an integer. Suppose that Property D is satisfied for the group $(\mathbb{Z}_p)^n$. Then*

$$s((\mathbb{Z}_p)^n) \leq p(p-1)\binom{\lceil \frac{n(2p-1)}{p} \rceil}{n} + 1.$$

We prove a generalization of Theorem 1.4 using Theorem 1.2.

Theorem 1.5. *Let $q = p^\alpha \geq 3$ be an odd prime power. Let $n \geq 1$ be an integer. Suppose that Property D is satisfied for the group $(\mathbb{Z}_p)^n$. Then*

$$s((\mathbb{Z}_q)^n) \leq p(q-1)\binom{2n}{n} + 1.$$

We can extend Theorem 1.5 from a prime power to an arbitrary composite number using Lemma 1.

Theorem 1.6. *Let A be a finite Abelian group. We can write A as*

$$A \cong A(p_1) \times \ldots \times A(p_m)$$

where each $A_i := A(p_i)$ is a p_i-group. Then each A_i is a product of cyclic groups whose orders are a power of p_i. Let n_i denote the number of these cyclic factors. Suppose that Property D is satisfied for each group $(\mathbb{Z}_{p_i})^{n_i}$, where $1 \leq i \leq m$. Then

$$s(A) < \exp(A)\Big(\sum_{j=1}^{m} p_j \binom{2n_j}{n_j} + \sum_{j=1}^{m} \frac{1}{p_j - 1}\Big).$$

In Section 2 we present our proofs.

2. Proofs of the Main Results

Before proving the main results, we need the following theorem.

Theorem 2.1. *Suppose that $A \subseteq (\mathbb{Z}_p)^n$ satisfies*

$$|A| > p\binom{\lceil \frac{n(2p-1)}{p} \rceil}{n}.$$

Then A contains p, not necessarily distinct but not all equal elements, $v_1, \ldots, v_p$, such that

$$\sum_i v_i = 0.$$

Proof. We will use an indirect argument. Suppose that A does not contain p, not necessarily distinct but not all equal elements, $v_1, \dots, v_p$ such that $\sum_i v_i = 0$. Then it follows from Tao's slice rank bounding method (see [9], Proposition 1 and Inequality 5.3) that

$$|A| \le p \cdot |\{x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} : \ 0 \le \alpha_i \le p-1 \text{ for each } i, \ \sum_i \alpha_i \le \frac{n(p-1)}{p}\}|.$$

But

$$|\{x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} : \ 0 \le \alpha_i \le p-1 \text{ for each } i, \ \sum_i \alpha_i \le \frac{n(p-1)}{p}\}|$$
$$\le |\{x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} : \ \alpha_i \ge 0 \text{ for each } i, \ \sum_i \alpha_i \le \frac{n(p-1)}{p}\}|$$
$$= \binom{\lceil \frac{n(2p-1)}{p} \rceil}{n}$$

by Lemma 2; hence,

$$|A| \le p \binom{\lceil \frac{n(2p-1)}{p} \rceil}{n}.$$

□

Proof of Theorem 1.4. This result follows easily from the assumption that Property D is satisfied for the group $(\mathbb{Z}_p)^n$ and Theorem 2.1. Namely, let S be an arbitrary sequence in $(\mathbb{Z}_p)^n$ of length $s((\mathbb{Z}_p)^n) - 1$ for which there exist no p elements that sum to zero. Then Property D implies that we can write S as a multi-set in the form

$$S = \cup_{i=1}^{p-1} B,$$

where $B \subseteq (\mathbb{Z}_p)^n$ is a subset. Clearly B does not contain p not necessarily distinct but not all equal elements that sum to zero. We get from Theorem 2.1 that

$$|B| \le p \binom{\lceil \frac{n(2p-1)}{p} \rceil}{n},$$

and consequently

$$s({\mathbb{Z}_p}^n) \le p(p-1) \binom{\lceil \frac{n(2p-1)}{p} \rceil}{n} + 1.$$

□

Proof of Theorem 1.5. Let $G := (\mathbb{Z}_q)^n$ and let H denote the subgroup of G isomorphic to $(\mathbb{Z}_p)^n$. Clearly $G/H \cong (\mathbb{Z}_{p^{\alpha-1}})^n$ and $\exp(G/H) = p^{\alpha-1}$. By the inductive hypothesis we get that

$$s(G/H) \le p(p^{\alpha-1} - 1)\binom{2n}{n} + 1.$$

It follows from Theorem 1.4 that

$$s(H) \leq p(p-1)\binom{\lceil \frac{n(2p-1)}{p} \rceil}{n} + 1 \leq p(p-1)\binom{2n}{n} + 1.$$

We can apply Theorem 1.2 for G and H, since $\exp(G) = \exp(H)\exp(G/H)$:

$$s(G) \leq \exp(G/H)(s(H)-1) + s(G/H) \leq$$

$$\leq p^{\alpha-1} \cdot \left(p(p-1)\binom{2n}{n}\right) + p(p^{\alpha-1}-1)\binom{2n}{n} + 1 = p(p^{\alpha}-1)\binom{2n}{n} + 1.$$

□

Proof of Theorem 1.6. It follows from Theorem 1.5 that

$$s(\mathbb{Z}_{p_j}^{n_j}) \leq p_j(p_j-1)\binom{2n_j}{n_j} + 1$$

for each $1 \leq i \leq m$. If we combine these inequalities with Lemma 1, then we get our result. □

References

[1] R. Chi, S. Ding, W. Gao, A. Geroldinger, and A. W. Schmid, On zero-sum subsequences of restricted size. IV., *Acta Math. Hungar.* **107(4)** (2005), 337-344.

[2] E. Croot, V. Lev and P. Pach, Progression-free sets in $\mathbb{Z}_4^n$, *Ann. of Math.* **185(1)** (2017), 331-337.

[3] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, Berlin, Heidelberg, 1992.

[4] J. S. Ellenberg and D. Gijswijt, On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression, *Ann. of Math.* **185(1)** (2017), 339-343.

[5] J. Fox and L. Sauermann, Erdős–Ginzburg–Ziv constants by avoiding three-term arithmetic progressions, *Electron. J. Combin.* **25(2)** (2018), 2-14.

[6] W. Gao, Two zero-sum problems and multiple properties, *J. Number Theory* **81(2)** (2000), 254-265.

[7] W. Gao and A. Geroldinger, Zero-sum problems in finite Abelian groups: a survey, *Expo. Math.* **24(4)** (2006), 337-369.

[8] H. Harborth, Ein Extremalproblem für Gitterpunkte, *J. Reine Angew. Math.* **262** (1973), 356-360.

[9] E. Naslund, Exponential Bound for the Erdős-Ginzburg-Ziv Constant, arXiv preprint, arXiv:1701.04942 (2017).

[10] T. Tao, A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound, `https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the-croot-lev-pachellenberg- gijswijt-capset-bound`, 2016.