Erdős-Ginzburg-Ziv constants by avoiding three-term arithmetic progressions

Jacob Fox* Lisa Sauermann†

Department of Mathematics
Stanford University
Stanford, CA 94305, U.S.A.

{jacobfox,lsauerma}@stanford.edu

Submitted: Aug 30, 2017; Accepted: Apri 10, 2018; Published: Apr 27, 2018

Abstract

For a finite abelian group G, the Erdős-Ginzburg-Ziv constant $\mathfrak{s}(G)$ is the smallest s such that every sequence of s (not necessarily distinct) elements of G has a zero-sum subsequence of length $\exp(G)$. For a prime p, let $r(\mathbb{F}_p^n)$ denote the size of the largest subset of $\mathbb{F}_p^n$ without a three-term arithmetic progression. Although similar methods have been used to study $\mathfrak{s}(G)$ and $r(\mathbb{F}_p^n)$, no direct connection between these quantities has previously been established. We give an upper bound for $\mathfrak{s}(G)$ in terms of $r(\mathbb{F}_p^n)$ for the prime divisors p of $\exp(G)$. For the special case $G = \mathbb{F}_p^n$, we prove $\mathfrak{s}(\mathbb{F}_p^n) \leqslant 2p \cdot r(\mathbb{F}_p^n)$. Using the upper bounds for $r(\mathbb{F}_p^n)$ of Ellenberg and Gijswijt, this result improves the previously best known upper bounds for $\mathfrak{s}(\mathbb{F}_p^n)$ given by Naslund.

Mathematics Subject Classifications: 11B25, 11B30, 05D40, 05D10

1 Introduction

Let G be a non-trivial finite abelian group, additively written. We denote the exponent of G by $\exp(G)$; this is the least common multiple of the orders of all elements of G.

The Erdős-Ginzburg-Ziv constant $\mathfrak{s}(G)$ is the smallest integer s such that every sequence of s (not necessarily distinct) elements of G has a subsequence of length $\exp(G)$ whose elements sum to zero in G. Furthermore, let $\mathfrak{g}(G)$ denote the smallest integer a such that every subset $A \subseteq G$ of size $|A| \geqslant a$ contains $\exp(G)$ distinct elements summing to zero in G. It is easy to see that $\mathfrak{g}(G) \leqslant \mathfrak{s}(G)$ and $\mathfrak{s}(G) \leqslant (\exp(G) - 1)(\mathfrak{g}(G) - 1) + 1$.

*Research supported by a Packard Fellowship and by NSF Career Award DMS-1352121.
†Research supported by Jacob Fox's Packard Fellowship.

A three-term arithmetic progression is a subset of G consisting of three distinct elements such that the sum of two of these elements equals twice the third element, i.e. a set of the form $\{x, y, z\} \subseteq G$ with x, y, z distinct and $x + z = 2y$. For $y \in G$, a three-term arithmetic progression with middle term y is a set of the form $\{x, y, z\} \subseteq G$ with x, y, z distinct and $x + z = 2y$. For a finite abelian group G, let $r(G)$ denote the largest size of a subset of G without a three-term arithmetic progression. Note that $r(\mathbb{F}_2^n) = 2^n$, since there are no three-term arithmetic progressions in $\mathbb{F}_2^n$. Also note that in the case of $G = \mathbb{F}_3^n$, a three-term arithmetic progression is the same as a set of three distinct elements summing to zero, hence $r(\mathbb{F}_3^n) = \mathfrak{g}(\mathbb{F}_3^n) - 1$ (see also [2] and [10]).

In 1961, Erdős, Ginzburg and Ziv [13] proved for each positive integer k that any sequence of $2k - 1$ integers contains a subsequence of length k whose sum is divisible by k. The same statement is clearly not true for sequences of length $2k-2$. Thus, their result can be reformulated as $\mathfrak{s}(\mathbb{Z}/k\mathbb{Z}) = 2k - 1$. The work of Erdős, Ginzburg and Ziv [13] was the starting point for a whole field studying different zero-sum problems in various finite abelian groups; see for example the survey article by Gao and Geroldinger [15].

Note that $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n)$ has a simple geometric interpretation: it is the smallest number s such that among any s points in the lattice $\mathbb{Z}^n$ one can choose k points such that their centroid is again a lattice point in $\mathbb{Z}^n$. Harborth [18] investigated $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n)$ in this context and was the first to study Erdős-Ginzburg-Ziv constants for non-cyclic groups. He proved

$$(k-1)2^n + 1 \leqslant \mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) \leqslant (k-1)k^n + 1,$$

where the upper bound is easily obtained from the pigeonhole principle. Harborth [18] also established $\mathfrak{s}((\mathbb{Z}/2^m\mathbb{Z})^n) = (2^m - 1)2^n + 1$ and in particular $\mathfrak{s}(\mathbb{F}_2^n) = 2^n + 1$. For $n = 2$, Reiher [20] determined that $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^2) = 4k - 3$ for all positive integers k. Alon and Dubiner [3] proved $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) \leqslant (cn \log n)^n k$ for some absolute constant c. Hence, for any fixed n, the quantity $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n)$ grows linearly with k. It remains an interesting question to estimate $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n)$ when k is fixed and n is large. Elsholtz [12] obtained the lower bounds $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) \geqslant 1.125^{\lfloor n/3 \rfloor}(k-1)2^n + 1$ for $k \geqslant 3$ odd and all n, and in particular $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) \geqslant 2.08^n$ if $k \geqslant 3$ is odd and n is sufficiently large.

For general finite abelian groups, Gao and Yang [16] proved the upper bound $\mathfrak{s}(G) \leqslant |G| + \exp(G) - 1$ (see also [17, Theorem 5.7.4]). Alon and Dubiner's result [3] has been used to obtain upper bounds on $\mathfrak{s}(G)$ when G has small rank (the rank of G is $\max(n_1, \ldots, n_m)$, where $n_1, \ldots, n_m$ are defined as in Theorem 1 below), see [10, Theorem 1.4] and [8, Theorem 1.5]. In this paper, we will focus on the opposite case where at least one of $n_1, \ldots, n_m$ is large compared to $\exp(G)$.

The case $G = \mathbb{F}_p^n$ for a prime $p \geqslant 3$ has attracted particular interest. In this case, Naslund [19] proved that $\mathfrak{g}(\mathbb{F}_p^n) \leqslant (2^p - p - 2) \cdot (J(p)p)^n$ and $\mathfrak{s}(\mathbb{F}_p^n) \leqslant (p-1)2^p \cdot (J(p)p)^n$, where $0.8414 \leqslant J(p) \leqslant 0.9184$. To prove these bounds, Naslund introduced a variant of Tao's slice rank method [22]. Tao developed this method as an alternative formulation of the proof of $r(\mathbb{F}_p^n) \leqslant (J(p)p)^n$ by Ellenberg and Gijswijt [11], which in turn used the new polynomial method introduced by Croot, Lev and Pach [9] to prove $r((\mathbb{Z}/4\mathbb{Z})^n) \leqslant 3.62^n$. Note that the constant $J(p)p$ in Naslund's bounds for $\mathfrak{g}(\mathbb{F}_p^n)$ and $\mathfrak{s}(\mathbb{F}_p^n)$ is the same as in the bound $r(\mathbb{F}_p^n) \leqslant (J(p)p)^n$ by Ellenberg and Gijswijt [11], see also [6].

While similar methods have been applied to prove upper bounds for the Erdős-Ginzburg-Ziv constant and upper bounds for sets without arithmetic progressions, no direct connection between the two problems has previously been established (apart from the case $G = \mathbb{F}_3^n$ mentioned above). In this note, we derive upper bounds for $\mathfrak{s}(G)$ for all finite abelian groups G in terms of $r(\mathbb{F}_p^n)$ for the prime divisors p of $\exp(G)$. It is also possible to prove an upper bound of the form $\mathfrak{s}(G) \leqslant O(\exp(G)r(G))$. However, $\exp(G)r(G)$ is usually much larger than our upper bound in Theorem 1.

Theorem 1. *Let G be a non-trivial finite abelian group. Let $p_1, \dots, p_m$ be the distinct prime factors of $\exp(G)$. When writing G as a product of cyclic groups of prime power order, all the occurring prime powers are powers of $p_1, \dots, p_m$. For $i = 1, \dots, m$, let n_i be the number of cyclic factors of G whose order is a power of p_i. Then we have*

$$\mathfrak{s}(G) < 3\exp(G) \cdot (r(\mathbb{F}_{p_1}^{n_1}) + \cdots + r(\mathbb{F}_{p_m}^{n_m})).$$

For the case $G = (\mathbb{Z}/k\mathbb{Z})^n$ we obtain the following corollary (note that $\mathbb{Z}/k\mathbb{Z}$ has precisely one cyclic factor of prime power order for each distinct prime dividing k, hence $(\mathbb{Z}/k\mathbb{Z})^n$ has precisely n cyclic factors for each distinct prime dividing k).

Corollary 2. *Let $k \geqslant 2$ be an integer and let $p_1, \dots, p_m$ be its distinct prime factors. Then we have*

$$\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) < 3k(r(\mathbb{F}_{p_1}^n) + \cdots + r(\mathbb{F}_{p_m}^n))$$

for every positive integer n.

Recall that $r(\mathbb{F}_2^n) = 2^n$. For primes $p \geqslant 3$ it is known from [11] and [6] that $r(\mathbb{F}_p^n) \leqslant (J(p)p)^n$, with $0.8414 \leqslant J(p) \leqslant 0.9184$ and with $J(p)$ being a decreasing function that tends to $0.8414\dots$ as $p \to \infty$ (see [6] for more details and for the precise definition of the function $J(p)$). As a lower bound, we have $r(\mathbb{F}_p) \geqslant p^{1-o(1)}$ by Behrend's construction [5] and $r(\mathbb{F}_p^n) \geqslant p^{(1-o(1))n}$ by taking a product with Behrend's construction in each coordinate (here $o(1) \to 0$ as $p \to \infty$ independently of n). Furthermore, Alon, Shpilka and Umans [4], relying on a construction of Salem and Spencer [21], proved $r(\mathbb{F}_p^n) \geqslant (p/2)^{(1-o(1))n}$, where $o(1) \to 0$ as $n \to \infty$ with p fixed. A variant of Behrend's construction due to Alon gives an improvement of the $o(1)$-term (see [14, Lemma 17]). Note that in light of $r(\mathbb{F}_p^n) \geqslant (p/2)^{(1-o(1))n}$, for large n and odd $k \geqslant 3$ there is still a big gap between Elsholtz' lower bound $\mathfrak{s}((\mathbb{Z}/k\mathbb{Z})^n) \geqslant 2.08^n$ and the upper bound for $s((\mathbb{Z}/k\mathbb{Z})^n)$ in Corollary 2.

The bounds in Theorem 1 and Corollary 2 look clean and simple, but they are not the optimal results that can be obtained from our arguments (see Remark 9 and the second inequality in Lemma 10 where certain terms are just ignored). However, the improvements when optimizing the estimates in our proof are not very significant as long as $\exp(G)$ is small compared to at least one of $n_1, \dots, n_m$.

In Section 2, we will first prove the following upper bounds for $\mathfrak{g}(\mathbb{F}_p^n)$ and $\mathfrak{s}(\mathbb{F}_p^n)$ using the probabilistic method. In Section 3 we will then deduce Theorem 1 from Theorem 4.

Theorem 3. *Let $p \geqslant 3$ be a prime and $n \geqslant 2$ be an integer. Then $\mathfrak{g}(\mathbb{F}_p^n) \leqslant 2p \cdot r(\mathbb{F}_p^{n-1})$.*

Theorem 4. *Let $p \geqslant 3$ be a prime and $n \geqslant 1$ be an integer. Then $\mathfrak{s}(\mathbb{F}_p^n) \leqslant 2p \cdot r(\mathbb{F}_p^n)$.*

For $p \geqslant 3$ prime, using $r(\mathbb{F}_p^n) \leqslant (J(p)p)^n$, we obtain

$$\mathfrak{g}(\mathbb{F}_p^n) \leqslant 2p \cdot r(\mathbb{F}_p^{n-1}) \leqslant 2p \cdot (J(p)p)^{n-1} < 3(J(p)p)^n$$

and

$$\mathfrak{s}(\mathbb{F}_p^n) \leqslant 2p \cdot r(\mathbb{F}_p^n) \leqslant 2p \cdot (J(p)p)^n,$$

which slightly improves the previously best known bounds for $\mathfrak{g}(\mathbb{F}_p^n)$ and $\mathfrak{s}(\mathbb{F}_p^n)$ from [19].

To obtain an upper bound for $\mathfrak{g}(\mathbb{F}_p^n)$ in terms of $r(\mathbb{F}_p^n)$, note that a product construction shows

$$r(\mathbb{F}_p^n) \geqslant r(\mathbb{F}_p^{n-1}) \cdot r(\mathbb{F}_p) \geqslant 2r(\mathbb{F}_p^{n-1})p^{1-o(1)}.$$

Hence, Theorem 3 implies $\mathfrak{g}(\mathbb{F}_p^n) \leqslant p^{o(1)} r(\mathbb{F}_p^n)$, where $o(1) \to 0$ as $p \to \infty$ independently of n.

2 Proof of Theorems 3 and 4

Lemma 5. *Let $p \geqslant 3$ be a prime and $n \geqslant 1$. If $A \subseteq \mathbb{F}_p^n$ does not contain p distinct elements summing to zero, then for every $x \in A$ the set A contains at most $\frac{p-3}{2}$ different three-term arithmetic progressions with middle term x.*

Proof. Suppose that for some $x \in A$ the set A contains $\frac{p-1}{2}$ different three-term arithmetic progressions with middle term x. Each of them consists of x and two more elements of A whose sum equals $2x$. So we obtain $\frac{p-1}{2}$ pairs of elements of A, each pair with sum $2x$. It is not hard to see that the $p-1$ elements of A involved in these $\frac{p-1}{2}$ pairs are all distinct and distinct from x. So taking these $p-1$ elements together with x itself, we obtain p distinct elements of A with sum $\frac{p-1}{2} \cdot 2x + x = p \cdot x = 0$. This is a contradiction to the assumption on A. □

Remark 6. By definition, $r(\mathbb{F}_p^{n-1})$ is the largest size of a subset of $\mathbb{F}_p^{n-1}$ without a three-term arithmetic progression. Let V be an affine subspace of dimension $n-1$ in $\mathbb{F}_p^n$, i.e. a hyperplane in $\mathbb{F}_p^n$. We can consider a translation moving V to the origin (so that it becomes a linear subspace of dimension $n-1$) and then an isomorphism to $\mathbb{F}_p^{n-1}$. This gives a bijection between V and $\mathbb{F}_p^{n-1}$ which preserves three-term arithmetic progressions. Hence the largest size of a subset of V without a three-term arithmetic progression is also equal to $r(\mathbb{F}_p^{n-1})$.

We will now prove Theorem 3. Note that $\exp(\mathbb{F}_p^n) = p$.

Proof of Theorem 3. Let $A \subseteq \mathbb{F}_p^n$ be a subset that does not contain p distinct elements summing to zero. We need to show that $|A| < 2p \cdot r(\mathbb{F}_p^{n-1})$.

By Lemma 5 we know that for every $x \in A$ the set A contains at most $\frac{p-3}{2}$ different three-term arithmetic progressions with middle term x. Hence the total number of three-term arithmetic progressions contained in the set A is at most $\frac{p-3}{2}|A|$.

Pick an affine subspace V of dimension $n-1$ in $\mathbb{F}_p^n$ uniformly at random. Let $X_1 = |A \cap V|$ and let X_2 be the number of three-term arithmetic progressions that are contained in $A \cap V$. Since each point of A is contained in V with probability $\frac{1}{p}$, we have $\mathbb{E}[X_1] = \frac{1}{p}|A|$.

For any three-term arithmetic progression, the probability that its first element is contained in V is equal to $\frac{1}{p}$. Conditioned on this, the probability that its second element is also contained in V is $\frac{p^{n-1}-1}{p^n-1} < \frac{1}{p}$ (and note that then the third element will be contained in V as well). Hence for any three-term arithmetic progression contained in A, the probability that it is contained in $A \cap V$ is less than $\frac{1}{p^2}$. Since A contains at most $\frac{p-3}{2}|A|$ three-term arithmetic progressions, we obtain

$$\mathbb{E}[X_2] < \frac{1}{p^2} \cdot \frac{p-3}{2}|A| < \frac{1}{2p}|A|.$$

Thus, $\mathbb{E}[X_1 - X_2] > \frac{1}{2p}|A|$. So we can choose an affine subspace V of dimension $n-1$ in $\mathbb{F}_p^n$ such that $X_1 - X_2 > \frac{1}{2p}|A|$. Let B be a set obtained from $A \cap V$ after deleting one element from each three-term arithmetic progression contained in $A \cap V$. Then $|B| \geqslant X_1 - X_2 > \frac{1}{2p}|A|$. By construction, B is a subset of V that does not contain any three-term arithmetic progression. By Remark 6, we can conclude that $|B| \leqslant r(\mathbb{F}_p^{n-1})$. Thus, $\frac{1}{2p}|A| < |B| \leqslant r(\mathbb{F}_p^{n-1})$ and therefore $|A| < 2p \cdot r(\mathbb{F}_p^{n-1})$. □

Our proof of Theorem 3 is somewhat similar to the first half of the proof of Proposition 2.5 in Alon's paper [1]. There, he also considered points which are the middle term of only few three-term arithmetic progressions and obtained a subset without any three-term arithmetic progressions, yielding a contradiction. However, Alon's work [1] is in a very different context and does not use a subspace sampling argument.

Finally, we will deduce Theorem 4 from Theorem 3.

Proof of Theorem 4. Assume we are given a sequence of vectors in $\mathbb{F}_p^n$ without a zero-sum subsequence of length p. Every vector occurs at most $p-1$ times in the sequence. Hence by attaching one additional coordinate we can make all the vectors in the sequence distinct. This way, we obtain a subset of $\mathbb{F}_p^{n+1}$ without p distinct elements summing to zero. Since this subset has size at most $\mathfrak{g}(\mathbb{F}_p^{n+1}) - 1$, we can conclude that the original sequence had length at most $\mathfrak{g}(\mathbb{F}_p^{n+1}) - 1$. This shows $\mathfrak{s}(\mathbb{F}_p^n) \leqslant \mathfrak{g}(\mathbb{F}_p^{n+1})$ and together with Theorem 3 with n replaced by $n+1$, we obtain $\mathfrak{s}(\mathbb{F}_p^n) \leqslant \mathfrak{g}(\mathbb{F}_p^{n+1}) \leqslant 2p \cdot r(\mathbb{F}_p^n)$ as desired. □

3 Proof of Theorem 1

In this section we will first bound $\mathfrak{s}(G)$ for any finite abelian group G by terms of the form $\mathfrak{s}(\mathbb{F}_p^n)$. Then, applying Theorem 4, we will obtain Theorem 1.

The following lemma was proved by Chi, Ding, Gao, Geroldinger and Schmid [7, Proposition 3.1] and is a generalization of [18, Hilfssatz 2]. For the reader's convenience we repeat the proof here.

Lemma 7 (Proposition 3.1 in [7])**.** *Let G be a non-trivial finite abelian group and $H \subseteq G$ be a subgroup such that* $\exp(G) = \exp(H)\exp(G/H)$. *Then*

$$\mathfrak{s}(G) \leqslant \exp(G/H)(\mathfrak{s}(H) - 1) + \mathfrak{s}(G/H).$$

Proof. Consider a sequence of length $\exp(G/H)(\mathfrak{s}(H) - 1) + \mathfrak{s}(G/H)$ with elements in G. Then we can find a subsequence of length $\exp(G/H)$ summing to zero in G/H, i.e. summing to an element of H. Delete this subsequence and repeat. We can do this $\mathfrak{s}(H)$ many times (since after $\mathfrak{s}(H) - 1$ many times we still have $\mathfrak{s}(G/H)$ elements left). So we find $\mathfrak{s}(H)$ disjoint subsequences each of length $\exp(G/H)$ and the sum of each of the subsequences is in H. Now writing down these $\mathfrak{s}(H)$ sums, we get a sequence of length $\mathfrak{s}(H)$ with elements in H. So we can choose $\exp(H)$ of them summing to zero. Now taking the union of the corresponding subsequences of the original sequence we obtain $\exp(H)\exp(G/H) = \exp(G)$ elements summing to zero. □

Lemma 8. *For any finite abelian p-group $G = (\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_n}\mathbb{Z})$, where $a_1 \geqslant \ldots \geqslant a_n$ are positive integers and $p \geqslant 2$ is prime, we have*

$$\mathfrak{s}(G) = \mathfrak{s}((\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_n}\mathbb{Z})) \leqslant \frac{p^{a_1} - 1}{p - 1}\mathfrak{s}(\mathbb{F}_p^n) < \frac{\exp(G)}{p - 1}\mathfrak{s}(\mathbb{F}_p^n).$$

Proof. Since $\exp(G) = p^{a_1}$, the second inequality is clearly true. Now, let us prove the first inequality by induction on a_1. If $a_1 = 1$, then $a_1 = \cdots = a_n = 1$ and so

$$\mathfrak{s}((\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_n}\mathbb{Z})) = \mathfrak{s}(\mathbb{F}_p^n) = \frac{p^{a_1} - 1}{p - 1}\mathfrak{s}(\mathbb{F}_p^n).$$

For $a_1 > 1$ we can apply Lemma 7 to $H = pG$. Indeed, $G/H \cong \mathbb{F}_p^n$ and $H \cong (\mathbb{Z}/p^{a_1-1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_n-1}\mathbb{Z})$. In particular, $\exp(G) = p^{a_1} = p^{a_1-1} \cdot p = \exp(H)\exp(G/H)$. So by Lemma 7 we have

$$\begin{aligned}\mathfrak{s}(G) &\leqslant \exp(\mathbb{F}_p^n)(\mathfrak{s}((\mathbb{Z}/p^{a_1-1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_n-1}\mathbb{Z})) - 1) + \mathfrak{s}(\mathbb{F}_p^n)\\ &< p\mathfrak{s}((\mathbb{Z}/p^{a_1-1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_n-1}\mathbb{Z})) + \mathfrak{s}(\mathbb{F}_p^n).\end{aligned}$$

Let $n' \leqslant n$ be such that $a_1 \geqslant \ldots \geqslant a_{n'} \geqslant 2$ and $a_{n'+1} = \cdots = a_n = 1$. Then by the induction assumption we have

$$\begin{aligned}\mathfrak{s}((\mathbb{Z}/p^{a_1-1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_n-1}\mathbb{Z})) &= \mathfrak{s}((\mathbb{Z}/p^{a_1-1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_{n'}-1}\mathbb{Z}))\\ &\leqslant \frac{p^{a_1-1} - 1}{p - 1}\mathfrak{s}(\mathbb{F}_p^{n'}) \leqslant \frac{p^{a_1-1} - 1}{p - 1}\mathfrak{s}(\mathbb{F}_p^n).\end{aligned}$$

Thus,

$$\mathfrak{s}(G) = \mathfrak{s}((\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_n}\mathbb{Z})) \leqslant p \cdot \frac{p^{a_1-1} - 1}{p - 1}\mathfrak{s}(\mathbb{F}_p^n) + \mathfrak{s}(\mathbb{F}_p^n) = \frac{p^{a_1} - 1}{p - 1}\mathfrak{s}(\mathbb{F}_p^n),$$

completing the induction. □

Remark 9. The proof of Lemma 8 also gives the stronger but more complicated bound

$$\mathfrak{s}((\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_n}\mathbb{Z})) \leqslant \sum_{j=1}^{a_1} p^{j-1}\mathfrak{s}(\mathbb{F}_p^{b_j}),$$

where $b_j = \max\{i \mid a_i \geqslant j\}$ for $j = 1, \ldots, a_1$. Note that $b_1 \geqslant \ldots \geqslant b_{a_1}$ is the conjugate of $a_1 \geqslant \ldots \geqslant a_n$ in the sense of Young diagrams.

Lemma 10. *Let G be a non-trivial finite abelian group. Let $p_1, \ldots, p_m$ be the distinct prime factors of $\exp(G)$. Let us write $G \cong G_1 \times \cdots \times G_m$ where each G_i is a p_i-group. Then*

$$\mathfrak{s}(G) \leqslant \sum_{i=1}^{m} \exp(G_1)\cdots\exp(G_{i-1})\mathfrak{s}(G_i) \leqslant \exp(G)\left(\frac{\mathfrak{s}(G_1)}{\exp(G_1)} + \cdots + \frac{\mathfrak{s}(G_m)}{\exp(G_m)}\right).$$

Proof. First, note that $\exp(G) = \exp(G_1)\cdots\exp(G_m)$. In particular

$$\exp(G_1)\cdots\exp(G_{i-1}) \leqslant \frac{\exp(G)}{\exp(G_i)}$$

for every i, which makes the second inequality true. We prove the first inequality by induction on m. If $m = 1$, the statement is trivial. If $m > 1$, note that we can apply Lemma 7 to $H = G_m$ and obtain

$$\mathfrak{s}(G) \leqslant \exp(G_1 \times \cdots \times G_{m-1})(\mathfrak{s}(G_m) - 1) + \mathfrak{s}(G_1 \times \cdots \times G_{m-1}).$$

Plugging in $\exp(G_1 \times \cdots \times G_{m-1}) = \exp(G_1)\cdots\exp(G_{m-1})$ as well as using the induction assumption for $G_1 \times \cdots \times G_{m-1}$ yields

$$\begin{aligned}\mathfrak{s}(G) \leqslant \exp(G_1)\cdots\exp(G_{m-1})\mathfrak{s}(G_m) + \sum_{i=1}^{m-1}\exp(G_1)\cdots\exp(G_{i-1})\mathfrak{s}(G_i)\\ = \sum_{i=1}^{m}\exp(G_1)\cdots\exp(G_{i-1})\mathfrak{s}(G_i)\end{aligned}$$

as desired. □

Lemma 11. *Under the assumptions of Theorem 1 we have*

$$\mathfrak{s}(G) < \exp(G)\left(\frac{\mathfrak{s}(\mathbb{F}_{p_1}^{n_1})}{p_1 - 1} + \cdots + \frac{\mathfrak{s}(\mathbb{F}_{p_m}^{n_m})}{p_m - 1}\right).$$

Proof. As in Lemma 10, let us write $G \cong G_1 \times \cdots \times G_m$ where each G_i is a p_i-group. Each G_i can be written as a product of cyclic groups whose orders are powers of p_i. Note that the number of factors of each G_i is precisely n_i, because together all these factorizations form the unique representation of G as a product of cyclic groups of prime power order. So, by Lemma 8, we have

$$\mathfrak{s}(G_i) < \frac{\exp(G_i)}{p_i - 1}\mathfrak{s}(\mathbb{F}_{p_i}^{n_i})$$

for $i = 1, \ldots, m$. Now the desired inequality follows directly from Lemma 10. □

Proof of Theorem 1. Note that by Theorem 4 we have

$$\frac{\mathfrak{s}(\mathbb{F}_{p_i}^{n_i})}{p_i-1} \leqslant \frac{2p_i}{p_i-1} r(\mathbb{F}_{p_i}^{n_i}) \leqslant 3r(\mathbb{F}_{p_i}^{n_i})$$

for all the odd p_i. Since $\mathfrak{s}(\mathbb{F}_2^n) = 2^n + 1$ (see [18, Korollar 1]) and $r(\mathbb{F}_2^n) = 2^n$, we also have $\frac{\mathfrak{s}(\mathbb{F}_{p_i}^{n_i})}{p_i-1} \leqslant 3r(\mathbb{F}_{p_i}^{n_i})$ if $p_i = 2$. Thus, Lemma 11 gives

$$\mathfrak{s}(G) < \exp(G) \cdot \left(3r(\mathbb{F}_{p_1}^{n_1}) + \cdots + 3r(\mathbb{F}_{p_m}^{n_m})\right) = 3\exp(G) \cdot (r(\mathbb{F}_{p_1}^{n_1}) + \cdots + r(\mathbb{F}_{p_m}^{n_m})),$$

as desired. □

Acknowledgements.

We would like to thank the anonymous referees for helpful comments, including pointing out the reference [1].

References

[1] N. Alon, Subset sums, *J. Number Theory* **27** (1987), 196–205.

[2] N. Alon and M. Dubiner, Zero-sum sets of prescribed size, *Combinatorics, Paul Erdős is eighty*, Vol. 1, 33–50, János Bolyai Math. Soc., Budapest, 1993.

[3] N. Alon and M. Dubiner, A lattice point problem and additive number theory, *Combinatorica* **15** (1995), 301–309.

[4] N. Alon, A. Shpilka, and C. Umans, On sunflowers and matrix multiplication, *Comput. Complexity* **22** (2013), 219–243.

[5] F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U.S.A.* **32** (1946), 331–332.

[6] J. Blasiak, T. Church, H. Cohn, J. A. Grochow, E. Naslund, W. F. Sawin, and C. Umans, On cap sets and the group-theoretic approach to matrix multiplication, *Discrete Anal.* 2017, Paper No. 3, 27pp.

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

[8] M. N. Chintamani, B. K. Moriya, W. D. Gao, P. Paul, and R. Thangadurai, New upper bounds for the Davenport and for the Erdős-Ginzburg-Ziv constants, *Arch. Math.* **98** (2012), 133–142.

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

[10] Y. Edel. C. Elsholtz, A. Geroldinger, S. Kubertin, and L. Rackham, Zero-sum problems in finite abelian groups and affine caps, *Q. J. Math.* **58** (2007), 159–186.

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

[12] C. Elsholtz, Lower bounds for multidimensional zero sums, *Combinatorica* **24** (2004), 351–358.

[13] P. Erdős, A. Ginzburg, and A. Ziv, Theorem in the additive number theory, *Bull. Res. Council Israel* **10F** (1961), 41–43.

[14] J. Fox and H. T. Pham, Popular progression differences in vector spaces II, *Discrete Analysis*, to appear.

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

[16] W. D. Gao and Y. X. Yang, Note on a combinatorial constant, *J. Math. Res. Expo.* **17** (1997), 139–140.

[17] A. Geroldinger and F. Halter-Koch, Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory, *Pure and Applied Mathematics*, vol. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006.

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

[19] E. Naslund, Exponential Bounds for the Erdős-Ginzburg-Ziv Constant, preprint, 2018, arXiv:1701.04942v2

[20] C. Reiher, On Kemnitz' conjecture concerning lattice-points in the plane, *Ramanujan J.* **13** (2007), 333–337.

[21] R. Salem and D. C. Spencer, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U.S.A.* **28** (1942), 561–563.

[22] T. Tao, A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound, blog post, 2016, http://terrytao.wordpress.com/2016/05/18/a.