Arch. Math. 122 (2024), 17–29

0003-889X/24/010017-13
published online October 7, 2023
https://doi.org/10.1007/s00013-023-01916-4

Archiv der Mathematik

Bounds on the higher degree Erdős–Ginzburg–Ziv constants over $\mathbb{F}_q^n$

Simone Costa and Stefano Della Fiore

Abstract. The classical Erdős–Ginzburg–Ziv constant of a group G denotes the smallest positive integer ℓ such that any sequence S of length at least ℓ contains a zero-sum subsequence of length $\exp(G)$. In the recent paper (Integers 22: Paper No. A102, 17 pp., 2022), Caro and Schmitt generalized this concept, using the m-th degree symmetric polynomial $e_m(S)$ instead of the sum of the elements of S and considering subsequences of a given length t. In particular, they defined the higher degree Erdős–Ginzburg–Ziv constants $EGZ(t, R, m)$ of a finite commutative ring R and presented several lower and upper bounds to these constants. This paper aims to provide lower and upper bounds for $EGZ(t, R, m)$ in case $R = \mathbb{F}_q^n$. The lower bounds here presented have been obtained, respectively, using the Lovász local lemma and the expurgation method and, for sufficiently large n, they beat the lower bound provided by Caro and Schmitt for the same kind of rings. Finally, we prove closed form upper bounds derived from the Ellenberg–Gijswijt and Sauermann results for the cap-set problem assuming that $q = p^k$, $t = p$, and $m = p-1$. Moreover, using the slice rank method, we derive a convex optimization problem that provides the best bounds for $q = 3^k$, $t = 3$, $m = 2$, and $k = 2, 3, 4, 5$.

Mathematics Subject Classification. 05D40, 11B75.

Keywords. Higher degree Erdős–Ginzburg–Ziv constants, Probabilistic method, Lovász local lemma, Slice rank.

1. Introduction. One significant subfield of additive group theory and combinatorial number theory is the zero-sum theory that studies the sums behavior of suitable sequences of elements in an abelian finite group G (see, for instance, the surveys [7,20]). In this context, a typical kind of problem considers the existence of constants ℓ such that any sequence of elements of G whose length is

bigger than ℓ satisfies an additive property $\mathcal{P}$. Among these constants, an important role is taken by the classical Erdős–Ginzburg–Ziv constant of a group G that denotes the smallest positive integer ℓ such that any sequence of length $|S| \geq \ell$ contains a zero-sum subsequence of length $\exp(G)$. This constant has been well studied in the literature, we refer to the survey paper [20]. Here we recall that in [16], Erdős, Ginzburg, and Ziv completely determined its value over cyclic groups and that in [18,21,23], respectively Fox, Sauermann, and Naslund derived nontrivial upper bounds on groups of type $\mathbb{F}_p^n$ (they assumed a slightly different definition of the Erdős–Ginzburg–Ziv constant).

In the recent paper [10], Caro and Schmitt generalized this concept, using the m-th degree symmetric polynomial $e_m(g_1, \ldots, g_t) = \sum_{1 \leq i_1 < \cdots < i_m \leq t} \prod_{j=1}^{m} g_{i_j}$ instead of the sum of the elements of S and considering subsequences of a given length t (see also [1,3–5] that considered some related problems). In particular, they defined the higher degree Erdős–Ginzburg–Ziv constants $EGZ(t, R, m)$ as follows. For a finite commutative ring R, $EGZ(t, R, m)$ is the smallest positive integer ℓ such that every sequence S over R of length $|S| \geq \ell$ contains a subsequence S' of length t for which $e_m(S')$ evaluates to the zero element in R. If such ℓ does not exists, $EGZ(t, R, m)$ is set to ∞.

They also present several lower and upper bounds to these constants solving the case where R is $\mathbb{Z}_2$ and the case where R is $\mathbb{Z}_{p^s}$ if t and m are powers of the same prime. For a generic finite commutative ring R, their best lower bound is expressed in term of the generalized Davenport constant $D(R, m)$ of the ring R (see Caro et al. [11]), that is, the smallest integer ℓ such that any sequence S over R of length $|S| \geq \ell$ contains a subsequence S' of length $|S'| \geq m$ for which $e_m(S')$ equals the zero element of R. Indeed they prove that

$$EGZ(t, R, m) \geq t + D(R, m) - m. \tag{1.1}$$

This paper aims to determine lower and upper bounds for $EGZ(t, R, m)$ in case $R = \mathbb{F}_q^n$ (viewed as a commutative ring) for some prime power q (in the following we will always use the letter q for a prime power and p for a prime). The article is organized as follows. In Section 2, we will present two lower bounds obtained, respectively, using the Lovász local lemma and the expurgation method. Then, in Section 3, we will show that, for sufficiently large n, our bounds improve the ones given by Caro and Schmitt in the same context. Finally, in Section 4, we prove closed form upper bounds to $EGZ(p, R, p-1)$, derived from the Ellenberg–Gijswijt [15] and Sauermann [23] bounds for the cap-set problem, in case $R = \mathbb{F}_q^n$ and $q = p^k$. Moreover, we will apply Tao's slice rank method to provide an upper bound to $EGZ(3, \mathbb{F}_q^n, 2)$ and we derive a convex optimization problem that we can solve numerically providing better bounds for $q = 3^k$ and $k = 2, 3, 4, 5$.

2. Lower bounds. In this section, we will present two kinds of probabilistic lower bounds on the Erdős–Ginzburg–Ziv constants of rings of type $\mathbb{F}_q^n$. Both those bounds exploit the following upper bound on the probability that a given t-sequence S of elements in (vectors of) $\mathbb{F}_q^n$ is such that $e_m(S) = 0$. To provide such an upper bound, we exploit the following famous lemma.

Lemma 2.1 (Schwartz–Zippel lemma [24,27]). *Let $P \in \mathbb{F}[x_1, x_2, \ldots, x_t]$ be a non-zero polynomial with degree d. Consider a finite subset $A \subseteq \mathbb{F}$. If we pick uniformly at random $r_1, r_2, \ldots, r_t$ from A, then*

$$\mathbb{P}[P(r_1, r_2, \ldots, r_t) = 0] \leq \frac{d}{|A|}.$$

Using Lemma 2.1, we easily obtain the follow proposition.

Proposition 2.2. *Let us choose, uniformly at random, a sequence $S = (g_1, g_2, \ldots, g_t)$ of $t \geq m$ vectors of $\mathbb{F}_q^n$. Then*

$$\mathbb{P}[e_m(S) = 0] \leq \left(\frac{m}{q}\right)^n.$$

Proof. We prove this result first assuming $n = 1$. Since $e_m(S)$ is a polynomial of degree m, by Lemma 2.1, taking $A = \mathbb{F}_q$, we obtain

$$\mathbb{P}[e_m(S) = 0] \leq \frac{m}{|A|} = \frac{m}{q}.$$

Now we note that, if we consider a sequence S of $t \geq m$ vectors of $\mathbb{F}_q^n$, then $e_m(S) = 0$ if and only if each of the n projections $\pi_i(S)$ of S over the i-th coordinate satisfies $e_m(\pi_i(S)) = 0$. Since those projections are independent, it follows that

$$\mathbb{P}[e_m(S) = 0] = \prod_{i=1}^{n} \mathbb{P}[e_m(\pi_i(S)) = 0] \leq \left(\frac{m}{q}\right)^n.$$

□

We provide a first new lower bound on $EGZ(t, \mathbb{F}_q^n, m)$ by exploiting the so-called Lovász local lemma, see also the work [5] of Bitz, Griffith, and He for a similar application of this method. Here we state the lemma (in the symmetric case) for the reader's convenience.

Lemma 2.3 ([17] (see also [2])). *Let $E_1, E_2, \ldots, E_k$ be events in an arbitrary probability space. Suppose that each event E_i is mutually independent of the set of all other events E_j but at most d, and that $\mathbb{P}[E_i] \leq P$ for all $1 \leq i \leq k$. If*

$$edP \leq 1,$$

then $\mathbb{P}[\cap_{i=1}^{k} \overline{E_i}] > 0$.

Now, we are ready to state the following theorem.

Theorem 2.4. *Let ℓ be such that*

$$e\left[\binom{\ell}{t} - \binom{\ell - t}{t}\right]\left(\frac{m}{q}\right)^n \leq 1$$

where $\binom{\ell-t}{t}$ is set to zero if $\ell < 2t$. Then $EGZ(t, \mathbb{F}_q^n, m) > \ell$.

Proof. Here we need to prove the existence of a sequence S of length ℓ for which any subsequence S' of length t is such that $e_m(S') \neq 0$.

Let us choose, uniformly at random, a sequence S of length ℓ in $\mathbb{F}_q^n$. For a given subsequence S' of length t contained in S, let $E_{S'}$ be the event such that $e_m(S') = 0$. Clearly, there are $\binom{\ell}{t}$ such events. Due to Proposition 2.2, we know that

$$\mathbb{P}[E_{S'}] \leq \left(\frac{m}{q}\right)^n \quad \text{for all } S' \subseteq S,\ |S'| = t.$$

It is easy to see that each event $E_{S'}$ is mutually independent from all the events $E_{S''}$ where $S'' \subseteq S \setminus S'$ and $|S''| = t$. Therefore each event $E_{S'}$ is dependent on at most $\binom{\ell}{t} - \binom{\ell-t}{t}$ other events. Hence, due to Lemma 2.3, we obtain the thesis. □

Now we provide a second lower bound that, in some regime of the parameters, turns out to improve that of Theorem 2.4. The method we use here is sometimes called expurgation in the literature. We refer the reader to the book [2, Chapter 3 (Alterations)].

Theorem 2.5. *Let ℓ be such that*

$$\binom{\ell+s}{t}\left(\frac{m}{q}\right)^n < s+1$$

for some $s \geq 0$. Then $EGZ(t, \mathbb{F}_q^n, m) > \ell$.

Proof. We first note that the thesis is equivalent to prove the existence of a sequence S of length ℓ for which any subsequence S' of length t is such that $e_m(S') \neq 0$.

Here we choose, uniformly at random, a sequence T of length $\ell + s$ and we evaluate the expected value of the random variable X given by the number of subsequences T' of T of length t and such that $e_m(T') = 0$. Because of Proposition 2.2, we have that

$$\mathbb{E}(X) \leq \sum_{T' \subseteq T : |T'| = t} \left(\frac{m}{q}\right)^n = \binom{\ell+s}{t}\left(\frac{m}{q}\right)^n.$$

Moreover, due to the hypothesis, we have that $\mathbb{E}(X) < s+1$. It follows that there exists a set T of length $\ell + s$ with at most s subsequences T' such that $e_m(T') = 0$ that we call bad subsequences. If we remove from T one element from each bad subsequence, we have removed at most s elements and we are left with a sequence S of length at least ℓ for which any subsequence S' of length t is such that $e_m(S') \neq 0$. Clearly, we may assume, without loss of generality, that the length of S is exactly ℓ obtaining the thesis. □

Remark 2.6. We have been able to compute the optimal value of s in the expurgation bound (Theorem 2.5) only for small values of t, i.e., $t = 2, 3, 4, 5$. In all these cases, the expurgation bound performs better than the bound given in Theorem 2.4 obtained using the Lovász local lemma. In view of these results, we are inclined to conjecture that the expurgation bound provides the best bound for every $\ell \geq t \geq 2$. However, since we did not succeed to

prove this conjecture, we considered it useful to report also the bound given in Theorem 2.4.

3. Comparison to Caro and Schmitt's bounds. In this section, we discuss the bounds we have obtained in comparison to that of Caro and Schmitt. In particular, in [11, Theorems 3.1 and 3.4], it was proved that for rings of type $\mathbb{F}_p^n$ (where p is a prime), the following bounds on $D(\mathbb{F}_p^n, m)$ hold:

$$nmp - (n-1)m \geq D(\mathbb{F}_p^n, m) \geq np - (n-1)m. \tag{3.1}$$

It follows that the lower bound of Caro and Schmitt (1.1) becomes

$$EGZ(t, \mathbb{F}_p^n, m) \geq t + n(p-m). \tag{3.2}$$

Now we consider our lower bound of Theorem 2.5 with $s = 0$ in the case $q = p$. Note that this is not, in general, our best lower bound but it is the easiest to consider. We have that $EGZ(t, \mathbb{F}_p^n, m) \geq \ell$ if ℓ is such that

$$\binom{\ell}{t}\left(\frac{m}{p}\right)^n < 1.$$

We note that $\frac{\ell^t}{t!} > \binom{\ell}{t}$ and hence $EGZ(t, \mathbb{F}_p^n, m) \geq \ell$ for any ℓ such that

$$\frac{\ell^t}{t!}\left(\frac{m}{p}\right)^n < 1,$$

that is,

$$\frac{\ell^t}{t!} < \left(\frac{p}{m}\right)^n$$

and hence

$$EGZ(t, \mathbb{F}_p^n, m) \geq (t!)^{\frac{1}{t}}\left(\frac{p}{m}\right)^{\frac{n}{t}}. \tag{3.3}$$

Now, since (3.3) is, when $p > m$, exponential in n, it is clear that asymptotically in n, it improves the lower bound of Equation (3.2).

Remark 3.1. From Equation (3.3), we also have that, if $p > m$, for sufficiently large n:

$$EGZ(t, \mathbb{F}_p^n, m) \geq (t!)^{\frac{1}{t}}\left(\frac{p}{m}\right)^{\frac{n}{t}} > t + nm(p-1) \geq t + D(\mathbb{F}_p^n, m) - m$$

where the last inequality follows from the upper bound of Equation (3.1). This means that, for these kinds of parameters, it does not yield a Caro-Gao-type relation (see [8,9,19]), i.e., it does not hold the equality in Equation (1.1).

We also note that the bound of Equation (3.3) can be trivially improved for several values of $q = p^k$. Indeed, if $\binom{t}{m} \not\equiv 0 \pmod{p}$, we have that $EGZ(t, \mathbb{F}_q^n, m) = \infty$. It suffices to consider the infinite constant sequence such that $g_i = 1$ for any $i \in \mathbb{N}$. In this case, we have that, for any subsequence S' of length t, $e_m(S') = \binom{t}{m} \not\equiv 0 \pmod{p}$. On the other hand, this is a subset of the parameters for which our bounds of Section 2 (and in particular Equation (3.3)) hold. Moreover, we will show in the upcoming section that, at least when $q = p^k$, $t = p$, and $m = p - 1$, it is possible to provide nontrivial upper bounds.

Finally, we also note that the bounds here presented can be easily generalized to rings of type $\mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \times \cdots \times \mathbb{F}_{q_n}$ (similarly to those of [10] that Caro and Schmitt stated for rings of type $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$) but, since we believe this is not a substantial improvement, we prefer to keep the notation of this note as simple as possible and to explicitly consider only rings of type $\mathbb{F}_q^n$.

4. Upper bounds. In this section, we provide an upper bound to $EGZ(p, \mathbb{F}_q^n, p-1)$ with $q = p^k$, where p is an odd prime. In the first part of this section, we provide, using the Ellenberg–Gijswijt [15] and Sauermann [23] bounds for the cap-set problem, a general upper bound to $EGZ(p, \mathbb{F}_q^n, p-1)$ for every prime $p \geq 3$. Then, we use the so-called slice rank method, introduced by Tao in [25] and revisited by Tao and Sawin in [26] (see also [12] and [22] for a discussion on the method) in order to generalize the polynomial approach introduced in [14] and in [15], to improve the bounds that can be deduced by the Ellenberg–Gijswijt bound for $p = 3$ and $k = 2, 3, 4, 5$. Our application of the method is somehow reminiscent of works on the classical Erdős–Ginzburg–Ziv constants of Fox and Sauermann [18] and Naslund [21].

Let us first state the following theorems that will be used in Theorem 4.3 to provide a general bound on $EGZ(p, \mathbb{F}_q^n, p-1)$ for $q = p^k$ and $k \geq 2$.

Theorem 4.1 (Ellenberg–Gijswijt [15]). *Let A be a subset of $\mathbb{F}_3^n$ which does not contain 3 distinct elements x_1, x_2, x_3 such that $x_1 + x_2 + x_3 = 0$. Then, for $n \to \infty$, we have that*

$$|A| \leq \left(\frac{3}{8} \sqrt[3]{207 + 33\sqrt{33}} + o(1) \right)^n \approx (2.756 + o(1))^n.$$

Theorem 4.2 (Sauermann [23]). *Let $p \geq 5$ be a prime and let A be a subset of $\mathbb{F}_p^n$ which does not contain p distinct elements $x_1, x_2, \ldots, x_p$ such that $x_1 + x_2 + \cdots + x_p = 0$. Then, for $n \to \infty$, we have that*

$$|A| \leq \left(2\sqrt{p} + o(1)\right)^n.$$

Now we consider a sequence $S = (g_1, g_2, \ldots, g_\ell)$ of elements in $\mathbb{F}_q^n$ with $q = p^k$ such that every p-tuple of elements $g_1', g_2', \ldots, g_p'$ of S satisfies $e_{p-1}(g_1', g_2', \ldots, g_p') = \sum_{1 \leq i_1 < \cdots < i_{p-1} \leq p} \prod_{j=1}^{p-1} g_{i_j}' \neq 0$. We note that S cannot have elements repeated more than $p-1$ times since $e_{p-1}(g_1', g_2', \ldots, g_p') = 0$ whenever $g_1' = g_2' = \cdots = g_p'$. It means that we can remove the repeated elements in S obtaining a set S_1 with $|S_1| \geq \frac{|S|}{p-1}$. Clearly, to upper bound the length of the sequence S, it suffices to bound the cardinality of S_1 considered as a set (it has no repetitions). Since it does not admit repeated elements, we already have that

$$\frac{|S|}{p-1} \leq |S_1| \leq q^n. \tag{4.1}$$

Now, we are ready to state our first result whose proof has been pointed out by an anonymous referee.

Theorem 4.3. *Let p be an odd prime and k a positive integer. Then we have that, when q is not a power of p,*

$$EGZ(p, \mathbb{F}_q^n, p-1) = \infty.$$

While for $q = p^k$, we have that

$$EGZ(p, \mathbb{F}_q^n, p-1) \leq \begin{cases} q^{n+o(n)} & \text{for } p = 3, 5 \text{ and } k = 1, \\ (2.756^k + 1)^{n+o(n)} & \text{for } p = 3 \text{ and } k \geq 2, \\ \left(2^k \sqrt{q} + 1\right)^{n+o(n)} & \text{for } p \neq 3 \text{ and } q \geq 7. \end{cases}$$

Proof. We note that, if $\mathbb{F}_q$ has characteristic $p' \neq p$, $\binom{p}{p-1} = p \not\equiv 0 \pmod{p'}$. In this case, we consider the infinite constant sequence such that $g_i = 1$ for any $i \in \mathbb{N}$. Here we have that, for any subsequence S' of length p, $e_{p-1}(S') = \binom{p}{p-1} = p \not\equiv 0 \pmod{p'}$ and hence $EGZ(p, \mathbb{F}_q^n, p-1) = \infty$ whenever q is not a power of p. Therefore we can assume that $q = p^k$. For $k = 1$ and $p = 3, 5$, the upper bound of this theorem follows directly from Equation (4.1). Hence we can suppose that $k \geq 2$.

Now, let $S \subseteq \mathbb{F}_q^n$ be a subset not containing p distinct elements $x_1, x_2, \ldots, x_p \in S$ such that $e_{p-1}(x_1, x_2, \ldots, x_p) = 0$. For every $P \subseteq \{1, 2, \ldots, n\}$, let us denote by $S_P = \{v \in S \mid \operatorname{supp}(v) = P\}$, where $\operatorname{supp}(v)$ is defined as the set of coordinates in which v is nonzero, the set of vectors in S that have the same support P. Let also denote by $S'_P \subseteq \mathbb{F}_q^{|P|}$ the set obtained from S_P restricting every vector $v \in S_P$ only to coordinates in P. This guarantees us that all the entries of S'_P are nonzero elements of $\mathbb{F}_q$. Then we construct a new set $S''_P \subseteq \mathbb{F}_q^{|P|}$ by replacing every vector $(a_1, a_2, \ldots, a_{|P|}) \in S'_P$ by $(a_1^{-1}, a_2^{-1}, \ldots, a_{|P|}^{-1}) \in S''_P$. Clearly, $|S_P| = |S'_P| = |S''_P|$. We claim that S''_P does not contain p distinct elements summing to zero in $\mathbb{F}_q^{|P|}$. Indeed, suppose by contradiction there exist p distinct vectors $x_1, x_2, \ldots, x_p \in S'_P$ such that $x_{1,i}^{-1} + x_{2,i}^{-1} + \cdots + x_{p,i}^{-1} = 0$ for every i, then we can multiply both sides of the previous equation by $x_{1,i} x_{2,i} \cdots x_{p,i}$ to obtain that $e_{p-1}(x_1, x_2, \ldots, x_p) = 0$. But this is absurd due to the initial hypothesis on S.

Since, as an abelian group under addition, $\mathbb{F}_q^{|P|}$ is isomorphic to $\mathbb{F}_p^{k|P|}$, by Theorems 4.1 and 4.2, we have that, for fixed p and k, $|S_P| \leq (u_{p,k} + o(1))^{|P|}$ for every $P \subseteq \{1, 2, \ldots, n\}$ such that $|P| = \alpha n(1 + o(1))$ for some $0 < \alpha < 1$, where

$$u_{p,k} := \begin{cases} 2.756^k & \text{for } p = 3 \text{ and } k \geq 2, \\ (2\sqrt{p})^k & \text{for } p \neq 3 \text{ and } p^k \geq 7. \end{cases}$$

Hence, for any real $0 < \alpha \leq 1/4$, we get

$$|S| \leq \sum_{\substack{P \subseteq \{1,2,\ldots,n\} \\ |P| \leq \alpha n}} |S_P| + \sum_{\substack{P \subseteq \{1,2,\ldots,n\} \\ |P| \geq \alpha n}} |S_P| \overset{\text{(i)}}{\leq} 2^n q^{\alpha n} + \sum_{i \geq \alpha n}^{n} \sum_{\substack{P \subseteq \{1,2,\ldots,n\} \\ |P| = i}} |S_P|$$

$$\overset{\text{(ii)}}{\leq} o(u_{p,k}^n) + \sum_{i \geq \alpha n}^{n} \binom{n}{i} (u_{p,k} + o(1))^i \overset{\text{(iii)}}{\leq} o(u_{p,k}^n) + (u_{p,k} + 1 + o(1))^n$$
$$= (u_{p,k} + 1)^{n+o(n)},$$

where (i) follows since $|S_P| \leq q^{\alpha n}$ for $|P| \leq \alpha n$. Since $2q^\alpha = 2p^{\alpha k} < u_{p,k}$ for every $\alpha < 1/4$ and $k \geq 1$, inequality (ii) holds due to the fact that $|S_P| \leq (u_{p,k} + o(1))^{|P|}$. Finally inequality (iii) is due to the binomial theorem. Therefore the theorem follows. □

We will see that it is possible to improve the bounds given in Theorem 4.3 using the slice rank method for $q = 3^k$ and $k = 2, 3, 4, 5$.

As done before, let $S = (g_1, g_2, \ldots, g_\ell)$ be a sequence of elements in $\mathbb{F}_q^n$ with $q = 3^k$ such that every three elements g_1', g_2', g_3' of S satisfy $e_2(g_1', g_2', g_3') \neq 0$. Let S_1 be the set obtained from removing the repeated elements in S. By Equation (4.1), we have that $|S_1| \geq |S|/2$. Now we split S_1 in $n+1$ sets $S_1^0, S_1^1, \ldots, S_1^n$ where $g_i \in S_1^j$ if g_i has exactly j coordinates equal to zero. We note that there exists j such that

$$|S_1^j| \geq \frac{|S_1|}{n+1} \geq \frac{|S|}{2(n+1)}.$$

Now, let us recall some definitions and lemmas from [25,26].

Definition 4.4. A function $T : A^k \to \mathbb{F}$ is said to be a slice if it can be written in the form

$$T(x_1, \ldots, x_k) = T_1(x_i) T_2(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$$

where $T_1 : A \to \mathbb{F}$ and $T_2 : A^{k-1} \to \mathbb{F}$.

Definition 4.5. The slice rank $srk(T)$ of a general function $T : A^k \to \mathbb{F}$ is the smallest number m such that T is a linear combination of m slices.

Lemma 4.6 ([25]). *Let A be a finite set and $\mathbb{F}$ be a field. Let $T(x, y, z)$ be a function $A \times A \times A \to \mathbb{F}$ such that $T(x, y, z) \neq 0$ if and only if $x = y = z$. Then $srk(T) = |A|$.*

In order to apply Lemma 4.6, we want to consider a function that is zero whenever we consider three different elements of S_1^j. In particular, given $x, y, z \in \mathbb{F}_q^n$, we consider

$$P(x, y, z) = \prod_{i=1}^{n} (1 - (x_i y_i + y_i z_i + z_i x_i)^{q-1}). \tag{4.2}$$

Lemma 4.7. *Let us consider the function $P(x, y, z)$ on the restricted domain $S_1^j \times S_1^j \times S_1^j \to \mathbb{F}_q$ where $q = 3^k$. Then $P(x, y, z) \neq 0$ if and only if $x = y = z$.*

Proof. Here we have that, if x, y, z are in S_1^j, then $P(x, y, z) \neq 0$ if and only if $x = y = z$. Indeed, if x, y, and z are three different elements of S_1^j, they are such that $xy + yz + zx \neq 0$ and hence $x_i y_i + y_i z_i + z_i x_i \neq 0$ for at least

one $i \in [1,n]$. This means that $1-(x_iy_i+y_iz_i+z_ix_i)^{q-1}=0$ and hence $P(x,y,z)=0$.

We note that also if we consider an element $x \in S_1^j$ repeated twice and $z \neq x$, we have that $P(x,x,z)=0$. Indeed, since x and z have the same number of zero components, there exists i such that $x_i \neq 0$ and $x_i \neq z_i$. Here we have that

$$x_ix_i+x_iz_i+z_ix_i = x_i^2+2x_iz_i = x_i(x_i-z_i) \neq 0$$

since both x_i-z_i and x_i are nonzero. It follows that $P(x,x,z)=0$. Similarly, we prove that also $P(z,x,x)=0$ and $P(x,z,x)=0$.

Finally, we consider an element x repeated three times. In this case, we have that

$$P(x,x,x)=\prod_{i=1}^{n}(1-(x_ix_i+x_ix_i+x_ix_i)^{q-1})=\prod_{i=1}^{n}(1-(3x_ix_i)^{q-1})=1\neq 0.$$

□

As a corollary of Lemmas 4.6 and 4.7, we have that:

Corollary 4.8.

$$|S| \leq 2(n+1)|S_1^j| = 2(n+1)srk(P|_{S_1^j\times S_1^j\times S_1^j}).$$

Now the goal is to upper bound the $srk(P|_{S_1^j\times S_1^j\times S_1^j})$. The following lemma will help us to make the first step in this direction.

Lemma 4.9 ([25]). *Let A be a finite set, $A_1 \subseteq A$, and $\mathbb{F}$ be a field. Let $T(x,y,z)$ be a function $A\times A\times A \to \mathbb{F}$. Then*

$$srk(T|_{A_1\times A_1\times A_1}) \leq srk(T).$$

We immediately get the following corollary:

Corollary 4.10. *Considering the function P on the domain $\mathbb{F}_q^n\times\mathbb{F}_q^n\times\mathbb{F}_q^n$, we have that*

$$|S| \leq 2(n+1)|S_1^j| = 2(n+1)srk(P).$$

Now we aim to prove that $srk(P)$ improves the bound given in Theorem 4.3. For this purpose, we recall the asymptotic rank theory studied by Tao and Sawin in [26] in the special case of polynomial functions (we do not need to consider the very general case of tensor slice rank).

Given a polynomial $p(x,y,z)$ whose degree in each variables is at most δ, we define Γ as the subset of $\{0,1,\dots,\delta\}^3$ of the triples (d_1,d_2,d_3) such that $x^{d_1}y^{d_2}z^{d_3}$ has a nonzero coefficient in p. Hence we state the following proposition derived from [26].

Proposition 4.11. *Let $p(x,y,z)$ be a polynomial and let Γ be its support. Then*:

$$srk\left(\prod_{i=1}^{n}p(x_i,y_i,z_i)\right) \leq \exp((H(\Gamma)+o(1))n)$$

where

$$H(\Gamma) := \sup_{(X_1,\dots,X_k)} \min(h(X_1),\dots,h(X_k)),$$

$(X_1,\dots,X_k)$ *takes values in* Γ, *and* $h(X)$ *is the entropy of the random variable* X *defined as* $-\sum_{\gamma\in\Gamma'} \mathbb{P}[X=\gamma]\log(\mathbb{P}[X=\gamma])$ *and* Γ' *is the support of* X.

In our case, we will not find the exact value of $H(\Gamma)$ but we will compute it numerically when $k=2,3,4,5$ solving a convex optimization problem and providing then an upper bound of type $\exp(H(\Gamma))^{(n+o(n))}$ where $\exp(H(\Gamma))$ is strictly smaller than the bounds given in Theorem 4.3. For this purpose, we will recall the following theorem from [6].

Theorem 4.12 ([6, Theorem 8]). *Let* Γ *be a finite subset of* $S\times S\times S$ *for some set* S *and let* $\sigma\in Sym(3)$ *be a permutation such that, for each* $a=(a_1,a_2,a_3)\in\Gamma$, *also* $\sigma(a)=(a_{\sigma(1)},a_{\sigma(2)},a_{\sigma(3)})\in\Gamma$. *Then there is a random variable* Y *taking values in* Γ *such that, for all* $y\in\Gamma$, *we have that* $\mathbb{P}[Y=y]=\mathbb{P}[Y=\sigma(y)]$ *and*

$$\min(h(Y_1),h(Y_2),h(Y_3)) = H(\Gamma).$$

This theorem essentially ensures that the value $H(\Gamma)$ is attained as a minimum of the entropy of the marginal variables of some random variable Y and that this variable is invariant under permutations that fix Γ. We are now ready to state the following theorem.

Theorem 4.13. *Let* $q=3^k$, *then we have that*

$$EGZ(3,\mathbb{F}_q^n,2) \le \begin{cases} 8.315^{n+o(n)} & \text{for } k=2,\\ 21.802^{n+o(n)} & \text{for } k=3,\\ 58.557^{n+o(n)} & \text{for } k=4,\\ 159.812^{n+o(n)} & \text{for } k=5. \end{cases}$$

Proof. We set $p(x,y,z)=(1-(xy+yz+zx)^{q-1})$ and we consider the following polynomial defined in (4.2):

$$P(x,y,z)=\prod_{i=1}^{n} p(x_i,y_i,z_i).$$

Hence we can use Proposition 4.11 to evaluate $srk(P)$. For $q=9,27,81,243$, we compute the support Γ of p and then, using Theorem 4.12, we have been able to compute $H(\Gamma)$ numerically for these cases:

q	9	27	81	243
$H(\Gamma)$	2.118	3.082	4.07	5.074

Hence the theorem follows by Corollary 4.10 and Proposition 4.11. □

Remark 4.14. One can prove that $H(\Gamma)<\log q$ for every $q=3^k\ge 9$, where Γ is the support of the polynomial $p(x,y,z)$ defined in Theorem 4.13. The reader can find a proof in a previous version of this paper [13].

Remark 4.15. We observe that, in Theorem 4.13, for $q = 3$, we obtain a weaker bound than for the other cases of q. Indeed, in this case

$$\Gamma = \{(0,0,0),(2,2,0),(0,2,2),(2,0,2),(2,1,1),(1,2,1),(1,1,2)\}$$

and one can easily check that defining Y that has, neatly, the distribution

$$(1/4, 1/12, 1/12, 1/12, 1/6, 1/6, 1/6)$$

over Γ, Y_1, Y_2, and Y_3 all have uniform distributions. It follows that, in this case, $H(\Gamma) = \log 3$ and hence our proof fails to provide a better upper bound for $q = 3$. □

For the other values of q (i.e., $q > 243$), we have not been able to explicitly evaluate $H(\Gamma)$ since it seems that there are too many variables for this problem to be treated even with the help of a computer.

Acknowledgements. We would like to thank the anonymous reviewer for the simple proof of Proposition 2.2 and for pointing out the procedure used in Theorem 4.3. The first author was partially supported by INdAM–GNSAGA.

Funding Open access funding provided by Università degli Studi di Salerno within the CRUI-CARE Agreement.

References

[1] Ahmed, T., Bialostocki, A., Pham, T., Vinh, L.A.: Power sum polynomials as relaxed EGZ polynomials. Integers **19**, Paper No. A49, 10 pp. (2019)

[2] Alon, N., Spencer, J.H.: The Probabilistic Method. Wiley, Hoboken (2004)

[3] Bialostocki, A., Luong, T.D.: An analogue of the Erdős–Ginzburg–Ziv theorem for quadratic symmetric polynomials. Integers **9**, Paper No. A36, 459–465 (2009)

[4] Bialostocki, A., Luong, T.D.: Cubic symmetric polynomials yielding variations of the Erdős–Ginzburg–Ziv theorem. Acta Math. Hung. **142**, 152–166 (2014)

[5] Bitz, J., Griffith, S., He, X.: Exponential lower bounds on the generalized Erdős–Ginzburg–Ziv constant. Discret. Math. **343**, 112083, 4 pp. (2020)

[6] Borst, S.J.: Using the slice rank for finding upper bounds on the size of cap sets. Bachelor Thesis, TU Delft (2018). http://resolver.tudelft.nl/uuid:a619c626-8a7e-45d5-90e4-1ff4cfa5268b. [Accessed 16 November 2022]

[7] Caro, Y.: Zero-sum problems—a survey. Discret. Math. **152**, 93–113 (1996)

[8] Caro, Y.: Zero-sum sequences in abelian non-cyclic groups. Israel J. Math. **92**, 221–233 (1995)

[9] Caro, Y.: Remarks on a zero-sum theorem. J. Comb. Theory Ser. A **76**, 315–322 (1996)

[10] Caro, Y., Schmitt, J.R.: Higher degree Erdős–Ginzburg–Ziv constants. Integers **22**, Paper No. A102, 17 pp. (2022)

[11] Caro, Y., Girard, B., Schmitt, J.R.: Higher degree Davenport constants over finite commutative rings. Integers **21**, Paper No. A120, 17 pp. (2021)

[12] Costa, S., Dalai, M.: A gap in the slice rank of k-tensors. J. Comb. Theory Ser. A **177**, Paper No. 105335, 12 pp. (2021)

[13] Costa, S., Della Fiore, S.: Bounds on the higher degree Erdős–Ginzburg–Ziv constants over $\mathbb{F}_q^n$. arXiv:2211.03682v2 (2022)

[14] Croot, E., Lev, V.F., Pach, P.P.: Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small. Ann. of Math. (2) **185**, 331–337 (2017)

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

[16] Erdős, P., Ginzburg, A., Ziv, A.: Theorem in the additive number theory. Bull. Res. Counc. Isr. Sect. **10**, 41–43 (1961)

[17] Erdős, P., Lovász, L.: Problems and results on 3-chromatic hypergraphs and some related questions. In: Hajnal, A., Rado, R., Sos, V.T. (eds.) Infinite and Finite Sets, Keszthely, vol. II, pp. 609–627. North-Holland, Amsterdam (1975)

[18] Fox, J., Sauermann, L.: Erdős–Ginzburg–Ziv constants by avoiding three-term arithmetic progressions. Electron. J. Comb. **25**, Paper No. 2.14, 9 pp. (2018)

[19] Gao, W.D.: A combinatorial problem on finite abelian groups. J. Number Theory **58**, 100–103 (1996)

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

[21] D Naslund, E.: Exponential bound for the Erdős–Ginzburg–Ziv constant. J. Comb. Theory Ser. A **174**, 105185, 19 pp. (2020)

[22] Naslund, E., Sawin, W.: Upper bounds for sunflower-free sets. Forum Math. Sigma **5**, Paper No. e15, 10 pp. (2017)

[23] Sauermann, L.: On the size of subsets of $\mathbb{F}_p^n$ without p distinct elements summing to zero. Israel J. Math. **243**, 63–79 (2021)

[24] Schwartz, J.T.: Fast probabilistic algorithms for verification of polynomial identities. J. Assoc. Comput. Mach. **27**(4), 701–717 (1980)

[25] Tao, T.: A symmetric formulation of the Croot–Lev–Pach–Ellenberg–Gijswijt capset bound. https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-thecroot-lev-pach-ellenberg-gijswijt-capset-bound/ (2016)

[26] Tao, T., Sawin, W.: Notes on the slice rank of tensors. https://terrytao.wordpress.com/2016/08/24/notes-on-the-slice-rank-oftensors/ (2016)

[27] Zippel, R.: Probabilistic algorithms for sparse polynomials. In: Symbolic and Algebraic Computation (EUROSAM '79, Internat. Sympos., Marseille, 1979), pp. 216–226. Lecture Notes in Comput. Sci., 72. Springer, Berlin-New York (1979)

Simone Costa
DICATAM, Sez. Matematica
Università degli Studi di Brescia
Via Branze 43
25123 Brescia
Italy
e-mail: simone.costa@unibs.it

Stefano Della Fiore
DI, Università degli Studi di Salerno
Via Giovanni Paolo II 132
84084 Fisciano
Italy
e-mail: sdellafiore@unisa.it

Received: 28 April 2023

Revised: 28 April 2023

Accepted: 25 August 2023