Electronic Colloquium on Computational Complexity, Report No. 180 (2012)

The Freiman-Ruzsa Theorem in Finite Fields

Chaim Even-Zohar *   Shachar Lovett †

December 20, 2012

Abstract

Let G be a finite abelian group of torsion r and let A be a subset of G. The Freiman-Ruzsa theorem asserts that if $|A+A| \leq K|A|$ then A is contained in a coset of a subgroup of G of size at most $K^2 r^{K^4}|A|$. It was conjectured by Ruzsa that the subgroup size can be reduced to r^{CK} for some absolute constant $C \geq 2$. This conjecture was verified for $r = 2$ in a sequence of recent works, which have, in fact, yielded a tight bound. In this work, we establish the same conjecture for any prime torsion.

1 Introduction

Let A be a subset of a finite abelian group. The *doubling constant* of A is defined by $|A+A|/|A|$, where as usual $|A+B| = \{a+b \mid a \in A, b \in B\}$. The *spanning constant* of A is defined by $|\langle A\rangle|/|A|$, where $\langle A\rangle$ is the *affine span* of A, i.e., the smallest subgroup or subgroup's coset containing A.

The Freiman-Ruzsa Theorem in Finite Torsion Groups [11] explores the relation between these two parameters, in groups of fixed torsion r. Namely, we are assuming that r is the largest order of an element in the underlying group.

Theorem 1 (Ruzsa [11])**.** *Let A be a finite subset of an abelian group of torsion r. Then*

$$\frac{|A+A|}{|A|} \leq K \qquad \Rightarrow \qquad \frac{|\langle A\rangle|}{|A|} \leq K^2 r^{K^4}.$$

It is natural to ask how tight this bound is. To this end, the following function is defined for $r \in \mathbb{N}$ and $K \geq 1$.

$$F(r,K) = \sup\left\{ \frac{|\langle A\rangle|}{|A|} \;\middle|\; A \subseteq \mathbb{Z}_r^n,\ n \in \mathbb{N},\ \frac{|A+A|}{|A|} \leq K \right\}.$$

Note that there is no loss of generality in assuming $A \subseteq \mathbb{Z}_r^n$, rather than considering a general abelian r-torsion group. Otherwise, $A \subseteq G = \mathbb{Z}_r^n/H$ for some n and H, and the same doubling and spanning constants can be achieved by taking the preimage of A under the quotient map.

A lower bound on $F(r,K)$ is obtained by taking a set of affinely independent elements. Specifically, if we choose $A = \{0, e_1, e_2, ..., e_{2K-2}\} \subseteq \mathbb{Z}_r^{2K-2}$ for $K \in \frac{1}{2}\mathbb{N}$ and $r \geq 3$, then the doubling constant of A equals K, and we have

$$F(r,K) \;\geq\; \frac{r^{2K-2}}{2K-1}. \tag{1}$$

This leads to the following conjecture.

Conjecture 2 (Ruzsa [11])**.** *There exists some $C \geq 2$ for which $F(r,K) \leq r^{CK}$.*

*Einstein Institute of Mathematics, HUJI, Israel. e-mail: `chaim.evenzohar@mail.huji.ac.il`.
†CSE department, UC San-Diego. e-mail: `slovett@cse.ucsd.edu`.

ISSN 1433-8092

Green and Ruzsa [7] lowered the bound in Theorem 1 to $F(r,K) \le K^2 r^{2K^2-2}$. In the special case $r = 2$, further progress has been made [4, 12, 8, 10, 6]. In particular, Green and Tao [8] showed that $F(2,K) \le 2^{2K+O(\sqrt{K}\log K)}$, thus settling Conjecture 2 for $r = 2$. A refinement of their argument enabled the first author [6] to find the exact value of $F(2,K)$, which turned out to be $\Theta(2^{2K}/K)$. In this note we extend these techniques to the case of general prime torsion.

Theorem 3. *For $p > 2$ prime and K large enough,*

$$F(p,K) \ \le \ \frac{p^{2K-2}}{2K-1}.$$

This bound is proved in Section 3. Note that it verifies Ruzsa's conjecture with $C = 2$ for prime r, and by (1) it is best possible for half-integer K.

The proof elaborates on methods of subset compressions in $\mathbb{F}_2^n$, which were first employed in the present context by Green and Tao [8]. Although the general scheme of the proof is similar to [6], the transition from 2 to general p requires a new type of compressions. The definition and properties of these compressions appear in Section 2. We also make use of the following classical result [2, 3].

Theorem 4 (Cauchy-Davenport)**.** *For non-empty $C, D \subseteq \mathbb{F}_p$, $|C + D| \ge \min(|C| + |D| - 1, p)$.*

2 Compressions in $\mathbb{F}_p^n$

Let $e_1, ..., e_n$ be the standard basis of $\mathbb{F}_p^n$. For $u \in \mathbb{F}_p^n$ we denote $u = \sum_{i=1}^n u_i e_i$ where $u_i \in \{0, ..., p-1\}$. For $u, v \in \mathbb{F}_p^n$ we say that $u \prec v$ in the *lexicographic order*, if $u_i < v_i$ for the largest coordinate i for which $u_i \ne v_i$. For $L \subseteq \mathbb{F}_p^n$ and $k \le |L|$, we denote by $\mathrm{IS}(k, L)$ the *initial segment* of size k of L, which is the set of the k smallest elements of L in the lexicographic order.

The line passing through $u \in \mathbb{F}_p^n$ in the direction of a nonzero $v \in \mathbb{F}_p^n$ is denoted $L_v^u = u + \mathbb{F}_p v = \{u + kv \mid k \in \mathbb{F}_p\}$, and the partition of $\mathbb{F}_p^n$ to *v-lines* is denoted $\mathcal{L}_v = \{L_v^u | u \in \mathbb{F}_p^n\}$. Let $A \subseteq \mathbb{F}_p^n$. The *$v$-compression* of A is defined by replacing $L \cap A$ with a same-cardinality initial segment of L for every v-line L:

$$C_v(A) = \bigcup_{L \in \mathcal{L}_v} \mathrm{IS}(|A \cap L|, L).$$

Note that $|C_v(A)| = |A|$. If $C_v(A) = A$, we say that A is *v-compressed.* One can check easily that $C_v(A)$ is v-compressed. For $p = 2$ and $v = e_i$, the compression operator C_v coincides with $C_{\{i\}}$ as in [8, 6]. Compressions along general multidimensional subspaces can be defined analogously, but are not necessary for this work.

Lemma 5. *Let $A, B \in \mathbb{F}_p^n$ and $v \in \mathbb{F}_p^n \setminus \{0\}$. Then $C_v(A) + C_v(B) \subseteq C_v(A + B)$.*

Proof. Let $i \in \{1, ..., n\}$ be the largest coordinate such that $v_i \ne 0$. Without loss of generality $v_i = 1$, otherwise replace v with $v_i^{-1} v$ without affecting $\mathcal{L}_v$. We first show that for every two v-lines L_v^u, L_v^w and $c, d \in \{1, ..., p\}$,

$$IS\left(c, L_v^u\right) + IS\left(d, L_v^w\right) \ = \ IS\left(min(c + d - 1, p), L_v^{u+w}\right). \tag{2}$$

Note that for each v-line L, there exists a unique $u \in \mathbb{F}_p^n$ such that $L = L_v^u$ and $u_i = 0$. Therefore, we can assume without loss of generality $u_i = w_i = 0$, and hence $(u + w)_i = 0$ as well. For this choice of u, the lexicographic order of L_v^u is $u \prec u + v \prec u + 2v \prec ... \prec u + (p-1)v$, and of course the same holds if we replace u with w or $u + w$. Now (2) reduces to addition of initial segments in $\mathbb{F}_p$, which can be checked easily.

More generally, if $C, D \subseteq \mathbb{F}_p$ are non-empty such that $A \cap L_v^u = u + Cv$ and $B \cap L_v^w = w + Dv$, then $(A \cap L_v^u) + (B \cap L_v^w) = u + w + (C + D)v$. By the Cauchy-Davenport theorem (Theorem 4) applied on C and D,

$$\min(|A \cap L_v^u| + |B \cap L_v^w| - 1, p) \ \le \ |(A \cap L_v^u) + (B \cap L_v^w)| \ \le \ |(A + B) \cap L_v^{u+w}|.$$

Putting this into (2), we have

$$IS\left(|A \cap L_v^u|, L_v^u\right) + IS\left(|B \cap L_v^w|, L_v^w\right) \subseteq IS\left(|(A+B) \cap L_v^{u+w}|, L_v^{u+w}\right).$$

Note that this holds also when one of the summands on the left hand side is empty. The proof is completed by taking the union over all u and w. $\square$

Corollary 6. $|C_v(A) + C_v(A)| \leq |A + A|$.

By Corollary 6, compressions can reduce $|A + A|$. However, they might reduce $|\langle A \rangle|$ as well. In order to apply compressions most effectively in the proof of Theorem 3, we only apply compressions that preserve the affine span. For $A \subseteq \mathbb{F}_p^n$, we say that A is $\langle\langle E \rangle\rangle$*-compressed* if $E = \{0, e_1, e_2 ... e_n\} \subseteq A$ and A is v-compressed for every v-compression preserving this inclusion. We conclude this section with a lemma describing the structure of $\langle\langle E \rangle\rangle$-compressed subsets.

Lemma 7 (Structure of Compressed Subsets)**.** *Let A be an $\langle\langle E \rangle\rangle$-compressed subset of $\mathbb{F}_p^n$. Suppose:*

- $H = span\{e_1, ..., e_h\}$ *is the maximal such subgroup contained in A,*
- $a_i = e_{h+i}$ *for $i \in \{1, ..., m\}$, where $m = codim H = n - h$,*
- $A_i = A \cap (a_i + H)$ *for $i \in \{2, ..., m\}$,*
- $A_1 = A \cap (qa_1 + H)$ *where $q \in \{1, ..., p-1\}$ is maximal such that the intersection is non-empty.*

Then

$$A = H \cup (a_1 + H) \cup (2a_1 + H) \cup ... \cup ((q-1)a_1 + H) \cup A_1 \cup A_2 \cup ... \cup A_m.$$

Proof. We start with a useful observation regarding $\langle\langle E \rangle\rangle$-compressed subsets: If $i \in \{1, ..., n\}$ and $v \in A \cap \text{span}\{e_1, ..., e_{i-1}\}$, then A is $(e_i - v)$-compressed. Indeed, $E \subseteq C_{e_i - v}(A)$ since every element in E is the lexicographically smallest in its $(e_i - v)$-line, except for e_i which is preceded only by v, and $v \in A$. In particular, taking $v = 0$, A is e_i-compressed for $i \in \{1, ..., n\}$. In other words, A is a down-set in the partial order of comparison in all coordinates.

Now, let H, h, m, $a_1, ..., a_m$, $A_1, ..., A_m$ and q be as in the statement of the theorem. By the above observation, A has the following properties.

1. Every element in $(q-1)a_1 + H$ is lexicographically smaller than every element in $qa_1 + H$, and such two elements lie on some $(a_1 - v)$-line where $v \in H$. Since A is $(a_1 - v)$-compressed for all $v \in H$ and A intersects $qa_1 + H$, this means that $(q-1)a_1 + H$ is contained in A.

2. By maximality, H is contained in A but $H + \mathbb{F}_p a_1$ is not. In other words, there exists $v \in A \cap (H + \mathbb{F}_p a_1)$ such that $v + a_1 \notin A$. Now, A is $(a_i - v)$-compressed for $i \in \{2, ..., n\}$. Since $a_1 + a_i$ is larger than $v + a_1$ in an $(a_i - v)$-line, $a_1 + a_i \notin A$ too.

3. A is $(a_i - a_1)$-compressed for $i > 1$. As $a_1 + a_i \prec 2a_i$, $2a_i \notin A$ as well.

4. A is $(a_i - a_j)$-compressed for $i > j > 1$. As $2a_j \prec a_j + a_i$, also $a_j + a_i \notin A$.

Examination of the above, together with use of the down-set property, yield the desired H-cosets structure of A. $\square$

3 An Upper Bound on $F(p, K)$

Proof. (of Theorem 3) Suppose $A \subseteq \mathbb{F}_p^n$ such that $|\langle A \rangle|/|A| = p^{2K-2}/(2K-1)$ for some $K \geq K_0(p)$, where $K_0(p)$ will be determined later. We have to show that $|A+A|/|A| \geq K$. Since $p^{2K-2}/(2K-1)$ is monotone in K, the theorem would follow.

Without loss of generality we may assume that $E = \{0, e_1, ..., e_n\} \subseteq A$. Indeed, $|A|$, $|A+A|$ and $|\langle A \rangle|$ are unaffected by affine transformations. Let *height*(a) be a's index in the lexicographic order.

Now by induction on $\sum_{a\in A}$ height(a), A is reduced to be $\langle\langle E\rangle\rangle$-compressed. Otherwise apply a v-compression such that $\langle\langle C_v(A)\rangle\rangle = \langle E\rangle = \langle A\rangle$, while $|A+A|/|A| \geq |C_v(A)+C_v(A)|/|C_v(A)| \geq K$ by Corollary 6 and the induction hypothesis.

Therefore, A has the structure described in Lemma 7. Let H, m, $a_1,...,a_m$, $A_1,...,A_m$ and q be as in the lemma. We estimate $|A|$ and $|A+A|$:

$$A = \bigcup_{i=0}^{q-1}(ia_1+H) \,\cup\, \bigcup_{i=1}^{m} A_i \quad \Rightarrow \quad \frac{q}{p^m} \;\leq\; \frac{|A|}{|\langle A\rangle|} \;\leq\; \frac{m+q}{p^m}, \tag{3}$$

$$A+A = \bigcup_{i=0}^{2q-1}(ia_1+H) \,\cup\, \bigcup_{j=2}^{m}\bigcup_{i=0}^{q-1}(ia_1+a_j+H) \,\cup \bigcup_{1\leq i\leq j\leq m}(A_i+A_j) \tag{4}$$

$$\Rightarrow \quad |A+A| \;\geq\; \big(\min(2q,p-1)+(m-1)q\big)\cdot|H| + \sum_{i\leq j}|A_i+A_j|. \tag{5}$$

Note that (5) is in fact an equality, unless $2q > p$ in which case we use $|H| \geq |A_1+A_1|$. We can further simplify,

$$\sum_{i\leq j}|A_i+A_j| \geq \sum_{i\leq j}\max(|A_i|,|A_j|) \geq \sum_{i\leq j}\frac{|A_i|+|A_j|}{2} = \frac{m+1}{2}\sum_i |A_i| = \frac{m+1}{2}(|A|-q|H|).$$

We substitute this and $|H| = |\langle A\rangle|/p^m$ into (5), to obtain

$$|A+A| \;\geq\; \min_{q,m}\left[\left(\min(2q,p-1)+\frac{(m-3)q}{2}\right)\frac{|\langle A\rangle|}{p^m} \;+\; \frac{m+1}{2}|A|\right], \tag{6}$$

where $1 \leq q < p$ and m is restricted by bounds that follow from (3): a lower bound $m \geq \log_p(q|\langle A\rangle|/|A|)$, and an (implicit) upper bound

$$F_q(m) \;:=\; \frac{p^m}{m+q} \;\leq\; \frac{|\langle A\rangle|}{|A|}.$$

As we show below (Claim 1), the right-hand side of (6) decreases with m (real) for fixed q. It suffices therefore to consider only the largest possible value of m, namely $m = F_q^{-1}(|\langle A\rangle|/|A|)$. After some rearrangement, (6) becomes

$$\frac{|A+A|}{|A|} \;\geq\; \min_q\, G_q\left(F_q^{-1}\left(\frac{|\langle A\rangle|}{|A|}\right)\right),$$

where

$$G_q(m) \;:=\; \left(\min(2q,p-1)+\frac{(m-3)q}{2}\right)\frac{1}{m+q} + \frac{m+1}{2} \;=\; \frac{\binom{m+1}{2}+q(m-1)+\min(2q,p-1)}{m+q}.$$

We also show (Claim 2) that of the $p-1$ real functions $F_q(m) \mapsto G_q(m)$, the smallest one corresponds to $q=1$. The theorem is then established by routine verification of the identity $F_1(m) = p^{2G_1(m)-2}/(2G_1(m)-1)$.

We now turn to justify the choice of m and q.

Claim 1 (choosing m)**.** *The right-hand side of (6) is a decreasing function of m in the relevant interval. That is, for any fixed q, $(2\min(2q,p-1)+(m-3)q)\frac{|\langle A\rangle|}{2p^m}+(m+1)\frac{|A|}{2}$ is a decreasing function of m whenever $|\langle A\rangle|/|A| = p^{2K-2}/(2K-1) \in [p^m/(m+q), p^m/q]$ and $K \geq K_0(p)$*

Proof. Differentiating with respect to m gives $\frac{|A|}{2}+\frac{|\langle A\rangle|}{2p^m}(q-((m-3)q+2\min(2q,p-1))\log p)$. For this expression to be negative when $|A| \leq (m+q)\frac{|\langle A\rangle|}{p^m}$, it is sufficient to require

$$m+q \leq ((m-3)q+2\min(2q,p-1))\log p - q,$$

or equivalently

$$m \;\geq\; m(p,q) := \max\left(\frac{2q-1}{q\log p - 1} - 1\ ,\ \frac{2q+3-2(p-1)\log p}{q\log p - 1} + 3\right).$$

Since $m \geq \log_p\left(q\cdot|\left\langle A\right\rangle|/|A|\right)$, requiring $|\left\langle A\right\rangle|/|A| \geq \max_q\left(p^{m(p,q)}/q\right)$ would clearly make it happen. In terms of our assumption $|\left\langle A\right\rangle|/|A| = p^{2K-2}/(2K-1)$ for $K \geq K_0(p)$, we only have to choose $K_0(p)$ accordingly. □

Claim 2 (choosing q)**.** *The function $G_q \circ F_q^{-1}$ is minimal for $q=1$. That is,*

$$G_q \circ F_q^{-1}(|\left\langle A\right\rangle|/|A|) \;\geq\; G_1 \circ F_1^{-1}(|\left\langle A\right\rangle|/|A|),$$

where $|\left\langle A\right\rangle|/|A| = p^{2K-2}/(2K-1)$ for $K \geq K_0(p)$

Proof. Since G_q and F_q are both increasing functions, the claim is equivalent to $F_q \circ G_q^{-1}$ being maximal for $q=1$. Solving the quadratic gives $G_q^{-1}(x+\frac{1}{2}) = x - q + \sqrt{x^2+g(q)}$ where $g(q) := q^2+3q-2\min(2q,p-1)$. Note that $g(q)$ is always between $q(q-1)$ and $q(q+1)$. Now,

$$F_q\left(G_q^{-1}\left(x+\frac{1}{2}\right)\right) \;=\; \frac{p^{-q+x+\sqrt{x^2+g(q)}}}{x+\sqrt{x^2+g(q)}} \;=\; \frac{p^{-q+2x+O(q^2/x)}}{2x+O(q^2/x)}\ ,$$

which is maximized by $q=1$ for large enough x. In our setting $x+\frac{1}{2} = |\left\langle A\right\rangle|/|A| = p^{2K-2}/(2K-1)$, hence the claim follows by choosing $K_0(p)$ large enough. □

This concludes the proof of Theorem 3. □

Remarks. (on the proof)

1. It is interesting to note that if we fix q, then the function $F_q \circ G_q^{-1}$ gives a tight upper bound. This can be seen by setting $A_{q,m} = \{0, e_1, 2e_1, ..., qe_1, e_2, e_3, ..., e_m\}$.

2. Although no attempt was made to optimize $K_0(p)$, we note that the proofs of Claims 1-2 can be used to obtain an explicit $K_0(p)$ for a given p. For example, one can take $K_0(3) = 6.72$ and $K_0(5) = 2.30$. We also state without proof that a closer analysis would enable showing that $K_0(p) \to 1$ as $p \to \infty$.

4 Discussion

We established in this work the conjecture of Ruzsa for all groups of prime torsion. The fact that a lexicographic order can be defined in $\mathbb{Z}_{p^k}$ (see, e.g., [1, 5]), such that initial segments minimize cardinalities of sumsets as in the Cauchy–Davenport Theorem, suggests that these techniques can be extended to prime-power torsion. Still, a number of technical challenges need to be resolved.

The case of general composite torsion seems more challenging, as no effective analogs of the compression operators are known in this case. We note that in some instances, over groups of composite torsion one can find significantly different extremal structures than over prime or prime-power torsion groups. For example, in [9] explicit Ramsey graphs are constructed, based on incidence structure over $\mathbb{Z}_6$ which cannot exist over prime-power torsion groups. Whether this is the case also in our setting remains to be seen.

References

[1] B. Bollobás and I. Leader. Sums in the grid. *Discrete Mathematics*, 162(1-3):31–48, 1996.

[2] A. L. Cauchy. Recherches sur les nombres. *J. École Polytechnique*, 9:99–123, 1813.

[3] H. Davenport. On the addition of residue classes. *Journal of the London Mathematical Society*, 1(1):30, 1935.

[4] J. M. Deshouillers, F. Hennecart, and A. Plagne. On small sumsets in $(\mathbb{Z}/2\mathbb{Z})^n$. *Combinatorica*, 24(1):53–68, 2004.

[5] S. Eliahou, M. Kervaire, and A. Plagne. Optimally small sumsets in finite abelian groups. *Journal of Number Theory*, 101(2):338–348, 2003.

[6] C. Even-Zohar. On sums of generating sets in $\mathbb{Z}_2^n$. *Combinatorics, Probability and Computing, Available on CJO*, page doi:10.1017/S0963548312000351, 2012.

[7] B. Green and I. Z. Ruzsa. Sets with small sumset and rectification. *Bulletin of the London Mathematical Society*, 38(1):43, 2006.

[8] B. Green and T. Tao. Freiman's theorem in finite fields via extremal set theory. *Combinatorics, Probability and Computing*, 18(03):335–355, 2009.

[9] V. Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20:71–86, 2000.

[10] S. V. Konyagin. On the Freiman theorem in finite fields. *Mathematical Notes*, 84(3):435–438, 2008.

[11] I. Z. Ruzsa. An analog of Freiman's theorem in groups. *Astérisque*, pages 323–326, 1999.

[12] T. Sanders. A note on Freiman's theorem in vector spaces. *Combinatorics, Probability and Computing*, 17(02):297–305, 2008.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de