J. Combin. Theory Ser. A 125 (2014) 333–341

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

The Freiman–Ruzsa theorem over finite fields

Chaim Even-Zohar [a], Shachar Lovett [b,1]

[a] Einstein Institute of Mathematics, HUJI, Israel
[b] CSE Department, UC San Diego, United States

ARTICLE INFO

Article history:
Received 25 September 2013
Available online 16 April 2014

Keywords:
Sumset
Abelian
Doubling
Compression

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 $|A+A| \leqslant K|A|$ 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 $r^{CK}|A|$ for some absolute constant $C \geqslant 2$. 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 coset of a subgroup containing A.

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

E-mail addresses: chaim.evenzohar@mail.huji.ac.il (C. Even-Zohar), slovett@cse.ucsd.edu (S. Lovett).
[1] Supported by NSF CAREER award 1350481.

http://dx.doi.org/10.1016/j.jcta.2014.03.011
0097-3165/

Theorem 1. *(Ruzsa [11]) Let A be a finite subset of an abelian group of torsion r. If $|A+A|/|A| \leqslant K$, then $|\langle A\rangle|/|A| \leqslant K^2 r^{K^4}$.*

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

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

Here and throughout, $\mathbb{Z}_r = \mathbb{Z}/r\mathbb{Z}$. 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 $A = \{0, e_1, e_2, \ldots, e_{2K-2}\}$, the canonical basis of $\mathbb{Z}_r^{2K-2}$, for $K \in \frac{1}{2}\mathbb{N}$ and $r \geqslant 3$, then the doubling constant of A equals K, and we have

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

This leads to the following conjecture.

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

Green and Ruzsa [7] lowered the bound in Theorem 1 to $F(r,K) \leqslant K^2 r^{2K^2-2}$. In the special case $r = 2$, further progress has been made [4,12,8,10,6]. In particular, Green and Tao [8] showed that $F(2,K) \leqslant 2^{2K+O(\sqrt{K}\log K)}$, 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 $K \geqslant K_0$,*

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

Here $K_0 = 8$ is an absolute constant.

This verifies Ruzsa's conjecture for prime torsion. Moreover, the prescribed upper bound is best possible for half-integer K, as was demonstrated in (1). Although no attempt was made to optimize K_0, we note that our method is essentially applicable to lower values of K. For more details, see our comments at the end of Section 3.

Theorem 3 is proven in Section 3. 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].