DIMACS Technical Report 93-77
November 1993

An analog of Freiman's theorem in groups

by

Imre Z. Ruzsa [1]
Mathematical Institute of the Hungarian Academy of Sciences,
Budapest, Pf. 127,
H-1364 Hungary

[1]Paper was finished while author was visiting DIMACS. Support by DIMACS is gratefully acknowledged.

DIMACS is a cooperative project of Rutgers University, Princeton University, AT&T Bell Laboratories and Bellcore.

DIMACS is an NSF Science and Technology Center, funded under contract STC–91–19999; and also receives support from the New Jersey Commission on Science and Technology.

ABSTRACT

It is proved that any set A in a commutative group G where the order of elements is bounded by an integer r having n elements and at most αn sums is contained in a subgroup of size An with $A = f(r, \alpha)$ depending on r and α but not on n. This is an analog of a theorem of G. Freiman which describes the structure of such sets in the group of integers.

Let A be a set of integers, $|A|=n$, and suppose that $|A+A|\leq cn$. A famous theorem of Freiman [1, 2] provides a certain structural description of these sets; in one of the possible formulations, it says that A can be covered by a generalized arithmetic progression

$$\{a+q_1x_1+q_2x_2+...+q_dx_d : 0\leq x_i\leq l_i-1\},$$

where $d<c$ and $\prod l_i\leq Cn$ with C depending on c.

One can ask for a description of sets with few sums in every Abelian group. In this paper we consider groups which are in a sense very far from $\mathbf{N}$.

Theorem. *Let $r\geq 2$ be an integer, and let G be a commuative group in which the order of every element is at most r. Let $A\subset G$ be a finite set, $|A|=n$. If there is another $B\subset G$ such that $|B|=n$ and $|A+B|\leq\alpha n$ (in particular, if $|A+A|\leq\alpha n$ or $|A-A|\leq\alpha n$), then A is contained in a subgroup H of G such that*

$$|H|\leq f(r,\alpha)n,$$

where

$$f(r,\alpha)=\alpha^2r^{\alpha^4}.$$

The proof goes along similar lines to my proof of Freiman's theorem [3, 4], but is considerably simpler.

For a nonnegative integer k and a set $A\subset G$ we introduce the notation

$$kA=A+...+A,\quad k \text{ summands},$$

$$0A=\{0\},\quad 1A=A.$$

Lemma. *If $A,B\subset G$, $|B|=n$ and $|A+B|\leq\alpha n$, then for arbitrary nonnegative integers k,l we have*

$$|kA-lA|\leq\alpha^{k+l}n.$$

See [3], Lemma 3.3.

Proof of the Theorem. Let $b_1,b_2,...,b_k$ be a maximal collection of elements such that $b_i\in 2A-A$ and the sets b_i-A are all disjoint. We have

$$b_i-A\subset 2A-2A,$$

hence

$$\left|\bigcup(b_i-A)\right|=kn\leq|2A-2A|\leq\alpha^4n$$

(the last inequality follows from the Lemma). This implies $k\leq\alpha^4$.

Take an arbitrary $x\in 2A-A$. Since the collection $b_1,...,b_k$ was maximal, there must be an i such that

$$(x-A)\cap(b_i-A)\neq\emptyset,$$

that is, $x - a_1 = b_i - a_2$ with some $a_1, a_2 \in A$, which means

$$x = b_i + a_1 - a_2 \in b_i + (A - A).$$

Hence

$$2A - A \subset \bigcup (b_i + (A - A)) = B + A - A, \tag{1}$$

where $B = \{b_1, ..., b_k\}$.

Now we prove

$$jA - A \subset (j-1)B + A - A \quad (j \geq 2) \tag{2}$$

by induction on j. By (1), this holds for $j = 2$. Now we have

$$\begin{aligned}(j+1)A - A &= (2A - A) + (j-1)A \\ &\subset B + A - A + (j-1)A \text{ by (1)} \\ &= B + (jA - A) \subset B + (j-1)B + A - A \\ &= jB + A - A,\end{aligned}$$

which provides the inductive step.

Let H and I be the subgroups generated by A and B, respectively. By (2) we have

$$jA - A \subset I + (A - A) \tag{3}$$

for every j. We have also

$$\bigcup (jA - A) = H, \tag{4}$$

which easily follows from the fact that the order of elements of G is bounded. (3) and (4) imply that

$$H \subset I + (A - A).$$

Since I is generated by k elements of order $\leq r$ each, we have

$$|I| \leq r^k \leq r^{\alpha^4},$$

consequently

$$|H| \leq |I||A - A| \leq \alpha^2 r^{\alpha^4} n$$

(the estimate for $|A - A|$ follows from the Lemma). QED

Remarks.

Take a group of the form $G = Z_r^m$, where Z_r is a cyclic group of order m, and a set $A \subset G$ of the form

$$A = (a_1 + G') \cup ... \cup (a_k + G')$$

with a subgroup G'. Here $|A| = n = k|G'|$, and if all the sums $a_i + a_j$ lie in different cosets of G', then

$$|A + A| = \frac{k(k+1)}{2}|G'| = \alpha n, \quad \alpha = \frac{k+1}{2}.$$

The subgroup generated by A can have as many as $r^k|G'|$ elements, hence our function

$$f(r,\alpha)=\alpha r^{\alpha^4}$$

cannot be replaced by anything smaller than

$$r^k=r^{2\alpha-1}.$$

Conjecture. The Theorem holds with $f(r,\alpha)=r^{C\alpha}$ with a suitable constant C.

The following conjecture of Katalin Marton would yield a more efficient covering in a slightly different form.

Conjecture. If $|A|=n$, $|A+A|\le\alpha n$, then there is a subgroup H of G such that $|H|\le n$ and A is contained in the union of α^c cosets of H, where the constant c may depend on r but not on n or α.

This also suggests that perhaps in Freiman's original problem a better result can be formulated in terms of covering by a small number of generalized arithmetical progressions than just one.

References

[1] G. A. Freiman, *Foundations of a structural theory of set addition*, Translation of Math. Monographs vol. 37, Amer. Math. Soc., Providence, R. I., USA, 1973.

[2] G. A. Freiman, What is the structure of K if $K+K$ is small?, in: *Lecture Notes in Mathematics 1240*, Springer-Verlag, New York – Berlin 1987, 109–134.

[3] I. Z. Ruzsa, Arithmetical progressions and the number of sums, Periodica Math. Hung. **25** (1992), 104–111.

[4] I. Z. Ruzsa, Generalized arithmetical progressions and sumsets, Acta Math. Sci. Hung., to appear.

Imre Z. Ruzsa

Mathematical Institute of the Hungarian Academy of Sciences, Budapest, Pf. 127, H-1364 Hungary

e-mail: h1140ruz@ella.hu