SYMMETRY SETS, APPROXIMATE GROUPS

NORBERT HEGYVÁRI

ABSTRACT. We show that the set $Sym_\alpha(A) = \{h : |A \cap (A+h)| \geq \alpha|A|\}$ is a $c_1 \log|A|-$approximate group and $2Sym_\alpha(A)$ is a c_2-approximate group, where c_1 depends only on α, K, r, and c_2 depends only on α, K, provided $|A-A| < K|A|$, and the order of elements of commutative group G is at most r.

2000 Mathematics Subject Classification:11B75,05D10.

Keywords: Sumset, Approximate group

1. INTRODUCTION

Let G be (and in the rest of the paper) a commutative group, and let A, B be subsets of G. An easy observation that $A \pm B = A$ if and only if that there exists a finite subgroup G' of G such that B is contained in a coset of G', and A is the union of cosets of G'. In the proof of this fact one can introduce the symmetry group of A as follows

$$Sym_1(A) = \{h : A + h = A\}.$$

In an excellent book of Tao and Vu [1] introduced a generalization of this notion by the following way: let

$$Sym_\alpha(A) = \{h : |A \cap (A+h)| \geq \alpha|A|\}.$$

It is also defined a $K-$approximate group.

Definition. Let $K \geq 1$. A set H is called $K-$approximate, if
(i) it is symmetric, i.e. $H = -H$,
(ii) contains the origin $0 \in H$
(iii) $H + H$ can be covered by at most K translates of H;

$$H + H \subseteq H + X,$$

for some $|X| \leq K$.

Clearly that the $1-$approximate group is really a subgroup and $Sym_\alpha(A)$ plays important rules some equivalent formulation of additive theorems. Since $Sym_\alpha(A)$ is symmetric and contains the origin it is reasonable to ask wether it is a $P-$approximate group for some P. Generally perhaps we cannot say more so we concentrate to sets with property $|A-A| < K|A|$.

Date: August 30, 2007.

2. Results

First we investigate $2Sym_\alpha(A)$ proving the following theorem:

Theorem 2.1. *Let $A \subseteq G$ and assume $|A-A| < K|A|$ for some $K \geq 1$ and let $0 < \alpha < \frac{1}{K}$. Define $Sym_\alpha(A) = \{h : |A \cap (A+h)| \geq \alpha|A|\}$. Then $2Sym_\alpha(A)$ is a $K^{16}\big(\frac{1-\alpha}{1-\alpha K}\big)^2-$approximate group.*

Proof. Since $0 < \alpha < \frac{1}{K} \leq 1$, the set $Sym_\alpha(A)$ is non-empty containing 0. If $|A \cap (A+h)| \geq \alpha|A|$ for some h then clearly $|A \cap (A-h)| \geq \alpha|A|$ also holds, i.e. $Sym_\alpha(A) = -Sym_\alpha(A)$. Furthermore by $|A \cap (A+h)| \geq \alpha|A| > 0$, we conclude $h \in A-A$, so $Sym_\alpha(A) \subseteq A-A$.

Let $L = K^{16}\big(\frac{1-\alpha}{1-\alpha K}\big)^2$. We have to have ensure that $4Sym_\alpha(A)$ can be covered by at most L translates of $2Sym_\alpha(A)$. We need the following lemmas.

Lemma 2.2. *Let $A \subseteq G$ and assume $|A-A| < K|A|$. Then*

$$|mA - nA| \leq K^{m+n}|A|.$$

It is the well-known theorem of Plünnecke-Ruzsa.

Lemma 2.3. *Let $A \subseteq G$ and assume $|A-A| < K|A|$ for some $K \geq 1$. We have*

$$|Sym_\alpha(A)| \geq |A| \cdot \frac{1-\alpha K}{1-\alpha}.$$

Proof. Note that $|A \cap (A+h)|$ is the solution of $h = a - a'$ $a, a' \in A$, denoted by $d_{A-A}(h) = d(h)$. Clearly $d(h) < \alpha|A|$, for $h \notin Sym_\alpha(A)$, and $d(h) \leq |A|$, for $h \in Sym_\alpha(A)$. Thus

$$|A|^2 = \sum_{h \in A-A} d(h) \leq |Sym_\alpha(A)||A| + \alpha|A| \cdot (|A-A| - |Sym_\alpha(A)|).$$

Using $|A-A| < K|A|$ and rearranging the inequality we obtain

$$|Sym_\alpha(A)| \geq |A|\frac{1-\alpha K}{1-\alpha}.$$

□

Now we follow the idea of covering process (see in [1]and [2]). We collect of a maximal disjoint system of sets $x_i - Sym_\alpha(A)$, where $x_i \in 2Sym_\alpha(A) - Sym_\alpha(A) = 3Sym_\alpha(A)$. By $Sym_\alpha(A) \subseteq A-A$,

$$x_i - Sym_\alpha(A) \subseteq 2Sym_\alpha(A) - 2Sym_\alpha(A) = 4Sym_\alpha(A) \subseteq 4A - 4A,$$

and by the disjointness, by Lemma 2.2 with $n = m = 4$ and by Lemma 2.3 we have

$$\left| \cup_{i=1}^{t} (x_i - Sym_\alpha(A)) \right| = t \cdot |Sym_\alpha(A)| \leq K^8|A| \leq$$

$$\leq K^8 \frac{1-\alpha}{1-\alpha K}|Sym_\alpha(A)|,$$

so

$$t \leq K^8 \frac{1-\alpha}{1-\alpha K}.$$

Let $X = \{x_1, x_2, \dots x_t\}$. We prove that $3Sym_\alpha(A)$ can be covered by $X + 2Sym_\alpha(A)$, and that $4Sym_\alpha(A)$ by $2X + 2Sym_\alpha(A)$.

For the maximality of X we get that for every $y \in 3Sym_\alpha(A)$ $y = x_i + s + s'$, for some $x_i \in X$, $s, s' \in Sym_\alpha(A)$, i.e.

$$3Sym_\alpha(A) \subseteq X + 2Sym_\alpha(A),$$

and hence

$$4Sym_\alpha(A) \subseteq X + 3Sym_\alpha(A) \subseteq 2X + 2Sym_\alpha(A).$$

The cardinality of $|2X|$ is at most

$$|X|^2 \leq K^{16}\big(\frac{1-\alpha}{1-\alpha K}\big)^2.$$

We obtain that $2Sym_\alpha(A)$ is a $K^{16}\big(\frac{1-\alpha}{1-\alpha K}\big)^2-$approximate group as we wanted.

□

Theorem 2.4. *Assume that the order of every element of G is at most $r \geq 2$. Let $K \geq 1$, and let $A \subseteq G$, for which $|A - A| \leq K$. Then $Sym_\alpha(A)$ is a $P-$approximate group, where $L = K^{16}\big(\frac{1-\alpha}{1-\alpha K}\big)^2$ and $P = \frac{(1-\alpha)K^4 r^L \cdot \log|A|}{(1-\alpha K)} + \frac{(1-\alpha)K^4 r^L \log(K^4 r^L)}{(1-\alpha K)}$.*

Roughly speaking $Sym_\alpha(A)$ is an $f(\alpha, K, r)\log|A|-$approximate group, where $f(\alpha, K, r)$ depends only on α, K and r.

Proof. We need a lemma.

Lemma 2.5. *Let G be a group for which the order of every element is at most $r \geq 2$. Let $H \subseteq G$ be an $L-$approximate group. Then the order of $\langle H \rangle$ is at most $r^L|H|$.*

Proof. Since H is an $L-$approximate group, we have that there exists a set X, with cardinality at most L. We state that $H + \langle X \rangle$ is a subgroup and by

$$\langle H \rangle \subseteq H + \langle X \rangle$$

we have $|\langle H \rangle| \leq |H + \langle X \rangle| \leq r^L|H|$, since the order of every element of G is at most r. Indeed we get

$$H + \langle X \rangle \subseteq H + \langle X \rangle + H + \langle X \rangle = H + H + \langle X \rangle \subseteq$$

$$\subseteq H + \langle X\rangle + X = H + \langle X\rangle,$$

so

$$(H + \langle X\rangle) + (H + \langle X\rangle) = H + \langle X\rangle.$$

□

By Theorem 2.1 we have that $2Sym_\alpha(A)$ is a $K^{16}\big(\frac{1-\alpha}{1-\alpha K}\big)^2-$approximate group. Keep the notation $L = K^{16}\big(\frac{1-\alpha}{1-\alpha K}\big)^2$ and let $\widetilde{G} := \langle 2Sym_\alpha(A)\rangle$. By Lemma 2.2

$$|2Sym_\alpha(A)| \le K^4|A|,$$

and by Lemma 2.5

$$|\widetilde{G}| \le K^4 r^L |A|.$$

Finally we use the following lemma:

Lemma 2.6. *Let $U \subseteq \widetilde{G}$. There exists a set Y such that $\widetilde{G} = U + Y$, and*

$$|Y| \le \frac{|\widetilde{G}|}{|U|}\log|\widetilde{G}| - 1.$$

It is $[Q8]$ in [3]. For the completeness we prove this lemma (at $[Q8]$ there is no an explicit detailed proof, although a probabilistic type is given in another place.)

Proof. 1. Let B be any set in $\widetilde{G}$. Since

$$\sum_{x\in G}|U\cap(B+x)| = |U||B|,$$

thus there exists $x \in \widetilde{G}$, for which

$$|U\cap(B+x)| \le \frac{|U||B|}{|G|}.$$

2. With this $x \in \widetilde{G}$ we have

$$\frac{|\widetilde{G}| - |U\cup(B+x)|}{|\widetilde{G}|} \le \frac{|\widetilde{G}| - |U|}{|\widetilde{G}|}\cdot\frac{|\widetilde{G}| - |B|}{|\widetilde{G}|}.$$

Indeed

$$\frac{|\widetilde{G}| - |U| - |B|}{|\widetilde{G}|} = \frac{|\widetilde{G}| - |U\cup(B+x)| - |U\cap(B+x)|}{|\widetilde{G}|} \ge$$

$$\ge \frac{|\widetilde{G}| - |U\cup(B+x)| - \frac{|U||B|}{|\widetilde{G}|}}{|\widetilde{G}|},$$

from which we have

$$|\widetilde{G}| - |U \cup (B+x)| \leq |\widetilde{G}| - |U| - |B| + \frac{|U||B|}{|\widetilde{G}|} = |\widetilde{G}|\big(1 - \frac{|U|}{|\widetilde{G}|}\big) \cdot \big(1 - \frac{|B|}{|\widetilde{G}|}\big).$$

With $U = B$ we obtain

$$|\widetilde{G}| - |U \cup (U+x)| \leq |\widetilde{G}|\big(1 - \frac{|U|}{|\widetilde{G}|}\big)^2.$$

By induction we have that there exists a set $Y = \{y_1 = 0, y_2, \dots y_s\}$, such that

$$|\widetilde{G}| - |U+Y| \leq |\widetilde{G}|\big(1 - \frac{|U|}{|\widetilde{G}|}\big)^{|Y|} \leq |\widetilde{G}| \cdot e^{\frac{-|U||Y|}{|\widetilde{G}|}}.$$

Finally if

$$|\widetilde{G}| \cdot e^{\frac{-|U||Y|}{|\widetilde{G}|}} < 1,$$

which is equivalent to $|Y| \leq \frac{|\widetilde{G}|}{|U|} \log |\widetilde{G}| - 1$, we obtain that

$$|\widetilde{G}| = |U+Y|,$$

and hence $\widetilde{G} = U + Y$, as we wanted. □

Let $U := Sym_\alpha(A)$. By Lemma 2.6 we get a set Y,

$$|Y| \leq \frac{|\widetilde{G}|}{|U|} \log |\widetilde{G}| - 1,$$

such that Y translates of $Sym_\alpha(A)$ cover $\widetilde{G}$ and hence cover $2Sym_\alpha(A)$ as well. It means that $Sym_\alpha(A)$ is a $|Y|-$approximate group.

Finally we give an estimation for $|Y|$.

Since $|\widetilde{G}| \leq K^4 r^L |A|$, we have

$$|Y| \leq \frac{K^4 r^L |A|}{|A|^{\frac{1-\alpha K}{1-\alpha}}} \cdot \log(K^4 r^L |A|) =$$

$$= \frac{(1-\alpha) K^4 r^L \cdot \log |A|}{(1-\alpha K)} + \frac{(1-\alpha) K^4 r^L \log(K^4 r^L)}{(1-\alpha K)}.$$

□

3. Concluding remarks

1. In the proof of Theorem 2.4 we cover a subgroup generated by $2Sym_\alpha(A)$ and not directly the set $2Sym_\alpha(A)$; we have two reasons: the first is that by Theorem 2.1 we obtain that the cardinality of the generated group is not too "big" comparing with the cardinality of $2Sym_\alpha(A)$. The second reason is that although we can use Lemma 2.6 for the set $2Sym_\alpha(A)$ instead of $\widetilde{G}$, but $|2Sym_\alpha(A)| = |U+Y|$ does not imply that $2Sym_\alpha(A) = U+Y$.

2. Let $A \subseteq G$, and let $A(x)$ be its indicator function of the set A, i.e. $A(x) = 1$ if $x \in A$, and zero otherwise. Write the Fourier transform of it by the formula

$$\widehat{A}(r) = \sum_{r\in G} A(x)e(xr),$$

where xr is a bilinear form and $e(xr)$ is a character in G (see details in [1]). For example when $G = \mathbb{Z}_n$, then $e(\theta) := e^{\frac{2\pi i\theta}{n}}$.

A similar notion of $Sym_\alpha(A)$ would be the $\alpha-$spectrum $Spec_\alpha(A) \subseteq G$ by the definition

$$Spec_\alpha(A) := \{r : |\widehat{A}(r)| \geq \alpha|A|\}.$$

It is not too hard to check that $Spec_\alpha(A)$ is symmetric, contains the origin. In case when $G = \mathbb{Z}_n$ (and some generalization of any commutative group G) by the celebrated theorem of Chang we infer that $Spec_\alpha(A)$ is also a $K-$approximate group, where $K = (1/\varrho)^{\log 3/\alpha^2}$, for sets $A \subseteq \mathbb{Z}_n$, $|A| = \varrho n$.

Indeed Chang's theorem says that if $A \subseteq \mathbb{Z}_n$, A has size ϱn, then $Spec_\alpha(A)$ can be covered by $Span(L)$, $|L| = O(\log(1/\varrho)/\alpha^2$, and

$$Span(L) = \{\sum \varepsilon_i\lambda_i; \lambda_i \in L; \varepsilon_i \in \{-1, 0, 1\}\}.$$

Hence

$$Spec_\alpha(A) + Spec_\alpha(A) \subseteq Spec_\alpha(A) + Span(L),$$

and $|Span(L)| \leq (1/\varrho)^{\log 3/\alpha^2}$.

$Spec_\alpha(A)$ can be consider as a dual of $Sym_\alpha(A)$ as noted also in [1].

Acknowledgement: This paper is supported by "Balaton Program Project" and OTKA grants T0 43623,49693,38396.

References

[1] T.Tao, V.Vu: Additive Combinatorics, Cambridge University Press, Cambridge 2006
[2] I.Z. Ruzsa: An Analog of Freiman's Theorem, DIMACS Technical Report 93-77
[3] T.Tao, Lecture Notes 1. available in

Norbert Hegyvári, ELTE TTK, Eötvös University, Institute of Mathematics, H-1117 Pázmány st. 1/c, Budapest, Hungary
E-mail address: hegyvari@elte.hu