ANNALES UNIV. SCI. BUDAPEST., **50** (2007), 1–7

ITERATED DIFFERENCE SETS IN σ-FINITE GROUPS

By

NORBERT HEGYVÁRI and FRANÇOIS HENNECART

(Received July 11, 2008)

Abstract. We improve on a previous result on iterated difference sets in arbitrary $\sigma-$finite groups.

1. Introduction

We investigate here the concept of iterated difference sets in the following way: for a given subset X of an arbitrary additively written group G, we define $D(X) = X - X = \{x - x' : x, x' \in X\}$ called difference set of X. We put $D_1 = D$, and for $k \geq 2$, $D_k(X) = D(D_{k-1}(X))$ for any $X \subseteq G$. In the case where G is the set of integers, Stewart and Tijdeman in [5] investigated the so-called iterated positive difference operation: for an infinite set A of positive integers, let $D^+(A)$ be the positive difference set defined by $D^+(A) = \{a - a' \mid a \geq a', a, a' \in A\}$. The k-fold iterated positive difference sequence $\{D^+{}_k(A);\ k \geq 0\}$ of A is defined by $D^+{}_0(A) = A$ and $D^+{}_k(A) = D^+(D^+{}_{k-1}(A))$ for $k \geq 1$. Stewart and Tijdeman observed that if a sequence A has positive upper density i.e.

$$\overline{d}(A) := \limsup_{n \to \infty} \frac{|A \cap \{1, 2, \ldots, n\}|}{n} > 0,$$

then the sequence $\{D^+{}_k(A);\ k \geq 0\}$ is stable i.e. there exists a k_0 such that, $D^+{}_{k+1}(A) = D^+{}_k(A)$ for every $k \geq k_0$.

We define the time of stability of A by $T(A) = \min\{k \mid D^+{}_{k+1}(A) = D^+{}_k(A)\}$. For instance, if $\overline{d}(A) > 1/2$, it is readily seen that $D^+(A)$ is

AMS Subject Classification (2000): 11B75, 05D10, 37A45

Research of the authors are partially supported by "Balaton Program Project" and OTKA grants K61908, K67676. The second author is partially supported by the CNRS

the whole set of nonnegative integers, hence $T(A) \leq 1$. In [5] Stewart and Tijdeman gave an upper bound for $T(A)$ if the upper density of A is positive. They proved that if $0 < \overline{d}(A) \leq 1/2$ then $T(A) \leq 2\log_2(\overline{d}(A)^{-1})$, where $\log_2$ denotes the logarithmic function in base 2. This result was improved by Ruzsa in [4] where it is shown that under the same assumption on $\overline{d}(A)$, we have $T(A) \leq 2 + \log_2(\overline{d}(A)^{-1} - 1)$ and this bound is sharp.

At this point we note that a seemingly similar question is to consider the sequence $\{D_k(A);\ k \geq 1\}$ of the iterated difference sets without any restriction. The advantage of this question is that it can be handled in more general groups. Let G be a countable torsion group and let $H_1 \subseteq H_2 \subseteq \cdots \subseteq \subseteq H_n \subseteq \cdots$ be a sequence of finite subgroups of G. Then G is said to be σ-finite with respect to $\{H_n\}$ if $G = \bigcup_{n=1}^{\infty} H_n$.

We assume that G is a such group. Let $A \subseteq G$. The asymptotic upper density of A is defined by

$$\overline{d}(A) = \limsup_{n\to\infty} \frac{|A \cap H_n|}{|H_n|}. \tag{1}$$

We introduce the time of stability in groups as well.

Assume the sequence $\{D_k(A);\ k \geq 0\}$ is stable (i.e. for some k, $D_{k+1}(A) = D_k(A)$). Let $T(A, G)$ be the time of stability defined by

$$T(A, G) = \min\{k \mid D_{k+1}(A) = D_k(A)\}.$$

In [1] the first named author extended the results of Stewart, Tijdeman and Ruzsa to σ-finite Abelian groups. He proved

Theorem A. *Let G be a σ-finite abelian group with respect to $\{H_n\}$ and let A be a non empty subset of G. Let $\overline{d}(A)$ be the upper density of A defined by (1). If $\overline{d}(A) > 0$, then*

$$T(A, G) \leq \log_2(\overline{d}(A)^{-1}) + 2.$$

It is worth mentioning that generalization to arbitrary linear operations (i.e. instead of $D(X)$, we consider operation $\Gamma(X) = aX - bX$) of this kind of problem is investigated in [2].

In the next section, we present some basic multiplicative results which are used in the rest of the section in order to show that Theorem A holds with an optimal bound in some sense without assuming G to be abelian.

ACKNOWLEDGEMENT. We would like to thank Y. Ould Hamidoune to direct our attention to a paper of Olson and for the discussion on it.

2. Iterated difference sets in finite group and σ-finite group

In this section, groups are not necessarily abelian and are written multiplicatively with identity element denoted by 1. Let G be any group and $A, A_1, A_2, \ldots, A_k$ be subsets of G. We denote by $A_1A_2\cdots A_k$ the subset of G of all products $x_1x_2\ldots x_k$ with $x_j \in A_j$, $j = 1\ldots,k$. We also define for $k \geq 1$, the k-fold product set $A^k = A\cdots A$ (k times), $A^{-1} = \{x^{-1} \mid x \in A\}$, and we put $D(A) = AA^{-1}$. We denote by $|A|$ the cardinality of A. Finally let $D_0(A) = A$, $D_1(A) = D(A)$ and $D_k(A) = D(D_{k-1}(A))$ for $k \geq 2$.

2.1. Preliminary results

LEMMA 2.1. *Let A and B be subsets of a finite group G such that $|A| + |B| \geq |G| + 1$. Then $AB = G$.*

PROOF. Indeed if there is a $g \in G$ which is not in AB, then $A^{-1}g \cap B = \emptyset$ and so $|A^{-1}g| + |B| = |A| + |B| \leq |G|$, a contradiction. ∎

LEMMA 2.2. *Let A be a generating subset of a finite group G such that $1 \in A$. For any non-empty subset X of G*

$$|XA| \geq \min\{|G|, |X| + |A|/2\}.$$

PROOF. It is Theorem 1 in [3]. ∎

A straightforward consequence, which is obtained by an iterated application of this lemma, is that for any generating subsets $A_1, \ldots, A_j$ of a finite group G such that $1 \in A_i$, $i = 1, \ldots, j$, one has

$$|A_1A_2\ldots A_j| \geq \min\left(|G|, |A_1| + \frac{|A_2| + \cdots + |A_j|}{2}\right).$$

2.2. Results for finite and σ-finite groups

We extend Theorem A to arbitrary finite groups and σ-finite groups. We first consider the case of arbitrary groups.

THEOREM 2.3. *Let A be a generating subset of a finite group G such that $1 \in A$. Let k_0 defined by*

$$k_0 = \begin{cases} 1 & \text{if } |G|/2 < |A| \leq |G|, \\ \left\lfloor \log_2 \left(\frac{|G|}{|A|} - 1 \right) \right\rfloor + 2 & \text{if } |A| \leq |G|/2 \end{cases}$$

where $\lfloor u \rfloor$ denotes the greatest integer less than or equal to the real number u.

Then, for any integer $k \geq k_0$

$$D_k(A) = G. \tag{2}$$

PROOF. If $|A| > |G|/2$ then by Lemma 2.1. with $B = A^{-1}$, we get $D_1(A) = G$. In the remaining of the proof, we assume that $|A| \leq |G|/2$. To see that (2) holds if $k \geq k_0$, we shall use the remark following Lemma 2.2. For any $k \geq 1$, $D_{k-1}(A)$ is a product of $2^k - 1$ subsets, the factors being alternatively A or A^{-1}, which are both generating subsets of G and containing 1. It follows that $|D_{k-1}(A)| > |G|/2$ whenever $k > \log_2(|G|/|A| - 1) + 1$. By Lemma 2.1., we conclude that $D_k(A) = G$ under the same assumption on k. This gives our theorem. ∎

These bounds allow us to improve that on [1, Proposition1]. We obtain for k_0 defined in Theorem 2.3. that

$$T(A, G) \leq k_0 \tag{3}$$

for any subset A of an arbitrary finite group G.

We now show that Theorem A holds for any non abelian σ-finite group as well. In the case where A is a subset of a σ-finite group G with upper density $\overline{d}(A)$ larger than $1/2$, it is readily seen that $A - A = G$, hence $T(A, G) \leq 1$. We then formulate the remaining case:

THEOREM 2.4. *Let G be a σ-finite group with respect to $\{H_n\}$ and let A be a non empty subset of G. Assume that A has a positive upper density such that $\alpha := \overline{d}(A)^{-1} \geq 2$. Then*

$$T(A, G) \leq \lfloor \log_2(\alpha - 1) \rfloor + 2. \tag{4}$$

PROOF. Since the function $\lfloor\ \rfloor$ is right-continuous, there exists a real number $0 < \eta < 1$ such that the right-hand side of (4) is equal to

$$k := \lfloor \log_2(\alpha - \eta) \rfloor + 2.$$

Let

$$\varepsilon := \min(-\log_2(\eta), 1 - \{\log_2(\alpha - \eta)\}) \tag{5}$$

where $\{u\} = u - \lfloor u \rfloor$ denotes the fractional part of u. Note that $\varepsilon > 0$ hence $2^{\varepsilon} > 1$, hence there exists an increasing sequence of integers $\{n_1 < n_2 < \cdots < n_i < \cdots\}$ such that

$$\overline{d}(A) < 2^{\varepsilon} \frac{|A \cap H_{n_i}|}{|H_{n_i}|}, \quad i \geq 1. \tag{6}$$

We claim that $T(A, G) \leq k$. Suppose that it is not the case. Thus

$$D_k(A) \neq D_{k+1}(A). \tag{7}$$

Let $A_n = A \cap H_n$. By (7) we infer that there exists an integer $n \in \{n_i\ ;\ i \geq 1\}$ such that (6) holds and

$$D_k(A_n) \neq D_{k+1}(A_n). \tag{8}$$

Then by (5) and (6), we get

$$\alpha - \eta > 2^{-\varepsilon} \frac{|H_n|}{|A_n|} - \eta \geq 2^{-\varepsilon} \left(\frac{|H_n|}{|A_n|} - 1 \right),$$

hence, by (5) again,

$$k \geq \log_2(\alpha - \eta) + 1 + \varepsilon > \log_2 \left(\frac{|H_n|}{|A_n|} - 1 \right) + 1 + \varepsilon - \log_2(2^{\varepsilon}) =$$

$$= \log_2 \left(\frac{|H_n|}{|A_n|} - 1 \right) + 1.$$

By Theorem 2.3. and (3), we get $k \geq T(A_n, H_n)$, i.e. A_n is stable after k steps, a contradiction to (8). This ends the proof. ∎

3. Concluding remarks

In order to show that bounds (3) for $T(A, G)$ deduced from Theorem 2.3. (and thus the bounds in Theorem 2.4.) are sharp, we provide the following example:

Let m be a positive integer and put $n = 2^{m+1} + 1$. We denote by U_n the abelian multiplicative group formed by the complex n-th roots of unity and let $A = \{1, \omega := \exp(2i\pi/n)\}$. It is clear that for any $k \geq 1$

$$D_k(A) = \{\omega^j,\ -2^{k-1} \leq j \leq 2^{k-1}\},$$

hence $T(A, U_n) = m+1$, which coincides with the corresponding upper bound given in Theorem 2.3.

We may extend this example as follows. Let G be a finite group and H be a normal subgroup of G such that the factor group G/H is cyclic generated by gH for some $g \in G$. We let $A = H \cup gH$. Then clearly $T(A, G) = T(\overline{A}, G/H)$ where $\overline{A}$ is the image of A by the canonical morphism from G onto G/H. If we assume further that G/H has order $n = 2^{m+1} + 1$ for some $m \geq 1$, we get

$$T(A, G) = T(\overline{A}, G/H) = T(\{1, \omega\}, U_n) = m + 1 = \left\lfloor \log_2 \left(\frac{|G|}{|A|} - 1 \right) \right\rfloor + 2.$$

To conclude, we stress the fact that upper bounds in Theorems 2.3. and 2.4. can be sligthly improved if we consider particular groups G and subsets A of G. For instance, we easily deduce from Cauchy-Davenport theorem that $T(A, \mathbb{Z}/p\mathbb{Z}) \leq \log_2 \left(\frac{p-1}{k-1} \right)$ where p is a prime number and A any subset of $\mathbb{Z}/p\mathbb{Z}$ with cardinality $k \geq 2$. Another way to derive better bounds is to observe that in fact we have $|XA| \geq \min(|G|, |X| + \lceil |A|/2 \rceil)$ in Lemma 2.2. where $\lceil u \rceil$ denotes the smallest integer larger than or equal to the real number u.

References

[1] N. HEGYVÁRI: On iterated difference sets in groups, *Period. Math. Hung.,* **43** (2001), 105–110.

[2] N. HEGYVÁRI, F. HENNECART and A. PLAGNE: Iterated linear operation on sets of positive upper density, to appear in *International J. of Number Theory*.

[3] J. E. OLSON: On the Sum of Two Sets in a Group, *J. Number Th.,* **18** (1984), 110–120.

[4] I. Z. RUZSA: Iterated difference sets, *Studia Sci. Math. Hungar.,* **22** (1987), 197–202.

[5] C. L. STEWART and R. TIJDEMAN: On density-difference sets of sets of integers, in: *Studies in Pure Mathematics,* pp. 701–710, Birkhäuser Verlag, Basel, 1983.

Norbert Hegyvári
Loránd Eötvös University,
Faculty of Sciences
Institute of Mathematics
H-1117 Pázmány st. 1/c
Budapest, Hungary
hegyvari@elte.hu

François Hennecart
LaMUSE, Univ. Jean-Monnet
23 rue Michelon
42023 Saint-Etienne
cedex 2, France
francois.hennecart@univ-st-etienne.fr