ANNALES DE L'INSTITUT FOURIER

ROBERT KAUFMAN

Small subsets of finite abelian groups

Annales de l'institut Fourier, tome 18, n° 1 (1968), p. 99-102

<http://www.numdam.org/item?id=AIF_1968__18_1_99_0>

© Annales de l'institut Fourier, 1968, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (http://annalif.ujf-grenoble.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. Inst. Fourier, Grenoble
18, 1 (1968), 99-102

SMALL SUBSETS OF FINITE ABELIAN GROUPS

par Robert KAUFMAN

Varopoulos [2], in constructing certain sets in infinite compact abelian groups, made special use of various properties of finite groups. In this note a method is given by which many of the results of [2] can be recovered in a uniform manner. To explain the utility of the theorem stated below, let $G = \prod_{i=1}^{\infty} G_i$ be the product of infinitely many finite abelian groups, μ_i a probability measure on G_i $(1 \leqslant i < \infty)$. As usual, the Fourier-Stieltjes transform is defined for a measure ν as

$$\hat{\nu}(x) = \int_G \overline{x(t)}\, \nu(dt), \quad x \in \hat{G}.$$

Then $\hat{\mu}(x) \longrightarrow 0$ as $x \longrightarrow \infty$ in $\hat{G}$ if and only if

$$\max \{|\hat{\mu}_i(x_i)| : x_i \in \hat{G}_i, x_i \neq 1\}$$

converges to 0 as $i \longrightarrow \infty$.

THEOREM. – *For each* $\varepsilon > 0$ *there is an* M *such that any finite abelian group* G *of order* $>$ M *contains a subset* S *with the properties*

1) $\log |S| \leqslant \varepsilon \log |G|$

2) $|\sum_{s \in S} x(s)| < \varepsilon |S|$ *for any character* $x \neq 1$ *of* G.

(Here $|A|$ means the number of elements of a set A).

Observe that by 2) S generates G, and by 1) that the r-fold sum $\pm S \pm \ldots \pm S$ contains at most $2^r |S|^r$ elements ; this is the kind of estimate needed often in [2].

In the proof it is necessary to decompose finite subgroups of the circle T, the decomposition depending upon a positive integer K. If H is such a subgroup and H has order $r \leqslant K^2$, H is partitioned into singletons. Otherwise, let ω be an element of $H - \{1\}$ for which the Euclidean distance $|\omega - 1|$ is smallest. Set

$$H_i = \{\omega^j : (i-1)rK^{-1} \leqslant j < irK^{-1}\}, \ 1 \leqslant i < K,$$

$$H_K = \{\omega^j : rK^{-1}(K-1) \leqslant j < r\}.$$

Note that $$rK^{-1} \leqslant |H_i| + 1 \leqslant rK^{-1} + 1.$$

Each character $x \neq 1$ maps G onto a finite subgroup H of T, decomposed into subsets depending on some K chosen in advance. Suppose that for some $p > 0$ and every H_i, $1 \leqslant i \leqslant K^2$, depending on any $x \neq 1$,

$$p\left(1 - \frac{1}{2}\varepsilon\right)|x^{-1}(H_i)| \leqslant |S \cap x^{-1}(H_i)| \leqslant p\left(1 + \frac{1}{2}\varepsilon\right)|x^{-1}(H_i)|.$$

Then requirement 2) is met for large enough K. Because $|S| = 0(p) \cdot |G|$, requirement 1) for large $|G|$ follows from

$$\log p = \left(\frac{1}{2}\varepsilon - 1\right)\log|G|.$$

S is chosen as a "random" element of 2^G, each element being chosen with probability p. More precisely, let $\{X_g : g \in G\}$ be a set of $|G|$ independent random variables indexed by G, and

$$P\{X_g = 1\} = p, P\{X_g = 0\} = 1 - p, g \in G.$$

Of course $g \in S$ means $X_g = 1$ and so

$$|S \cap x^{-1}(H_i)| = \sum_{g \in x^{-1}(H_i)} X_g.$$

All of this can be stated without reference to any special properties of G. The sums in question are, in number, $\leqslant K^2 |G|$, and the number of independent random variables in each sum is $\geqslant K^{-2}|G|$. Write

$Y = \sum_1^N X_j$ for any of these sums ; it is enough to show that for all such Y,

$$P\left\{|Y - pN| \geqslant \frac{1}{2}\varepsilon pN\right\} = o(|G|)$$

as $|G| \longrightarrow \infty$.

Writing $\bar{E}$ for expectation, for any number λ

$$\bar{E}(e^{\lambda Y}) = \bar{E}^N(e^{\lambda X_1}) = (1 + p(e^\lambda - 1))^N .$$

If

$$\lambda = \log\left(1 + \frac{1}{2}\varepsilon\right) \text{ and } Y \geqslant \left(1 + \frac{1}{2}\varepsilon\right) pN, e^{\lambda Y} \geqslant \left(1 + \frac{1}{2}\varepsilon\right)^{(1+\frac{1}{2}\varepsilon)pN},$$

so that

$$P\left\{Y \geqslant \left(1 + \frac{1}{2}\varepsilon\right) pN\right\} \leqslant \left(1 + \frac{1}{2}\varepsilon p\right)^N \Big/ \left(1 + \frac{1}{2}\varepsilon\right)^{(1+\frac{1}{2}\varepsilon)pN},$$

$$N^{-1} \log P\left\{Y \geqslant \left(1 + \frac{1}{2}\varepsilon\right) pN\right\} \leqslant \log\left(1 + \frac{1}{2}\varepsilon p\right) - p\left(1 + \frac{1}{2}\varepsilon\right) \log\left(1 + \frac{1}{2}\varepsilon\right) .$$

Now $\log\left(1 + \frac{1}{2}\varepsilon p\right) - p\left(1 + \frac{1}{2}\varepsilon\right) \log\left(1 + \frac{1}{2}\varepsilon\right) =$

$$O(p^2) + \frac{1}{2}\varepsilon p - p\left(1 + \frac{1}{2}\varepsilon\right)\log\left(1 + \frac{1}{2}\varepsilon\right),$$

while $s < (1 + s)\log(1 + s)$ for $s > 0$.

Hence $P\left\{Y \geqslant \left(1 + \frac{1}{2}\varepsilon\right) pN\right\} \leqslant c^{pN}$

for some $c < 1$.

This is clearly $o(|G|)$, and the magnitude of $P\left\{Y \leqslant \left(1 - \frac{1}{2}\varepsilon\right) Np\right\}$ is subject to entirely similar estimates. The proof is complete.

We indicate briefly how the argument can be applied to the a-adic integers, defined by Hewitt and Ross ([1], pp. 108-111). The analogue of the first result is as follows.

For each $\varepsilon > 0$ there is an M such that for any numbers

$$a_1 > 1, \ldots, a_N > 1 \quad \text{with} \quad a_1 \ldots a_N > M,$$

there is a subset S of the set $\{(u_1, \ldots, u_N), 0 \leqslant u_i < a_i\}$ with the properties

1′) $\log |S| \leqslant \varepsilon \log(a_1 \ldots a_N)$.

2′) For any complex number $w \neq 1$, but $w^{a_1 a_2 \cdots a_N} = 1$,

$$\left| \sum_{s \in S} w^{u_1 + a_1 u_2 + \ldots + a_1 \ldots a_{N-1} u_N} \right| < \varepsilon |S|.$$

In fact, the collection of all possible exponents

$$\{u_1 + a_1 u_2 + \ldots + a_1 \ldots a_{N-1} u_N : 0 \leqslant u_i < a_i\}$$

is a complete residue system modulo $a_1 a_2 \ldots a_N$, so the previous arguments are valid.

BIBLIOGRAPHIE

[1] E. HEWITT and K.A. ROSS, Abstract Harmonic Analysis I, (1963).

[2] N. Th. VAROPOULOS, Sets of multiplicity in locally compact abelian groups, *Ann. Inst. Fourier, Grenoble*, XVI (1966), 123-158.

Manuscrit reçu le 18 mai 1967.

Robert KAUFMAN,
Department of Mathematics,
University of Illinois,
Urbana, Illinois 61801