Discrete Mathematics 84 (1990) 197–200
North-Holland

COMMUNICATION

AN UNCERTAINTY INEQUALITY AND ZERO SUBSUMS

Roy MESHULAM
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

Communicated by J. Kahn
Received 15 February 1990

Let G be a finite abelian group, and let m be the maximal order of elements in G. It is shown that if $s > m\left(1 + \log \frac{|G|}{m}\right)$, then any sequence $a_1, \ldots, a_s$ of elements in G, has a non-empty subsequence which sums to zero. The result is a consequence of an inequality for the finite Fourier transform.

1. Introduction

For a finite abelian group G, let $s(G)$ denote the maximal s for which there exists a sequence $a_1, \ldots, a_s \in G$ such that $\sum_{i \in I} a_i \neq 0$ for all $\phi \neq I \subset \{1, \ldots, s\}$.

Olson [4], addressing a problem of Davenport, showed that for a p-group $G = \mathbf{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbf{Z}_{p^{e_r}}$, $s(G) = \sum_{i=1}^{r} (p^{e_i} - 1)$, so in particular $s(\mathbf{Z}_q^n) = (q-1)n$ whenever q is a prime power.

The exact value of $s(G)$ is known in some other cases – see [3, 5].

In this note we obtain an upper bound on $s(G)$ for general G. Let t denote the number of prime divisiors of $|G|$ counted with multiplicities, and let m be the maximum order of the elements of G.

Baker and Schmidt [1] proved that

$$s(G) \leq 5m^2 t \log(3mt),$$

where log denotes the natural logarithm.

Our purpose is to prove the following

Theorem 1. $s(G) \leq m\left(1 + \log \frac{|G|}{m}\right)$.

Since $|G| \leq m^t$ Theorem 1 implies

Corollary 1. $s(G) \leq m \cdot \log |G| \leq m \cdot \log m \cdot t$.

The second inequality verifies a conjecture of Baker and Schmidt ([1, p. 462]).

In Section 2 we prove an uncertainty type inequality for the finite Fourier transform (Theorem 2), which directly implies Theorem 1 (Section 3).

2. An inequality for the Fourier transform

Let F be a field which contains a primitive kth root of unity ζ. The Fourier transform of a function $f: Z_k^n \to F$ is the function $\hat{f}: Z_k^n \to F$ defined by $\hat{f}(x) = \sum_{y \in Z_k^n} f(y) \zeta^{-y \cdot x}$ (where $y \cdot x$ denotes the standard inner product in Z_k^n).

Let $\delta: Z_k \to F$ be defined by $\delta(x) = \delta_{0,x}$.

For an integer $s \geq 0$, we define $\alpha(k, s)$ as follows: $\alpha(k, 0) = 1$ and $\alpha(k, s) = \lceil \alpha(k, s-1) \cdot k/(k-1) \rceil$ for $s > 0$.

The main result of this section is the following;

Theorem 2. *If $f: Z_k^n \to F$ satisfies $f(0) = 1$ and $f(\varepsilon) = 0$ for all $0 \neq \varepsilon \in \{0, 1\}^n$, then $|\operatorname{Supp} \hat{f}| \geq \alpha(k, n)$.*

Proof. We argue by induction on n.

First note that if $g: Z_k \to F$ satisfies $|\operatorname{Supp} \hat{g}| \leq 1$, then $\hat{g}(x) = C\delta(x - x_0)$ for some $C \in F$ and $x_0 \in Z_k$, hence $g(x) = (1/k) \sum_{y \in Z_k} \hat{g}(y) \zeta^{yx} = (C/k) \zeta^{x_0 x}$, and in particular $g(0) = \zeta^{-x_0} g(1)$.

Therefore if $f: Z_k \to F$ satisfies $f(0) = 1$ and $f(1) = 0$, then $|\operatorname{Supp} \hat{f}| \geq 2 = \alpha(k, 1)$.

Assume now that $n > 1$ and $f: Z_k^n \to F$ satisfies $f(0) = 1$ and $f(\varepsilon) = 0$ for all $0 \neq \varepsilon \in \{0, 1\}^n$.

For $y \in Z_k$ define $f_y: Z_k^{n-1} \to F$ by $f_y(x) = f(x, y)$, and for $a \in Z_k^{n-1}$ define $g_a: Z_k \to F$ by $g_a(y) = \widehat{f_y}(a)$.

For $(a, b) \in Z_k^{n-1} \oplus Z_k$ we have:

$$\hat{f}(a, b) = \sum_{x \in Z_k^{n-1}} \sum_{y \in Z_k} f(x, y) \zeta^{-x \cdot a - yb} = \sum_{y \in Z_k} \widehat{f_y}(a) \zeta^{-yb} = \widehat{g_a}(b).$$

Hence $|\operatorname{Supp} \hat{f}| = \sum_{a \in Z_k^{n-1}} |\operatorname{Supp} \widehat{g_a}|$.

For $0 \leq i \leq k-1$ define $h_i: Z_k^{n-1} \to F$ by $h_i(x) = f_0(x) - \zeta^i f_1(x)$. Clearly $h_i(0) = 1$ and $h_i(\varepsilon) = 0$ for all $0 \neq \varepsilon \in \{0, 1\}^{n-1}$, so by induction hypothesis $A_i = \operatorname{Supp} \widehat{h_i}$ satisfies $|A_i| \geq \alpha(k, n-1)$.

Now, $A_i = \{a \in Z_k^{n-1} : \widehat{f_0}(a) \neq \zeta^i \widehat{f_1}(a)\} = \{a \in Z_k^{n-1} : g_a(0) \neq \zeta^i g_a(1)\}$, hence the following hold:

(1) If $a \in A_i$ then $g_a \not\equiv 0$ and therefore $|\operatorname{Supp} \widehat{g_a}| \geq 1$.

(2) If $a \in \bigcap_{i=0}^{k-1} A_i$, then $g_a(y)$ is not of the form $C\zeta^{-yy_0}$ (for otherwise $g_a(0) = \zeta^{y_0} g_a(1)$, contradicting $a \in A_{y_0}$), and therefore $|\operatorname{Supp} \widehat{g_a}| \geq 2$.

To complete the proof we need the following easy

Lemma. *If $B_1, \ldots, B_k$ are sets of cardinality at least u, then*

$$\left| \bigcup_{i=1}^{k} B_i \right| + \left| \bigcap_{i=1}^{k} B_i \right| \geq \frac{ku}{k-1}.$$

Proof. Let $|\bigcap_{j=1}^{k} B_j| = v$ and $C_i = B_i - \bigcap_{j=1}^{k} B_j$ for $1 \leq i \leq k$. Since $\bigcap_{i=1}^{k} C_i = \emptyset$ we obtain:

$$(u - v)k \leq |\{(x, i) : x \in C_i\}| \leq \left|\bigcup_{i=1}^{k} C_i\right| \cdot (k - 1),$$

and so

$$\left|\bigcup_{i=1}^{k} B_i\right| + \left|\bigcap_{i=1}^{k} B_i\right| = \left|\bigcup_{i=1}^{k} C_i\right| + 2v \geq \frac{(u - v)k}{k - 1} + 2v \geq \frac{ku}{k - 1}. \quad \square$$

Now (1), (2), and the lemma imply

$$|\operatorname{Supp} \hat{f}| = \sum_{a \in \mathbf{Z}_k^{n-1}} |\operatorname{Supp} \widehat{g_a}| \geq \left|\bigcup_{i=0}^{k-1} A_i\right| + \left|\bigcap_{i=0}^{k-1} A_i\right| \geq \left\lceil \frac{k}{k - 1} \alpha(k, n - 1) \right\rceil = \alpha(k, n). \quad \square$$

Corollary 2. *If f is as in Theorem* 1, *and $n \geq k - 1$ then* $|\operatorname{Supp} \hat{f}| \geq \frac{k}{e} \cdot \left(\frac{k}{k-1}\right)^n$.

Proof. Clearly $\alpha(k, k - 1) = k$, hence

$$|\operatorname{Supp} \hat{f}| \geq \alpha(k, n) \geq \alpha(k, k - 1) \cdot \left(\frac{k}{k - 1}\right)^{n-(k-1)} \geq \frac{k}{e} \cdot \left(\frac{k}{k - 1}\right)^n. \quad \square$$

Remark. The proof of Theorem 2 can be extended to show:

Theorem 2'. *Let $0 < d < k$. If $f : \mathbf{Z}_k^n \to \mathbf{F}$ satisfies $f(0) = 1$ and $f(\varepsilon) = 0$ for all $0 \neq \varepsilon \in \{0, 1, \ldots, d\}^n$, then*

$$|\operatorname{Supp} \hat{f}| \geq \left\lceil \cdots \left\lceil \left\lceil \frac{k}{k - d} \right\rceil \frac{k}{k - d} \right\rceil \cdots \frac{k}{k - d} \right\rceil \ (n \text{ times}).$$

3. Zero subsums in a finite abelian group

First note that if H is a subgroup of $\mathbf{Z}_m^s$, then the transform of the indicator function of H satisfies $\widehat{1_H} = |H| \cdot 1_{H^\perp}$ where $H^\perp = \{a \in \mathbf{Z}_m^s : a \cdot h = 0 \text{ for all } h \in H\}$. We shall also use $H^{\perp\perp} = H$.

We proceed with the proof of Theorem 1: Let $G = \mathbf{Z}_{m_1} \oplus \cdots \oplus \mathbf{Z}_{m_n}$ where $m_i \mid m$ for all $1 \leq i \leq n$. Let $s = s(G)$ and suppose $a_1, \ldots, a_s \in G$ satisfy $\sum_{i=1}^{s} \varepsilon_i a_i \neq 0$, for all $0 \neq (\varepsilon_1, \ldots, \varepsilon_s) \in \{0, 1\}^s$. We write $a_i = (a_{i1}, \ldots, a_{in})$ where $0 \leq a_{ij} < m_j$ and define $b_1, \ldots, b_n \in \mathbf{Z}_m^s$ by $b_j = (m/m_j) \cdot (a_{1j}, \ldots, a_{sj})$ for $1 \leq j \leq n$. Let H be the subgroup of $\mathbf{Z}_m^s$ generated by $b_1, \ldots, b_n$. The order of b_j is at most m_j, hence $|H| \leq m_1 \cdots m_n = |G|$.

By our assumptions $H^\perp \cap \{0, 1\}^s = \{0\}$, hence $1_{H^\perp}$ satisfies the conditions of

Theorem 2. Since $s \geqslant m-1$ Corollary 2 implies

$$\frac{m}{e}\cdot\left(\frac{m}{m-1}\right)^{s} \leqslant |\mathrm{Supp}\,\widehat{1_{H^{\perp}}}| = |\mathrm{Supp}(|H^{\perp}|\cdot 1_H)| = |H| \leqslant |G|.$$

Therefore

$$s \leqslant \frac{1+\log\dfrac{|G|}{m}}{\log\dfrac{m}{m-1}} < m\left(1+\log\frac{|G|}{m}\right).$$

Remarks. (1) The proof of Theorem 1 and the obvious inequality $s(\mathbf{Z}_k^n) \geqslant (k-1)n$ show that the constant $k/(k-1)$ in Theorem 2, may not be replaced by any constant larger than $k^{1/k-1}$.

(2) After completing this paper (February 1989), it was brought to our attention that Theorem 1 was proved in 1969 by P. van Emde Boas and D. Kruyswijk [2]. Their methods are different and do not include Theorem 2.

Acknowledgment

I would like to thank Jeff Kahn for his helpful comments.

References

[1] R.C. Baker and W.M. Schmidt, Diophantine problems in variables restricted to the values 0 and 1, J. Number Theory 12 (1980) 460–486.
[2] P. van Emde Boas and D. Kruyswijk, A combinatorial problem on finite abelian groups III, Z.W. 1969-008 (Math. Centrum, Amsterdam).
[3] H.B. Mann, Additive group theory – A progress report, Bull. Amer. Math. Soc. 79 (1973) 1069–1075.
[4] J.E. Olson, A combinatorial problem on finite abelian groups I, J. Number Theory 1 (1969) 8–10.
[5] J.E. Olson, A combinatorial problem on finite abelian groups II, J. Number Theory 1 (1969) 195–199.