

Thin Bases for Finite Abelian Groups

XING-DE JIA

*Department of Mathematics,
Graduate School and University Center,
The City University of New York,
New York, New York 10036*

Communicated by R. L. Graham

Received June 10, 1989; revised November 30, 1989

Let $h \geq 2$ be any integer, let $c = h(1 + 2^{-1/h})^{h-1}$. In this paper, it is proved that every finite abelian group G contains a subset A such that $hA = G$ and $|A| \leq c|G|^{1/h}$, where hA denotes the set of all sums of h not necessarily distinct elements in A , and $|A|$ denotes the cardinality of the set A . © 1990 Academic Press, Inc.

1. INTRODUCTION

Let G be a finite group, and $h \geq 2$ an integer. A subset A of G is called a *basis of order h for G* if $A^h = G$, where A^h , hA in the abelian case, denotes the subset of G of all products of h not necessarily distinct elements from A . If A is a basis of order h for G , then $|A| \geq |G|^{1/h}$. It is natural to ask if there exists a constant c such that every finite group G contains a "thin" basis A of order h with $|A| \leq c|G|^{1/h}$. Rohrbach [2, 3] asked this question more than 50 year ago. Rohrbach observed that such thin bases exist for cyclic groups. Cherly [1] proved that every finite abelian group G of order n contains a basis A of order 2 for G such that $|A| \leq 2(n \log n)^{1/2} + 2$. In this paper, I shall prove the following theorem.

THEOREM. *Let $h \geq 2$ be an integer, $c = h(1 + 2^{-1/h})^{1/h}$. Then every finite abelian group G contains a basis A of order h such that $|A| \leq c|G|^{1/h}$.*

In particular, every finite abelian group G of order n contains a basis A of order 2 such that $|A| \leq (2 + \sqrt{2})\sqrt{n}$. This greatly improves Cherly's result.

2. PROOF OF THE THEOREM

LEMMA 1. Let P be a finite abelian group of order p^s , where p is a prime number, and s is a positive integer. Then $P = H \oplus K$, where $|H| = p^{uh}$, and K is a direct sum of at most $h - 1$ cyclic subgroups.

Proof. Suppose that $P = P_1 \oplus \dots \oplus P_r$, where $|P_i| = p^{u_i}$. It is well known that there exists a subset S of at most $h - 1$ positive integers so that $\sum_{i \notin S} u_i \equiv 0 \pmod{h}$. Let K be the sum of all P_i with $i \in S$, and H the sum of all other P_i 's. Then H is of order p^{uh} and K is a direct sum of at most $h - 1$ cyclic subgroups. The proof is complete.

LEMMA 2. If G is a finite cyclic group of order m , then there exist h subsets A_1, \dots, A_h in G such that

$$A_1 + \dots + A_h = G \quad \text{and} \quad |A_i| < m^{1/h} + 1 \quad \text{for } i = 1, \dots, h.$$

Proof. Let $u = \lceil m^{1/h} \rceil + 1$, where $\lceil x \rceil$ denotes the least integer not smaller than x . Let $A_i = \{0, u^{i-1}, \dots, (u-1)u^{i-1}\}$ for $i = 1, \dots, h$. Clearly

$$|A_i| = u < m^{1/h} + 1 \quad \text{for } i = 1, \dots, h.$$

Suppose that $A_1 + \dots + A_s$ contains $[0, u^s - 1]$, where $[a, b]$ denotes the set of integers between a and b . Choose $n : u^s \leq n < u^{s+1}$. Suppose $n = qu^s + r$, where $1 \leq q \leq u - 1$, and $0 \leq r \leq u^s - 1$. Then $r \in A_1 + \dots + A_s$, hence

$$n = qu^s + r \in A_1 + \dots + A_s + A_{s+1}.$$

Therefore, $A_1 + \dots + A_h \supseteq [0, u^h - 1] \supseteq [0, m - 1]$.

Proof of Theorem. Suppose $G = G_1 \oplus \dots \oplus G_r$, where $|G_i| = p_i^{s_i}$, $s_i > 0$, and p_1, \dots, p_r are distinct prime numbers. It follows from Lemma 1 that $G = H \oplus K$, where H is of order m^h and K is a direct sum of at most $h - 1$ cyclic subgroups. Suppose that H_1 is a subgroup of $H = H_0$ with $|H_1| = m^{h-1}$, and A_1 is a set of representatives of the cosets in H_0/H_1 . Let A_i be a set of representatives of the cosets in H_{i-1}/H_i , where H_i is a subgroup of H_{i-1} with $|H_i| = m^{h-i}$. It is clear that $H = A_1 + \dots + A_h$, and $|A_i| = m$. Now suppose that $K = K_1 \oplus \dots \oplus K_r$, where $r \leq h - 1$ and each K_j is cyclic. Lemma 2 implies that $K_j = A_{j1} + \dots + A_{jh}$, where $|A_{ji}| < |K_j|^{1/h} + 1$ for $i = 1, \dots, h$. Let $B_i = A_i + A_{1i} + \dots + A_{ri}$ for $i = 1, \dots, h$. Then $B_1 + \dots + B_h = G$, and

$$|B_i| = m \cdot \prod_{1 \leq j \leq r} (|K_j|^{1/h} + 1) < (1 + 2^{-1/h})^r n^{1/h}.$$

Define $A = B_1 \cup \dots \cup B_h$, and the proof is complete.

ACKNOWLEDGMENTS

I thank Professors Melvyn B. Nathanson and Paul Erdős and the referee for their helpful comments.

REFERENCES

1. J. CHERLY, Complementary sets of group elements, *Arch. Math.* **35** (1980), 313–318.
2. H. ROHRBACH, Eine Beitrag zur additiven Zahlentheories, *Math. Z.* **42** (1937), 1–30.
3. H. ROHRBACH, Anwendung eines States der additiven Zahlentheorie auf eine gruppen-theoretische Frage, *Math. Z.* **42** (1937), 537–542.