Order Number 9029946

Some results in additive number theory

Jia, Xing-De, Ph.D.

City University of New York, 1990

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

SOME RESULTS IN ADDITIVE NUMBER THEORY

by
XING-DE JIA

A dissertation submitted to the Graduate Faculty in
Mathematics in partial fulfillment of the requirements for the
Degree of Doctor of Philosophy
The City University of New York

1990

This documentation was prepared with LaTeX.

AMS 1980 Mathematics Subject Classification (1985 revision).
Primary 05A05, 05C25, 11B13, 11B34, 11B75, 20F05.
Secondary 05B10, 11N45, 11P68, 20F18, 20K01, 20M14.

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

April 26, 1990
Date

Melvin B. Nathanson
Chair of Examining Committee

April 30, 1990
Date

Robert Sacksteder
Executive Officer

Carlos J. Moreno

Harvey Cohn

Mark

Supervisory Committee

The City University of New York

To my wife, Xuewei

ACKNOWLEDGEMENTS

First of all, I would like to acknowledge my deepest indebtedness to my advisor Dr. Melvyn B. Nathanson, from whom I learned number theory and started to do research in this field. His constant encouragement, valuable advice and continued interest in my research played an important role in the progress and completion of this thesis. Dr. Nathanson not only stimulated and guided my research in mathematics, but also helped me so much tiding over serious financial difficulties and many other unexpected difficulties during the past years. I really appreciate every thing he has done for me.

I would like to thank Professor Paul Erdös for his simple proof of Lemma 4.1 in Chapter 4, and his nice talks with me, which led the work in Sections 4.3 and 4.5 in Chapter 4.

I would like to thank Dr. Frank Hsu for his discussion with me which led the work in Section 4.6.

I also would like to thank the CUNY Graduate School, CUNY Research Foundation and Lehman College for their continuous financial support, and all professors in the Department of Mathematics at the CUNY Graduate School for their interesting lectures.

I wish to thank my parents for their love, understanding and encouragement. They would be very proud of their son at this wonderful moment and always.

Finally, I wish to thank my wonderful wife for her love, understanding and encouragement. She made my life so enjoyable and she helped me so much that words cannot express my appreciation.

Abstract

SOME RESULTS IN ADDITIVE NUMBER THEORY

by

XING-DE JIA

Thesis Advisor: **Dr. Melvyn B. Nathanson**

The thesis is devoted to the study of bases in additive number theory. It contains four chapters.

Chapter One investigates the order of subsets of asymptotic bases. Let $g(A)$ denote the smallest integer h such that the set A is an asymptotic basis of order h. Some estimates are proved for the extremal function

$$G_k(h) = \max_{g(A)\le h} \max_{\substack{|F|=k \\ g(A\setminus F)<\infty}} g(A\setminus F),$$

including

$$G_k(h) \ge (k+1)\left(\frac{k+1}{k+2}\right)^k \left(\frac{h}{k+1}\right)^{k+1} + O(h^k)$$

as h tends to infinity for any fixed k. It is also proved that $G_k(h)$ has order of magnitude k^{h-1} as k tends to infinity for any fixed h. An interesting connection between this problem and the theory of extremal bases in the postage stamp problem is also proved in this chapter.

Chapter Two describes a simple and explicit construction of minimal asymptotic bases of order h for every $h \ge 2$ by using either powers of 2 or g-adic representations of integers. It is also proved in this chapter that

there exist minimal bases for commutative monoids, which generalizes some results in additive number theory concerning minimal bases.

In Chapter Three, it is proved that if $\Phi = \{S_1, S_2, \ldots, S_s\}$ and $\Psi = \{T_1, T_2, \ldots, T_t\}$ are two families of nonempty, pairwise disjoint sets such that $|S_i| \leq h$, $|T_j| \leq k$ ($h \geq 2$ and $k \geq 1$) and $S_i \not\subseteq T_j$ for all i and j, then

$$N(\Phi, \Psi) \leq h^s \left(1 - \frac{h-r}{h^{q+1}}\right)^t,$$

where $k = q(h-1) + r$ with $0 \leq r \leq h-2$, and $N(\Phi, \Psi)$ is the number of sets X such that X is a minimal system of representatives for Φ and X is simultaneously a system of representatives for Ψ. This was a conjecture of Nathanson. A further result is also proved in this chapter. This study was motivated by a problem in additive number theory concerning the existence of minimal bases in given asymptotic bases.

Chapter Four considers the existence of thin bases for finite groups. Let $h \geq 2$ be any integer. It is proved that every finite abelian group G of order n contains a subset A such that $hA = G$ and

$$|A| < c_1 n^{1/h}, \quad \text{where} \quad c_1 = h(1 + 2^{-1/h})^{h-1},$$

and that every finite nilpotent group G of order n contains a subset A such that $A^h = G$ and

$$|A| < c_2 n^{1/h}, \quad \text{where} \quad c_2 = 2^{h-1} h,$$

which completely answers an old question by Rohrbach in the nilpotent case. Some applications of these results to Cayley graphs are also given. It is also proved in this chapter that bases with given number of representations exist for certain infinite abelian groups.

Contents

1 ON SUBSETS OF ASYMPTOTIC BASES

1.1 Introduction

Let $\mathbf{N}$ denote the set of all nonnegative integers. Let A be a subset of $\mathbf{N}$, and let h be a positive integer. Let hA denote the set of all sums of h not necessarily distinct elements in A. If hA contains all nonnegative integers then A is called a *basis of order h*. If hA contains all sufficiently large integers then A is called an *asymptotic basis of order h*. The major problem in additive number theory is to describe the structure of various kinds of bases. Most famous examples are Goldbach's Conjecture which states that any large even integer is expressable as a sum of two prime numbers, and Waring's Problem about the kth powers of integers. More recent work in additive number theory is concerned with general bases.

The simplest example of a basis is the set of all odd integers and 0, which is a basis of order two because any even integer is a sum of two odd integers and any odd integer is a sum of 0 and the odd integer itself. Lagrange's Theorem asserts that each positive integer can be written as a sum of at most four squares of integers, thus the set of squares is a basis of order four.

Let A be an asymptotic basis, and $a \in A$. The $A\backslash\{a\}$ is not necessarily an asymptotic basis. For instance,

$$H = \{n \in \mathbf{N} \mid m \equiv 0 \bmod h\} \cup \{1\}$$

is a basis of order h, but $H\backslash\{1\}$ is not an asymptotic basis of any order.

We denote by I the set of elements $a \in A$ such that $A\backslash\{a\}$ is an asymptotic basis. Erdös and Graham [8] and Grekos [16] showed that $a \in I$ if and only if

$$\gcd\{x - x' \mid x, x' \in A\backslash\{a\}\} = 1.$$

Let $g(A)$ denote the least integer h such that A is a basis of order h. For any $a \in I$, Erdös and Graham investigated how large $g(A\backslash\{a\})$ could be in terms of $g(A)$. Define

$$G_1(h) = \max_{g(A)\leq h} \max_{a\in I} g(A\backslash\{a\}).$$

Erdös and Graham [8] proved that

$$\frac{1}{4}(1 + o(1))h^2 \leq G_1(h) \leq \frac{5}{4}(1 + o(1))h^2.$$

In his doctoral thesis, Grekos [16] improved this estimate to

$$\frac{1}{3}h^2 + O(h) \leq G_1(h) \leq h^2 + h,$$

and Nash [38] improved the upper bound even further:

$$G_1(h) \leq \frac{1}{2}h^2 + h.$$

However, there is still a big gap between the upper and lower bounds. Some exact values of $G_1(h)$ are known for small h. Erdös and Graham [8] showed that $G_1(2) = 3$, Nash [38] showed that $G_1(3) = 7$ and $G_2(3) = 13$. Li [34] showed that $G_1(4) = 10$ and $G_1(5) = 15$. It would be interesting to calculate more values of $G_1(h)$.

Nathanson [43] first considered the general form of this problem. Let $k \geq 1$ be an integer. If A is an asymptotic basis, let $I_k(A)$ denote the set of all subsets F of A such that F has cardinality k and the set $A\backslash F$ is still an asymptotic basis. Define

$$G_k(h) = \max_{g(A)\leq h} \max_{F\in I_k(A)} g(A\backslash F).$$

Nathanson proved that

$$G_k(h) \geq \left(\left[\frac{h}{k+1}\right]+1\right)^{k+1} - 1,$$

where $h > k$, and $[x]$ denotes the largest integer not exceeding x. In [24], I improved this result to

$$G_k(h) \geq \frac{4}{3}\left(\frac{h}{k+1}\right)^{k+1} + O(h^k) \quad (\text{as } h \to \infty), \tag{1.1}$$

and recently I have proved that

$$G_k(h) \geq (k+1)\left(\frac{k+1}{k+2}\right)^{k}\left(\frac{h}{k+1}\right)^{k+1} + O(h^k) \quad (\text{as } h \to \infty). \tag{1.2}$$

It is clear that (1.2) is sharper than (1.1) for all $k > 1$. But the proof of (1.1) is much simpler. So in Section 1.2, I shall present the proofs of these two results. In Section 1.2, I shall also prove a connection between this problem and the theory of extremal bases in the postage stamp problem, which provides some lower bounds for $G_k(h)$ by using a result of Mrose [36] about finite h-bases for integers.

In Section 1.3, I shall prove the following estimate for $G_k(h)$ as k tends to infinity for any fixed integer $h \geq 2$:

$$G_k(h) + 1 \geq 2\left(\frac{k}{h-1}\right)^{h-1} + (4h-5)\left(\frac{k}{h-1}\right)^{h-2} + O(k^{h-3}),$$

and

$$G_k(h) + 1 \leq \frac{2}{(h-1)!}k^{h-1} + \frac{h-1}{(h-2)!}k^{h-2} + O(k^{h-3}).$$

In particular, we have that $G_k(2) = 2k + 2$ for all $k \geq 1$, which is a result by Nash [38].

1.2 Lower Bounds for $G_k(h)$ for Fixed k

Theorem 1.1 *Let $k \geq 1$. Then*

$$G_k(h) \geq \frac{4}{3}\left(\frac{h}{k+1}\right)^{k+1} + O(h^k)$$

as h tends to infinity.

In order to prove this theorem, we need the following lemmas.

Lemma 1.1 *Let $h \geq k+1$ and $k \geq 1$. Define*

$$\begin{aligned} u &= \left[\frac{h}{k+1}\right], \\ u' &= \left[\frac{2h}{3k+3}\right], \\ \sigma &= h-(k-1)u-2u', \\ b_1 &= \left[\frac{2h}{k+1}\right], \\ b_i &= ub_{i-1}+\sigma \quad \text{for } i=2,3,\ldots,k, \\ d &= u'b_k+b_1-h+(k-1)u+u'. \end{aligned}$$

Then

$$md+\sum_{i=1}^{k}x_ib_i+h-\sum_{i=1}^{k}x_i \geq (m-1)d+\sum_{i=1}^{k}x_ib_i+b_1+u'b_k \qquad (1.3)$$

and

$$(m-1)d+\sum_{i=1}^{k}x_ib_i+u'b_k+h-\sum_{i=1}^{k}x_i-u' \geq md+\sum_{i=1}^{k}x_ib_i \qquad (1.4)$$

hold for any $m \geq 1$, and $0 \leq x_i \leq u$ for $i=1,\ldots,k-1, 0 \leq x_k \leq u'$.

Proof. From the definition, we have

$$md+\sum_{i=1}^{k}x_ib_i+h-\sum_{i=1}^{k}x_k = (m-1)d+\sum_{i=1}^{k}x_ib_i+h-\sum_{i=1}^{k}x_i+d$$

$$\begin{aligned} &= (m-1)d + \sum_{i=1}^{k} x_i b_i + b_1 + u'b_k + \sum_{i=1}^{k-1}(u - x_i) + (u' - x_k) \\ &\geq (m-1)d + \sum_{i=1}^{k} x_i b_i + b_1 + u'b_k, \end{aligned}$$

which shows (1.3). It follows from the definition that

$$\begin{aligned} &(m-1)d + \sum_{i=1}^{k} x_i b_i + u'b_k + h - \sum_{i=1}^{k} x_i - u' \\ &= md - u'b_k - b_1 + h - (k-1)u - u' + \sum_{i=1}^{k} x_i b_i + u'b_k + h - \sum_{i=1}^{k} x_i - u' \\ &= md + \sum_{i=1}^{k} x_i b_i + 2h - (k-1)u - 2u' - \sum_{i=1}^{k} x_i - b_1 \\ &\geq md + \sum_{i=1}^{k} x_i b_i + 2h - 2(k-1)u - 3u' - b_1. \end{aligned}$$

Noticing that

$$\begin{aligned} 2(k-1)u + 3u' + b_1 &\leq 2(k-1) \cdot \frac{h}{k+1} + 3 \cdot \frac{2h}{3k+3} + \frac{2h}{k+1} \\ &= 2h\left(\frac{k-1}{k+1} + \frac{3}{3k+3} + \frac{1}{k+1}\right) \\ &= 2h, \end{aligned}$$

we have that

$$(m-1)d + \sum_{i=1}^{k} x_i b_i + 2h - 2(k-1)u - 3u' - b_1 \geq md + \sum_{i=1}^{k} x_i b_i,$$

which implies (1.4). The proof of Lemma 1.1 is complete.

Lemma 1.2 *Let $h, k, u, u', \sigma, b_1, \ldots, b_k$ be as in Lemma 1.1. If*

$$0 \leq x_i \leq u \quad \textit{for} \quad i = 1, \ldots, k-1, \qquad \textit{and} \qquad 0 \leq x_k \leq 2u',$$

then

$$\sum_{i=s+1}^{k} x_i b_i + u b_s + h - \sum_{i=s+1}^{k} x_i - u \geq \sum_{i=s+1}^{k} x_i b_i + b_{s+1}$$

holds for any $1 \leq s \leq k-1$.

Proof. Noticing that $s \geq 1$, we have

$$\begin{aligned} h - \sum_{i=s+1}^{k} x_i - u &\geq h - (k-2)u - 2u' - u \\ &= h - (k-1)u - 2u' \\ &= \sigma. \end{aligned}$$

Therefore,

$$\begin{aligned} \sum_{i=s+1}^{k} x_i b_i + u b_s + h - \sum_{i=s+1}^{k} x_i - u &\geq \sum_{i=s+1}^{k} x_i b_i + u b_s + \sigma \\ &= \sum_{i=s+1}^{k} x_i b_i + b_{s+1}, \end{aligned}$$

which proves Lemma 1.2.

Lemma 1.3 *Let d be as in Lemma 1.1. Then*

$$D = \{a \mid a \equiv 0 \text{ or } 1 \bmod d\}$$

is an asymptotic basis of order

$$g(D) = \frac{4}{3}\left(\frac{h}{k+1}\right)^{k+1} + O(h^k).$$

Proof. It is clear that $h \geq 3k+3$ implies $d > 4$. Let n be any positive integer with $n = qd + r$, where $0 \leq r \leq d-1$. If $r = 0$ then $n = qd \in D$, hence $n \in (d-1)D$. If $r > 0$ then

$$n = (qd+1) + (r-1) \in rD,$$

so $n \in (d-1)D$, hence D is an asymptotic basis of order $g(D) \leq d-1$.

For any m, if

$$md + (d-1) = \sum_{i=1}^{t} a_i, \quad a_i \in D,$$

then it follows from the definition of D that there exist at least $d-1$ elements a_i in $\{a_1, a_2, \ldots, a_t\}$ such that $a_i \equiv 1 \bmod d$, which implies that $t \geq d-1$. Therefore,

$$\begin{aligned} g(D) &= d-1 \\ &= u'b_k + b_1 - h + u' - 1 \\ &= u'ub_{k-1} + u'\sigma + b_1 - h + (k-1)u + u' - 1 \\ &= \cdots \\ &= u'u^{k-1}b_1 + u'(u^{k-2} + \cdots + u + 1) + b_1 - h + (k-1)u + u' - 1 \\ &= \frac{2h}{3k+3} \cdot \left(\frac{h}{k+1}\right)^{k-1} + O(h^k) \\ &= \frac{4}{3}\left(\frac{h}{k+1}\right)^{k+1} + O(h^k). \end{aligned}$$

The proof is complete.

Proof of Theorem 1.1. Let $F = \{b_1, b_2, \ldots, b_k\}$, and let $A = F \cup D$, where $b_1, b_2, \ldots, b_k, d$, and D are as in Lemmas 1.1 and 1.2, we obtain with Lemma 1.3 that A is an asymptotic basis. We now assume that $h \geq 3k+3$. Then

$$4 \leq b_1 < b_2 < \cdots < b_k < d,$$

which implies $A \backslash F = D$. Therefore, $F \in I_k(A)$. By Lemma 1.3, it is sufficient to prove $g(A) \leq h$.

Let $m \geq 1$ and

$$0 \leq x_i < u \quad \text{for} \quad i = 1, 2, \ldots, k-1, \qquad 0 \leq x_k \leq u'.$$

Since

$$\begin{aligned} 2 + \sum_{i=1}^{k} x_i + u' &< 2 + (k-1)u + 2u' \\ &\leq 2 + (k-1) \cdot \frac{h}{k+1} + 2 \cdot \frac{2h}{3k+3} \end{aligned}$$

$$\begin{aligned} &= h - \left(\frac{2h}{3k+3} - 2\right) \\ &\leq h, \end{aligned}$$

we have that

$$md + \sum_{i=1}^{k} x_i b_i \in hA,$$

and

$$(m-1)d + \sum_{i=1}^{k} x_i b_i + b_1 + u' b_k \in hA.$$

Therefore, any integer x satisfying

$$md + \sum_{i=1}^{k} x_i b_i \leq x \leq md + \sum_{i=1}^{k} x_i b_i + h - \sum_{i=1}^{k} x_i$$

or

$$(m-1)d + \sum_{i=1}^{k} x_i b_i + b_1 + u' b_k \leq x \leq$$

$$\leq (m-1)d + \sum_{i=1}^{k} x_i b_i + b_1 + u' b_k + h - \sum_{i=1}^{k} x_i - 1 - u'$$

is contained in hA. Let $[a, b]$ denote the set of integers n satisfying $a \leq n \leq b$. It therefore follows from Lemma 1.1 that

$$\left[md + \sum_{i=1}^{k} x_i b_i,\ md + (x_1 + 1)b_1 + \sum_{i=2}^{k} x_i b_i\right] \subseteq hA.$$

The arbitrariness of $x_1 : 0 \leq x_1 \leq u - 1$ implies that

$$\left[md + \sum_{i=2}^{k} x_i b_i,\ md + ub_1 + \sum_{i=2}^{k} x_i b_i\right] \subseteq hA.$$

Using Lemma 1.2, we have that

$$md + \sum_{i=2}^{k} x_i b_i + ub_i + h - \sum_{i=2}^{k} x_i - u \geq md + (x_2 + 1)b_2 + \sum_{i=3}^{k} x_i b_i,$$

hence,

$$\left[md + \sum_{i=2}^{k} x_i b_i,\ md + (x_2+1)b_2 + \sum_{i=3}^{k} x_i b_i\right] \subseteq hA.$$

Again by the arbitrariness of $x_2 : 0 \leq x_2 \leq u-1$, we have that

$$\left[md + \sum_{i=2}^{k} x_i b_i,\ md + ub_2 + \sum_{i=3}^{k} x_i b_i\right] \subseteq hA.$$

Again using Lemma 1.2, we see

$$\left[md + \sum_{i=3}^{k} x_i b_i,\ md + (x_3+1)b_3 + \sum_{i=4}^{k} x_i b_i\right] \subseteq hA.$$

Continuing this procedure, we obtain that

$$[md,\ md + u'b_k] \subseteq hA.$$

Noticing that

$$\begin{aligned} b_1 - h + (k-1)u + u' &\leq \frac{2h}{k+1} - h + (k-1)\cdot\frac{h}{k+1} + \frac{2h}{3k+3} \\ &\leq \frac{2h}{3k+3} < h - u' - 1, \end{aligned}$$

we finaly obtain that $[md,\ (m+1)d] \subseteq hA$ for any $m > 1$. This means that $x \in hA$ for all $x \geq 2d$, i.e., $g(A) \leq h$. This completes the proof of Theorem 1.1.

Theorem 1.2 *For any given positive integer k,*

$$G_k(h) \geq (k+1)\left(\frac{k+1}{k+2}\right)^k \left(\frac{h}{k+1}\right)^{k+1} + O(h^k) \tag{1.5}$$

as h tends to infinity.

In order to prove this theorem, we need the following two lemmas.

Lemma 1.4 *Let $h \geq 2$ and $k \geq 1$ be integers. Let*

$$\begin{aligned} u &= \left[\frac{h}{k+2}\right], \\ b_1 &= (k+1)h - k(k+2)u + 2k + 1, \\ b_{i+1} &= ub_i + ih - i(k+1)u + 2i \quad \text{for } i = 1, 2, \ldots, k-1, \\ d &= ub_k + kh - k(k+1)u + 2k - 1. \end{aligned}$$

If $1 \leq x_i \leq u$ for $i = 1, 2, \ldots, k$, then

(i) $ub_k + h - \sum_{i=1}^{k} x_i - u \geq d + ub_{k-1} - b_k - 1$;

(ii) For any $1 \leq s \leq j-2$,

$$ub_{s+1} - b_{s+2} + h - \sum_{i=1}^{k} x_i - u + 1 \geq ub_s - b_{s+1} - 1.$$

Proof. It follows from the definition that

$$\begin{aligned} ub_k + h - \sum_{i=1}^{k} x_i - u &\geq ub_k + h - ku - u \\ &= ub_{k-1} - b_k + (k-1)h - (k-1)(k+1)u \\ &\qquad + 2(k-1) + ub_k + h - (k+1)u \\ &= ub_{k-1} - b_k + ub_k + kh - k(k+1)u + 2k - 2 \\ &= d + ub_{k-1} - b_k - 1, \end{aligned}$$

which proves (i).

From the definition, we see that

$$\begin{aligned} ub_{s+1} - b_{s+2} + h - \sum_{i=1}^{k} x_i - u + 1 & \\ \geq\ & ub_{s+1} - b_{s+2} + h - (k+1)u + 1 \\ =\ & -(s+1)h + (s+1)(k+1)u - 2(s+1) + h - (k+1)u + 1 \\ =\ & -sh + s(k+1)u - 2s - 1 \\ =\ & ub_s - b_{s+1} - 1, \end{aligned}$$

and this shows (ii).

Lemma 1.5 *Let $h, k, b_1, \dots, b_k$ be as in Lemma 1.4. If $h \geq (k+2)^3$, then*

$$ub_s + h - \sum_{i=s+1}^{k} x_i - u - s + 1 \geq b_{s+1}$$

holds for any $1 \leq x_i \leq u$ $(i = s+1, \dots, k)$ and $1 \leq s \leq k-1$.

Proof. Since $h \geq (k+2)^3$, we have that

$$\begin{aligned}
ub_s + h - \sum_{i=s+1}^{k} x_i - u - s + 1 &\geq ub_s + h - (k-s)u - u - s + 1 \\
&= b_{s+1} - (sh - s(k+1)u + 2s) + h - (k+1)u + su - s + 1 \\
&= b_{s+1} + (s-1)((k+2)u - h) + u - 3s + 1 \\
&\geq b_{s+1} + (s-1)\left((k+2)\left(\frac{h}{k+2} - 1\right) - h\right) + \frac{h}{k+2} - 3s \\
&= b_{s+1} + \frac{h}{k+2} - ((k+2)(s-1) + 3s) \\
&> b_{s+1} + \frac{h}{k+2} - (k+2)^2 \\
&\geq b_{s+1},
\end{aligned}$$

which proves the lemma.

Proof of Theorem 1.2. Let $h \geq (k+4)^3$. Let $u, b_1, \dots, b_k$ and d be as in Lemma 1.4. Then

$$1 < b_1 < b_2 < \cdots < b_k < d. \tag{1.6}$$

Let $D = \{md,\ md+1 \mid m = 0, 1, \dots\}$. Then D is a basis of order $d-1$. Since

$$b_1 = (k+1)h - k(k+2)u + 2k + 1 = h + O(1),$$

we see that

$$b_2 = ub_1 + h - (k+1)u + 2 = \frac{h^2}{k+2} + O(h).$$

Similarly,

$$\begin{aligned} b_k &= ub_{k-1} + kh - (k-1)(k+1)u + 2(k-1) \\ &= \frac{h^k}{(k+2)^{k-1}} + O(h^{k-1}). \end{aligned}$$

Therefore,

$$\begin{aligned} g(D) = d - 1 &= ub_k + kh - k(k+1)u + k \\ &= \frac{uh^k}{(k+2)^{k-1}} + O(h^k) \\ &= \frac{h^{k+1}}{(k+2)^k} + O(h^k) \\ &= (k+1)\left(\frac{k+1}{k+2}\right)^k \left(\frac{h}{k+1}\right)^{k+1} + O(h^k). \end{aligned}$$

Let $F = \{b_1, \ldots, b_k\}$, and define $A = D \cup F$. Then (1.6) implies that $A \backslash F = D$. Therefore, it is sufficient to prove that A is an asymptotic basis of order h.

Let m be a positive integer. Let $1 \le x_i \le u$ for $i = 1, 2, \ldots, k$. Since

$$u + \sum_{i=1}^{k} x_i \le (k+1)u < h,$$

we see that

$$md + \sum_{i=1}^{k} x_i b_i \in hA, \qquad md + \sum_{i=1}^{k} x_i b_i + ub_s \in hA \quad \text{for any } s. \tag{1.7}$$

Hence, we have that

$$\left[md + \sum_{i=1}^{k} x_i b_i,\ \ md + \sum_{i=1}^{k} x_i b_i + h - \sum_{i=1}^{k} x_i\right] \subseteq hA$$

and

$$\left[md + \sum_{i=1}^{k} x_i b_i + ub_s,\ \ md + \sum_{i=1}^{k} x_i b_i + ub_s + h - \sum_{i=1}^{k} x_i - u\right] \subseteq hA.$$

Since

$$\begin{aligned} d+h-\sum_{i=1}^{k} x_i+1 &\geq d+h-ku+1 \\ &= ub_k+kh-k(k+1)u+2k-1+h-ku+1 \\ &= ub_k+(k+1)h-k(k+2)u+2k+1-1 \\ &= ub_k+b_1-1, \end{aligned}$$

we see that

$$md+\sum_{i=1}^{k} x_ib_i-b_1+h-\sum_{i=1}^{k} x_i+1 \geq (m-1)d+\sum_{i=1}^{k} x_ib_i+ub_k-1.$$

Noticing (1.7), we have

$$\left[md+\sum_{i=1}^{k} x_ib_i-b_1,\ \ (m-1)d+\sum_{i=1}^{k} x_ib_i+ub_k\right] \subseteq hA.$$

It follows from the first inequality of Lemma 1.4 that

$$(m-1)d+\sum_{i=1}^{k} x_ib_i+ub_k+h-\sum_{i=1}^{k} x_i-u \geq md+\sum_{i=1}^{k} x_ib_i+ub_{k-1}-b_k-1,$$

which implies that

$$\left[(m-1)d+\sum_{i=1}^{k} x_ib_i+ub_k,\ \ md+\sum_{i=1}^{k} x_ib_i+ub_{k-1}-b_k\right] \subseteq hA.$$

Therefore,

$$\left[md+\sum_{i=1}^{k} x_ib_i-b_1,\ \ md+\sum_{i=1}^{k} x_ib_i+ub_{k-1}-b_k\right] \subseteq hA. \qquad (1.8)$$

Form (1.7) and the second inequality of Lemma 1.4, we see that

$$md+\sum_{i=1}^{k} x_ib_i+ub_{s+1}-b_{s+2}+h-\sum_{i=1}^{k} x_i-u+1 \geq md+\sum_{i=1}^{k} x_ib_i+ub_s-b_{s+1}-1$$

for $s=1,\ldots,k-2$. This implies that

$$\left[md+\sum_{i=1}^{k} x_ib_i+ub_{s+1}-b_{s+2},\ \ md+\sum_{i=1}^{k} x_ib_i+ub_s-b_{s+1}\right] \subseteq hA$$

for $s = 1, \ldots, k-2$. Therefore,

$$\left[md + \sum_{i=1}^{k} x_i b_i + ub_{k-1} - b_k, \quad md + \sum_{i=1}^{k} x_i b_i + ub_1 - b_2\right] \subseteq hA. \tag{1.9}$$

Since

$$ub_1 - b_2 + h - \sum_{i=1}^{k} x_i + 1 - u \geq ub_1 - b_2 + h - (k+1)u + 2 - 1 \geq -1,$$

we see that

$$md + \sum_{i=1}^{k} x_i b_i + ub_1 - b_2 + h - \sum_{i=1}^{k} x_i + 1 - u \geq md + \sum_{i=1}^{k} x_i b_i - 1,$$

which implies

$$\left[md + \sum_{i=1}^{k} x_i b_i + ub_1 - b_2, \quad md + \sum_{i=1}^{k} x_i b_i\right] \subseteq hA. \tag{1.10}$$

Therefore, by (1.8), (1.9) and (1.10), we obtain that

$$\left[md + \sum_{i=1}^{k} x_i b_i - b_1 \quad md + \sum_{i=1}^{k} x_i b_i\right] \subseteq hA.$$

Thus the arbitrariness of $x_1 : 1 \leq x_1 \leq u$ implies that

$$\left[md + \sum_{i=2}^{k} x_i b_i, \quad md + ub_1 + \sum_{i=2}^{k} x_i b_i\right] \subseteq hA. \tag{1.11}$$

It follows from Lemma 1.5 with $s = 1$ that

$$md + ub_1 + \sum_{i=2}^{k} x_i b_i + h - \sum_{i=2}^{k} x_i - u - 1 \geq md + (x_2 + 1)b_2 + \sum_{i=3}^{k} x_i b_i,$$

hence,

$$\left[md + ub_1 + \sum_{i=2}^{k} x_i b_i, \quad md + (x_2 + 1)b_2 + \sum_{i=3}^{k} x_i b_i\right] \subseteq hA.$$

It therefore follows from (1.11) that

$$\left[md + \sum_{i=2}^{k} x_i b_i, \quad md + (x_2 + 1)b_2 + \sum_{i=3}^{k} x_i b_i\right] \subseteq hA.$$

Again by the arbitrariness of $x_2 : 1 \leq x_2 \leq u$, we see that

$$\left[md + b_2 + \sum_{i=3}^{k} x_i b_i, \quad md + b_2 + ub_2 + \sum_{i=3}^{k} x_i b_i\right] \subseteq hA.$$

By Lemma 1.5 with $s = 2$, we have that

$$\begin{aligned} md + (u+1)b_2 + \sum_{i=3}^{k} x_i b_i + h - \sum_{i=3}^{k} x_i - u - 1 \\ \geq md + b_2 + (x_3 + 1)b_3 + \sum_{i=4}^{k} x_i b_i. \end{aligned}$$

Hence,

$$\left[md + b_2 + \sum_{i=3}^{k} x_i b_i, \quad md + b_2 + (x_3 + 1)b_3 + \sum_{i=4}^{k} x_i b_i\right] \subseteq hA.$$

By a similar argument, we obtain that

$$\left[md + \sum_{i=2}^{k} b_i, \quad md + \sum_{i=2}^{k} b_i + ub_k\right] \subseteq hA.$$

Observing that, for $h > (k+4)^3$,

$$\begin{aligned} ub_k + h - u - k &= d - kh + k(k+1)u - (2k-1) + h - u - k \\ &= d - (k-1)h + (k^2 + k - 1)u - 3k + 1 \\ &\geq d - (k-1)h + (k^2 + k - 1)\left(\frac{h}{k+2} - 1\right) - 3k + 1 \\ &= d + \frac{h}{k+2} - k(k+4) + 2 \\ &> d, \end{aligned}$$

we finally obtain that

$$\left[md + \sum_{i=2}^{k} b_i, \quad (m+1)d + \sum_{i=2}^{k} b_i\right] \subseteq hA$$

for all $m \geq 1$. Therefore, hA contains all integers $n \geq d + \sum_{i=1}^{k} b_i$, i.e., A is an asymptotic basis and $g(A) \leq h$. This completes the proof of Theorem 1.2.

Let $A_k = \{0 < a_1 = 1 < a_2 < \cdots < a_k\}$ be a set of $k+1$ integers. A_k is called an *h-basis* for n if every nonnegative integer $\leq n$ can be written as a sum of h elements of A_k, i.e., $hA_k \supseteq \{0, 1, \ldots, n\}$. Let $n(h, A_k)$ denote the largest n for which A_k is an h-basis for n. Define

$$n(h,k) = \max_{A_k} n(h, A_k).$$

This is the famous postage stamp problem. A_k represents the set of stamp face values available, and the evelope has room for at most h stamps. $n(h, A_k) + 1$ is the smallest postage that cannot stamp. For more about this problem, see Hofmeister [21,22] and Selmer [57]. Now we prove the following connection between $G_k(h)$ and $n(h,k)$.

Theorem 1.3 *$G_k(h) \geq n(h-1, k+1)$ for $h \geq 3$ and $k \geq 1$.*

Proof. Let $h \geq 3$ and $k \geq 1$. Suppose that

$$A_{k+1} = \{0 < a_1 = 1 < a_2 < \cdots < a_{k+1}\}$$

is such that $n(h-1, A_{k+1}) = n(h-1, k+1)$. Let

$$\begin{aligned} d &= n(h-1, k+1) + 1, \\ D &= \{md, md+1 \mid m = 0, 1, \ldots\}. \end{aligned}$$

Then D is an asymptotic basis of order $g(D) = d - 1 = n(h-1, k+1)$. Let $F = \{a_2, \ldots, a_{k+1}\}$. Let $A = D \cup F$. Then $A \backslash F = D$. We must show that A is an asymptotic basis of order h. Let n be any nonnegative integer. Suppose $n = md + n'$ with $0 \leq n' < d$. Since $n' \in (h-1)A_{k+1}$, we have

$$n' = a_{i_1} + a_{i_2} + \cdots + a_{i_r} + t,$$

where $a_{i_j} \in F$ and $r + t \leq h - 1$. Then

$$n = md + t + a_{i_1} + a_{i_2} + \cdots + a_{i_r} \in hA,$$

which implies that A is a basis of order h. This completes the proof of Theorem 1.3.

The best lower bound for $n(h,k)$ as h tends to infinity is due to Mrose [37], who showed that, for $k \geq 4$,

$$n(h,k) \geq \gamma_k \cdot 2^{[\frac{k}{4}]} \cdot \left(\frac{h}{k}\right)^k + O(h^{k-1}),$$

where $\gamma_k = 1, 1.024, 1.205$ or 1.388 according to $k \equiv 0, 1, 2$ or $3 \bmod 4$. Therefore, we have the following corollary.

Corollary 1.3.1 *For any $k \geq 4$, we have*

$$G_k(h) \geq \gamma_{k+1} \cdot 2^{[\frac{k+1}{4}]} \cdot \left(\frac{h}{k+1}\right)^{k+1} + O(h^k) \quad \text{as} \quad h \to \infty,$$

where γ_k is defined as above.

1.3 Estimate of $G_k(h)$ for Given h

As in the prevoius section, $[a,b]$ denotes the set of all integers n such that $a \leq n \leq b$.

Lemma 1.6 *Let $h \geq 2, k \geq h - 1$. Let $\eta = \left[\frac{k}{h-1}\right]$. Define $b_0 = 1$ and*

$$b_{i\eta+j} = b_{i\eta} + j \cdot \left(2 + \sum_{\mu=1}^{i} b_{\mu\eta}\right),$$

for $i = 0, 1, \ldots, h-2$ *and* $j = 1, 2, \ldots, \eta$. *Let* $m \geq 2$. *Let*

$$D = \{0, 1, md, md+1\}.$$

Then

$$\left[md + 2 + \sum_{\mu=1}^{i-1} b_{\mu\eta},\ \ md + 1 + \sum_{\mu=1}^{i} b_{\mu\eta}\right] \subseteq (i+1)(\{b_1, \ldots, b_{i\eta}\} \cup D) \quad (1.12)$$

for $i = 1, 2, \ldots, h-1$.

Proof. For any $1 \leq s \leq h-1$, let $A_s = \{b_1, \ldots, b_{s\eta}\} \cup D$. If $n \in [md+2,\ md+1+b_1]$, then $2 \leq n - md \leq b_1 + 1$. If $n - md$ is odd, then there exists a b_j $(1 \leq j \leq \eta)$ such that $b_j = n - md$, i.e., $a = md + b_j$. If $n - md$ is even then $n = (md+1)+1$ or there exists a b_j such that $n = (md+1) + b_j$. Hence $n \in 2A_1$. Now assume that (1.12) holds for any $i \leq s-1$. Then, for any $i \leq s-1$,

$$\left[md,\ \ md + 1 + \sum_{\mu=1}^{i} b_{\mu\eta}\right] \subseteq (i+1)A_i.$$

Let

$$n \in \left[md + 2 + \sum_{\mu=1}^{s-1} b_{\mu\eta},\ \ md + 1 + \sum_{\mu=1}^{s} b_{\mu\eta}\right].$$

If

$$md + 2 + \sum_{\mu=1}^{s-1} b_{\mu\eta} \leq n \leq md + b_{(s-1)\eta+1} - 1,$$

then

$$md + 2 + \sum_{\mu=1}^{s-2} b_{\mu\eta} \leq n - b_{(s-1)\eta} \leq md + 1 + \sum_{\mu=1}^{s-1} b_{\mu\eta}.$$

It follows that $n - b_{(s-1)\eta} \in sA_{s-1}$, which means $n \in (s+1)A_{s-1} \subseteq (s+1)A_s$. If there exists a $j:\ 1 \leq j \leq \eta - 1$ such that

$$md + b_{(s-1)\eta+j} \leq n \leq md + d_{(s-1)\eta+j+1} - 1,$$

then

$$md \leq n - b_{(s-1)\eta+j} \leq md + 1 + \sum_{\mu=1}^{s-1} b_{\mu\eta}.$$

It follows that $n \in (s+1)A_s$. If

$$md + b_{s\eta} \leq n \leq md + 1 + \sum_{\mu=1}^{s} b_{\mu\eta},$$

then $n - b_{s\eta} \in sA_{s-1}$, thus $n \in (s+1)A_s$. The proof is complete.

Let $A_1, \ldots, A_r$ be sets of integers. Define

$$\sum_{i=1}^{r} A_i = \{a_1 + \cdots + a_r \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, r\}.$$

Let B be a set of integers and let g be a positive integer. $B^{(g)}$ denotes the set of nonnegative integers congrruent to some element of B. By $A \approx B$ we mean that

$$A \cap \{n \geq M \mid n \in \mathbf{N}\} = B \cap \{n \geq M \mid n \in \mathbf{N}\}$$

for some M. $A(m)$ is the size of the set $\{a \in A \mid 0 < a \leq m\}$. The *lower density of* A is defined by

$$dA = \liminf_{m \to \infty} \frac{A(m)}{m}.$$

To give an upper bound for $G_k(h)$, we need the following Kneser's Theorem.

Theorem 1.4 (Kneser's Theorem) *Let $C = A_1 + \cdots + A_n$. Then either*

$$dC \geq \sum_{i=1}^{n} dA_i$$

or $C \approx C^{(g)}$ for some g.

The following is slight improvemnet of the upper bound for $G_k(h)$ by Nash [38].

Lemma 1.7 *Let $h \geq 2$. Then*

$$G_k(h) + 1 \leq \frac{2}{(h-1)!}k^{h-1} + \frac{h+1}{(h-2)!}k^{h-2} + O(k^{h-3}) \tag{1.13}$$

as k tends to infinity.

Proof. Let A be an asymptotic basis of order h. Let $F \in I_k(A)$. Let $B = A \backslash F$. Then

$$hB \cup (F + (h-1)B) \cup \cdots \cup ((h-1)F + B) \cup hF \approx \mathbf{N}. \tag{1.14}$$

Hence $dhB > 0$ and

$$dhB + kd(h-1)B + \binom{k+1}{2} d(h-2)B + \cdots + \binom{k+h-2}{h-1} dB \geq 1.$$

Let $k \geq \max\{h-1, 2\}$. Then we have that $\binom{k+h-1}{h-1} - 1 \geq h$. Therefore,

$$d\left(\binom{k+h-1}{k} - 1\right) B + dhB + kd(h-1)B$$
$$+ \binom{k+1}{2} d(h-1)B + \cdots + \binom{k+h-2}{h-1} dB > 1.$$

It follows from Kneser's Theorem that we have a g such that

$$\left(\binom{k+h-1}{k} - 1 + \sum_{i=0}^{h-1} \binom{k+i-1}{i} (h-i)\right) B$$
$$\approx \left(\binom{k+h-1}{k} - 1 + \sum_{i=0}^{h-1} \binom{k+i-1}{i} (h-i)\right) B^{(g)}.$$

Take the smallest g for which this last relation holds. We show that $g = 1$.

It follows from (1.14) that

$$hB^{(g)}(g) + k((h-1)B^{(g)}(g)) + \cdots + \binom{k+h-2}{h-1} (B^{(g)}(g)) \geq g.$$

Using Kneser's Theorem, we have that

$$\left(\sum_{i=0}^{h-1} \binom{k+i-1}{i} (h-i)\right) B^{(g)}(g) \geq g - \binom{h+k-1}{k} + 1.$$

It is clear that if $nB^{(g)}(g) < g$, then

$$(n+1)B^{(g)}(g) > nB^{(g)}(g).$$

Therefore,

$$\left(\binom{h+k-1}{k} - 1 + \sum_{i=0}^{h-1} \binom{k+i-1}{i}(h-i)\right) B^{(g)}(g) = g.$$

This implies that $g = 1$. Therefore,

$$\begin{aligned} G_k(h)+1 &\leq \binom{h+k-1}{k} - 1 + \sum_{i=0}^{h-1} \binom{k+i-1}{i}(h-i) \\ &= \frac{2}{(h-1)!}k^{h-1} + \frac{h+1}{(h-2)!}k^{h-2} + O(k^{h-3}) \end{aligned}$$

as k tends to infinity. This completes the proof.

Theorem 1.5 *Let $h \geq 2$. Then*

$$\begin{aligned} G_k(h)+1 &\geq 2\left(\frac{k}{h-1}\right)^{h-1} + (4h-5)\left(\frac{k}{h-1}\right)^{h-2} + O(k^{h-3}), \\ G_k(h)+1 &\leq \frac{2}{(h-1)!}k^{h-1} + \frac{h-1}{(h-2)!}k^{h-2} + O(k^{h-3}) \end{aligned}$$

as k tends to infinity. In particular, $G_k(2) = 2k+2$ holds for any positive integer k.

Proof. The second inequality has already been established in Lemma 1.7. We now prove the first one.

Suppose $k \geq h-1$. Let $\eta, b_0, \ldots, b_{(h-1)\eta}$ be as in Lemma 1.6. Define

$$b_{(h-1)\eta+j} = b_{(h-1)\eta} + j\left(2 + \sum_{\mu=1}^{h-2} b_{\mu\eta}\right)$$

for $j = 1, 2, \ldots, k-(h-1)\eta$, and define

$$d = b_k + 2 + \sum_{\mu=1}^{h-2} b_{\mu\eta}.$$

Let

$$\begin{aligned} F &= \{b_1, \ldots, b_k\}, \\ A &= F \cup \{a \in \mathbf{N} \mid a \equiv 0 \text{ or } 1 \bmod d\}. \end{aligned}$$

It is clear that both A and $A\backslash F$ are asymptotic bases.

We prove that A is of order h. Let $m \geq 0$ be any integer. It follows from Lemma 1.6 that

$$\left[md + 2 + \sum_{\mu=1}^{s-1} b_{\eta\mu},\ \ md + 1 + \sum_{\mu=1}^{s} b_{\mu\eta}\right] \subseteq (s+1)A$$

for $s = 1, 2, \ldots, h-1$, which implies that

$$\left[md,\ \ md + 1 + \sum_{\mu=1}^{h-1} b_{\mu\eta}\right] \subseteq hA.$$

Let

$$n \in \left[md + 2 + \sum_{\mu=1}^{h-1} b_{\mu\eta},\ \ md + d - 1\right].$$

Suppose

$$md + b_{(h-1)\eta} + t\left(2 + \sum_{\mu=1}^{h-2} b_{\mu\eta}\right) \leq n <$$

$$< md + b_{(h-1)\eta} + (t+1)\left(2 + \sum_{\mu=1}^{h-2} b_{\mu\eta}\right)$$

for some t. Then

$$n - b_{(h-1)\eta+t} = n - \left(b_{(h-1)\eta} + t\left(2 + \sum_{\mu=1}^{h-2} b_{\mu\eta}\right)\right)$$

is contained in $\left[md,\ md + 1 + \sum_{\mu=1}^{h-2} b_{\mu\eta}\right]$, hence in $(h-1)A$. Hence $n \in hA$. Therefore, $[md,\ (m+1)d - 1] \subseteq hA$. This implies $g(A) \leq h$.

Since $A\backslash F = \{a \in \mathbf{N} \mid a \equiv 0 \text{ or } 1 \bmod d\}$, it follows that $g(A\backslash F) = d-1$. Hence $G_k(h) + 1 \geq d$. From the definition, a simple calculation shows that

$$b_{\mu\eta} = \eta b_{(\mu-1)\eta} + (b_{(\mu-1)\eta} + \eta b_{(\mu-2)\eta}) + O(\eta^{\mu-2})$$

holds for $\mu = 2, 3, \ldots, h-1$. This implies that

$$b_{(h-1)\eta} = 2\eta^{h-1} + (4h-7)\eta^{h-2} + O(\eta^{h-3}).$$

Therefore,

$$\begin{aligned}
G_k(h)+1 &\geq d = b_k + 2 + \sum_{\mu=1}^{h-2} b_{\mu\eta} \\
&= b_{(h-1)\eta} + (k-(h-1)\eta)\Big(2+\sum_{\mu=1}^{h-2} b_{\mu\eta}\Big) + 2 + \sum_{\mu=1}^{h-2} b_{\mu\eta} \\
&= 2\eta^{h-1} + (4h-7)\eta^{h-2} + b_{(h-2)\eta} + 2 + \sum_{\mu=1}^{h-3} b_{\mu\eta} \\
&\quad + (k-(h-1)\eta)\Big(2+\sum_{\mu=1}^{h-2} b_{\mu\eta}\Big) + O(\eta^{h-3}) \\
&\geq 2\eta^{h-1} + (4h-5)\eta^{h-2} + 2\eta^{h-2}(k-(h-1)\eta) + O(\eta^{h-3}) \\
&\geq 2\Big(\frac{k}{h-1}\Big)^{h-1} + (4h-5)\Big(\frac{k}{h-1}\Big)^{h-2} \\
&\quad - 2(h-1)\Big(\frac{k}{h-1}-1\Big)\Big(\frac{k}{h-1}\Big)^{h-2} \\
&\quad + 2(k-(h-1)\eta)\Big(\frac{k}{h-1}\Big)^{h-2} + O(k^{h-3}) \\
&= 2\Big(\frac{k}{h-1}\Big)^{h-1} + (4h-5)\Big(\frac{k}{h-1}\Big)^{h-2} + O(k^{h-3}).
\end{aligned}$$

This proves the first inequality.

From Lemma 1.7 and the argument above, we see that the lower bound and the upper bound are polynomials of k with integral coefficients. Hence when $h=2$, the remainders $O(k^{h-3})$ in the inequalities are zero. Therefore, $G_k(2) = 2k+2$. It is readily seen that this holds for any $k \geq 2$, hence for any $k \geq 1$ since $G_1(2) = 4$. The proof is complete.

Theorem 1.6 *$G_k(h) \geq 2n(h-1,k) + h$ for $h \geq 2$ and $k \geq 1$.*

Proof. Let $h \geq 2, k \geq 1$. Suppose that

$$A_k = \{0 < a_1 = 1 < a_2 < \cdots < a_k\}$$

is such that $n(h-1, A_k) = n(h-1,k)$. Let

$$d = 2n(h,k) + h + 1,$$

$$D = \{md, md+1 \mid m = 0, 1, \dots\}.$$

Then D is a basis of order

$$g(D) = d - 1 = 2n(h,k) + h.$$

Let

$$\begin{aligned} b_0 &= 1, \\ b_i &= 2a_i + 1 \quad \text{for} \quad i = 1, 2, \dots, k, \\ F &= \{b_1, b_2, \dots, b_k\}. \end{aligned}$$

It is clear that $F \cap D = \emptyset$. Let $A = D \cup F$. To prove the theorem, it is sufficient to prove that A is an asymptotic basis of order h. Let n be a positive integer. I shall show that $n \in hA$. Since $md, md+1 \in hA$, we may assume without loss of generality that $n = md + n'$ where $1 < n' < d$. We must consider the following two cases which may occur.

If $n' - h + 1 = 2s$ is even, then

$$0 \le s \le \left[\frac{d-1-h+1}{2}\right] = n(h-1,k).$$

Hence, $s = a_{i_1} + \cdots + a_{i_{h-1}}$, where $a_{i_j} \in A_k$. Therefore,

$$\begin{aligned} n = md + n' &= md + 2s + h - 1 \\ &= md + (2a_{i_1} + 1) + \cdots + (2a_{i_{h-1}} + 1) \\ &= md + b_{i_1} + \cdots + b_{i_{h-1}}, \end{aligned}$$

which implies that $n \in hA$.

If $n' - h + 1 = 2s + 1$ is odd, then

$$1 \le s \le \frac{d-h-1}{2} = n(h-1,k).$$

Hence $s = a_{i_1} + \cdots + a_{i_{h-1}}$, where $a_{i_j} \in A_k$. Therefore,

$$\begin{aligned} n = md + n' &= md + 2s + 1 + h - 1 \\ &= (md+1) + (2a_{i_1} + 1) + \cdots + (2a_{i_{h-1}} + 1) \\ &= (md+1) + b_{i_1} + \cdots + b_{i_{h-1}}, \end{aligned}$$

which implies that $n \in hA$.

Therefore A is a basis of order h, which completes the proof of the theorem.

The best lower bound for $n(2,k)$ was given by Mrose [37], who proved that

$$n(2,k) > \frac{2}{7}k^2 + O(k).$$

For $h = 3$, Windecker [59] has proved that

$$n(3,k) > \frac{4}{3}\left(\frac{k}{3}\right)^3$$

for all k. Therefore, we have the following corollaries.

Corollary 1.6.1 $G_k(3) \geq \frac{4}{7}k^2 + O(k)$.

Corollary 1.6.2 $G_k(4) \geq \frac{8}{81}k^3 + 4$.

2 MINIMAL ASYMPTOTIC BASES

2.1 Introduction

A basis A of order h is called *minimal* if no proper subset of A is a basis of order h. Similarly, an asymptotic basis A of order h is called *minimal* if no proper subset of A is an asymptotic basis of order h. This concept of minimality of bases was first introduced by Stöhr [58]. Härtter [20] showed the existence of minimal asymptotic bases by a nonconstructive argument. Nathanson [40] constructed the first nontrivial example of minimal asymptotic bases of order $h \geq 2$. Nathanson and I [33] discovered a simple construction of minimal asymptotic bases of any order h by using powers of 2. Furthermore, for any $1/h \leq \alpha < 1$, we can construct a minimal asymptotic basis A of order h such that

$$x^{\alpha} \ll A(x) \ll x^{\alpha}.$$

I shall present the proof of these results in Section 2.2, and generalize these results to g-adic representations of integers in Section 2.3.

There are generalizations of bases and asymptotic bases for integers. One interesting case is to replace the set of integers by the collection of all finite subsets of integers, and the operation of addition by the set-theoretic union of sets. Deza and Erdös [4] proved analogues of the Erdös–Landau Theorem and Schnirelmann's Theorem. Nathanson [41] and Grekos [16,17] studied minimal union bases and maximal union nonbases. Nathanson [45]

also studied multiplicative bases for integers. In Section 2.4, I shall define analogue concepts for commutative monoids, and prove some existence theorems for minimal bases for commutative monoids.

2.2 A Simple Construction of Minimal Asymptotic Bases

Let W be a subset of $\mathbf{N}$. Denote by $\mathcal{F}(W)$ the set of all finite, nonempty subsets of W. Let

$$A(W) = \left\{ \sum_{f \in F} 2^f \;\middle|\; F \in \mathcal{F}(W) \right\}.$$

Note that $\emptyset \notin \mathcal{F}(W)$, hence $0 \notin A(W)$. Let π be a partition of the set $\mathbf{N}$ of integers into h pairwise disjoint subsets $W_0, \ldots, W_{h-1}$. It is clear that $A(W_0), A(W_1), \ldots, A(W_{h-1})$ are disjoint. Define

$$A(\pi) = A(W_0) \cup \cdots \cup A(W_{h-1}).$$

For any real number x, let $[x]$ denote the greatest integer n such that $n \leq x$, and $\lceil x \rceil$ the least integer n such that $n \geq x$. Let $A(x)$ denote the counting function of A.

Theorem 2.1 *Let $h \geq 2$, and let*

$$t = \left\lceil \frac{\log(h+1)}{\log 2} \right\rceil.$$

Let π be a partition of $\mathbf{N}$ into h pairwise disjoint subsets $W_0, \ldots, W_{h-1}$ such that each set W_r contains infinitely many intervals of t consecutive integers. Then

$$A(\pi) = A(W_0) \cup \cdots \cup A(W_{h-1}).$$

is a minimal asymptotic basis of order h.

The proof uses the following two lemmas of Nathanson [48].

Lemma 2.1 (Nathanson) *(i) If W is a subset of $\mathbf{N}$ such that $W(x) = \alpha x + O(1)$ for some $\alpha \in (0,1]$, then there exist two constants c_1 and c_2 such that*

$$c_1 x^\alpha < A(W)(x) < c_2 x^\alpha$$

for all x sufficiently large.

(ii) Let π be a partition of $\mathbf{N}$ into h pairwise disjoint nonempty subsets $W_0, \ldots, W_{h-1}$. Then $A(\pi)$ is an asymptotic basis of order h. Indeed,

$$hA = \{n \in \mathbf{N} \mid n \geq h\}.$$

Lemma 2.2 (Nathanson) *Let $w_1, \ldots, w_s$ be s distinct nonnegative integers. If*

$$\sum_{i=1}^{s} 2^{w_i} = \sum_{j=1}^{t} 2^{x_j},$$

where $x_1, \ldots, x_t$ are nonnegative integers that are not necessarily distinct, then there is a partition of $\{1, 2, \ldots, t\}$ into s nonempty sets $J_1, \ldots, J_s$ such that

$$2^{w_i} = \sum_{j \in J_i} 2^{x_j}$$

for $i = 1, 2, \ldots, s$.

Proof of Theorem 2.1. By Lemma 2.1, the set A is an asymptotic basis of order h. We must show that A is minimal.

Let $a \in A$. Then $a \in A(W_r)$ for some r. Without loss of generality, we may assume that $a \in A(W_0)$. Then there is a finite, nonempty subset F of W_0 such that

$$a = \sum_{i \in F} 2^i.$$

Let M denote the largest element of F.

Let $a_0 = a$. We shall construct positive integers a_r for $r = 1, 2, \ldots, h-1$. Choose $m_r \in W_r$ such that $m_r > M$ and the t consecutive integers $m_r, m_r + 1, \ldots, m_r + t - 1$ belong to W_r. Let F_r be any subset of $(M, m_r) \cap W_r$. Define a_r by

$$a_r = \sum_{\substack{i < M \\ i \in W_r}} 2^i + \sum_{i \in F_r} 2^i + \sum_{i=m_r}^{m_r+t-1} 2^i. \tag{2.1}$$

Then $a_r \in A(W_r)$ and

$$2^{m_r} \leq a_r < 2^{m_r+t}.$$

Let $n = a_0 + \cdots + a_{h-1}$. We shall show that this is the unique representation of n as a sum of h elements of A.

Suppose $n = b_0 + \cdots + b_{h-1}$, where $b_r \in A$ for $r = 0, \ldots, h-1$. Then $b_r \in A(W_{k_r})$ for some $k_r \in [0, h-1]$. Suppose that there exists $s \in \{1, 2, \ldots, h-1\}$ such that $b_r \notin A(W_s)$ for $r = 0, 1, \ldots, h-1$. By Lemma 2.2 there are subsets U_r of W_{k_r} such that

$$\sum_{i=m_s}^{m_s+t-1} 2^i = \sum_{r=0}^{h-1} \sum_{i \in U_r} 2^i.$$

Clearly, each i in U_r is less than m_s. It follows from the definition of t that

$$\begin{aligned} 2^{m_s}(2^t - 1) &= \sum_{i=m_s}^{m_s+t-1} 2^i \\ &= \sum_{r=0}^{h-1} \sum_{\substack{i < m_s \\ i \in U_r}} 2^i \\ &\leq h \cdot \sum_{i=0}^{m_s-1} 2^i \\ &< h \cdot 2^{m_s} \\ &\leq 2^{m_s}(2^t - 1), \end{aligned}$$

which is impossible. Therefore, after suitable renumbering, $b_r \in A(W_r)$ for $r = 1, 2, \ldots, h-1$.

Next we show that $b_0 \in A(W_0)$. Suppose $b_0 \notin A(W_0)$. We may assume without loss of generality that $b_0 \in A(W_1)$. Since $b_r \in A(W_r)$, it follows from Lemma 2.2 that there exist subsets V_0 of W_1 and V_r of W_r for $r = 1, 2, \ldots, h-1$ such that

$$\sum_{r=0}^{h-1} \sum_{i \in V_r} 2^i = a_0 + \sum_{r=1}^{h-1} \sum_{\substack{i<M \\ i \in W_r}} 2^i. \tag{2.2}$$

Since $i < M$ for all $i \in \bigcup_{r=0}^{h-1} V_r$, it follows that

$$\begin{aligned} \sum_{r=0}^{h-1} \sum_{i \in V_r} 2^i &= \sum_{i \in V_0} 2^i + \sum_{r=1}^{h-1} \sum_{i \in V_r} 2^i \\ &\leq \sum_{i \in V_0} 2^i + \sum_{r=1}^{h-1} \sum_{\substack{i<M \\ i \in W_r}} 2^i \\ &< 2^M + \sum_{r=1}^{h-1} \sum_{\substack{i<M \\ i \in W_r}} 2^i \\ &\leq a_0 + \sum_{r=1}^{h-1} \sum_{\substack{i<M \\ i \in W_r}} 2^i, \end{aligned}$$

which contradicts (2.2). Hence, $b_0 \in A(W_0)$. Since the representation of an integer as a sum of distinct powers of 2 is unique, it follows that $a_r = b_r$ for $r = 0, 1, \ldots, h-1$. In particular, $b_0 = a$. This completes the proof.

Corollary 2.1.1 *Let π be a partition of $\mathbf{N}$ into two disjoint subsets W_0 and W_1 such that each W_i contains infinitely many pairs of consecutive integers. Then*

$$A(\pi) = A(W_0) \cup A(W_1)$$

is a minimal asymptotic basis of order 2.

Corollary 2.1.2 *Let π be a partition of $\mathbf{N}$ into three disjoint subsets W_0, W_1, and W_2 such that each W_i contains infinitely many pairs of consecutive integers. Then*

$$A(\pi) = A(W_0) \cup A(W_1) \cup A(W_2)$$

is a minimal asymptotic basis of order 3.

These two corollaries are immediate consequences of Theorem 2.1 with $t = 2$.

Lemma 2.3 *Let $t \geq 2$ and $h \geq 2$. Let $\alpha_0, \ldots, \alpha_{h-1}$ be positive real numbers such that*

$$\alpha_0 + \cdots + \alpha_{h-1} = 1.$$

Then there exists a partition π of $\mathbf{N}$ into h pairwise disjoint subsets W_0, $W_1, \cdots, W_{h-1}$ such that, for $r = 0, 1, \ldots, h-1$,

(i) $W_r(x) = \alpha_r x + O(1)$;

(ii) *W_r contains infinitely many intervals of t consecutive integers;*

(iii) *In W_r, the gaps between successive intervals of length t are bounded.*

Proof. For any integer $n \geq 1$, define $a_r(n)$ and R_n by

$$a_r(n) = [n\alpha_r] \quad \text{for} \quad r = 0, 1, \ldots, h-1,$$

and

$$R_n = \sum_{r=0}^{h-1} a_r(n).$$

Let $\{R_{n(k)}\}_{k=1}^{\infty}$ be the maximal strictly increasing subsequence of $\{R_n\}_{n=1}^{\infty}$. It follows from $\sum_{r=0}^{h-1} \alpha_r = 1$, and the definition of R_n that

$$n(k) < n(k+1) \leq n(k) + h, \tag{2.3}$$

$$R_{n(k)} < R_{n(k+1)} \leq R_{n(k)} + h, \tag{2.4}$$

$$R_{n(k)} \leq n(k) < R_{n(k)} + h, \tag{2.5}$$

$$d_r(k) = a_r(n(k+1)) - a_r(n(k)) = 0 \text{ or } 1.$$

Let $R_{n(k+1)} - R_{n(k)} = u$. Then there are u distinct integers $r_i \in \{0, \ldots, h-1\}$ such that

$$d_{r_1}(k) = \cdots = d_{r_u}(k) = 1.$$

The remaining $h - u$ integers $r_i \in \{0, 1, \ldots, h-1\}$ satisfy

$$d_{r_{u+1}}(k) = \cdots = d_{r_h}(k) = 0.$$

Let $t \geq 2$. Define

$$W_{r_i,k} = [(R_{n(k)} + i - 1)t,\ (R_{n(k)} + i)t - 1]$$

for $i = 1, \ldots, u$; and define

$$W_{r_i,k} = \emptyset \text{ for } i = u+1, \ldots, h.$$

For each $r = 0, 1, \ldots, h-1$, we define

$$W_r = \bigcup_{k=1}^{\infty} W_{r,k}. \tag{2.6}$$

It is clear that $\mathbf{N} = W_0 \cup \cdots \cup W_{h-1}$, that $W_i \cap W_j = \emptyset$ for $i \neq j$, and that each W_r contains infinitely many intervals of length t. It follows from $\alpha_r > 0$ that (iii) holds.

Let $x \geq 1$. Suppose that

$$tR_{n(k)} \leq x < tR_{n(k+1)}.$$

Then, by (2.4) and (2.5), we have

$$\begin{aligned} |x - tn(k)| &< th, \\ |x - tn(k+1)| &< 2th. \end{aligned}$$

Therefore, for each $r = 0, 1, \ldots, h-1$,

$$W_r(x) \leq \alpha_r(n(k+1))t$$

$$\begin{aligned} &= [n(k+1)\alpha_r]t \\ &\leq tn(k+1)\alpha_r \\ &< \alpha_r x + 2th\alpha_r, \\ W_r(x) &\geq a_r(n(k))t \\ &= [n(k)\alpha_r]t \\ &> tn(k)\alpha_r - t \\ &> \alpha_r x - th\alpha_r - t, \end{aligned}$$

and so

$$W_r(x) = \alpha_r x + O(1).$$

This completes the proof of Lemma 2.3.

Theorem 2.2 *For every α such that $\frac{1}{h} \leq \alpha < 1$, there is a minimal asymptotic basis A of order h such that*

$$c_1 x^\alpha < A(x) < c_2 x^\alpha \tag{2.7}$$

for all sufficiently large x.

Proof. Let $\alpha_0 = \alpha$, and define $\alpha_r = \frac{1-\alpha}{h-1}$ for $r = 1, 2, \ldots, h-1$. Then $\alpha_0 + \cdots + \alpha_{h-1} = 1$ and $\alpha_0 \geq \alpha_r > 0$ for $r = 1, 2, \ldots, h-1$. Let

$$t = \left\lceil \frac{\log(h+1)}{\log 2} \right\rceil.$$

By Lemma 2.3, there is a partition π of $\mathbf{N}$ into h pairwise disjoint subsets $W_0, \ldots, W_{h-1}$ such that each subset W_r contains infinitely many intervals of length t, and

$$W_r(x) = \alpha_r x + O(1).$$

Theorem 2.1 implies that $A(\pi)$ is a minimal asymptotic basis of order h, and Lemma 2.1 implies that (2.7) holds for all sufficiently large x. This completes the proof.

Theorem 2.3 *Let $h \geq 2$ and let $t = \left\lceil \dfrac{\log(h+1)}{\log 2} \right\rceil$. Let $\alpha_0, \ldots, \alpha_{h-1}$ be positive real numbers such that $\alpha_0 + \cdots + \alpha_{h-1} = 1$. Let π be a partition of $\mathbf{N}$ into h pairwise disjoint subsets $W_0, \ldots, W_{h-1}$ satisfying conditions (i), (ii), and (iii) of Lemma 2.3. Let $A = A(\pi)$ and $a \in A$. Define $E_a = hA \backslash h(A \backslash \{a\})$. If $a \in A(W_r)$ and $\alpha = \alpha_r$, then*

$$E_a(x) \gg x^{1-\alpha}.$$

Proof. Condition (iii) implies that there is an integer L such that in every interval $(y - L, y - 1]$ there are t consecutive integers belonging to W_r for each $r = 0, 1, \ldots, h-1$.

Let $a \in A$. Without loss of generality we can assume that $a \in A(W_0)$. We must show that

$$E_a(x) \gg x^{1-\alpha_0}.$$

Let 2^M be the largest power of 2 that appears in the binary representation of a. Let x be a large positive number, and let $y = \dfrac{\log x}{\log 2}$. Then the interval $(y - L, y - 1]$ contains integers $m_1, \ldots, m_{h-1}$ such that

$$m_r + j \in (y - L, y - 1] \cap W_r$$

for $r = 1, 2, \ldots, h-1$, and $j = 0, \ldots, t-1$. Let F_r be a subset of $(M, y - L] \cap W_r$. Define a_r by (2.1). Let $n = a + a_1 + \cdots + a_{h-1}$. Then $n < 2^y = x$. The proof of Theorem 2.1 shows that $n \in hA \backslash h(A \backslash \{a\}) = E_a$, and that different choices of the $h - 1$ sets $F_1, \ldots, F_{h-1}$ lead to different numbers n. Since there are $2^{W_r(y-L) - W_r(M)}$ choices of the set F_r, it follows that the number of n determined by $F_1, \ldots, F_{h-1}$ is

$$\prod_{r=1}^{h-1} 2^{W_r(y-L) - W_r(M)}.$$

Noticing that

$$\log_2\left(\prod_{r=1}^{h-1} 2^{W_r(y-L) - W_r(M)}\right) \geq -M + W_1(y - L) + \cdots + W_{h-1}(y - L)$$

$$\begin{aligned} &= -M + \sum_{i=1}^{h-1}(\alpha_i y + O(1)) \\ &= y(\alpha_1 + \cdots + \alpha_{h-1}) + O(1) \\ &= y(1-\alpha_0) + O(1) \\ &= (1-\alpha_0)\log_2 x + O(1), \end{aligned}$$

we see that

$$\prod_{r=1}^{h-1} 2^{W_r(y-L)-W_r(M)} \gg x^{1-\alpha_0}.$$

Therefore, $E_a(x) \gg x^{1-\alpha_0}$. This completes the proof.

An asymptotic basis A of order h is called *strongly minimal* if $E_a(x) \gg (A(x))^{h-1}$ for each $a \in A$ and for all x sufficiently large.

Corollary 2.3.1 *Let A satisfy the conditions of Theorem 2.3. If $\alpha_r = \frac{1}{h}$ for $r = 0, 1, \ldots, h-1$, then A is a strongly minimal asymptotic basis of order h.*

Proof. Since $A(x) \ll x^{1/h}$, this follows immediately from Theorem 2.3.

2.3 Minimal Bases and g-adic Representations of Integers

In this section, I shall use g-adic representations of integers to construct minimal asymptotic bases. This generalizes the method used in Section 2.2. As always, $\mathbf{N}$ denotes the set of all nonnegative integers, and $\mathbf{Z}$ denotes the set of integers. Let W be a subset of $\mathbf{N}$. In this section, denote by $\mathcal{F}(W)$ the set of all finite nonempty subsets of W. Let $g \geq 2$ be an integer. Let

$$A_g(W) = \left\{ \sum_{f \in F} c_f g^f \;\middle|\; c_f \in \mathbf{N}, 1 \leq c_f < g; F \in \mathcal{F}(W) \right\}.$$

Let π be a partition of $\mathbf{N}$ into h pairwise disjoint subsets $W_0, \ldots, W_{h-1}$. Define

$$A_g(\pi) = A_g(W_0) \cup A_g(W_1) \cup \cdots \cup A_g(W_{h-1}).$$

Lemma 2.4 *Let π be any partition of $\mathbf{N}$ into h pairwise disjoint subsets $W_0, \ldots, W_{h-1}$ such that each $W_r \neq \emptyset$. Then $A_g(\pi)$ is an asymptotic basis of order h.*

Proof. Let n be an integer $\geq h$. I am going to prove that $n \in hA_g(\pi)$. Suppose

$$n = \sum_{f \in F} c_f g^f,$$

where $F \in \mathcal{F}(\mathbf{N})$, and $1 \leq c_f \leq g-1$ for all $f \in F$. If

$$\sum_{f \in F} c_f \geq h,$$

then it is clear from the definition of $A_g(\pi)$ that n may be written as a sum of h elements of $A_g(\pi)$, i.e., $n \in hA_g(\pi)$. Now assume that

$$1 \leq \sum_{f \in F} c_f < h.$$

Without loss of generality, we may write

$$n = \sum_{i=1}^{s} g^{f_i},$$

where $f_i \in F$ and the f_i are not necessarily distinct. Since $n \geq h$, there exists at least one $f_{i'} \geq 1$, thus

$$n = \sum_{i=1}^{s} g^{f_i} = \sum_{i \neq i'} g^{f_i} + d_1 g^{f_{i'}-1} + \cdots + d_t g^{f_{i'}-1} \in (s+t)A_g(\pi),$$

where $1 \leq d_j < g$ and $d_1 + \cdots + d_t = g$. Noticing $n \geq h$, we can continue in this way to divide powers of g until n is a sum of exactly h powers of g with positive integral coefficients $< g$. This means that $n \in hA_g(\pi)$, and the proof is complete.

Lemma 2.5 *Suppose $f_1 < f_2 < \cdots < f_s$ are nonnegative integers. If*

$$\sum_{i=1}^{s} c_i g^{f_i} = \sum_{j=1}^{t} d_j g^{h_j}, \tag{2.8}$$

where $1 \le c_i < g$, $1 \le d_j < g$ and the h_j's are nonnegative integers, then for any $u : 1 \le u \le s$,

$$\sum_{i=1}^{u} c_i g^{f_i} \le \sum_{h_j \le f_u} d_j g^{h_j} \tag{2.9}$$

Proof. If (2.9) is not true, then, for some $u < s$,

$$\sum_{i=1}^{u} c_i g^{f_i} - \sum_{h_j \le f_u} d_j g^{h_j} > 0.$$

By (2.8), we have

$$\begin{aligned} \sum_{h_j > f_u} d_j g^{h_j} &= \sum_{i=1}^{s} c_i g^{f_i} - \sum_{h_j \le f_u} d_j g^{h_j} \\ &= \sum_{i=u+1}^{s} c_i g^{f_i} + \Big(\sum_{i=1}^{u} c_i g^{f_i} - \sum_{h_j \le f_u} d_j g^{h_j} \Big). \end{aligned}$$

Since g^{f_u+1} divides the left hand side term and the first term on the right hand side, we see that g^{f_u+1} must divide the second term on the right hand side. On the other hand,

$$\begin{aligned} 0 &< \sum_{i=1}^{u} c_1 g^{f_i} - \sum_{h_j \le f_u} d_j g^{h_j} \\ &\le \sum_{i=1}^{u} c_i g^{f_i} \\ &\le \sum_{k=0}^{f_u} (g-1) g^k \\ &< g^{f_u+1}, \end{aligned}$$

which contradicts the divisibility by g^{f_u+1}. This completes the proof.

Lemma 2.6 *Let W be a set of nonnegative integers. If*

$$W(x) = \alpha x + O(1) \quad \textit{for some} \quad 0 < \alpha \leq 1,$$

then there exist positive constants c and c' such that

$$cx^{\alpha} < A_g(W)(x) < c'x^{\alpha}$$

for all x sufficiently large.

Proof. Let $x \geq 1$. Choose $k \geq 0$ so that

$$g^k \leq x < g^{k+1}.$$

Let $n \in A_g(W)$ and $n \leq x$. Assume

$$n = \sum_{f \in F} c_f g^f, \quad 1 \leq c_f < g, \quad F \in \mathcal{F}(W).$$

Then $g^f \leq n < x$ for all $f \in F$, thus $0 \leq f \leq k$. This means that F is a subset of $\{0, 1, \ldots, k\} \cap W$. Since the cardinality of $\{0, 1, \ldots, k\} \cap W$ is $W(k) + 1$, it follows that there are $\binom{W(k)+1}{j}$ different j-element subsets of $\{0, 1, \ldots, k\} \cap W$, which may produce at most

$$\binom{W(k)+1}{j}(g-1)^j$$

different numbers in $A_g(W)$. Therefore,

$$\begin{aligned} A_g(W)(x) &\leq \sum_{j=1}^{W(k)+1} \binom{W(k)+1}{j}(g-1)^j \\ &= (1 + (g-1))^{W(k)+1} - 1 \\ &< g^{W(\log x / \log g)+1} - 1 \\ &= g^{\alpha \log x / \log g + O(1)} - 1 \\ &< c'x^{\alpha}. \end{aligned}$$

Let F be a nonempty subset of $\{0,1,\ldots,k-1\} \cap W$, and $1 \leq c_f < g$ for $f \in F$. Then

$$\sum_{f \in F} c_f g^f \leq \sum_{i=0}^{k-1} (g-1)g^i = g^k - 1 < x.$$

Since every nonnegative integer has a unique g-adic representation, we have that

$$\begin{aligned} A_g(W)(x) &\geq \sum_{j=1}^{W(k-1)} \binom{W(k-1)}{j} (g-1)^j \\ &= g^{W(k-1)} - 1 \\ &= g^{\alpha \log x / \log g + O(1)} - 1 \\ &> cx^{\alpha}. \end{aligned}$$

The proof is complete.

Theorem 2.4 *Let $h \geq 2, g \geq 2$, let $t = \left\lceil \dfrac{\log(h+1)}{\log g} \right\rceil$. Let π be a partition of $\mathbf{N}$ into h pairwise disjoint subsets $W_0, W_1, \ldots, W_{h-1}$ such that each set W_r contains infinitely many intervals of t consecutive integers. Then*

$$A_g(\pi) = A_g(W_0) \cup \cdots \cup A_g(W_{h-1})$$

is a minimal asymptotic basis of order h.

Proof. Let $a \in A_g(\pi)$. Suppose $a \in A_g(W_0)$ and

$$a = \sum_{f \in F} c_f g^f,$$

where $F \in \mathcal{F}(W_0)$. Let $M = \max_{f \in F} f$. Let $a_0 = a$. I shall construct $h-1$ positive integers $a_r \in A_g(W_r)$. Choose $m_r \in W_r$ such that $m_r > M$ and the t consecutive integers $m_r, m_r + 1, \ldots, m_r + t - 1$ belong to W_r. Let

$$F_r \subseteq \{x \in W_r \mid M < x < m_r\},$$

and $1 \le c_f < g$ for all $f \in F_r$. Define

$$a_r = \sum_{M>i\in W_r} (g-1)g^i + \sum_{f\in F_r} c_f g^f + \sum_{i=m_r}^{m_r+t-1} (g-1)g^i. \tag{2.10}$$

Then $a_r \in A_g(W_r)$, and

$$(g-1)g^{m_r} \le a_r < g^{m_r+t}.$$

Let $n = a_0 + \cdots + a_{h-1}$. I shall show that this is the unique representation of n as a sum of h elements of $A_g(\pi)$.

Suppose that $n = b_0 + \cdots + b_{h-1}$, where $b_r \in A_g(\pi)$ for $r = 0, 1, \ldots, h-1$. Then $b_r \in A_g(W_{k(r)})$ for some $0 \le k(r) \le h-1$. Assume

$$b_r = \sum_{i\in G_r} d_{ri} g^i, \quad G_r \in \mathcal{F}(W_{k(r)})$$

for $r = 0, 1, \ldots, h-1$. Suppose there exists some $s \in \{1, \ldots, h-1\}$ such that $b_r \notin A_g(W_s)$ for all $r = 0, 1, \ldots, h-1$. Let U_r be the set of i in G_r so that $i < m_s + t - 1$. Then by Lemma 2.5, we have

$$\sum_{i=m_s}^{m_s+t-1} (g-1)g^i \le \sum_{r=0}^{h-1} \sum_{i\in U_r} d_{ri} g^i. \tag{2.11}$$

Noticing that $b_r \notin A_g(W_s)$ for $r = 0, 1, \ldots, h-1$, we see that $i < m_s$ for all $i \in U_r$ $(r = 0, 1, \ldots, h-1)$. It follows from the definition of t that

$$\begin{aligned} g^{m_s}(g^t - 1) &= \sum_{i=m_s}^{m_s+t-1} (g-1)g^i \\ &\le \sum_{r=0}^{h-1} \sum_{i\in U_r} d_{ri} g^i \\ &\le h \cdot \sum_{i=0}^{m_s-1} (g-1)g^i \\ &< h g^{m_s} \\ &\le g^{m_s}(g^t - 1), \end{aligned}$$

which is a contradiction. Therefore, we may assume that

$$b_r \in A_g(W_r), \text{ i.e., } G_r \subseteq W_r \text{ for } r = 1, 2, \ldots, h-1.$$

Now we show that $b_0 \in A_g(W_0)$. If not, we may assume, without loss of generality, that $b_0 \in A_g(W_1)$. Then by Lemma 2.5, we have

$$\begin{aligned} a_0 + \sum_{r=1}^{h-1} \sum_{\substack{i<M \\ i \in W_r}} (g-1)g^i &\leq \sum_{r=0}^{h-1} \sum_{\substack{i<M \\ i \in G_r}} d_{ri} g^i \\ &\leq \sum_{\substack{i<M \\ i \in G_0}} d_{0i} g^i + \sum_{r=1}^{h-1} \sum_{\substack{i<M \\ i \in W_r}} d_{ri} g^i \\ &< g^M + \sum_{r=1}^{h-1} \sum_{\substack{i<M \\ i \in W_r}} d_{ri} g^i \\ &\leq a_0 + \sum_{r=1}^{h-1} \sum_{\substack{i<M \\ i \in W_r}} (g-1)g^i, \end{aligned}$$

which is again a contradiction. Thus $b_0 \in A_g(W_0)$. Since the g-adic representation of an integer is unique, it follows that $a_r = b_r$ for $r = 0, 1, \ldots, h-1$. In particular, we have $b_0 = a_0 = a$. This means that $A_g(\pi)$ is a minimal asymptotic basis of order h, and the proof is complete.

Corollary 2.4.1 *Let π be a partition of nonnegative integers into two disjoint infinite subsets W_0 and W_1. then, for any $g \geq 3$,*

$$A_g(\pi) = A_g(W_0) \cup A_g(W_1)$$

is a minimal asymptotic basis of order two.

Corollary 2.4.2 *Let π be any partition of nonnegative integers into h pairwise disjoint infinite subsets $W_0, W_1, \ldots, W_{h-1}$. Then, for any $g \geq h+1$,*

$$A_g(\pi) = A_g(W_0) \cup A_g(W_1) \cup \cdots \cup A_g(W_{h-1})$$

is a minimal asymptotic basis of order h.

Theorem 2.5 *Let $g \geq 2$ be any integer, and let α be a real number such that $\frac{1}{h} \leq \alpha < 1$. Then there exists a partition π of $\mathbf{N}$ into h pairwise disjoint subsets such that*

$$A_g(\pi) = A_g(W_0) \cup A_g(W_1) \cup \cdots \cup A_g(W_{h-1})$$

is a minimal asymptotic basis of order h satisfying that

$$cx^{\alpha} < A_g(\pi)(x) < c'x^{\alpha} \tag{2.12}$$

for all x sufficiently large, where c and c' are constants.

Proof. Let $\alpha_0 = \alpha$, and define $\alpha_r = \dfrac{1-\alpha}{h-1}$ for $r = 1, 2, \ldots, h-1$. Then $\alpha_0 + \cdots + \alpha_{h-1} = 1$ and $\alpha_0 \geq \alpha_r > 0$ for $r = 1, 2, \ldots, h-1$. Let $t = \left\lceil \dfrac{\log(h+1)}{\log g} \right\rceil$. By Lemma 2.3, there exists a partition π of $\mathbf{N}$ into h pairwise disjoint infinite subsets $W_0, \ldots, W_{h-1}$ such that each subset W_r contains infinitely many intervals of length t and

$$W_r(x) = \alpha_r x + O(1).$$

Theorem 2.4 implies that $A_g(\pi)$ is a minimal asymptotic basis of order h, and Lemma 2.6 implies (2.12) holds for all sufficiently large x. Hence the proof is complete.

Theorem 2.6 *Let $h \geq 2$, $g \geq 2$, and let $t = \left\lceil \dfrac{\log(h+1)}{\log g} \right\rceil$. Let $\alpha_0, \ldots, \alpha_{h-1}$ be h positive real numbers such that $\alpha_0 + \cdots + \alpha_{h-1} = 1$. Let π be the partition satisfying conditions (i), (ii), and (iii) of Lemma 2.3. For any $a \in A_g(\pi)$, define $E_a = hA \backslash h(A \backslash \{a\})$. If $a \in A_g(W_r)$, then*

$$E_a(x) \gg x^{1-\alpha_r}.$$

Proof. Condition (iii) implies that there is an integer L such that in every interval $(y-L, y-1]$ there are t consecutive integers belonging to W_r for each $r = 0, 1, \ldots, h-1$. Let $a \in A(\pi)$, say, $a \in A_g(W_0)$. We show that $E_a(x) \gg x^{1-\alpha_0}$.

Suppose

$$a = \sum_{f \in F} c_f g^f, \quad \text{where } 1 \le c_f < g, \ F \in \mathcal{F}(W_0).$$

Define $M = \max_{f \in F} f$. Let x be sufficiently large, and $y = \dfrac{\log x}{\log g}$. Then the interval $(y - L, y - 1]$ contains $m_1, \dots, m_{h-1}$ such that

$$m_r + j \in (y - L, y - 1] \cap W_r$$

for $j = 0, 1, \dots, t - 1$, $r = 1, 2, \dots, h - 1$. Let $F_r \subseteq (M, y - L] \cap W_r$. Define a_r by (2.10), and let $n = a_0 + \cdots + a_{h-1}$. Then $n < g^y = x$. The proof of Theorem 2.4 shows that $n \in E_a$, and that different choices of c_f's and the $h - 1$ sets $F_1, \dots, F_{h-1}$ lead to different numbers n. For each j-element set F_r, there are $(g-1)^j$ different choices of c_f, $f \in F_r$. Noticing that there are

$$\binom{W_r(y - L) - W_r(M)}{j}$$

different j-element subsets of $(M, y - L] \cap W_r$, we see the number of n determined by various $F_1, \dots, F_{h-1}$ is

$$\prod_{r=1}^{h-1} \sum_{j=0}^{W_r(y-L)-W_r(M)} \binom{W_r(y - L) - W_r(M)}{j} (g-1)^j.$$

Noticing that

$$\log_g \left\{ \prod_{r=1}^{h-1} \sum_{j=0}^{W_r(y-L)-W_r(M)} \binom{W_r(y - L) - W_r(M)}{j} (g-1)^j \right\}$$

$$\begin{aligned} &= \log_g \prod_{r=1}^{h-1} g^{W_r(y-L)-W_r(M)} \\ &= \sum_{r=1}^{h-1} (W_r(y - L) - W_r(M)) \\ &\ge -M + \sum_{r=1}^{h-1} W_r(y - L) \end{aligned}$$

$$\begin{aligned} &= -M + \sum_{r=1}^{h-1}(\alpha_r y + O(1)) \\ &= y\sum_{r=1}^{h-1}\alpha_r + O(1) \\ &= (1-\alpha_0)\log_g x + O(1), \end{aligned}$$

we see that

$$\prod_{r=1}^{h-1}\sum_{j=0}^{W_r(y-L)-W_r(M)}\binom{W_r(y-L)-W_r(M)}{j}(g-1)^j \gg x^{1-\alpha_0}$$

which means that $E_a(x) \gg x^{1-\alpha_0}$. This completes the proof.

Remark. If we take $\alpha_r = 1/h$ for $r = 0, 1, \ldots, h-1$, then the minimal asymptotic basis $A_g(\pi)$ is strongly minimal. This follows immediately from Theorem 2.6.

2.4 Minimal Bases for Commutative Monoids

Let M be an infinite commutative monoid under addition. Let B be a subset of M, hB the set of all sums in the form $a_1 + \cdots + a_h$ with $a_i \in B$. A subset B is called a *basis of order* h for M if $hB = M$. A subset B is called an *asymptotic basis of order* h for M if hB contains all but finitely many elements in M. A basis B of order h is *minimal* if no proper subset of B is a basis of order h. Similarly, an asymptotic basis B of order h is *minimal* if no proper subset of B is an asymptotic basis of order h. A subset is called a *nonbasis* (resp. *asymptotic nonbasis*) *of order* h if it is not a basis (resp. asymptotic basis) of order h. Nathanson [40] introduced maximal nonbases, the dual concept of minimal bases. A nonbasis B of order h is called a *maximal nonbases of order* h if $B \cup \{a\}$ is a basis of order h for any element $a \notin B$.

Throughout this section, M denotes a countably infinite commutative monoid. Let B be a subset of M. For any element $u \in M$, $S(B,h,u)$ denotes the collection of the subsets $\{a_1,\dots,a_h\}$ of B such that $u = a_1 + \cdots + a_h$. Denote $r(B,h,u) = |S(B,h,u)|$.

Theorem 2.7 *Let B be a basis of order h for M. If $r(B,h,u) < \infty$ for any $u \in M$, then B contains a minimal basis of order h.*

Proof. Suppose that $B = \{a_1, a_2, \dots\}$. If B is a minimal basis of order h, then we have nothing to prove. Otherwise, $B\backslash\{a_i\}$ is also a basis of order h for some $a_i \in B$. Let i_1 be the least integer such that $B_1 = B\backslash\{a_{i_1}\}$ is also a basis of order h. If B_1 is minimal then it is done. Otherwise, let i_2 be the least integer such that $B_2 = B_1\backslash\{a_{i_2}\}$ is also a basis of order h. Continue this procedure inductively. If it stops in a finitely many steps, say, at B_{k_0}. then B_{k_0} is a minimal basis of order h which is contained in B and we are done. If it does not stop in a finitely many steps, we have the following infinite decreasing sequence of bases of order h:

$$B = B_0 \supset B_1 \supset B_2 \supset \cdots,$$

where $B_k = B_{k-1}\backslash\{a_{i_k}\}$ for $k = 1, 2, \dots$, and $i_1 < i_2 < \cdots$. Let

$$\overline{B} = \bigcap_{k=1}^{\infty} B_k = B\backslash\{a_{i_k} \mid k = 1, 2, \dots\}.$$

I shall prove that $\overline{B}$ is a minimal basis of order h.

Let $u \in M$. Since B_k is a basis of order h, we see that $S(B_k,h,u) \neq \emptyset$. Hence we have the following decreasing sequence:

$$S(B,h,u) = S(B_0,h,u) \supseteq S(B_1,h,u) \supseteq \cdots.$$

Noticing that $|S(B,h,u)| = r(B,h,u) < \infty$, we see that there exists an integer k_0 such that

$$S(B_{k_0},h,u) = S(B_{k_0+1},h,u) = S(B_{k_0+2},h,u) = \cdots.$$

Therefore, $S(\overline{B}, h, u) = S(B_{k_0}, h, u) \neq \emptyset$, which means that $u \in \overline{B}$. Hence $\overline{B}$ is a basis of order h.

If $\overline{B}\backslash\{a_i\}$ is also a basis of order h for some $a_i \in \overline{B}$, then there exists an integer k such that $i_{k-1} < i < i_k$ and $a_i \in B_{i_{k-1}}$. Since $B_{i_{k-1}} \supseteq \overline{B}$, we see that $B_{i_{k-1}}\backslash\{a_i\}$ is also a basis of order h. This contradicts the minimality of i_k. Therefore, $\overline{B}$ is a minimal basis of order h contained in B. The proof is complete.

Corollary 2.7.1 *If $r(M, h, u) < \infty$ for any $u \in M$, then every basis of order h contains a minimal basis of order h.*

Let $\Phi = \{S_i \mid i \in I\}$ be a family of nonempty sets. A set X is called a *system of representatives* for Φ if $X \cap S_i \neq \emptyset$ for all $i \in I$. A system X of representatives for Φ is called to be *minimal* if no proper subset of X is a system of representatives for Φ.

Theorem 2.8 *Let B be a nonbasis of order h. Then B is a maximal nonbasis of order h if and only if $X = M\backslash B$ is a minimal system of representatives for $S(M, h, u)$ for every $u \in M\backslash(hB)$.*

Proof. If B is not a maximal nonbasis of order h, then $B' = B \cup \{a\}$ is also a nonbasis of order h for some $a \notin B$. Hence, there exists $u \in M\backslash B'$ such that $S(u) \not\subseteq B'$ for every set $S(u) \in S(M, h, u)$. Therefore,

$$X_1 = \bigcup_{S(u) \in S(M,h,u)} (S(u)\backslash B')$$

is a system of representatives for $S(M, h, u)$. Noticing that $a \notin B$, we have that X_1 is a proper subset of $X = M\backslash B$, which contradicts the minimality of X. Therefore, B is a maximal nonbasis of order h.

Conversely, let B be a maximal nonbasis of order h. It is clear that $X = M\backslash B$ is a system of representatives for $S(M, h, u)$ for any $u \in M\backslash hB$. Now suppose that X is not a minimal system of representatives for $S(M, h, u)$

for some $u \in M \backslash hB$. Then there exists an $a \in X$ such that $X' = X \backslash \{a\}$ is also a system of representatives for $S(M,h,u)$, hence $X' \cap S(u) \neq \emptyset$ for all $S(u) \in S(M,h,u)$, i.e., $(M \backslash B') \cap S(u) \neq \emptyset$ for all $S(u) \in S(M,h,u)$, where $B' = B \cup \{a\}$. Therefore, $S(u) \not\subseteq B'$ for all $S(u) \in S(M,h,u)$, which means that $u \notin hB'$. Hence, B is not a maximal nonbasis of order h. This contradiction proves the theorem.

Theorem 2.9 *If $r(M,h,u) < \infty$ for all $u \in M$, then every nonbasis of order h is contained in a maximal nonbasis of order h.*

Proof. Let B be a nonbasis of order h. Then there exists $u \in M$ such that $u \notin hB$. Hence $S(u) \not\subseteq B$ for any $S(u) \in S(M,h,u)$. Let X be a minimal system of representatives for $S(M,h,u)$ such that $X \cap S(u) \subseteq S(u) \backslash B$ for any $S(u) \in S(M,h,u)$. The set X exists because $S(M,h,u)$ is finite. It is clear that $B_1 = M \backslash X$ is a nonbasis of order h. It follows from $r(M,h,u) < \infty$ that X is a finite set with at most $r(M,h,u)$ elements. Therefore, there exists a maximal nonbasis $\overline{B}$ of order h containing B_1, hence, $\overline{B} \supseteq B$. So the proof is complete.

Corollary 2.9.1 *Every basis of order h for nonnegative integers contains a minimal basis of order h for nonnegative integers. Every nonbasis of order h for nonnegative integers is contained in a maximal nonbasis of order h for nonnegative integers.*

Proof. This immediately follows from Theorem 2.7 and 2.9.

A set A of positive integers is a *LCM basis* of order h if every positive integer is the least common multiple of h not necessarily distinct elements in A. This concept was introduced by Nathanson [42].

Corollary 2.9.2 *Every LCM basis of order h for positive integers contains a minimal LCM basis of order h for positive integers. Every LCM nonbasis*

of order h is contained in a LCM maximal nonbasis of order h for positive integers.

Proof. Let $\mathbf{N}$ be the set of all positive integers and let $a \cdot b$ denote the least common multiple of positive integers a and b. It is clear that $(\mathbf{N}, \cdot)$ is a commutative monoid satisfying $r(M, h, u) < \infty$ for all $u \in \mathbf{N}$. Therefore, the corollary follows immediately from Theorems 2.7 and 2.9.

Theorem 2.10 *Suppose S is a subset of M such that every element of M has only one representation as a sum of a finitely many elements in S. Let $\{S_1, \ldots, S_h\}$ be a partition of S. Let $\langle S_i \rangle$ denote the submonoind generated by S_i. If there are at least two $\langle S_i \rangle$ are infinite, then*

$$B = \langle S_1 \rangle \cup \langle S_2 \rangle \cup \cdots \cup \langle S_h \rangle$$

is a minimal asymptotic basis of order h for M.

Proof. Let $u \in M$. Then $u = a_1 + \cdots + a_n$ for some $a_i \in S$ $(i = 1, \ldots, n)$. Since $\{S_1, \ldots, S_h\}$ is a partition of S, we may assume that

$$\begin{aligned} a_\mu &\in S_1 \quad \text{for} \quad \mu = 1, \ldots, i_1, \\ &\cdots \quad \cdots \quad \cdots \\ a_\mu &\in S_h \quad \text{for} \quad \mu = i_{h-1} + 1, \ldots, n. \end{aligned}$$

Hence,

$$\sum_{\mu=1}^{i_1} a_\mu \in \langle S_1 \rangle, \quad \ldots, \quad \sum_{\mu=i_{h-1}+1}^{n} a_\mu \in \langle S_h \rangle.$$

This implies that $u \in hB$. Thus, B is an asymptotic basis of order h.

Let $u = u_1 \in B$, say, $u \in \langle S_1 \rangle$. Since every element in M has a unique representation as a sum of elements in S, it follows that

$$B_1 = \left\{ \sum_{i=1}^{h} u_i \;\middle|\; u_i \in \langle S_i \rangle \;\text{ for }\; i = 2, \ldots, h \right\}$$

is infinite because at least one of (S_i) is infinite. Clearly $B_1 \cap h(B\backslash\{u\}) = \emptyset$, hence $B\backslash\{u\}$ is not an asymptotic nonbasis of order h. therefore, B is minimal, and so the proof is complete.

Theorem 2.11 *Let B be a maximal asymptotic nonbasis of order h for M. If $u \notin B$, then all but finitely many elements $a \in hB$ have the form $a = u+b$, where $b \in (h-1)B$.*

Proof. Since B is a maximal asymptotic nonbasis of order h and $u \notin B$, then $B' = B \cup \{u\}$ is an asymptotic basis of order h. Hence hB' contains all but finitely many elements of M. Thus hB' contains all but finitely many elements not in hB. Therefore, the proof is complete.

This theorem generalizes a theorem by Grekos [16,17] on maximal asymptotic union nonbases.

3 REPRESENTATIVES FOR FINITE SETS

3.1 Introduction

It is important to notice that not every asymptotic basis of order h contains a minimal asymptotic basis of order h. A trivial example is $A = \{1, h, 2h, 3h, \ldots\}$, which is an asymptotic basis of order h containing no minimal asymptotic basis of order h. The set of all squares is a basis of order 4. It is not known if there exists a minimal basis of order 4 containing only squares. Nathanson [40] constructed the first nontrivial example of an asymptotic basis of order two, no subset of which is a minimal asymptotic basis of order two. Furthermore, Erdös and Nathanson [10] constructed a family of asymptotic bases A of order two such that $A \backslash S$ is an asymptotic basis of order two if and only if S is a finite subset of A. Therefore, A does not contain any minimal asymptotic basis of order two. It is an unsolved and difficult problem to determine if an asymptotic basis of order h contains a minimal asymptotic basis of order h. In the case $h = 2$, Erdös and Nathanson [11] proved the following remarkable theorem.

Theorem 3.1 (Erdös-Nathanson) *If* $c > \dfrac{1}{\log 4/3}$ *and if* A *is an asymptotic basis of order two such that* $r_2(n) > c \log n$ *for all sufficiently large* n, *then* A *contains a minimal asymptotic basis of order two.*

Surprisingly, the crucial part in their proof of this result is a special case of the following purely combinatorial result:

Theorem 3.2 *For $h \geq 2$ and $k \geq 1$, let*

$$k = q(h-1) + r, \quad \text{where } 0 \leq r < h-1.$$

Define

$$\alpha = \alpha(h,k) = 1 - \frac{h-r}{h^{q+1}}.$$

Let $s \geq 1$ and $t \geq 0$. Let

$$\Phi = \{S_i \mid i = 1,2,\ldots,s\} \quad \text{and} \quad \Psi = \{T_j \mid j = 1,2,\ldots,t\}$$

be two families of finite sets satisfying the following conditions:

(i) $1 \leq |S_i| \leq h$ *for* $i = 1,2,\ldots,s$, *and*
$1 \leq |T_j| \leq k$ *for* $j = 1,2,\ldots,t$;

(ii) $S_i \cap S_{i'} = T_j \cap T_{j'} = \emptyset$ *for all* $i \neq i'$ *and* $j \neq j'$;

(iii) $S_i \not\subseteq T_j$ *for all* i *and* j.

Let $N(\Phi,\Psi)$ denote the number of sets X such that

(iv) $|X| = s$;

(v) $|X \cap S_i| = 1$ *for* $i = 1,2,\ldots,s$;

(vi) $X \cap T_j \neq \emptyset$ *for* $j = 1,2,\ldots,t$.

Then

$$N(\Phi,\Psi) \leq \alpha^t h^s,$$

and this is the best possible result.

Nathanson [44] conjectured this result, and proved some special cases. I have recently proved the full theorem (see [25]). In Section 3.2, I shall present the proof of the theorem in the case $h = k$, and then in Section 3.3, I shall prove the general case. In Section 3.4, I shall prove a better estimate in the case $h = k = 3$.

Theorem 3.2 should be useful in the study of the existence of minimal asymptotic bases in asymptotic bases. As a matter of fact, using this result, Nathanson [46] has recently found sufficient conditions that an asymptotic basis of order h contains a minimal asymptotic basis of order h. This is an important approach to the problem in the general case, but it seems that the conditions are too restrictive because disjoint representations of integers as sums of distinct elements are involved in his conditions. So it would be very interesting to find a simple condition that an asymptotic basis of order h contains a minimal asymptotic basis of order h.

Let

$$\Phi = \{S_i \mid i = 1, 2, \ldots, s\} \text{ and } \Psi = \{T_j \mid j = 1, 2, \ldots, t\}$$

be two finite families of finte sets. The set X is called a *system of representatives* for Φ is $X \cap S_i \neq \emptyset$ for $i = 1, 2, \ldots, t$. If X is a system of representatives for Φ but no proper subset of X is a system of representatives for Φ, then X is called a *minimal system of representatives* for Φ. We denote by $D(\Phi)$ the number of minimal systems of representatives for Φ. A set X is called *simultaneous system of representatives* for Φ and Ψ if X is a minimal system of representatives for Φ and X is also a system of representatives for Ψ. By $N(\Phi, \Psi)$ we denote the number of the simultaneous systems of representatives for Φ and Ψ.

In order to modify Erdös and Nathanson's proof of Theorem 3.1 to obtain a similar condition that an asymptotic basis of order $h \geq 3$ contains a minimal asymptotic basis of order h, we study the following problem, which was proposed by Nathanson. On the other hand, this is also a very interesting combinatorial problem.

Problem 3.1 (Nathanson) *Let $h \geq 2$ and $k \geq 1$. Does there exist a real number $\mu = \mu(h, k) \in (0, 1)$ such that*

$$N(\Phi, \Psi) \leq D(\Phi, \Psi)\mu^t$$

holds for any families Φ and Ψ of finite sets satisfying the following properties?

(i) $\Phi = \{S_i \mid i = 1, 2, \ldots, s\}$ *is a family of* s *nonempty, distinct sets* S_i *with* $|S_i| \leq h$ *for all* i*;*

(ii) $\Psi = \{T_j \mid j = 1, 2, \ldots, t\}$ *is a family of* t *nonempty, distinct sets* T_j *with* $|T_j| \leq k$ *for all* j*;*

(iii) $S_i \not\subseteq T_j$ *for all* i *and* j*.*

In Section 3.5, I shall prove that the answer to this question is negative by giving a counterexample. However, after adding some further restriction on Φ, I shall prove that such μ exists in a special case. I hope this result would be useful in searching a simple condition that an asymptotic basis of order $h \geq 3$ contains a minimal asymptotic basis of order h.

3.2 A Special Case

In this section, I shall prove the following theorem, which is a special case of Theorem 3.2.

Theorem 3.3 *Let* $h \geq 2$*. Let*

$$\Phi = \{S_i \mid i = 1, 2, \ldots, s\} \quad \textit{and} \quad \Psi = \{T_j \mid j = 1, 2, \ldots, t\}$$

be two families of finite sets satisfying the following conditions:

(i) $1 \leq |S_i| \leq h$ *for* $i = 1, 2, \ldots, s$*, and*
$1 \leq |T_j| \leq h$ *for* $j = 1, 2, \ldots, t$*;*

(ii) $S_i \cap S_{i'} = T_j \cap T_{j'} = \emptyset$ *for all* $i \neq i'$ *and* $j \neq j'$*;*

(iii) $S_i \not\subseteq T_j$ *for all* i *and* j.

Then

$$N(\Phi,\Psi) \le h^s \left(\frac{h^2-h+1}{h^2}\right)^t,$$

and this is the best possible result.

In order to prove this theorem, we need the following lemma.

Lemma 3.1 *Let* $k \ge 1$, $h \ge 2$ *be integers, then*

$$h \cdot \prod_{j=1}^{k}(h-x_j) + \sum_{i=1}^{k} x_i^2 \cdot \prod_{\substack{j\ne i \\ 1\le j\le k}} (h-x_j) \le h \cdot \left(\frac{h^2-h+1}{h}\right)^k \tag{3.1}$$

for any real numbers $x_j : 1 \le x_j \le h-1$, $j = 1,2,\ldots,k$. *Moreover, the equality holds if and only if* $k = 1$ *and* $x_1 = 1$ *or* $h-1$.

Proof. It is clear that the equality holds if $k = 1$ and $x_1 = 1$ or $h-1$. Now we assume that $k > 1$.

Let $y_j = h - x_j$ for $j = 1,2,\ldots,k$. Then

$$h \cdot \prod_{j=1}^{k}(h-x_j) + \sum_{i=1}^{k} x_i^2 \cdot \prod_{\substack{j\ne i \\ 1\le j\le k}} (h-x_j)$$

$$= \left(h - 2kh + \sum_{i=1}^{k}\left(y_i + \frac{h^2}{y_i}\right)\right) \prod_{j=1}^{k} y_j.$$

Denote the term on the right hand side by $f(y_1,\ldots,y_k)$. Suppose that $1 \le a_j \le h-1$, $j = 1,2,\ldots,k$, are such that

$$f(a_1,\ldots,a_k) = \max_{\substack{1\le y_j\le h-1 \\ j=1,2,\ldots,k}} f(y_1,\ldots,y_k). \tag{3.2}$$

It is sufficient to prove that

$$f(a_1,\ldots,a_k) < h\left(\frac{h^2-h+1}{h}\right)^k. \tag{3.3}$$

First we claim that $a_1 = \cdots = a_k = h-1$. Otherwise, there is some u such that $1 \le a_u < h-1$. Then

$$\begin{aligned}
&f(a_1,\ldots,a_{u-1},h-1,a_{u+1},\ldots,a_k)\\
&= \left(h-2kh+\frac{h^2}{h-1}+h-1+\sum_{\substack{1\le i\le k\\ i\ne u}}\left(\frac{h^2}{a_i}+a_i\right)\right)(h-1)\prod_{\substack{1\le i\le k\\ j\ne u}} a_j\\
&= \left(h-2kh+\frac{h^2}{h-1}+h-1-\frac{h^2}{a_u}-a_u\right.\\
&\quad \left.+\sum_{i=1}^{k}\left(\frac{h^2}{a_i}+a_i\right)\right)\cdot\frac{h-1}{a_u}\cdot\prod_{j=1}^{k}a_j\\
&= f(a_1,\ldots,a_k)+\left(\left(h-2kh+\sum_{i=1}^{k}\left(\frac{h^2}{a_i}+a_i\right)\right)\left(\frac{h-1}{a_u}-1\right)\right.\\
&\quad \left.+\left(\frac{h^2}{h-1}+h-1-\frac{h^2}{a_u}-a_u\right)\cdot\frac{h-1}{a_u}\right)\cdot\prod_{j=1}^{k}a_j\\
&> f(a_1,\ldots,a_k)+\left\{\left(h-2kh+2(k-1)h+\frac{h^2}{a_u}+a_u\right)\left(\frac{h-1}{a_u}-1\right)\right.\\
&\quad \left.+\left(2h+\frac{1}{h-1}-\frac{h^2}{a_u}-a_u\right)\cdot\frac{h-1}{a_u}\right\}\prod_{j=1}^{k}a_j\\
&= f(a_1,\ldots,a_k)+\left(h-a_u-\frac{h-1}{a_u}\right)\prod_{j=1}^{k}a_j\\
&\ge f(a_1,\ldots,a_k),
\end{aligned}$$

which contradicts (3.2). Therefore, $a_1 = \cdots = a_k = h-1$.

I now prove that

$$f(h-1,\ldots,h-1) < h\left(\frac{h^2-h+1}{h}\right)^k.$$

Noticing that

$$\left(1+\frac{1}{h^2-h}\right)^{k-1} > 1+\frac{k-1}{h^2-h} > 1+\frac{k-1}{h^2-h+1},$$

we see that

$$\begin{aligned}\frac{f(h-1,\dots,h-1)}{h\cdot\left(\frac{h^2-h+1}{h}\right)^k} &= \frac{\left(h-2kh+\frac{kh^2}{h-1}+k(h-1)\right)(h-1)^k}{(h^2-h+1)\left(\frac{h^2-h+1}{h}\right)^{k-1}} \\ &= \frac{h^2-h+k}{h^2-h+1}\cdot\left(\frac{h^2-h}{h^2-h+1}\right)^{k-1} \\ &= \left(1+\frac{k-1}{h^2-h+1}\right)\cdot\frac{1}{\left(1+\frac{1}{h^2-h}\right)^{k-1}} \\ &< 1,\end{aligned}$$

this proves (3.3). Hence (3.1) holds, and the proof is complete.

Proof of Theorem 3.3. For any $s \geq 1$, and $t \geq 0$, define

$$M(s,t) = h^s\left(\frac{h^2-h+1}{h^2}\right)^t,$$

and denote by $N(s,t)$ the maximal value of $N(\Phi,\Psi)$ for all Φ and Ψ satisfying (i), (ii) and (iii) in Theorem 3.3. I shall prove that $N(s,t) \leq M(s,t)$ by induction on t. If $t = 0$, this is true because

$$N(s,0) = h^s = M(s,0).$$

Let $t \geq 1$. Now we assume that $N(s,t') \leq M(s,t')$ for any s and any $0 \leq t' < t$. I shall prove that $N(s,t) \leq M(s,t)$.

Suppose that

$$\Phi = \{S_i \mid i = 1,2,\dots,s\} \text{ and } \Psi = \{T_j \mid j = 1,2,\dots,t\}$$

be two families of finite sets satisfying (i), (ii) and (iii). Let

$$S = \bigcup_{i=1}^{s} S_i, \quad T = \bigcup_{j=1}^{t} T_j.$$

We may assume without loss of generality that $S \supseteq T$. Let S_{s+1} be a finite set such that

$$|S_{s+1}| = h \quad \text{and} \quad S_{s+1} \cap S = \emptyset.$$

Let $\Phi' = \Phi \cup \{S_{s+1}\}$, then it is clear that $N(\Phi', \Psi) = h \cdot N(\Phi, \Psi)$, which implies that $N(s+1,t) \geq h \cdot M(s,t)$. Therefore, it is sufficient to prove that $N(s,t) \leq M(s,t)$ for sufficiently large s.

Suppose that Φ and Ψ are such that $N(\Phi, \Psi) = N(s,t)$. Without loss of generality, we may assume that

$$|S_i| = |T_j| = h \quad \text{for} \quad i = 1, 2, \ldots, s, \; j = 1, 2, \ldots, t.$$

Since T is a proper subset of S, there is some S_i, say, S_1, such that $S_1 \cap T \neq \emptyset$ and $T \not\supseteq S_1$. It follows from the multiplicativity of $N(s,t)$ that we may assume that $T_1, \ldots, T_k$ are all of those T_j that intersects S_1. Then $k \geq 1$. Denote

$$n_0 = |S_1 \backslash T|,$$

and

$$n_j = |S_1 \cap T_j| \quad \text{for} \quad j = 1, 2, \ldots, k.$$

Then $1 \leq n_j \leq h-1$ for $j = 0, 1, \ldots, k$, and $\sum_{i=0}^{k} n_i = h$. Let

$$N_0 = n_0, \quad N_j = N_{j-1} + n_j \quad \text{for} \quad j = 1, 2, \ldots, k.$$

Suppose that

$$\begin{aligned}
S_1 &= \{a_1, \ldots, a_h\}, \\
S_1 \backslash T &= \{a_1, \ldots, a_{N_0}\}, \\
T_1 &= \{a_{N_0+1}, \ldots, a_{N_1}, a_{1,1}, \ldots, a_{1,h-n_1}\}, \\
&\cdots \quad \cdots \quad \cdots \\
T_k &= \{a_{N_{k-1}+1}, \ldots, a_{N_k}, a_{k,1}, \ldots, a_{k,h-n_k}\}.
\end{aligned}$$

For any $a \in S$, $S[a]$ denotes the unique S_i that contains a. We divide the family of simultaneous systems of representatives for Φ and Ψ into the following $k+1$ classes:

$$\begin{aligned} \mathbf{C}_0 &= \{X \mid X \cap (S_1 \backslash T) \neq \emptyset\}, \\ \mathbf{C}_j &= \{X \mid X \cap S_1 \cap T_j \neq \emptyset\} \text{ for } j = 1, 2, \ldots, k. \end{aligned}$$

It is clear that $\mathbf{C}_i \cap \mathbf{C}_j = \emptyset$ for all $i \neq j$.

Now suppose $X \in \mathbf{C}_0$. Then $X \cap (S_1 \backslash T) = \{a_i\}$ for a unique $i : 1 \leq i \leq N_0$. Therefore, $a_j \notin X$ for $j \neq i$ and $j = 1, 2, \ldots, k$, which implies that there exist $i_j : 1 \leq i_j \leq h - n_j$ for $j = 1, 2, \ldots, k$ such that X contains a_{j,i_j} for $j = 1, 2, \ldots, k$. (ii) implies that $a_{j,i_j} \in T_j$ and that a_{j,i_j} are distinct, hence $S[a_{j,i_j}]$ are distinct. Let

$$\begin{aligned} \Phi' &= \Phi \backslash \{S_1, S[a_{1i_1}], \ldots, S[a_{ki_k}]\}, \\ \Psi' &= \{T_{k+1}, \ldots, T_t\}, \\ X' &= X \backslash \{a_{1i_1}, \ldots, a_{ki_k}\}. \end{aligned}$$

It is easy to verify that Φ' and Ψ' satisfy conditions (i), (ii) and (iii), and that X' is a simultaneous system of representatives for Φ' and Ψ'. Conversely, if X' is a simultaneous system of representatives for Φ' and Ψ', then

$$X = X' \cap \{a_i, a_{1i_1}, \ldots, a_{ki_k}\}$$

is a simultaneous system of representatives for Φ and Ψ. Hence the number of simultaneous systems of representatives for Φ and Ψ containing the set $\{a_i, a_{1i_1}, \ldots, a_{ki_k}\}$ is

$$N(\Phi', \Psi') \leq N(s-k-1, t-k).$$

Since there are

$$n_0 \prod_{j=1}^{k} (h - n_j)$$

different ways to choose the set $\{a_i, a_{1,i_1}, \ldots, a_{ki_k}\}$, we see that

$$|\mathbf{C}_0| \leq N(s-k-1, t-k) n_0 \prod_{j=1}^{k} (h - n_j). \tag{3.4}$$

Given any $m : 1 \leq m \leq k$. Let $X \in \mathbf{C}_m$, then $X \cap S_1 \cap T_m = \{a_i\}$ for a unique $i : N_{m-1} < i \leq N_m$, thus $a_j \notin X$ for any $j \neq i$ and $j = 1, 2, \ldots, k$. Hence $a_{ji_j} \in X$ for some $i_j : j = 1, 2, \ldots, k,\ j \neq m$. It is clear that $S[a_{ji_j}]$ are distinct. Let

$$\begin{aligned} \Phi' &= \Phi \backslash \{S_1, S[a_{ji_j}] \mid j = 1, 2, \ldots, k,\ j \neq m\}, \\ \Psi' &= \{T_{k+1}, \ldots, T_t\}, \\ X' &= X \backslash \{a_i, a_{ji_j} \mid j = 1, 2, \ldots, k,\ j \neq m\}. \end{aligned}$$

It is easy to verify that Φ' and Ψ' satisfy the conditions in the theorem, and that X' is a simultaneous system of representatives for Φ' and Ψ' if and only if X is a simultaneous system of representatives for Φ and Ψ. Hence there are at most $N(s-k, t-k)$ sets $X \in \mathbf{C}_m$ containing

$$\{a_i, a_{ji_j} \mid j = 1, 2, \ldots, k,\ j \neq m\}.$$

Since there are only

$$n_m \cdot \prod_{\substack{j \neq m \\ 1 \leq j \leq k}} (h - n_j)$$

different ways to choose the set $\{a_i, a_{ji_j} \mid j = 1, 2, \ldots, k,\ j \neq m\}$, we see that

$$|\mathbf{C}_m| \leq N(s-k, t-k) \cdot n_m \cdot \prod_{\substack{j \neq m \\ 1 \leq j \leq k}} (h - n_j). \tag{3.5}$$

It therefore follows from (3.4) and (3.5) that

$$\begin{aligned} N(s,t) &= N(\Phi, \Psi) \\ &\leq N(s-k-1, t-k) \cdot n_0 \cdot \prod_{j=1}^{k} (h - n_j) \end{aligned}$$

$$+ N(s-k,t-k)\cdot\sum_{i=1}^{k} n_i \cdot \prod_{\substack{j\neq i\\ 1\le j\le k}} (h-n_j)$$

$$\le \frac{1}{h}N(s-k,t-k)\left(n_0\prod_{j=1}^{k}(h-n_j)+h\sum_{i=1}^{k} n_i \prod_{\substack{j\neq i\\ 1\le j\le k}} (h-n_j)\right).$$

Noticing that $\sum_{j=0}^{k} n_j = h$, we have that

$$\begin{aligned}
& n_0\cdot\prod_{j=1}^{k}(h-n_j)+h\cdot\sum_{i=1}^{k} n_i\cdot \prod_{\substack{j\neq i\\ 1\le j\le k}} (h-n_j)\\
&= \left(h-\sum_{i=1}^{k} n_i\right)\prod_{j=1}^{k}(h-n_j)+h\cdot\sum_{i=1}^{k} n_i\cdot \prod_{\substack{j\neq i\\ 1\le j\le k}} (h-n_j)\\
&= h\prod_{j=1}^{k}(h-n_j)+\sum_{i=1}^{k}(hn_i-(h-n_i)n_i) \prod_{\substack{j\neq i\\ 1\le j\le k}} (h-n_j)\\
&= h\prod_{j=1}^{k}(h-n_j)+\sum_{i=1}^{k} n_i^2 \prod_{\substack{j\neq i\\ 1\le j\le k}} (h-n_j)\\
&\le h\left(\frac{h^2-h+1}{h}\right)^k\\
&= M(k+1,k).
\end{aligned}$$

Therefore,

$$\begin{aligned}
N(s,t) &\le \frac{1}{h}N(s-k,t-k)M(k+1,k)\\
&\le \frac{1}{h}M(s-k,t-k)M(k+1,k)\\
&= M(s,t).
\end{aligned}$$

Now we prove that $M(s,t)$ is the best possible when $s \ge 2t$. Let

$$a_{11},\ldots,a_{1h},\ldots,a_{s1},\ldots,a_{sh}$$

be sh different positive integers. Let

$$\begin{aligned} S_i &= \{a_{i1}, \ldots, a_{ih}\} \text{ for } i = 1, 2, \ldots, s; \\ T_j &= \{a_{j1}, \ldots, a_{j,h-1}, a_{t+j,h}\} \text{ for } j = 1, 2, \ldots, t. \end{aligned}$$

Define

$$\Phi = \{S_1, S_2, \ldots, S_s\} \text{ and } \Psi = \{T_1, T_2, \ldots, T_t\}.$$

It is clear that Φ and Ψ satisfy conditions (i), (ii) and (iii), and and

$$N(\Phi, \Psi) = h^s \left(\frac{h^2 - h + 1}{h^2}\right)^t = M(s, t).$$

The proof is complete.

3.3 Proof of Theorem 3.2

In this section, I shall prove Theorem 3.2. The following lemma will be used in the proof.

Lemma 3.2 *Let $h \geq 2$ and $m \geq 1$ with $m \leq L < mh$. If*

$$L - m = u(h-1) - r,$$

where u is an integer, and $0 \leq r \leq h-2$, then

$$\prod_{i=1}^{m} x_i \geq h_{u-1}(h-r)$$

holds for any integers $1 \leq x_i \leq h$ $(i = 1, 2, \ldots, m)$ with $\sum_{i=1}^{m} x_i = L$.

Proof. Let

$$f(\mathbf{x}) = f(x_1, \ldots, x_m) = \prod_{i=1}^{m} x_i.$$

It is well known that f has no minimal point inside the inner $\mathbf{D}$ of the domain

$$\overline{\mathbf{D}} = \{\mathbf{x} = (x_1, \ldots, x_m) \mid 1 \leq x_i \leq h \text{ for } i = 1, \ldots, m\}$$

with the restriction $\sum_{i=1}^{m} x_i = L$. Hence, the minimal point of f must be on the boundary $\partial\mathbf{D}$.

Since $L < mh$, it follows from the definition of u that $u \leq m$. First we assume $u = m$, then $L = mh - r$. We prove

$$f(\mathbf{x}) \geq h^{m-1}(h - r) \tag{3.6}$$

by induction on m. It is clear that (3.6) is true if $m = 1$. Now assume that (3.6) holds for any $m' < m$. Let $\mathbf{x} = (x_1, \ldots, x_m)$ be a minimal point of f on the boundary $\partial\mathbf{D}$, where $x_1 \leq x_2 \leq \cdots \leq x_m$. Since

$$x_1 = L - \sum_{i=2}^{m} x_i \geq L - (m-1)h = h - r \geq 2,$$

it follows from $\mathbf{x} \in \partial\mathbf{D}$ that $x_m = h$. Therefore,

$$\sum_{i=1}^{m-1} x_i = L - r = (m-1)h - r,$$

thus,

$$\begin{aligned} f(\mathbf{x}) &= \prod_{i=1}^{m} x_i = h \cdot \prod_{i=1}^{m-1} x_i \\ &\geq h \cdot (h^{m-2}(h - r)) = h^{m-1}(h - r), \end{aligned}$$

which proves (3.6).

Now assume that $u < m$. If $\mathbf{x} \in \partial\mathbf{D}$ is such that $x_1 \leq \cdots \leq x_m$ and $f(\mathbf{x})$ is minimal, then $x_1 = 1$. Otherwise, we have that

$$2 \leq x_1 \leq \cdots \leq x_v < x_{v+1} = \cdots = x_m = h.$$

Then

$$\mathbf{x}' = (x_1 - 1, x_2, \ldots, x_{v-1}, x_v + 1, x_{v+1}, \ldots, x_m) \in \partial\mathbb{D},$$

and

$$\begin{aligned} f(\mathbf{x}') &= (x_1 - 1)x_2 \cdots x_{v-1}(x_v + 1)h^{m-v} \\ &= x_1 x_2 \cdots x_v h^{m-v} - x_2 \cdots x_{v-1} h^{m-v}(x_v + 1 - x_1) \\ &< f(\mathbf{x}), \end{aligned}$$

whixh contradicts the minimality of $f(\mathbf{x})$. Therefore,

$$\sum_{i=2}^{m} x_i = L - 1 = u(h-1) - r + (m-1),$$

thus,

$$f(\mathbf{x}) = \sum_{i=1}^{m} x_i = \sum_{i=2}^{m} x_i \geq h^{u-1}(h - r).$$

This shows that we can assume $u = m$. Hence the proof of the lemma is complete.

Proof of Theorem 3.2. Let

$$\Phi = \{S_1, S_2, \ldots, S_s\} \text{ and } \Psi = \{T_1, T_2, \ldots, T_t\}$$

be two finite families of finite sets that satisfy the conditions (i), (ii) and (iii) of Theorem 3.2. Let S_{s+1} be a set of h elements such that S_{s+1} does not intersect any S_i in Φ. Let $\Phi' = \Phi \cup \{S_{s+1}\}$, we have

$$N(\Phi', \Psi) \geq hN(\Phi, \Psi).$$

This allows us to assume that the integer s is sufficiently large. Therefore, we may assume without loss of generality that

$$\begin{aligned} |S_i| &= h \quad \text{for} \quad i = 1, 2, \ldots, s; \\ |T_j| &= k \quad \text{for} \quad j = 1, 2, \ldots, t; \end{aligned}$$

and

$$S = \bigcup_{i=1}^{s} S_i \supseteq T = \bigcup_{j=1}^{t} T_j.$$

I shall prove the theorem by induction on t for finxed $s > 2kt$. If $t = 0$ then $N(\Phi, \Psi) = h^s$. Let $t \geq 1$ and assume that Theorem 3.2 holds for any $0 \leq t' < t$ and any s.

We consider T_t. Let $\{S_1, S_2, \ldots, S_m\}$ be the set of those S_i that intersects T_t. Denote

$$n_i = |S_i \cap T_t| \quad \text{for} \quad i = 1, 2, \ldots, m,$$

then $\sum_{i=1}^{m} n_i = k$. It follows from $S_i \not\subseteq T_t$ that $1 \leq n_i \leq h - 1$ for $i = 1, 2, \ldots, m$. Suppose that

$$S_i = \{a_{i1}, a_{i2}, \ldots, a_{ih}\},$$

where $a_{i1} \in T_t, \ldots, a_{in_i} \in T_t$ for $i = 1, 2, \ldots, m$. Since $s > 2kt$, there exist m different S_i in Φ, say, $S_{m+1}, \ldots, S_{2m}$, such that $S_i \cap T = \emptyset$ for $i = m + 1, \ldots, 2m$. Suppose that

$$S_i = \{a_{i1}, a_{i2}, \ldots, a_{ih}\} \quad \text{for} \quad i = m + 1, \ldots, 2m.$$

We construct

$$\begin{aligned} S_i' &= \{a_{i1}, \ldots, a_{in_i}, a_{m+i,n_i+1}, \ldots, a_{m+i,h}\}, \\ S_{m+i}' &= \{a_{m+i,1}, \ldots, a_{m+i,n_i}, a_{i,n_i+1}, \ldots, a_{ih}\} \end{aligned}$$

for $i = 1, 2, \ldots, m$. Let

$$\Phi' = (\Phi \backslash \{S_1, \ldots, S_{2m}\}) \cup \{S_1', \ldots, S_{2m}'\}.$$

Then Φ' and Ψ satisfy the conditions (i), (ii) and (iii) of Theorem 3.2 with same s and t.

Let X be a simultaneous system of representatives counted in $N(\Phi, \Psi)$. Denote

$$X \cap S_i = \{x_i\} \quad \text{for} \quad i = 1, 2, \ldots, m,$$

and

$$X_1 = X \setminus \bigcup_{i=1}^{2m} S_i.$$

Then it follows from $S_i \cap T = \emptyset$ for $i = m+1, \ldots, 2m$ that exactly h^m simultaneous systems X of representatives counted in $N(\Phi, \Psi)$ contain

$$\{x_1, x_2, \ldots, x_m\} \cup X_1.$$

Suppose that $x_j \in S'_{i_j}$ for $j = 1, 2, \ldots, m$ where the subscripts of S'_i's are regarded as elements of the group $\mathbb{Z}/(2m)$. Therefore, for any $x_{j+m} \in S'_{i_j+m}$ for $j = 1, 2, \ldots, m$, let

$$X' = \{x_1, x_2, \ldots, x_m\} \cup X_1,$$

we see that X' is a minimal system of representatives for Φ' that contains a system of representatives for Ψ, and X' contains $\{x_1, x_2, \ldots, x_m\} \cup X_1$. Since there are h^m different simultaneous systems X of representatives counted in $N(\Phi', \Psi)$. Therefore, $N(\Phi', \Psi) \leq N(\Phi, \Psi)$. Hence, we may assume that T_t is the only T_j that $S_i \cap T_j \neq \emptyset$ for $i = 1, 2, \ldots, m$.

Let

$$\begin{aligned} \Phi' &= \{S_i \mid i = m+1, \ldots, s\}, \\ \Psi' &= \{T_j \mid j = 1, 2, \ldots, t-1\}. \end{aligned}$$

Clearly Φ' and Ψ' satisfy the conditions (i), (ii) and (iii) of Theorem 3.2 with s being replaced by $s-m$, and t by $t-1$. For any X_1 counted in $N(\Phi', \Psi')$, there are

$$h^m - \prod_{i=1}^{m} (h - n_i)$$

different X counted in $N(\Phi, \Psi)$ containing X_1. Since

$$L = \sum_{i=1}^{m} (h - n_i) = mh - \sum_{i=1}^{m} n_i = mh - k,$$

then

$$\begin{aligned} L - m &= m(h-1) - k \\ &= m(h-1) - q(h-1) - r \\ &= (m-q)(h-1) - r. \end{aligned}$$

It follows from the lemma that

$$\prod_{i=1}^{m}(h - n_i) \geq h^{m-q-1}(h-r).$$

Therefore,

$$\begin{aligned} N(\Phi, \Psi) &\leq \left(h^m - \prod_{i=1}^{m}(h-n_i)\right) N(\Phi', \Psi') \\ &\leq (h^m - h^{m-q-1}(h-r)) \cdot h^{s-m}\left(1 - \frac{h-r}{h^{q+1}}\right)^{t-1} \\ &= h^s\left(\frac{h-r}{h^{q+1}}\right)^t. \end{aligned}$$

This completes the proof of the theorem.

Nathanson [44] proved that the upper bound in the theorem is the best possible upper bound by giving the following example. Let $d_1, d_2, \ldots, d_s$ be positive integers such that $d_i \leq h-1$ for all i and

$$\sum_{i=1}^{s} d_i \leq k.$$

Let $S_1, S_2, \ldots, S_s$ be pairwise disjoint sets with $|S_i| = h$ for all i. Let T be a set such that $|T| = k$ and

$$|T \cap S_i| = d_i \quad \text{for} \quad i = 1, 2, \ldots, s.$$

Let

$$\Phi = \{S_1, S_2, \ldots, S_s\}, \quad \text{and} \quad \Psi = \{T\}.$$

Then

$$N(\Phi,\Psi) = h^s - \prod_{i=1}^{s}(h-d_i) = h^s\left(1-\prod_{i=1}^{s}\left(1-\frac{d_i}{h}\right)\right).$$

It is easy to see that Φ and Ψ satisfy the conditions (i), (ii) and (iii) of Theorem 3.2. Let $k = q(h-1)+r$, where $0 \le r \le h-2$. Let $s = q+1$. Let

$$d_i = h-1 \quad \text{for} \quad i = 1,2,\ldots,s-1, \quad \text{and} \quad d_s = r.$$

It is easy to see that the term on the right hand side is equal to the upper bound in Theorem 3.2.

3.4 A Further Result for Case $h = k = 3$

In this section, I shall prove the following theorem.

Theorem 3.4 *Let $r+s \ge 1$ and $t \ge 0$. Let*

$$\Phi = \{S_1, S_2, \ldots, S_{s+r}\} \quad \text{and} \quad \Psi = \{T_1, T_2, \ldots, T_t\}$$

be two families of finite sets satisfying the following conditions:

(i) $1 \le |S_i| \le 2$ *for* $i = 1,2,\ldots,r$,
$|S_{r+i}| = 3$ *for* $i = 1,2,\ldots,s$,
$1 \le |T_j| \le 3$ *for* $j = 1,2,\ldots,t$;

(ii) $S_i \cap S_{i'} = T \cap T_{j'} = \emptyset$ *for* $i \ne i'$ *and* $j \ne j'$;

(iii) $S_i \not\subseteq T_j$ *for all* i *and* j.

Then

$$N(\Phi,\Psi) \le 2^r 3^s \left(\frac{7}{8}\right)^t.$$

This is the best possible result.

Proof. Define

$$M(r,s,t) = 2^r 3^s \left(\frac{7}{8}\right)^t,$$

and let $N(r,s,t)$ denote the largest $N(\Phi,\Psi)$ where Φ and Ψ satisfy conditions(i), (ii) and (iii) in the theorem. I shall prove $N(r,s,t) \leq M(r,s,t)$ by induction on t.

If $t = 0$, then

$$N(r,s,t) = 2^r 3^s = M(r,s,0).$$

Now assume that $t \geq 1$, and that

$$N(r,s,t') \leq M(r,s,t')$$

holds for any $r+s \geq 1$ and $0 \leq t' < t$. Let

$$\Phi = \{S_1, S_2, \ldots, S_{r+s}\} \text{ and } \Psi = \{T_1, T_2, \ldots, T_t\}$$

be two families of finite sets satisfying (i), (ii) and (iii). Assume without loss of generality that

$$S = \bigcup_{i=1}^{r+s} S_i \supseteq T = \bigcup_{j=1}^{t} T_j.$$

Let S_0 be a set of two elements such that $S_0 \cap S = \emptyset$. Let $\Phi' = \Phi \cup \{S_0\}$, it is clear that Φ' and Ψ satisfy the condition (i), (ii) and (iii) with r being replaced by $r+1$, and that $N(\Phi',\Psi) = 2 \cdot N(\Phi,\Psi)$. This implies that

$$N(r+1,s,t) \geq 2N(r,s,t).$$

Similarly, we also have

$$N(r,s+1,t) \geq 3N(r,s,t).$$

It is sufficient to prove $N(r,s,t) \leq M(r,s,t)$ for sufficiently large integers r and s.

Now suppose that $r > 6t$ and $s > 3t$. Suppose $N(\Phi, \Psi) = N(r, s, t)$. Without loss of generality, we may that

$$|S_i| = 2 \quad \text{for} \quad i = 1, 2, \ldots, r,$$
$$|S_i| = 3 \quad \text{for} \quad i = r+1, \ldots, r+s,$$
$$|T_j| = 3 \quad \text{for} \quad j = 1, 2, \ldots, t.$$

There are four cases we must consider.

Case I There exists some $T_u = \{a_1, a_2, a_3\}$ such that

$$|S[a_k]| = 2 \quad \text{for} \quad k = 1, 2, 3.$$

Suppose

$$S_k = S[a_k] = \{a_k, a_k'\} \quad \text{for} \quad k = 1, \ldots, 6.$$

Since $r \geq 6t$ we may assume that $S_k \cap T = \emptyset$ for $k = 4, 5, 6$. For convenience, we write $(a_k)' = a_k'$ and $(a_k')' = a_k'' = a_k$ for $k = 1, \ldots, 6$. We also regard the subscripts of a's as elements in $\mathbf{Z}/(6)$, i.e.,

$$a_k = a_j \quad \text{and} \quad a_k' = a_j' \quad \text{if} \quad k \equiv j \bmod 6.$$

Define

$$S_k' = \{a_k, a_{k+3}'\} \quad \text{for} \quad k = 1, \ldots.$$

Let

$$\Phi' = (\Phi \backslash \{S_1, \ldots, S_6\}) \cup \{S_1', \ldots, S_6'\}.$$

It is clear that Φ' and Ψ satisfy condition (i), (ii) and (iii). Let X be a simultaneous system of representatives for Φ and Ψ. Suppose

$$X \cap S_k = \{x_k\} \quad \text{for} \quad k = 1, 2, 3.$$

Define

$$X_1 = X \setminus \bigcup_{k=1}^{6} S_k.$$

It is clear that exactly 8 simultaneous systems X of representatives for Φ and Ψ contain $\{x_1, x_2, x_3\} \cup X_1$.

Suppose

$$x_j \in S'_{k_j} \quad \text{for} \quad j = 1, 2, 3.$$

Then

$$x'_j \in S'_{k_j+3} \quad \text{for} \quad j = 1, 2, 3.$$

Hence $S[x_j] = S[x'_j]$ implies $x'_j \notin X$, and

$$S'_{k_j+3} \cap \{x_1, x_2, x_3\} = \emptyset \quad \text{for} \quad j = 1, 2, 3.$$

For any

$$x_j \in S_{k_j+3} \quad \text{for} \quad j = 4, 5, 6,$$

$X = \{x_1, \ldots, x_6\} \cup X_1$ is a simultaneous system of representatives for Φ' and Ψ containing x_1, x_2, x_3 and X_1. Since there are 8 different ways to shoose x_4, x_5, x_6, there are 8 different simultaneous systems X of representatives for Φ' and Ψ containing x_1, x_2, x_3 and X_1. Therefore, $N(\Phi, \Psi) \leq N(\Phi', \Psi)$. Hence we may assume that

$$|S[a_k] \cap T| = 1 \quad \text{for} \quad k = 1, 2, 3.$$

Let X be a simultaneous system of representatives for Φ and Ψ. Assume

$$X \cap S[a_k] = \{x_k\} \quad \text{for} \quad k = 1, 2, 3.$$

Define

$$\begin{aligned} \Phi' &= \Phi \backslash \{S[a_1], S[a_2], S[a_3]\}, \\ \Psi' &= \Psi \backslash \{T_u\}, \\ X' &= X \backslash \{x_1, x_2, x_3\}. \end{aligned}$$

It is clear that Φ' and Ψ' satisfy conditions (i), (ii) and (iii), and that X is a simultaneous system of representatives for Φ' and Ψ'. Conversely, if X' is a simultaneous system of representatives for Φ' and Ψ', then for any

$x_k \in S[a_k]$ $(k = 1, 2, 3)$, $X = \{x_1, x_2, x_3\} \cup X'$ is a simultaneous system of representatives for Φ and Ψ. Since there are only 7 different ways to choose x_1, x_2, x_3, we see that

$$\begin{aligned} N(r,s,t) &= N(\Phi,\Psi) \leq 7N(\Phi',\Psi') \\ &\leq 7N(r-3,s,t-1) \\ &\leq 7M(r-3,s,t-1) \\ &= M(r,s,t). \end{aligned}$$

Case II There exists some $T_u = \{a_1, a_2, a_3\}$ such that

$$\begin{aligned} S_k &= \{a_k, a_k'\} \text{ for } k = 1, 2, \\ S_3 &= \{a_3, a_3', a_3''\}. \end{aligned}$$

Suppose $S_4 \cap T = \emptyset$ and $S_4 = \{w, v\}$. Define

$$\begin{aligned} S_3' &= \{w, a_3', a_3''\}, \\ S_4' &= \{a_3, v\}, \\ \Phi' &= (\Phi \backslash \{S_3, S_4\}) \cup \{S_3', S_4'\}. \end{aligned}$$

Then Φ' and Ψ satisfy the conditions (i), (ii) and (iii), and the corresponding integers r and s are not changed.

Suppose that X is a simultaneous system of representatives for Φ and Ψ. Let

$$\begin{aligned} X \cap S_k &= \{x_k\} \text{ for } k = 1, 2, 3, \\ X_1 &= X \backslash (\{x_1, x_2, x_3\} \cup S_4). \end{aligned}$$

It form that $S_4 \cap T = \emptyset$ that there are two simultaneous systems X of representatives for Φ' and Ψ containing x_1, x_2, x_3 and X_1.

If $x_3 = a_3$, it is clear that there exist three simultaneous systems X of representatives for Φ' and Ψ containing x_1, x_2, x_3 and X_1. If $x_3 = a_3'$ or

a_3'', there exist two simultaneous systems X of representatives for Φ' and Ψ containing x_1, x_2, x_3 and X_1. Therefore,

$$N(r,s,t) = N(\Phi,\Psi) \leq N(\Phi',\Psi) \leq M(r,s,t),$$

by the argument in Case I.

Case III There exists some $T_u = \{a,b,c\}$ such that

$$\begin{aligned} S_1 &= S[a] = \{a,a'\}, \\ S_2 &= S[b] = \{b,b',b''\}, \\ S_3 &= S[c] = \{c,c',c''\}. \end{aligned}$$

If $a' \notin T$, then we divide the simultaneous systems X of representatives for Φ and Ψ into two classes: $a \in X$ or $a' \in X$. If $a \in X$, let

$$\Phi' = \Phi \backslash \{S_1\}, \quad \Psi' = \Psi \backslash \{T_u\}.$$

It is clear that Φ' and Ψ' satisfy condition 9i), (ii) and (iii). Let $X' = X \backslash \{a\}$. Then X' is a simultaneous system of representatives for Φ' and Ψ'. Conversely, if X' is a simultaneous system of representatives for Φ' and Ψ', then $X = X' \cup \{a\}$ is a simultaneous system of representatives for Φ and Ψ. Therefore,

$$N(\Phi',\Psi') \leq N(r-1,s,t-1).$$

If $a' \in X$, then $a \in X$. Then b or c belongs to X. A similar argument shows that there are not more than $2N(r-1,s-1,t-1)$ different X in this class. Hence,

$$\begin{aligned} N(\Phi,\Psi) &\leq N(r-1,s,t-1) + 2N(r-1,s-1,t-1) \\ &\leq M(r-1,s,t-1) + 2M(r-1,s-1,t-1) \\ &= 2^{r-1}3^s\left(\frac{7}{8}\right)^{t-1} + 2\cdot 2^{r-1}3^{s-1}\left(\frac{7}{8}\right)^{t-1} \\ &= 2^{r-1}3^{s-1}\left(\frac{7}{8}\right)^{t-1}(3+2) \\ &< 2^{r-1}3^{s-1}\left(\frac{7}{8}\right)^{t-1}\cdot 2\cdot 3\cdot\frac{7}{8} \\ &= M(r,s,t). \end{aligned}$$

If $a' \in T$, let $Y_{a'} = \{a', a_1', a_2'\}$. We may assume that

$$|S[a_1']| = |S[a_2']| = 3.$$

Let X be a simultaneous system of representatives for Φ and Ψ, then $a \in X$ or $a' \in X$. If $a \in X$, then $a' \notin X$, which implies that there is at least one of a_1', a_2' contained in X. By a similar argument as above, we see that there are at most $2N(r-1, s-1, t-1)$ different X containing a'. Therefore,

$$\begin{aligned} N(\Phi, \Psi) &\leq 4N(r-1, s-1, t-1) \\ &\leq 4M(r-1, s-1, t-1) \\ &< M(r, s, t). \end{aligned}$$

Case IV For any $T_j = \{a, b, c\}$,

$$|S[a]| = |S[b]| = |S[c]| = 3.$$

By Theorem 3.3, we have that

$$\begin{aligned} N(\Phi, \Psi) &\leq 2^r 3^s \left(\frac{7}{9}\right)^t \\ &< 2^r 3^s (78)^t = M(r, s, t). \end{aligned}$$

Now I prove that $M(r, s, t)$ is the best possible upper bound for $N(r, s, t)$. Let $r \geq 3t$. Let

$$\begin{aligned} a_i, b_i, &\quad i = 1, 2, \ldots, r. \\ u_j, v_j, w_j, &\quad j = 1, 2, \ldots, s \end{aligned}$$

be $2r + 3s$ different positive integers. Let

$$\begin{aligned} S_i &= \{a_i, b_i\} \text{ for } i = 1, \ldots, r, \\ S_{r+i} &= \{u_i, v_i, w_i\} \text{ for } i = 1, \ldots, s; \\ T_j &= \{a_j, a_{t+j}, a_{2t+j}\} \text{ for } j = 1, \ldots, t. \end{aligned}$$

It is clear that

$$\Phi = \{S_1, S_2, \ldots, S_{r+s}\} \text{ and } \Psi = \{T_1, T_2, \ldots, T_t\}$$

satisfy conditions (i), (ii) and (iii), and that

$$N(\Phi, \Psi) = 2^r 3^s \left(\frac{7}{8}\right)^t.$$

The proof is complete.

3.5 Representatives for Finite Sets

In this section, I shall prove the following theorem, which answers a question of Nathanson. By $D(\Phi)$ we denote the number of minimal systems of representatives for Φ.

Theorem 3.5 *Let $h \geq 2$ and $k \geq 1$. For any real number $\mu \in (0,1)$, there exist two families of finite sets*

$$\Phi = \{S_1, S_2, \ldots, S_s\} \text{ and } \Psi = \{T_1, T_2, \ldots, T_t\}$$

satisfying the following properties:

(i) $0 < |S_i| \leq h$ *for* $i = 1, 2, \ldots, s$;

(ii) $0 < |T_j| \leq k$ *for* $j = 1, 2, \ldots, t$;

(iii) $T_j \cap T_{j'} = \emptyset$ *for all* $j \neq j'$;

(iv) $S_i \not\subseteq T_j$ *for all* i *and* j;

(v) $N(\Phi, \Psi) > D(\Phi)\mu^t$.

Proof. Since $0 < \mu < 1$, there exists an integer t such that $\mu^t < 1/h$. Let $s = tk$. Let

$$a_1, a_2, \ldots, a_{h-1}, \ b_1, b_2, \ldots, b_s$$

be $h - 1 + s$ different elements. Define

$$\begin{aligned} S_i &= \{a_1, \ldots, a_{h-1}, b_i\} \ hboxfor \ i = 1, 2, \ldots, s; \\ T_j &= \{b_{(j-1)k+1}, \ldots, b_{jk}\} \text{ for } j = 1, 2, \ldots, t. \end{aligned}$$

Let

$$\Phi = \{S_1, S_2, \ldots, S_s\} \text{ and } \Psi = \{T_1, T_2, \ldots, T_t\}.$$

It is clear that Φ and Ψ satisfy conditions (i)–(iv) and that

$$N(\Phi, \Psi) = 1 \text{ and } D(\Phi) = h - 1 + 1 = h.$$

Therefore, we have

$$N(\Phi, \Psi) = 1 > h\mu^t = D(\Phi)\mu^t,$$

which proves the theorem.

Theorem 3.5 means that the answer to the question is negative for any $h \geq 2$ and $k \geq 1$. However, we have the following theorem.

Theorem 3.6 *Let $h \geq 2$. If*

(i) $\Phi = \{S_1, \ldots, S_s\}$ is a family of nonempty, distinct sets S_i with $|S_i| \leq h$ for all i;

(ii) Every S_i intersects at most one S_j in Φ other than S_i itself;

(iii) $\Psi = \{T_1, \ldots, T_t\}$ is a family of t sets T_j with $T_j = \{a_j\}$ for all j, where the a_j's are distinct elements;

(iv) S_i is not contained in T_j for any i and j.

Then

$$N(\Phi, \Psi) \leq D(\Phi) \left(\frac{h-1}{h}\right)^{t/2}. \tag{3.7}$$

Proof. By induction on t for any fixed s. If $t = 0$, then

$$N(\Phi, \Psi) = D(\Phi),$$

hence (3.7) holds for $t = 0$ and any s. Let $t \geq 1$. Assume that (3.7) holds for any s and any $t' < t$.

Let

$$\Phi = \{S_1, S_2, \ldots, S_s\} \text{ and } \Psi = \{T_1, T_2, \ldots, T_t\}$$

be two families of sets satisfying the conditions (i)–(iv). If there exists some $T_j = \{a_j\}$ such that $a_j \notin S_i$ for all i, then $N(\Phi, \Psi) = 0$, hence (3.7) holds for t and any s. Now we assume that

$$S = \bigcup_{i=1}^{s} S_i \supseteq \{a_1, a_2, \ldots, a_t\}.$$

We consider $T_t = \{a_t\}$. Then the following three cases may occur.

Case I There exists an i' such that $a_t \in S_{i'}$, where $S_{i'} \cap S_i = \emptyset$ for all $i \neq i'$. $S_i \not\subseteq T_t$ implies that $|S_{i'}| \geq 2$. It is readily verified that

$$\Phi' = \Phi \backslash \{S_{i'}\} \text{ and } \Psi' = \Psi \backslash \{T_t\}$$

satisfy the conditions (i)–(iv), and

$$D(\Phi) = |S_{i'}| \cdot D(\Phi').$$

If X is a simultaneous system of representatives for Φ and Ψ, then $X' = X \backslash \{a_t\}$ is a simultaneous system of representatives for Φ' and Ψ'. Conversely, if X' is a simultaneous system of representatives for Φ' and Ψ', then $X = X' \cup \{a_t\}$ is a simultaneous system of representatives for Φ and Ψ. Therefore,

$$N(\Phi, \Psi) = N(\Phi', \Psi')$$

$$\begin{aligned} &\leq D(\Phi')\left(\frac{h-1}{h}\right)^{(t-1)/2} \\ &= \frac{1}{|S_{i'}|}D(\Phi)\left(\frac{h-1}{h}\right)^{(t-1)/2} \\ &\leq \frac{1}{2}D(\Phi)\left(\frac{h-1}{h}\right)^{(t-1)/2} \\ &< D(\Phi)\left(\frac{h-1}{h}\right)^{t/2}. \end{aligned}$$

Case II there exists an i' such that $a_t \in S_{i'} \cap S_{i''}$ for some i''. It follows from (ii) that

$$(S_{i'} \cap S_{i''}) \cap S_i = \emptyset$$

for any $i : i \neq i'$ and $i \neq i''$. Let

$$|S_{i'} \cap S_{i''}| = r, \quad |S_{i'} \backslash S_{i''}| = u, \quad |S_{i''} \backslash S_{i'}| = v.$$

Since $a_t \in S_{i'} \cap S_{i''}$, it is clear that if X is a simultaneous system of representatives for Φ and Ψ, then $X \backslash \{a_t\}$ is a simultaneous system of representatives for

$$\Phi' = \Phi \backslash \{S_{i'}, S_{i''}\} \text{ and } \Psi' = \{t_j \mid j = 1, 2, \ldots, t-1\}.$$

Conversely, if X' is a simultaneous system of representatives for Φ' and Ψ', then $X = X' \cup \{a_t\}$ is a simultaneous system of representatives for Φ and Ψ. Hence

$$N(\Phi, \Psi) = N(\Phi', \Psi').$$

It is clear that

$$D(\Phi) = (r + uv)D(\Phi').$$

It follows from(iv) that $r + u \geq 2$ and $r + v \geq 2$. thus

$$\frac{1}{r+uv} \leq 1 - \frac{1}{h}.$$

Therefore,

$$N(\Phi, \Psi) = N(\Phi', \Psi')$$

$$\begin{aligned} &\leq D(\Phi')\left(1-\frac{1}{h}\right)^{\frac{t-1}{2}} \\ &= \frac{1}{r+uv}D(\Phi)\left(1-\frac{1}{h}\right)^{\frac{t-1}{2}} \\ &\leq \left(1-\frac{1}{h}\right)D(\Phi)\left(1-\frac{1}{h}\right)^{\frac{t-1}{2}} \\ &< D(\Phi)\left(1-\frac{1}{h}\right)^{\frac{t}{2}}. \end{aligned}$$

Case III There exists an i' such that

$$a_t \in S_{i'}\backslash S_{i''} \quad \text{and} \quad S_{i'} \cap S_{i''} \neq \emptyset$$

for some $i'' \neq i'$. Let

$$|S_{i'} \cap S_{i''}| = r, \quad |S_{i'}\backslash S_{i''}| = u, \quad |S_{i''}\backslash S_{i'}| = v.$$

It is clear that if there are two sets T_j such that $T_j \subseteq S_{i''}\backslash S_{i'}$, then $N(\Phi, \Psi) = 0$, hence (3.7) holds. If there exists exactly one $T_j = \{a_j\}$ such that $a_j \in S_{i''}\backslash S_{i'}$, then any simultaneous system X of representatives for Φ and Ψ contains a_t and a_j. Hence X is a simultaneous system of representatives for Φ and Ψ if and only if $X\backslash\{a_t, a_j\}$ is a simultaneous system of representatives for

$$\Phi' = \Phi\backslash\{S_{i'}, S_{i''}\} \quad \text{and} \quad \Psi' = \Psi\backslash\{T_t, T_j\}.$$

Therefore,

$$\begin{aligned} N(\Phi, \Psi) &= N(\Phi', \Psi') \\ &\leq D(\Phi')\left(1-\frac{1}{h}\right)^{\frac{t-1}{2}} \\ &= \frac{1}{r+uv}D(\Phi)\left(1-\frac{1}{h}\right)^{\frac{t-1}{2}} \\ &\leq \frac{1}{2}D(\Phi)\left(1-\frac{1}{h}\right)^{\frac{t-1}{2}} \\ &< D(\Phi)\left(1-\frac{1}{h}\right)^{\frac{t}{2}}. \end{aligned}$$

If there does not exist T_j such that $a_j \in S_{i''} \backslash S_{i'}$, i.e., if

$$(S_{i''} \backslash S_{i'}) \cap T_j = \emptyset \text{ for all } j,$$

then any simultaneous system of representatives for Φ and Ψ contains a_t and an element x of $S_{i''} \backslash S_{i'}$, hence $X \backslash \{a_t, x\}$ is a simultaneous system of representatives for

$$\Phi' = \Phi \backslash \{S_{i'}, S_{i''}\} \text{ and } \Psi' = \psi \backslash \{T_t, T_j\}.$$

Conversely, If X' is a simultaneous system of representatives for Φ' and Ψ', then $X = X' \cup \{a_t, x\}$ is a simultaneous system of representatives for Φ and Ψ for any $x \in S_{i''} \backslash S_{i'}$. It follows from $r \geq 1, 0 \leq v \leq h-1$ and $u \geq 1$ that

$$\frac{v}{r+uv} \leq 1 - \frac{1}{h}.$$

Therefore,

$$\begin{aligned} N(\Phi, \Psi) &= |S_{i''} \backslash S_{i'}| N(\Phi', \Psi') \\ &\leq v D(\Phi') \left(1 - \frac{1}{h}\right)^{\frac{t-1}{2}} \\ &= \frac{v}{r+uv} D(\Phi) \left(1 - \frac{1}{h}\right)^{\frac{t-1}{2}} \\ &\leq \left(1 - \frac{1}{h}\right) D(\Phi) \left(1 - \frac{1}{h}\right)^{\frac{t-1}{2}} \\ &< D(\Phi) \left(1 - \frac{1}{h}\right)^{\frac{t}{2}}. \end{aligned}$$

The proof is complete.

4 THIN BASES FOR GROUPS

4.1 Introduction

Let G be a group. Let $A_1, A_2, ..., A_h$ be subsets of G, $A_1A_2 \cdots A_h$ denotes the product of these subsets in G. In particular, if $A_1 = A_2 = \cdots = A_h$, we write A^h for the product $A_1A_2 \cdots A_h$. In the abelian case, we use $A_1+A_2+\cdots+A_h$ and hA instead. A subset A of G is called a *basis of order* h for G if $A^h = G$. If A is a basis of order h for a finite group G with $|G| = n$, then

$$n = |G| = |A^h| \leq |A|^h,$$

i.e., $|A| \geq n^{1/h}$. It is natural to ask if there exists a constant $c = c(h) > 0$ so that every finite group G contains a *thin* basis A of order h with $|A| \leq c|G|^{1/h}$. In fact, Rohrbach [54,55] asked this question more then fifty years 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

$$|A| \leq 2\sqrt{n \log n} + 2.$$

Recently, I have proved the existence of thin bases of order $h \geq 2$ for finite abelian groups [30] and the existence of thin bases for finite nilpotent groups [31]. This answers Rohrbach's question in the nilpotent case. In fact, I proved the following theorems:

Theorem 4.1 *Let $h \geq 2$ be any integer. Let $c_1 = h(1 + 2^{-1/h})^{h-1}$. Then every finite abelian group G contains a basis A of order h such that*

$$|A| \leq c_1 |G|^{1/h}.$$

In particular, every finite abelian group G of order n contains a basis of order 2 such that

$$|A| \leq (2 + \sqrt{2})\sqrt{n}.$$

This greatly improves Cherly's result.

Theorem 4.2 *Let $h \geq 2$ be any integer. Let $c_2 = h \cdot 2^{h-1}$. Then every finite nilpotent group G contains a basis A of order h such that*

$$|A| \leq c_2 |G|^{1/h}.$$

For arbitrary finite groups, Nathanson [49] has proved that every finite group G of order n contains a basis A of order 2 such that

$$|A| < 2\sqrt{n \cdot \log n} + 2,$$

and that, for every $h \geq 3$ and $\delta > 0$, there exists an integer $M = M(h, \delta)$ such that every finite group G of order $n \geq M$ contains a basis A of order h such that

$$|A| < (h + \delta)(n \cdot \log n)^{1/h}.$$

It is still not known if thin bases of order $h \geq 2$ exist for the class of all finite groups.

I shall present the proofs of Theorem 4.1 and 4.2 in Sections 4.2 and 4.3 respectively. I shall study the thin σ-bases for σ-finite groups in Section 4.4. In Section 4.5, I shall construct bases with given number of representations for certain infinite abelian groups. In Section 4.6, I shall discuss some applications of Theorems 4.1 and 4.2 to Cayley graphs.

4.2 Thin Bases for Finite Abelian Groups

Lemma 4.1 *Let P be a finite abelian group of order p^s, where p is a prime, and s is positive. 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

$$P = P_1 \oplus P_2 \oplus \cdots \oplus P_r, \quad \text{where} \quad |P_i| = p^{u_i}.$$

It is well known that there exists a subset S of at most $h-1$ positive integers so that

$$\sum_{i \notin S} u_i \equiv 0 \bmod h.$$

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 4.2 *If G is a finite cyclic group of order m, then there exist h subsets $A_1, \ldots, A_h$ in G such that*

$$\sum_{i=1}^{h} A_h = G \quad \textit{and} \quad |A_i| < m^{1/h} + 1 \quad \textit{for} \quad i = 1, 2, \ldots, h.$$

Proof. Let $u = \lceil m^{1/h} \rceil$, where $\lceil x \rceil$ denotes the least integer $\geq x$. Let

$$A_i = \{0, u^{i-1}, \ldots, (u-1)u^{i-1}\} \quad \text{for} \quad i = 1, 2, \ldots, h.$$

Clearly,

$$|A_i| = u < m^{1/h} + 1 \quad \text{for} \quad i = 1, 2, \ldots, h.$$

Suppose that $\sum_{i=1}^{s} A_i \supseteq [0, u^s - 1]$, where $[a, b]$ denotes the set of integers between a and b. Choose any $n : u^s \leq n < u^{s+1}$. Suppose

$$n = qu^s + r, \quad \text{where} \quad 1 \leq q \leq u-1 \quad \text{and} \quad 0 \leq r \leq u^s - 1.$$

Then $r \in \sum_{i=1}^{s} A_i$, hence

$$n = qu^s + r \in \sum_{i=1}^{s+1} A_i.$$

Therefore,

$$\sum_{i=1}^{h} A_i \supseteq [0, u^h - 1] \supseteq [0, m-1].$$

The proof of Lemma 4.3 is complete.

Proof of Theorem 4.1. Suppose that

$$G = G_1 \oplus \cdots \oplus G_r,$$

where $|G_i| = p_i^{s_i}$, $s_i > 0$, and $p_1, \ldots, p_r$ are distinct prime numbers. It follows from Lemma 4.1 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

$$H = \sum_{i=1}^{h} A_i, \quad \text{and} \quad |A_i| = m.$$

Now suppose that

$$K = K_1 \oplus \cdots \oplus K_t,$$

where $t \leq h-1$ and each K_j is cyclic. Lemma 4.2 implies that

$$K_j = A_{j1} + \cdots + A_{jh},$$

for some A_{ji} with

$$|A_{ji}| < |K_j|^{1/h} + 1 \quad \text{for} \quad i = 1, 2, \ldots, h.$$

Let

$$B_i = A_i + \sum_{j=1}^{t} A_{ji} \quad \text{for} \quad i = 1, 2, \ldots, h.$$

Then $\sum_{i=1}^{h} B_i = G$, and

$$\begin{aligned} |B_i| &= m \cdot \prod_{1 \le j \le t} (|K_j|^{1/h} + 1) \\ &\le (1 + 2^{-1/h})^t n^{1/h} \\ &\le (1 + 2^{-1/h})^{h-1} n^{1/h}. \end{aligned}$$

Define $A = B_1 \cup \cdots \cup B_h$, then A is a basis of order h for G, and

$$|A| \le \sum_{i=1}^{h} |B_i| \le h(1 + 2^{-1/h})^{h-1} n^{1/h}.$$

The proof of Theorem 4.1 is complete.

4.3 Thin Bases for Finite Nilpotent Groups

Let G be a finite group. For any subsets X and Y in G, the commutator subgroup $[X, Y]$ of X and Y is the subgroup of G generated by $xyx^{-1}y^{-1}$, $x \in X$ and $y \in Y$. The *lower central series of* G is defined by

$$L_1(G) = G, \quad L_i(G) = [L_{i-1}(G),\ G] \quad \text{for} \quad i > 1.$$

A group G is called *nilpotent* if $L_m(G) = 1$ for some m.

In order to prove Theorem 4.2, we need the following lemma.

Lemma 4.3 *If P is a p-group of order p^{uh} where u is an integer, then there exist h subsets $A_1, A_2, \ldots, A_h$ such that*

$$\prod_{i=1}^{h} A_i = P \quad \textit{and} \quad |A_i| = p^u \quad \textit{for} \quad i = 1, 2, \ldots, h.$$

Proof. Noticing that P is solvable with $|P| = p^{uh}$, we see that P possesses a normal series:

$$P = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_{uh} = 1$$

such that each H_{i-1}/H_i is a cyclic group of order p for $i = 1, 2, \ldots, uh$.

Assume that, for any i : $1 \leq i \leq uh$,

$$H_{i-1}/H_i = \{\overline{x}_{i1}, \ldots, \overline{x}_{ip}\},$$

where $\overline{x}_{ij}$ denotes the congruence class in H_{i-1} modulo H_i which contains $x_{ij} \in H_{i-1}$ for $j = 1, 2, \ldots, p$. Let

$$S_i = \{x_{i1}, \ldots, x_{ip}\}.$$

Define

$$A_j = \prod_{i=1}^{u} S_{(j-1)u+i} \quad \text{for} \quad j = 1, 2, \ldots, h.$$

Noticing that each S_i is the set of representatives of H_{i-1}/H_i, we see that

$$|A_j| = \prod_{i=1}^{u} |S_{(j-1)u+i}| = p^u \quad \text{for} \quad j = 1, 2, \ldots, h.$$

I now prove that $\prod_{i=1}^{h} A_i = P$. Let $x \in P$ be any element. Since $\overline{x} \in H_0/H_1$, we see that $x = x_{1j_1} y_1$ for some $x_{1j_1} \in S_1$ and some $y_1 \in H_1$. Since $\overline{y}_1 \in H_1/H_2$, we see that $y_1 = x_{2j_2} y_2$ for some $x_{2j_2} \in S_2$ and some $y_2 \in H_2$. Similarly, we have

$$\begin{aligned}
y_2 &= x_{3j_3} y_3, \\
y_3 &= x_{4j_4} y_4, \\
&\cdots \quad \cdots \quad \cdots \\
y_{uh-2} &= x_{uh-1,j_{uh-1}} y_{uh-1}, \\
y_{uh-1} &= x_{uh,j_{uh}} y_{uh},
\end{aligned}$$

where $x_{ij_i} \in S_i$, $y_i \in H_i$ for $i = 1, 2, \ldots, uh$. In particular, $y_{uh} = 1$. Therefore,

$$x = x_{1j_1} x_{2j_2} \cdots x_{uh,j_{uh}}.$$

Define

$$x_j = x_{(j-1)u+1} \cdots x_{ju} \quad \text{for} \quad j = 1, 2, \ldots, h.$$

Then $x_j \in A_j$ for $j = 1, 2, \ldots, h$, and

$$x = x_1 \cdots x_h \in \prod_{i=1}^{h} A_i.$$

The proof is complete.

Proof of Theorem 4.2. Let G be a finite nilpotent group of order n, where

$$n = \prod_{j=1}^{r} p_j^{u_j},$$

and $p_1, \ldots, p_r$ are distinct primes, $u_1, \ldots, u_r$ are positive integers. Because G is nilpotent, G can be written as a direct product of its Sylow subgroups (see [15]):

$$G = P_1 \otimes P_2 \otimes \cdots \otimes P_r,$$

where each P_j is the only Sylow p_j-subgroup in G for $j = 1, 2, \ldots, r$. Noticing that P_j is a p_j-group, we see that the center $Z(P_j)$ of P_j is not trivial, hence P_j possesses a normal subgroup K_j of order p_j in the center $Z(P_j)$ of P_j. Define

$$C_1 = \bigotimes_{\substack{j \\ u_j \not\equiv 0 \bmod h}} K_j.$$

Then C_1 is a normal cyclic subgroup of order

$$|C_1| = \prod_{\substack{j \\ u_j \not\equiv 0 \bmod h}} p_j$$

in the center $Z(G)$ of G. Let G_1 be the factor group G/C_1. Then G_1 is also nilpotent, and

$$|G_1| = \prod_{j=1}^{r} p_j^{u_{1j}},$$

where

$$u_{1j} = \begin{cases} u_j, & \text{if } u_j \equiv 0 \bmod h \\ u_j - 1, & \text{otherwise} \end{cases}$$

for $j = 1, 2 \ldots, r$. Apply this procedure to G_1, we obtain a normal cyclic subgroup C_2 of G_1 contained in its center $Z(G_1)$ such that the factor group $G_2 = G_1/C_2$ is of order

$$|G_2| = \prod_{j=1}^{r} p_j^{u_{2j}},$$

where

$$u_{2j} = \begin{cases} u_{1j}, & \text{if } u_{1j} \equiv 0 \bmod h \\ u_{1j} - 1, & \text{otherwise} \end{cases}$$

Continuing this procedure, we obtain two sequences of groups:

$$G_0 = G, G_1, \ldots, \quad \text{and} \quad C_1, C_2, \ldots$$

such that C_i is a normal cyclic subgroup of G_{i-1} contained in its center $Z(G_{i-1})$, and that $G_i = G_{i-1}/C_i$ is of order

$$|G_i| = \prod_{j=1}^{r} p_j^{u_{ij}},$$

where

$$u_{ij} = \begin{cases} u_{i-1,j}, & \text{if } u_{i-1,j} \equiv 0 \bmod h \\ u_{i-1,j} - 1, & \text{otherwise} \end{cases}$$

and $u_{0j} = u_j$ for $j = 1, 2, \ldots, r$.

It is clear from the construction that $C_h = 1$. Hence

$$u_{h-1,j} \equiv 0 \bmod h \quad \text{for} \quad j = 1, 2, \ldots, r.$$

Assume that

$$u_{h-1,j} = v_j h \quad \text{for} \quad j = 1, 2, \ldots, r.$$

Therefore,

$$G_{h-1} = Q_1 \otimes Q_2 \otimes \cdots \otimes Q_r,$$

where each Q_j is a p_j-group of order $|Q_j| = p_j^{v_j h}$ for $j = 1, 2, \ldots, r$. It follows from Lemma 4.3 that there exist subsets $A_{1j}, \ldots, A_{hj}$ of Q_j such that

$$\prod_{i=1}^{h} A_{ij} = Q_j \quad \text{and} \quad |A_{ij}| = p_j^{v_j} \quad \text{for} \quad i = 1, 2, \ldots, h.$$

Since C_j is a cyclic group, it then follows from Lemma 4.2 that there exist subsets $S_{1j}, \ldots, S_{hj}$ of C_j such that

$$\prod_{i=1}^{h} S_{ij} = C_j \quad \text{and} \quad |S_{ij}| < |C_j|^{1/h} + 1 \quad \text{for} \quad i = 1, 2, \ldots, h. \tag{4.1}$$

Let g be any element in G. Let $\overline{g}^{(1)}$ denote the element in $G_1 = G/C_1$, which, as a congruence class in G modulo C_1, contains g. Suppose $\overline{g}^{(1)} \in G_1, \ldots, \overline{g}^{(j)} \in G_j$ are defined. Define $\overline{g}^{(j+1)}$ as the element in $G_{j+1} = G_j/C_{j+1}$ which contains $\overline{g}^{(j)}$. It follows from the construction of G_j that any element in G_j is of the form $\overline{g}^{(j)}$, where $g \in G$. Therefore, we may assume that

$$A_{ij} = \{\overline{x}^{(h-1)} \mid x \in B_{ij}\},$$

where B_{ij} is a subset of G and $|A_{ij}| = |B_{ij}|$ for $i = 1, 2, \ldots, h$ and $j = 1, 2, \ldots, r$. Similarly we may assume that

$$S_{ij} = \{\overline{x}^{(j-1)} \mid x \in T_{ij}\},$$

where T_{ij} is a subset of G and $|S_{ij}| = |T_{ij}|$ for $i = 1, 2, \ldots, h$ and $j = 1, 2, \ldots, h-1$, and $\overline{x}^{(0)} = x$.

For any $i : 1 \leq i \leq h$, define

$$A_i = \prod_{j=1}^{r} B_{ij} \prod_{j=1}^{h-1} T_{i,h-j}.$$

Then

$$\begin{aligned}
|A_i| &= \left|\prod_{j=1}^{r} B_{ij} \prod_{j=1}^{h-1} T_{i,h-j}\right| \\
&\le \prod_{j=1}^{r} |B_{ij}| \cdot \prod_{j=1}^{h-1} |T_{i,h-j}| \\
&= \prod_{j=1}^{r} |A_{ij}| \cdot \prod_{j=1}^{h-1} |S_{ij}| \\
&= \prod_{j=1}^{r} p_j^{v_j} \cdot \prod_{j=1}^{h-1} (|C_j|^{1/h} + 1) \\
&\le |G|^{1/h} 2^{h-1}.
\end{aligned}$$

We now prove that $A_1 A_2 \cdots A_h = G$. Let g be any element in G. We are going to show that $g \in A_1 A_2 \cdots A_h$. Since

$$G_{h-1} = Q_1 \otimes \cdots \otimes Q_r,$$

we see that

$$\overline{g}^{(h-1)} = \prod_{j=1}^{r} \overline{g}_j^{(h-1)},$$

where $\overline{g}_j^{(h-1)} \in Q_j$ for $j = 1, 2, \ldots, r$. Therefore,

$$\overline{g}_j^{(h-1)} = \prod_{i=1}^{h} \overline{a}_{ij}^{(h-1)}$$

for some $a_{ij} \in B_{ij}$ for $i = 1, 2, \ldots, h$. Noticing that G_{h-1} is a direct product of Q_j $(j = 1, 2, \ldots, r)$, we see that elements from different Q_j's are commutative. Hence

$$\overline{g}^{(h-1)} = \prod_{j=1}^{r} \overline{g}_j^{(h-1)} = \prod_{i=1}^{h} \prod_{j=1}^{r} \overline{a}_{ij}^{(h-1)}$$

Since $G_{h-1} = G_{h-2}/C_{h-1}$, there exists an $f_{h-1} \in C_{h-1}$ such that

$$\overline{g}^{(h-2)} = \prod_{i=1}^{h} \prod_{j=1}^{r} \overline{a}_{ij}^{(h-2)} \cdot f_{h-1}.$$

It follws from (4.1) that

$$f_{h-1} = \prod_{i=1}^{h} t_{i,h-1}^{(h-2)},$$

where $t_{i,h-1} \in T_{i,h-1}$ for $i = 1, 2, \ldots, h$. Since C_{h-1} is a subgroup of G_{h-2} contained in its center $Z(G_{h-2})$, all $t_{i,h-1}^{(h-2)}$'s commute with all $a_{ij}^{(h-1)}$'s. Therefore,

$$\begin{aligned} g^{(h-2)} &= \prod_{i=1}^{h}\prod_{j=1}^{r} a_{ij}^{(h-2)} \cdot \prod_{i=1}^{h} t_{i,h-1}^{(h-2)} \\ &= \prod_{i=1}^{h}\Big(\prod_{j=1}^{r} a_{ij}^{(h-2)} \cdot t_{i,h-1}^{(h-2)}\Big). \end{aligned}$$

Noticing that $G_{h-2} = G_{h-3}/C_{h-2}$, there exists some $f_{h-2} \in C_{h-2}$ such that

$$g^{(h-3)} = \prod_{i=1}^{h}\Big(\prod_{j=1}^{r} a_{ij}^{(h-3)} \cdot t_{i,h-1}^{(h-3)}\Big) \cdot f_{h-2}.$$

It follws from (4.1) that

$$f_{h-2} = \prod_{i=1}^{h} t_{i,h-2}^{(h-3)},$$

where $t_{i,h-2} \in T_{i,h-2}$ for $i = 1, 2, \ldots, h$. Similarly, we see that

$$\begin{aligned} g^{(h-3)} &= \prod_{i=1}^{h}\Big(\prod_{j=1}^{r} a_{ij}^{(h-3)} \cdot t_{i,h-1}^{(h-3)}\Big) \cdot \prod_{i=1}^{h} t_{i,h-2}^{(h-3)} \\ &= \prod_{i=1}^{h}\Big(\prod_{j=1}^{r} a_{ij}^{(h-3)} \cdot t_{i,h-1}^{(h-3)} t_{i,h-2}^{(h-3)}\Big). \end{aligned}$$

Continuing this procedure, we have that $t_{ij} \in T_{ij}$ for $i = 1, 2, \ldots, h$, $j = 1, 2, \ldots, h-1$ such that

$$g^{(s-1)} = \prod_{i=1}^{h}\Big(\prod_{j=1}^{r} a_{ij}^{(h-3)} \cdot \prod_{j=1}^{h-s} t_{i,h-j}^{(s-1)}\Big), \quad \text{for } s = 1, \ldots, h.$$

In particular, we have that

$$g = g^{(0)} = \prod_{i=1}^{h}\Big(\prod_{j=1}^{r} a_{ij} \cdot \prod_{j=1}^{h-1} t_{i,h-j}\Big),$$

and this is contained in $A_1A_2\cdots A_h$. Let $A = \cup_{i=1}^{h} A_i$. Then

$$A^h \supseteq A_1A_2\cdots A_h = G.$$

The proof of Theorem 4.2 is complete.

4.4 Thin Bases for σ-finite Abelian Groups

Let G be an infinite abelian group. Use $+$ to denote the group operation. G is called *σ-finite* if there exists an ascending chain of finite subgroups of G:

$$0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n \subseteq \cdots$$

such that

$$G = \bigcup_{n=0}^{\infty} G_n = \lim_{n\to\infty} G_n.$$

It is easy to see that any countable abelian group with no element of infinite order is σ-finite.

Let $q = p^f$, p a prime, $\mathbf{F}_q$ the q-element field. It is clear that $\mathbf{F}_q[x]$ under addition is a σ-finite group by defining

$$G_n = \{g(x) \in \mathbf{F}_q[x] \mid \partial g \leq n \text{ or } g(x) = 0\}.$$

Let G be a σ-finite abelian group with the following ascending chain of finite subgroups:

$$0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n \subseteq \cdots \tag{4.2}$$

such that

$$G = \bigcup_{n=0}^{\infty} G_n.$$

A nonempty subset A of G is called a *basis of order h* for G (with respect to the chain (4.2) of finite subgroups) if for any $g \in G$ there exist h elements

$a_i \in G_n (i = 1, 2, \ldots, h)$ such that

$$g = a_1 + \cdots + a_h,$$

where n is the smallest integer n so that $g \in G_n$. Let A be any subset of G. We denote by $A(n)$ the cardinality of $A \cap G_n$. $A(n)$ depends on the chain of subgroups.

Suppose A is a basis of order h for G. By the definition, we see that $h(A \cap G_n) = G_n$, thus $A(n)^h \geq |G_n|$, i.e., $A(n) \geq |G_n|^{1/h}$. Therefore, we have the following definition.

Definition 4.1 *A basis A of order h for G is thin if there exists a constant $c > 0$ such that*

$$A(n) \leq c|G_n|^{1/h}$$

for all $n \geq 0$.

In this section, I shall prove the following theorem.

Theorem 4.3 *Let G be a σ-finite abelian group with the following ascending chain of finite subgroups:*

$$0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n \subseteq \cdots,$$

where $G = \bigcup_{n=0}^{\infty} G_n$. Let

$$k_{n+1} = [G_{n+1} : G_n] \quad \text{for} \quad n = 0, 1, \ldots.$$

If $\{k_n\}$ is bounded, then there exists a thin basis A of order h for G.

To prove this theorem, we need the following lemma.

Lemma 4.4 *If $\{x_n\}$ is a bounded sequence of positive numbers, then there exists a partition π of $\mathbf{N}$ into h pairwise disjoint subsets $I_1, \ldots, I_h$ such that, for each i, the sequence $\{y_{in}\}$ defined by*

$$y_{in} = h \cdot \sum_{n \geq m \in I_i} x_m - \sum_{m=1}^{n} x_m$$

is bounded.

Proof. Suppose $x_n \le M$ for all n. Let $I_{i0} = \emptyset$ for $i = 1, 2, \dots, h$. Suppose $I_{1n}, \dots, I_{hn}$ are defined and satisfy the following conditions:

(i) $\{I_{1n}, \dots, I_{hn}\}$ is a partition of $\{1, 2, \dots, n\}$;

(ii) $\left| \sum_{m \in I_{in}} x_m - \sum_{m \in I_{i'n}} x_m \right| \le M$ for any i and i'.

Let τ be the smallest number such that

$$\sum_{m \in I_{\tau n}} x_m = \min_{q \le i \le h} \sum_{m \in I_{in}} x_m. \tag{4.3}$$

Then define

$$I_{i,n+1} = I_{in} \text{ if } i \ne \tau, \quad \text{and} \quad I_{\tau,n+1} = I_{\tau n} \cup \{n+1\}.$$

It is clear from (i) that $\{I_{1,n+1}, \dots, I_{h,n+1}\}$ is a partition of $\{1, 2, \dots, n+1\}$. We need to show that for any $i \ne i'$,

$$\left| \sum_{m \in I_{i,n+1}} x_m - \sum_{m \in I_{i',n+1}} x_m \right| \le M.$$

It follows from (ii) that it is enough to show that

$$\left| \sum_{m \in I_{\tau n}} x_m + x_{n+1} - \sum_{m \in I_{in}} x_m \right| \le M$$

for any $i \ne \tau$. Noticing (4.3), we see that

$$0 \le \sum_{n \in I_{in}} x_m - \sum_{m \in I_{\tau n}} x_m \le M,$$

and so

$$\left| \sum_{m \in I_{in}} x_m - \sum_{m \in I_{\tau n}} x_m - x_{n+1} \right| \le M.$$

Thus $I_{1,n+1}, \ldots, I_{h,n+1}$ satisfy conditions (i) and (ii) with n being replaced by $n+1$. Therefore, for any positive integer n, the partition $\{I_{1n}, \ldots, I_{hn}\}$ of N satisfies properties (i) and (ii). For any $1 \leq i \leq h$, let

$$I_i = \bigcup_{n=1}^{\infty} I_{in}.$$

I shall show that $I_1, \ldots, I_h$ satisfy the condition of Lemma 4.4.

For any n, it follows from (i) and (ii) that

$$\begin{aligned} |y_{in}| &= \left| h \cdot \sum_{m \in I_{in}} x_m - \sum_{m=1}^{n} x_m \right| \\ &= \left| \sum_{s=1}^{h} \sum_{m \in I_{sn}} x_m - h \cdot \sum_{m \in I_{in}} x_m \right| \\ &\leq \sum_{\substack{1 \leq s \leq h \\ s \neq i}} \left| \sum_{m \in I_{sn}} x_m - \sum_{m \in I_{in}} x_m \right| \\ &\leq (h-1)M. \end{aligned}$$

i.e., $\{y_n\}$ is bounded. This proves the lemma.

Proof of Theorem 4.3 Assume without loss of generality that G_n is a proper subgroup of G_{n+1} for all n. Let

$$x_n = \log k_n \quad \text{for} \quad n = 1, 2, \ldots .$$

Since $\{k_n\}$ is bounded and $k_n \geq 2$, we see that $\{x_n\}$ is a bounded sequence of positive real numbers. It follows from Lemma 4.4 that there exists a partition π of N into h pairwise disjoint subsets $I_1, \ldots, I_h$ such that, for any i, the sequence $\{y_{in}\}$ defined by

$$y_{in} = h \cdot \sum_{\substack{m \in I_i \\ m \leq n}} x_m - \sum_{m=1}^{n} x_m$$

is bounded. Suppose $|y_{in}| \le M$ for all n. Then

$$\prod_{\substack{m\in I_i\\ m\le n}} k_m \le e^{M/h}\cdot |G_n|^{1/h} \tag{4.4}$$

for $i = 1, 2, \ldots, h$.

For any $n \ge 1$, assume

$$G_n/G_{n-1} = \{\overline{g}_{n1}, \ldots, \overline{g}_{nk_n}\},$$

where $\overline{g}_{nj}$ denotes the congruence class in G_n containing $g_{nj} \in G_n$ for $j = 1, 2, \ldots, k_n$, and $g_{n1} = 0$. Let

$$S_n = \{g_{n1}, \ldots, g_{nk_n}\}.$$

Define

$$B_{in} = \sum_{\substack{m\in I_i\\ m\le n}} S_m \quad \text{for} \quad i = 1, 2, \ldots, h.$$

Then

$$\sum_{i=1}^{h} B_{in} = \sum_{i=1}^{h}\sum_{\substack{m\in I_i\\ m\le n}} S_m = \sum_{m=1}^{n} S_m = G_n, \tag{4.5}$$

It follows from (4.4) that

$$|B_{in}| \le \prod_{\substack{m\in I_i\\ m\le n}} |S_m| = \prod_{\substack{m\in I_i\\ m\le n}} k_m \le e^{M/h}\cdot |G_n|^{1/h}. \tag{4.6}$$

Define $B_i = \bigcup_{n=1}^{\infty} B_{in}$ for any $i \ge 1$. Then $|B_i \cap G_n| = |B_{in}|$. Let $A = \sum_{i=1}^{h} B_i$. It follows from (4.5) and (4.6) that A is a basis of order h for G and

$$\begin{aligned} |A\cap G_n| &\le \sum_{i=1}^{h} |A\cap G_n| = \sum_{i=1}^{h} |A_{in}| \\ &\le h\cdot e^{M/h}|G_n|^{1/h} = c_1|G_n|^{1/h}. \end{aligned}$$

Therefore, A is a thin σ-basis of order h for G with respect to $\{G_n\}$. The proof is complete.

Corollary 4.3.1 *Let $\mathbf{F}_q[x]$ be the additive group of the polynomial ring over the finite field $\mathbf{F}_q$ of q elements. there exists a thin σ-basis A of order $h \geq 2$ for $\mathbf{F}_q[x]$.*

Proof. Let $G_n = \{f \in \mathbf{F}_q[x] \mid \partial f \leq n\}$. Then G_n is finite and $k_n = [G_n : G_{n-1}]$ is bounded. By Theorem 4.3, there exists a thin σ-basis of order h for $\mathbf{F}_q[x]$.

Let $G = \bigcup_{n=1}^{\infty} G_n$ be a σ-finite abelian group. If $\{G_{n_k}\}$ is a subsequence of $\{G_n\}$, then any thin σ-basis of order h with respect to $\{G_n\}$ is a thin σ-basis of order h with respect to $\{G_{n_k}\}$. The following corollary follows from Theorem 4.3 and this simple fact.

Corollary 4.3.2 *Let $\mathbf{P}$ be a finite set of prime numbers. If G is a σ-finite abelian group in which the order of any element is a product of primes in $\mathbf{P}$ with repetitions allowed, then there exists a thin σ-basis of order $h \geq 2$ for G with respect to any increasing sequence of finite subgroups of G.*

Proof. Let $G = \bigcup_{n=1}^{\infty} G_n$, where $0 = G_0 \subset G_1 \subset \cdots$ is a sequence of finite subgroups of G. Since the order of any element in G is a product of primes in $\mathbf{P}$, We see that there exists an increasing sequence $\{H_n\}$ of finite subgroups of G such that $\{H_n\}$ contains $\{G_n\}$ as a subsequence, and such that every index $k_n = [H_n : H_{n-1}]$ is a prime in $\mathbf{P}$ for $n = 1, 2, \ldots$. Therefore, $\{k_n\}$ is bounded, and it follows form Theorem 4.3 that there exists a thin σ-basis A of order h for G with respect to the sequence $\{H_n\}$. Therefore, A is a thin σ-basis of order h for G with respect to the sequence $\{G_n\}$. This proves the corollary.

This suggests the following problem. Let $G = \bigcup_{n=1}^{\infty} G_n$ be a σ-finite abelian group. If there are infinitely many prime numbers appearing as factors of the indices $k_n = [G_n : G_{n-1}]$, then does there exist a thin σ-basis of order

h for G with respect to $\{G_n\}$? In particular, let G be the direct sum of all $\mathbf{Z}_p$, p prime:

$$G = \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5 \oplus \cdots.$$

Does G contain a thin σ-basis of order h? We can prove the existence of thin σ-bases of order h for certain σ-finite abelian groups with infinitely many prime numbers appearing as factors of the indices k_n.

4.5 Bases with Given Number of Representations

Let A be a basis of order h. Denote by $r_{h,A}(n)$ the number of different representations of n as a sum of h not necessarily distinct elements in A. In 1941, Erdös and Turán [14] conjectured that

$$\limsup_{n\to\infty} r_{h,A}(n) = +\infty$$

for any basis A of order h. This has not been proved or disproved even for the simplest case $h = 2$. Recently, Ruzsa [56] proved that there exists a basis A of order two such that

$$\sum_{n\le N} r_{h,A}(n)^2 = O(N).$$

The problem still remains unsolved. However, the analogue of Erdös-Turán Conjecture does hold for some semigroups. Erdös [5] proved the analogue conjecture for multiplicative semigroup $(\mathbf{N}^+, \cdot)$. Nešetřil and Rödl [50] used Ramesay's Theorem to give a very simple proof of Erdös's result. Nathanson [42] had some generalizations of this result. Nathanson also proved the analogue conjecture holds for the semigroup $(\mathbf{N}, LCM)$, where LCM is the least common multiple. A commutative semigroup is said to be a *prime semigroup* if it contains an infinite prime set and it has only finitely many

units. Puš [53] recently proved that the analogue of Erdös-turán conjecture does hold for every prime semigroup.

On the other hand, Puš [52] recently proved that the analogue conjecture is false for certain infinite groups.

Theorem 4.4 (Puš) [1] *Let G be a countably infinite abelian group. Let $f : G \to \mathbf{N}$ be any function from G into positive integers. If for any $a \in G$ and any $2 \leq r \leq 4$, the equation $x^r = a$ has only finitely many solutions in G, then there exists a basis A of order 2 for G such that $r_{2,A}(n) = f(n)$.*

In this section, I shall show that the analogue conjecture is not true for every infinite abelian group. The basic idea in this section is based on a discussion with Professors Erdös and Nathanson.

For convinience, we use $f_A(n)$ to denote $r_{2,A}(n)$.

Theorem 4.5 *Suppse that $G = F \oplus \mathbf{Z}_2^\infty$, where F is a finite group. Let $f : G\backslash F \to \mathbf{N}^+$ be any function such that $f(x) \geq 2$ for all $x \in G\backslash F$. Then there exists a bsis A of order 2 for G such that $f_A(x) = f(x)$ for all $x \in G\backslash F$.*

Proof. Order the elements in $G\backslash F$, say $G\backslash F = \{a_1, a_2, \ldots\}$. Any element in G can be regarded as an infinite dimensional vector. Let $x \in G$. By $v(x)$ we denote the largest number v such that the vth coordinate of x is not zero. For $n > 1$, u_n denotes the nth unit vector, whose nth coordinate is 1 and all other coordinates are zero, i.e., $u_n = (0, \ldots, 0, 1, 0, \ldots)$.

Pick up an integer n such that $n > v(a_1)$. Define

$$x_{1,i} = a_1 + u_{n+i}, \quad \text{and} \quad y_{1,i} = u_{n+i} \quad \text{for} \quad i = 0, 1, 2, \ldots, f(a_1) - 1.$$

Then

$$x_{1,i} = y_{1,i} = a_1 \quad \text{for} \quad i = 0, 1, \ldots, f(a_1) - 1.$$

[1] In fact, this is a special case of his theorem.

Let

$$A_1 = F \cup \{x_{1,i}, y_{1,i} \mid i = 0, 1, \ldots, f(a_1) - 1\}.$$

Clearly $f_{A_1}(a_1) = f(a_1)$. Noticing that

$$\{i,j\} \neq \{i',j'\} \text{ implies } \begin{cases} x_{1,i} + x_{1,j} \neq y_{1,i'} + y_{1,j'}, \text{ and} \\ x_{1,i} + y_{1,j} \neq x_{1,i'} + y_{1,j'} \end{cases},$$

we see that $f_{A_1}(x) \leq 2$ for every $x \in G\backslash(\{a_1\} \cup F)$.

Suppose that A_s has been constructed so that

(i) $f_{A_s}(a_j) = f(a_j)$ for $j = 1, 2, \ldots, s$, and

(ii) $f_{A_s}(x) \leq 2$ for every $x \in G\backslash(\{a_1, \ldots, a_s\} \cup F)$.

If $f_{A_s}(a_{s+1}) = f(a_{s+1}) = 2$, then define $A_{s+1} = A_s$. It is clear that A_{s+1} also possesses properties (i) and (ii) above with s being replaced by $s+1$. Now suppose that $f_{A_s}(a_{s+1}) < f(a_{s+1})$. Let $r = f(a_{s+1}) - f_{A_s}(a_{s+1})$. Pick up an integer n such that $n > v(a_{s+1})$ and $n > v(x)$ for all $x \in A_s$. Define

$$x_{s+1,i} = a_{s+1} + u_{n+i} \text{ and } y_{s+1,i} = u_{n+i}$$

for $i = 0, 1, \ldots, r-1$, and define

$$A_{s+1} = A_s \cup \{x_{s+1,i}, y_{s+1,i} \mid i = 0, 1, \ldots, r-1\}.$$

Let $\alpha, \alpha', \beta, \beta'$ be four distinct elements in A_{s+1} such that $\alpha \notin A_s$. It follows from the construction that, except $a_{s+1} = x_{s+1,i} + y_{s+1,i}$ for $i = 0, 1, \ldots, r-1$, the only possible equalities in the form $\alpha + \alpha' = \beta + \beta'$ are as follows:

$$\begin{aligned} x_{s+1,i} + x &= y_{s+1,i} + y, \text{ where } x, y \in A_s \text{ and } 0 \leq 1 \leq r-1; \\ x_{s+1,i} + x_{s+1,j} &= y_{s+1,i} + y_{s+1,j}, \text{ where } 0 \leq i, j \leq r-1,\ i \neq j; \\ x_{s+1,i} + y_{s+1,j} &= x_{s+1,j} + y_{s+1,i}, \text{ where } 0 \leq i, j \leq r-1,\ i \neq j. \end{aligned}$$

Thus $f_{A_{s+1}}(a_{s+1}) = f(a_{s+1})$, and $f_{A_{s+1}}(x) \leq 2$ for all $x \in G\backslash(F \cup A_s)$. This means that A_{s+1} also satisfies (i) and (ii) with s being replaced by $s+1$.

Define $A = \bigcup_{s=1}^{\infty} A_s$. For any $s \geq 1$, it is clear that $f_{A_s}(a_i) = f_A(a_i)$ for all $i \leq s$. Therefore, $f_A(a_i) = f(a_i)$ for $i = 1, 2, \ldots$. The proof is complete.

On the other hand, we can construct a basis A for the group $G = F \oplus \mathbb{Z}_2^\infty$ with $f_A(x) = 1$ for all $x \in G \backslash F$.

Theorem 4.6 *Suppose $G = F \oplus \mathbb{Z}_2^\infty$, where F is a finite group. Then there exists a basis A of order 2 for G such that $f_A(x) = 1$ for all $x \in G \backslash F$.*

Proof. As in the proof of the theorem above, $v(x)$ denotes the largest number v such that the vth coordinate is not zero, and u_n denotes the nth unit vector. Suppose $G \backslash F = \{a_1, -a_1, a_2, -a_2, \ldots\}$.

Define $A_1 = F \cup \{x, y, -x\}$, where $x = a_1 + u_n$, $y = u_n$, and $n > v(a_1)$. It is clear that $x + y = a_1$, and $-x + y = -a_1$. (If $2a_1 = 0$, then $2x = 0$). It is clear that $f_{A_1}(a_1) = f_{A_1}(-a_1) = 1$ and $f_{A_1}(x) \leq 1$ for all $x \in G \backslash (F \cup \{a_1\})$. Suppose that A_s has been constructed so that

(i) $f_{A_s}(\pm a_i) = 1$ for $i = 1, 2, \ldots, s$, and

(ii) $f_{A_s}(x) \leq 1$ for all $x \in G \backslash (F \cup \{\pm a_1, \ldots, \pm a_s\})$,

(iii) A_s is symmetric, i.e., $w \in A_s$ implies $-w \in A_s$.

It follows from (iii) that $f_{A_s}(a_{s+1}) = f_{A_s}(-a_{s+1})$. If $f_{A_s}(\pm a_{s+1}) = 1$ then define $A_{s+1} = A_s$. Otherwise, pick up an integer n such that $n > v(w)$ for every $w \in A_s \cup \{a_{s+1}\}$, and define

$$A_{s+1} = A_s \cup \{x, y, -x\}, \quad \text{where} \quad x = a_{s+1} + u_n, \; y = u_n.$$

Then $\pm x + y = \pm a_{s+1}$. If $\pm x + w = y + w'$ for some $w, w' \in A_s$, then $\pm a_{s+1} + w = w'$, thus $\pm a_{s+1} = -w + w'$, which contradicts the fact $f_{A_s}(\pm a_{s+1}) = 0$. Therefore, A_{s+1} also satisfies conditions (i), (ii) and (iii) with s being replaced by $s+1$. Define $A = \bigcup_{s=1}^{\infty} A_s$. Then $f_A(\pm a_i) = 1$ for all i. It is clear that $2A = G$. The proof is complete.

Theorem 4.7 *Suppose that $G = F \oplus \mathbb{Z}_3^\infty$ or $G = F \oplus \mathbb{Z}_4^\infty$, where F is a finite group. If f is a function from G into positive integers such that $f(x) \geq 2$ for all $x \in G$, then there exists a basis A of order 2 for G such that $f_A(x) = f(x)$ for all $x \in G$.*

Proof. First we consider $G = F \oplus \mathbb{Z}_3^\infty$. Assume that $G = \{a_1, a_2, \ldots\}$. Pick up an integer n such that $n > v(a_1)$. Let

$$A_1 = \{x_i, y_i \mid i = 0, 1, \ldots, f(a_1) - 1\},$$

where

$$x_i = a_1 + u_{n+i}, \quad y_i = 2u_{n+i} \quad \text{for} \quad i = 0, 1, \ldots, f(a_1) - 1.$$

Then $x_i + y_i = a_1$ for all i. It is clear that $x_i + y_j$, $2x_i$, and $2y_i$ are distinct elements in G if $i = \neq j$, and none of these sums is equal to a_1. Therefore, $f_{A_1}(a_1) = f(a_1)$ and $f_{A_1}(x) \leq 2$ for all $x \in G \backslash \{a_1\}$. Assume that A_s has been constructed with the following properties:

(i) $f_{A_s}(a_i) = f(a_i)$ for $i = 1, 2, \ldots, s$;

(ii) $f_{A_s}(a_i) \leq 2$ for $i \geq s + 1$.

If $f_{A_s}(a_{s+1}) = f(a_{s+1}) = 1$, then define $A_{s+1} = A_s$. Now suppose that $r = f(a_{s+1}) - f_{A_s}(a_{s+1}) > 0$. Let $n > v(x)$ for all $x \in A_s \cup \{a_{s+1}\}$. Let

$$x_i = a_{s+1} + u_{n+i}, \quad y_i = 2u_{n+i} \quad \text{for} \quad i = 0, 1, \ldots, r - 1.$$

Define

$$A_{s+1} = A_s \cup \{x_i, y_i \mid i = 0, 1, \ldots, r - 1\}.$$

It is easily verified that $f_{A_{s+1}}(a_{s+1}) = f(a_{s+1})$, and that $f_{A_{s+1}}(a_{s+1}) = f(a_{s+1})$, and that $f_{A_{s+1}}(a_i) \leq 2$ for all $i \geq s + 2$. This means that A_{s+1} also satifies (i) and (ii) with s being replaced by $s + 1$. Define $A = \bigcup_{s=1}^{\infty} A_s$. Therefore $f_A(a_i) = f(a_i)$ for $i = 1, 2, \ldots$.

The case of $G = F \oplus \mathbf{Z}_4^\infty$ can be proved in a similar way. The proof is complete.

If G contains an element of order infinity, it is easy to show that G contains a basis A of order 2 so that $f_A(x) = f(x)$ for all $x \in G$, where f is any given function from G into positive integers. For torsion abelian groups, we have the following theorem.

Theorem 4.8 *Suppose that G is an abelian group. If G can be written as a direct sum*

$$G = G_0 \oplus G_1 \oplus G_2 \oplus \cdots$$

such that each G_i is a cyclic subgroup of order ≥ 5, then, for any function f from G into positive integers, there exists a basis A of order 2 for G such that $f_A(x) = f(x)$ for all $x \in G$.

Proof. Suppose $G = \{a_1, a_2, \ldots\}$. Let $n > v(a_1)$. Let $A_1 = \{x_i, y_i \mid i = 0, 1, \ldots, f(a_1) - 1\}$, where $x_i = a_1 + u_{u+i}$ for $i = 0.1\ldots., f(a_1) - 1$. Then $x_i + y_i = a_1$ for all i. Noticing that u_{n+i} is of order ≥ 5, we see that $f_{A_1}(a_1) = f(a_1)$ and $f_{A_1}(x) \leq 1$ for all $x \in G\backslash\{a_1\}$. Assume that A_s has been constructed with the following properties:

(i) $f_{A_s}(a_i) = f(a_i)$ for $i = 1, 2, \ldots, s$;

(ii) $f_{A_s}(a_s) \leq 1$ for $i \geq s + 1$.

If $f_{A_s}(a_{s+1}) = f(a_{s+1}) = 1$, then define $A_{s+1} = A_s$. Otherwise, define

$$A_{s+1} = A_s \cup \{a_i, y_i \mid i = 0, 1, \ldots, f(a_{s+1}) - 1\},$$

where

$$x_i = a_{s+1} + u_{n+i} \text{ and } y_i = -u_{n+i} \text{ for } i = 0, 1, \ldots, f(a_{s+1}) - 1,$$

and $n > v(w)$ for $w \in A_s \cup \{a_1, \ldots, a_s\}$. Noticing that u_{n+i} is of order ≥ 5, we see that $f_{A_{s+1}}(a_{s+1}) = f(a_{s+1})$ and $f_{A_{s+1}}(a_i) \leq 1$ for $i \geq s+1$. Hence A_{s+1} also satisfies (i) and (ii) with s being replaced by $s+1$. Define

$$A = \bigcup_{s=1}^{\infty} A_s,$$

then $f_A(x) = f(x)$ for all $x \in G$. The proof is complete.

The finite case is different. In fact, for any constant M, there exists a finite abelian group G such that $\max f_{h,A} > M$ for any basis A. Let $G = \mathbf{Z}_h^m$, where $\mathbf{Z}_h$ is the group of $\mathbf{Z}$ modulo h. If A is a basis of order h for G, then

$$f_A(0) \geq |A| > |G|^{1/h},$$

which is not bounded by any absolute constant. Furthermore, we may find a nonzero element x_0 with $f_A(x_0)$ large. In the case $h \geq 3$, we consider the group $G = \mathbf{Z}_{h-1}^m$. Let A be any basis of order h for G. It is clear that

$$f_A(x) \geq |A| > |G|^{1/h} \quad \text{for every} \quad x \in A.$$

In the case $h = 2$, we have the following theorem.

Theorem 4.9 *Let M be any positive number. There exists a finite group G such that, for every basis A of order 2, there exists a nonzero element x_0 such that $f_A(x_0) > M$.*

Proof. Let $M > 0$ be any number. Let m be an integer such that

$$\frac{2^m}{M} - M^2 > (3 \cdot 2^m)^{3/4} \quad \text{and} \quad \sqrt{3} \cdot 2^{m/2} - 1 > 2M. \tag{4.7}$$

Let $G = \mathbf{Z}_3 \oplus (\mathbf{Z}_2^m$. Then $|G| = 3 \cdot 2^m$. Let A be any basis of order 2 for G. Let

$$\Gamma_i = \{(i, a_1, \ldots, a_m) \in G\} \quad \text{and} \quad A_i = \Gamma_i \cap A$$

for $i = 0, 1, 2$. Then $|A| = \sum |A_i|$. If $|A| > |G|^{3/4}$, then

$$\sum_{x \in G} f_A(x) = \frac{1}{2}|A|^2 + \frac{1}{2}|A| > \frac{1}{2}(|G|^{3/2} + |A|). \tag{4.8}$$

Notice that, if $0 = a + b$ with $a, b \in A$, then either $a, b \in A_0$ or one of a and b is in A_1 and the other is in A_2. In the later case, if $0 = a + b = a' + b'$ and $a, a' \in A_1, b, b' \in A_2$, and if $a \neq a'$, then $b \neq b'$. Therefore,

$$f_A(0) \leq |A_0| + \min\{|A_1|, |A_2|\} \leq |A|.$$

It follows from (4.8) that

$$\sum_{\substack{x \neq 0 \\ x \in G}} f_A(x) > \frac{1}{2}(|G|^{3/2} - |A|) \geq \frac{1}{2}(|G|^{3/2} - |G|).$$

Noticing (4.7), we see that there exists at least one nonzero element $x_0 \in G$ such that

$$f_A(x_0) > \frac{1}{2}\left(\sqrt{|G|} - 1\right) = \frac{1}{2}\sqrt{3} \cdot 2^{m/2} - \frac{1}{2} > M.$$

This shows the existence of x_0 in the case $|A| > |G|^{3/4}$.

Now assume that $|A| \leq |G|^{3/4}$. It is clear that if either $|A_1| \geq M$ or $|A_2| \geq M$ then the proof is done. If $|A_1| < M$ and $|A_2| < M$, noticing (4.7) and

$$\Gamma_1 = 2A_2 \cup (A_0 + A_1),$$

we see that

$$|A_0| \geq \frac{2^m}{M} - M^2 > (3 \cdot 2^m)^{3/4} = |G|^{3/4}.$$

The proof is complete.

4.6 Applications to Cayley Graphs

Let Γ be a given nontrivial finite group with S a generating set for Γ. We associate a digraph with Γ and S called the *Cayley graph* of Γ generated by S and denote by $G(\Gamma, S)$. The vertex set of $G(\Gamma, S)$ is the set of group elements of Γ, and x is adjacent to y if and only if $yx^{-1} \in S$.

Let G be a graph. The *distance* between two vertices x and y, denoted $d(x, y)$ is the length of a shortest path from x to y. The *diameter* $d(G)$ of the graph G is the maximum distance between two vertices of the graph.

We are interested in finding a smallest generating set S of the Cayley graph $G = G(\Gamma, S)$ with given finite group Γ and the diameter d. In other words, for any finite group Γ, and an integer $d \geq 2$, we are interested in a smallest subset S such that the diameter $d(G(\Gamma, S)) \leq d$.

This problem arises quite naturally in the study of computer networks. Elements in the group represent the stations or processors, the generating set S represents the links between stations or processors, and the diameter of the graph represents the maximum number of links to be used to transmit a message within the network. For more problems and results, see Bermond, Comellas and Hsu [3] and Erdös and Hsu [9].

Let Γ be a finite group of order n. Let $G = G(\Gamma, S)$ be the Cayley graph of Γ generated by S. If the diameter of the G is d, then $n \leq |S|^d$, i.e., $|S| \geq n^{1/d}$. Naturally, we have the following question: For any $d \geq 2$, is there a constant $c = c(d) > 0$ such that every finite group Γ contains a subset S such that

$$d(G(\Gamma, S)) \leq d \quad \text{and} \quad |S| \leq c|\Gamma|^{1/d}?$$

It follows from Lemma 4.5 below that this is another version of Rohrbach's question on the existence of thin bases for finite groups.

I shall prove that such constant exists for the class of finite abelian groups and the class of finite nilpotent groups.

Lemma 4.5 *Let Γ be a finite group, S a subset of Γ. Then S is a basis of order d for Γ if and only if $d(G(\Gamma, S)) \leq d$.*

Proof. Suppose that S is basis of order d for Γ. Let $x, y \in \Gamma$. Then there exist d elements $a_1, a_2, \ldots, a_d$ in S such that

$$yx^{-1} = a_1 a_2 \cdots a_d.$$

Define

$$\begin{aligned} x_0 &= x, \\ x_i &= a_{d-i+1} x_{i-1} \text{ for } i = 1, 2, \ldots, d. \end{aligned}$$

Then

$$x_d = a_1 x_{d-1} = a_1 a_2 x_{d-2} = \cdots = a_1 a_2 \cdots a_d \cdot x = y$$

and

$$x_{i-1} x_i^{-1} = a_{d-i+1} \in S \text{ for } i = 1, 2, \ldots, d.$$

Therefore, $d(x, y) \leq d$, hence the diameter of the $G(\Gamma, S)$ is $\leq d$.

Conversely, suppose that $d(G(\Gamma, S)) = d$. we need to show that S is a basis of order d for Γ. Let $x \in \Gamma$. Then there exists a path from the identity element 1 to x with distance $\leq d$:

$$1 = x_0, x_1, \ldots, x_d = x$$

in the graph, i.e. ,

$$x_i x_{i-1}^{-1} = a_i \in S \text{ for } i = 1, 2, \ldots, d.$$

Then

$$x = a_d a_{d-1} \cdots a_2 a_1 \in S^d.$$

Hence S is a basis of order d for Γ. The proof of the lemma is complete.

Theorem 4.10 *Let $d \geq 2$. Let $c_1 = d(1 + 2^{-1/d})^{d-1}$. Then every finite abelian group Γ contains a subset S such that*

(i) the diameter of the Cayley graph $G(\Gamma, S)$ is d;

(ii) $|S| \leq c_1|\Gamma|^{1/d}$.

Proof. It follows immediately from Lemma 4.5 and Theorem 4.1.

Theorem 4.11 *Let $d \geq 2$. Let $c_2 = d \cdot 2^{d-1}$. Then every finite nilpotent group Γ contains a subset S such that*

(i) the diameter of the Cayley graph $G(\Gamma, S)$ is d;

(ii) $|S| \leq c_2|\Gamma|^{1/d}$.

Proof. It follows immediately from Lemma 4.5 and Theorem 4.2.

Using Lemma 4.5 and the results by Nathanson [49] on thin bases for finite groups, which I mentioned in the Introduction of this chapter, we have the following theorems.

Theorem 4.12 *Every finite group Γ of order n contains a subset S such that*

(i) the diameter of the Cayley graph $G(\Gamma, S)$ is two;

(ii) $|S| \leq 2\sqrt{n \cdot \log n} + 2$.

Theorem 4.13 *Let $d \geq 3$, $\delta > 0$. Then there exists an integer $M = M(d, \delta)$ such that every finite group Γ of order n contains a subset S such that*

(i) the diameter of the Cayley graph $G(\Gamma, S)$ is d;

(ii) $|S| \leq (d + \delta)(n \cdot \log n)^{1/d}$.

References

[1] J. Cherly, On complementary sets of group elements, *Arch. Math.*, **35**(1980), 313–318.

[2] J. Cherly and J.-M. Deshouillers, Un théorème d'addition dans $\mathbf{F}_q[x]$, *preprint.*

[3] J.-C. Bermond, F. Comellas and D. F. Hsu, Distributed loop computer networks: a survey, *to appear.*

[4] M. Deza and P. Erdös, Extension de quelques theoremes sur les densities de series d'elements de **N** a des series de sousensembles finis de **N**, *Discrete Math.*, **12**(1975), 295–308.

[5] P. Erdös, On the multiplicative representation of integers, *Israel J. Math.* **2**(1964), 251-261.

[6] P. Erdös, Personal communication, 1989.

[7] P. Erdös and R. L. Graham, *Old and New Problems and Results in Combinatorial Number theorey*, L'enseignement Matheématique, Universitè de Genève, 1980.

[8] P. Erdös and R. L. Graham, On bases with an exact order, *Acta Arith.*, **37**(1980), 201–207.

[9] P. Erdös and F. Hsu, Distributed loop network with minimum transmission delay, *to appear.*

[10] P. Erdös and M. B. Nathanson, Oscillations of bases for the natural numbers, *Proc. Amer. Math. Soc.*, **35**(1975), 253–258.

[11] P. Erdös and M. B. Nathanson, Systems of distinct representatives and minimal bases in additive number theory, in: Proceedings, Number theory, Carbondale 1979 (M. B. Nathanson ed.), *Lecture Notes in Mathematics*, **751**, Springer-Verlag, Berlin and New York, 1979, 89–107.

[12] P. Erdös and M. B. Nathanson, Problems and results on minimal bases in additive number theory, *Lecture Notes in Mathematics*, **1240**, Springer-Verlag, Berlin 1987, 87-96.

[13] P. Erdös and M. B. Nathanson, Additive bases with many representations, *preprint.*

[14] P. Erdös and P. Turán, On a problem of Sidon in additive number theory and some related questions, *J. London Math. Soc.*, **16**(1941), 212-215.

[15] D. Gorenstein, *Finite Groups*, Harper & Row, Publishers, New York, 1968.

[16] G. Grekos, *Quelques Aspects de la Théorie Additive des Nombres*, Thesis, Université de Bordeaux I, 1982.

[17] G. Grekos, Nonexistence of maximal asymptotic union nonbases, *Discrete Math.*, **33**(1981), 267–270.

[18] H. Halberstam and K. F. Roth, *Sequences*, Oxford university Press, Oxford, 1966.

[19] N. Hämmerer and G. Hofmerster, Zu einer Vermutung von Rohrbach, *J. reine angew. Math.*, **286/287**(1976), 239–247.

[20] E. Härtter, Ein Beitrag zur Theorie der Minimalbasen, *J. reine angew. Math.*, **196**(1956), 170–204.

[21] G. Hofmeister, Asymptotische Abschatzungen für dreielementige Extremalbasen in natrurlichen Zahlen, *J. reine angew. Math.*, **232**(1968), 77–101.

[22] G. Hofmeister, Die dreielementigen Extremalbasen, *J. reine angew. Math.*, **339**(1983), 239–247.

[23] N. Jacobson, *Basic Algebra I,II*, W. H. Freeman Co., 1974.

[24] X.-D. Jia, Exact order of subsets of asymptotic bases in additive number theory, *J. Number theory*, **28**(1988), 207–214.

[25] X.-D. Jia, Simultaneous systems of representatives for finite families of finite sets, *Proc. Amer. Math. Soc.*, **104**(1988), 33–36.

[26] X.-D. Jia, On a combinatorial problem of Erdös and Nathanson, *Chinese Ann. Math.* (Ser A), **9**(1988), 555–560.

[27] X.-D. Jia, Representatives for finite sets, *Proc. Amer. Math. Soc.*, **107**(1989), 347–351.

[28] X.-D. Jia, Minimal spanning vertex systems for graphs, *preprint.*

[29] X.-D. Jia, On the order of subsets of asymptotic bases, *J. Number Theory*, to appear.

[30] X.-D. Jia, Thin bases for finite abelian groups, *J. Number Theory*, to appear.

[31] X.-D. Jia, Thin bases for finite nilpotent groups, *preprint.*

[32] X.-D. Jia and M. B. Nathanson, Addition theorems for σ-finite abelian groups, *preprint.*

[33] X.-D. Jia and M. B. Nathanson, A simple construction of minimal asymptotic bases, *Acta Arith.*, **52**(1989), 95–101.

[34] Y.-F. Li, On the Exact order of asymptotic bases, *preprint.*

[35] H. B. Mann, *Addition Theorems*, Interscience Publishers., New York, 1965.

[36] A. Mrose, Ein rekursives Konstruktionsverfahren fur Abschnittsbasen, *J. reine angew. Math.*, **271**(1974), 214-217.

[37] A. Mrose, Untere Schranken fur die reichweiten von Extremalbasen fester ordung, *Abh. Math. Sem. Univ. Hamburg*, **48**(1979), 118-124.

[38] J. C. M. Nash, *Results in Bases in Additive Number Theory*, Thesis, Rutgers University, New Jersey, 1985.

[39] J. C. M. Nash and M. B. Nathanson, Cofinite subsets of asymptotic bases for positive integers, *J. Number Theory*, **20**(1985), 363–372.

[40] M. B. Nathanson, Minimal bases and maximal nonbases in additive number theory, *J. Numbe Theory*, **6**(1974), 324–333.

[41] M. B. Nathanson, Oscillations of bases in number theory and combinatorics, Number Theory Day, *Lecture Notes in Mathematics*, **626** Springer-Verlag, 1977, 217–231.

[42] M. B. Nathanson, Multiplicative representation of integers, *Israel J. Math.* **57**(1987), 129–136.

[43] M. B. Nathanson, The exact order of subsets of additive bases, in: Proceedings, Number Theory Seminar, 1982, *Lecture Notes in Mathematics*, **1052**, Springer-Verlag, 1984, 273–277.

[44] M. B. Nathanson, Simultaneous systems of representatives for families of finite sets, *Proc. Amer. Math. Soc.*, **103**(1988), 1322–1326.

[45] M. B. Nathanson, An extremal problem for least common multiples, *Distcrete Math.*, **64**(1987), 221–228.

[46] M. B. Nathanson, Simultaneous systems of representatives and combinatorial number theory, *Discrete Math.*, **79**(1989/90), 197–205.

[47] M. B. Nathanson, Combinatorial pairs, and sumsets contained in sequences, *in*: Combinatorial Mathematics, *Proceedings of the Third International Conference*, Volume **555** of the *Annals of the New York Academy of Sciences*, 1989, 316-319.

[48] M. B. Nathanson, Minimal bases and powers of 2, *Acta Arith.*, **49**(1988), 525–532.

[49] M. B. Nathanson, On a problem of Rohrbach for finite groups, *preprint.*

[50] J. Nešetřil and V. Rödl, Two proofs in combinatorial number theory, *Proc. Amer. Math. Soc.*, **93**(1985), 185-188.

[51] V. Puš, Combinatorial properties of products of graphs, *preprint.*

[52] V. Puš, On multiplicative bases in Abelian groups, *preprint.*

[53] V. Puš, On multiplicative bases in commutative semigroups, *preprint.*

[54] H. Rohrbach, Ein Beitrag zur additiven Zahlentheorie, *Math. Zeit.*, **42**(1937), 1-30.

[55] H. Rohrbach, Anwendung eines Satzes der additiven Zahlentheorie auf eine grupentheoretische Grage,, *Math. Zeit.*, **42**(1937), 538–542.

[56] I. Z. Ruzsa, A just basis, *preprint.*

[57] E. S. Selmer, *The Local Postage Stamp Problem*, Department of Mathematics, University of Bergen.

[58] S. A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe, II, *J. reine angew. Math.*, **194**(1955), 111–140.

[59] R. Winderecher, Eine Abschnittsbasis dritter Ordung, *Det Kongelige Norske Videnskabers Selskab*, **9**(1976), 1–3.

[60] C. K. Wong and D. Coppersmith, A combinatorial problem related to multimodule menory organizations, *J. Assoc. Computing Machinery*, **21**(1974), 392–402.