ACTA ARITHMETICA
LXIX.3 (1995)

Independence of solution sets and minimal asymptotic bases

by

PAUL ERDŐS (Budapest), MELVYN B. NATHANSON (Bronx, N.Y.) and PRASAD TETALI (Murray Hill, N.J.)

1. Introduction. Let A be a set of positive integers, and let $k \geq 2$ be a fixed integer. Let $r_A(n)$ denote the number of representations of n in the form

$$n = a_1 + a_2 + \ldots + a_k, \tag{1}$$

where

$$0 < a_1 \leq a_2 \leq \ldots \leq a_k \tag{2}$$

and $a_i \in A$ for $i = 1, \ldots, k$. Let $r'_A(n)$ denote the number of "strict" representations of n in the form

$$n = a_1 + a_2 + \ldots + a_k, \tag{3}$$

where

$$0 < a_1 < a_2 < \ldots < a_k \tag{4}$$

and $a_i \in A$ for $i = 1, \ldots, k$. The set A is called an *asymptotic basis* of order k if there exists a natural number n_1 such that $r_A(n) > 0$ for all $n \geq n_1$. The set A is called a *strict asymptotic basis* of order k if there exists a natural number n_1 such that $r'_A(n) > 0$ for all $n \geq n_1$. All bases considered in this paper will be either asymptotic or strict asymptotic bases of order k. Erdős and Tetali [7] gave a probabilistic construction of a strict asymptotic basis $\mathcal{S}$ of order k whose representation function satisfies $\log n \ll r'_{\mathcal{S}}(n) \ll \log n$.

An asymptotic basis (resp. strict asymptotic basis) A is called *minimal* if the removal of any element from the basis destroys all representations of some infinite sequence of numbers, that is, $A \setminus \{a\}$ is not an asymptotic

Research of the second author supported in part by grants from the PSC–CUNY Research Award Program, was done while visiting the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), Rutgers University, Piscataway, NJ 08855.

basis (resp. strict asymptotic basis) for any $a \in A$. An asymptotic basis (resp. strict asymptotic basis) A is defined to be $\aleph_0$-*minimal* if $A \setminus F$ is an asymptotic basis (resp. strict asymptotic basis) for every finite subset F of A, but $A \setminus I$ fails to be a basis for every infinite subset I of A. Erdős and Nathanson [3, 4] survey results concerning minimal asymptotic bases. In [2], they derived conditions under which an asymptotic basis of order 2 contains a minimal asymptotic basis, and they also constructed in [1] a family of $\aleph_0$-minimal asymptotic bases of order 2.

This paper has two aims. First, we give a simple set of criteria under which an asymptotic basis (resp. strict asymptotic basis) contains a minimal asymptotic basis (resp. strict asymptotic basis). These criteria also enable us to construct $\aleph_0$-minimal bases. Second, we show that the strict asymptotic basis $\mathcal{S}$ constructed in [7] satisfies this set of criteria and so contains a minimal as well as an $\aleph_0$-minimal asymptotic basis. These results answer two important questions posed in [4].

Notation. Let kA denote the set of all sums of k elements of A, and let $k^\wedge A$ denote the set of all sums of k distinct elements of A. Let $r_A(n;a)$ (resp. $r'_A(n;a)$) denote the number of representations of n in the form (1)–(2) (resp. (3)–(4)) such that $a_i = a$ for some $i = 1, \ldots, k$. The solution set of n, denoted by $S_A(n)$ (resp. $S'_A(n)$), is the set of integers in A that appear in some representation of n; that is,

$$S_A(n) = \{a \in A \mid r_A(n;a) > 0\}$$

and

$$S'_A(n) = \{a \in A \mid r'_A(n;a) > 0\}.$$

2. Minimal and $\aleph_0$-minimal asymptotic bases. Erdős and Nathanson [2] discovered a set of simple criteria for an asymptotic basis of order 2 to contain a minimal asymptotic basis of order 2. We shall generalize this result to asymptotic bases of order $k \geq 3$. The following theorem is a natural extension of Theorem 3 of [2]. Condition (ii) is trivially satisfied in the case $k = 2$, but is a nontrivial restriction for asymptotic bases of orders $k \geq 3$.

THEOREM 1. *Let A be a strictly increasing sequence of positive integers, and let $k \geq 2$. If*

(i) $\lim_{n\to\infty} r_A(n) = \infty$,
(ii) $r_A(n;a)$ *is bounded for all* $n \geq 1, a \in A$,
(iii) $|S_A(m) \cap S_A(n)|$ *is bounded for all* $m \neq n$,

then A contains

(a) *a minimal asymptotic basis of order k, and*
(b) *an $\aleph_0$-minimal asymptotic basis of order k.*

P r o o f. Let $r_A(n;a) \le c$ for all $n \ge 1$ and $a \in A$. It follows that if F is any finite subset of A and if $|F \cap S_A(n)| \le w$, then

$$r_{A\setminus F}(n) \ge r_A(n) - cw$$

for all n, since the removal of any one element of $S_A(n)$ destroys at most c representations of n. Let $|S_A(m) \cap S_A(n)| \le d$ for all $m \ne n$. If $F \subseteq S_A(m)$, then

$$|F \cap S_A(n)| \le |S_A(m) \cap S_A(n)| \le d,$$

and so

$$r_{A\setminus F}(n) \ge r_A(n) - cd$$

for all $n \ne m$.

We shall use induction to construct a decreasing sequence of sets

$$A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots$$

such that

$$A^* = \bigcap_{j=0}^{\infty} A_j$$

is a minimal asymptotic basis of order k. We shall also construct a second decreasing sequence of subsets of A whose intersection is an $\aleph_0$-minimal asymptotic basis of order k.

Let $A_0 = A$. Since $\lim_{n\to\infty} r_A(n) = \infty$, we can choose an integer n_1 so that $r_{A_0}(n) = r_A(n) > c(1+d)$ for all $n \ge n_1$.

Choose $a_1, b_1 \in A_0$ such that $a_1 \le n_1$ and $b_1 > kn_1$. Let $m_1 = a_1 + (k-1)b_1$. Then

$$kn_1 < b_1 \le (k-1)b_1 < m_1 < kb_1.$$

We shall construct a set $A_1 \subseteq A_0$ such that $r_{A_1}(n) > 0$ for all $n \ge n_1$, but $m_1 \notin k(A_1 \setminus \{a_1\})$. Thus, every representation of m_1 as a sum of k elements of A_1 must include the integer a_1 as a summand.

We first determine a subset F_1 of A_0 that "destroys" every representation of m_1 that does not include a_1 as a summand. Every such representation is of the form

$$m_1 = a'_1 + a'_2 + \ldots + a'_t + (k-t)b_1,$$

where $a'_i \in A_0$ and $a'_i \ne a_1, b_1$ for $i = 1, 2, \ldots, t$. Note that $m_1 < kb_1$ implies that $t \ne 0$. If $t = 1$, then

$$a_1 + (k-1)b_1 = m_1 = a'_1 + (k-1)b_1$$

implies that $a'_1 = a_1$, which is false. Therefore, $2 \le t \le k$. Let $a'_1 \le a'_2 \le \ldots \le a'_t$. Then

$$(k-1)b_1 < m_1 \le ta'_t + (k-t)b_1 \le ka'_t + (k-2)b_1$$

implies that

$$a'_t > b_1/k > n_1.$$

Let F_1 be the set of all such integers a'_t, and let $A_1 = A_0 \setminus F_1$. Then $F_1 \subseteq [n_1+1, m_1]$. Since $a_1, b_1 \notin F_1$, it follows that $m_1 = a_1 + (k-1)b_1$ is a representation of m_1 as a sum of k elements of A_1, and so $r_{A_1}(m_1) > 0$. On the other hand, we have destroyed every representation of m_1 as the sum of k elements of A_0 all different from a_1, and so $m_1 \notin k(A_0 \setminus \{a_1\})$.

Let $n \geq n_1, n \neq m_1$. Since $F_1 \subseteq S_A(m_1)$, it follows that

$$r_{A_1}(n) = r_{A \setminus F_1}(n) \geq r_A(n) - cd > c(1+d) - cd = c > 0.$$

This completes the first step of the induction.

Let $j \geq 2$. Suppose we have constructed sets $A = A_0 \supseteq A_1 \supseteq \ldots \supseteq A_{j-1}$ and integers n_i, a_i, m_i for $i = 1, \ldots, j-1$ with the following properties:

(i) $kn_1 < m_1 < n_2 < kn_2 < m_2 < n_3 < \ldots < kn_{j-1} < m_{j-1}$,
(ii) $F_i = A_{i-1} \setminus A_i \subseteq [n_i + 1, m_i]$ for $i = 1, \ldots, j-1$,
(iii) $a_1, \ldots, a_{j-1} \in A_{j-1}$,
(iv) $r_{A_{j-1}}(n) > 0$ for $n \geq n_1$,
(v) $m_i \notin k(A_i \setminus \{a_i\})$ for $i = 1, \ldots, j-1$.

We now construct the set A_j and integers n_j, a_j, and m_j.

Let $G_j = A \setminus A_{j-1} \subseteq [1, m_{j-1}]$. Choose $n_j > m_{j-1}$ such that $r_A(n) > c(j + d + |G_j|)$ for all $n \geq n_j$. Choose $a_j, b_j \in A_{j-1}$ such that $a_j < n_j$ and $b_j > kn_j$. Let $m_j = a_j + (k-1)b_j$. Then

$$kn_j < b_j \leq (k-1)b_j < m_j < kb_j.$$

Exactly as in the first step of the induction, we shall determine a subset F_j of A_{j-1} that "destroys" every representation of m_j as a sum of k elements of A_{j-1} that does not include a_j as a summand. Every such representation is of the form

$$m_j = a'_1 + a'_2 + \ldots + a'_t + (k-t)b_j,$$

where $2 \leq t \leq k$, and $a'_i \in A_{j-1}, a'_i \neq a_j, b_j$ for $i = 1, 2, \ldots, t$. Let

$$a'_1 \leq a'_2 \leq \ldots \leq a'_t.$$

Then

$$(k-1)b_j < m_j \leq ta'_t + (k-t)b_j \leq ka'_t + (k-2)b_j$$

implies that

$$a'_t > b_j/k > n_j.$$

Let F_j be the set of all such integers a'_t, and let $A_j = A_{j-1} \setminus F_j$. Then

$$F_j \subseteq [n_j + 1, m_j] \cap S_{A_{j-1}}(m_j) \subseteq [n_j + 1, m_j] \cap S_A(m_j).$$

Since $a_j, b_j \notin F_j$, it follows that $m_j = a_j + (k-1)b_j$ is a representation of m_j as a sum of k elements of A_j, and so $r_{A_j}(m_j) > 0$. However, $m_j \notin$

$k(A_j \setminus \{a_j\})$, since the set A_j was constructed so that every representation of m_j as the sum of k elements of A_j has at least one summand equal to a_j.

Let $n_1 \leq n \leq n_j$. Since $A_{j-1} \setminus A_j = F_j \subseteq [n_j + 1, m_j]$, it follows that $r_{A_j}(n) = r_{A_{j-1}}(n) > 0$. Let $n > n_j, n \neq m_j$. Since

$$A \setminus A_j = F_j \cup G_j$$

and

$$(F_j \cup G_j) \cap S_A(n) \subseteq (F_j \cap S_A(n)) \cup G_j \subseteq (S_A(m_j) \cap S_A(n)) \cup G_j,$$

it follows that

$$|(F_j \cup G_j) \cap S_A(n)| \leq d + |G_j|$$

and so

$$r_{A_j}(n) \geq r_A(n) - c(d + |G_j|) > c(j + d + |G_j|) - c(d + |G_j|) = cj > 0.$$

This completes the induction.

Let $A^* = \bigcap_{j=1}^{\infty} A_j$. Let $n \geq n_1$. Choose $j \geq 1$ so that $n_j \leq n < n_{j+1}$. Since $A_j \setminus A^* \subseteq [n_{j+1} + 1, \infty)$, it follows that

$$r_{A^*}(n) = r_{A_j}(n) > cj > 0,$$

and so A^* is an asymptotic basis of order k. Moreover, since

$$m_j \notin k(A_j \setminus \{a_j\})$$

for every $j \geq 1$, it follows that

$$m_j \notin k(A^* \setminus \{a_j\}).$$

Recall that at each step j of the induction, we chose an integer a_j. We had complete freedom to select this integer, subject only to the conditions that $a_j \in A_{j-1}$ and $a_j \leq n_j$. Let us choose these integers in such a way that every element $a \in A^*$ is chosen infinitely often, that is, if $a \in A^*$, then $a = a_j$ for infinitely many j. Then the set A^* will be a minimal asymptotic basis of order k, since the deletion of any element $a \in A^*$ will destroy all representations of infinitely many integers m_j.

To construct an $\aleph_0$-minimal asymptotic basis, we choose the numbers a_j such that, if $a \in A^*$, then $a = a_j$ for exactly one integer j. If an infinite subset I is deleted from A^*, then there are infinitely many integers of the form m_j that cannot be written as the sum of k terms of $A \setminus I$, and so $A \setminus I$ is not an asymptotic basis of order k.

Let F be a finite subset of A^*, and let $|F| = f$. We shall show that $A^* \setminus F$ is an asymptotic basis of order k.

Since $a_j \in F$ for exactly f indices j, and since $b_j \in F$ for at most f indices j, it follows that $m_j \in k(A^* \setminus F)$ for all but at most $2f$ numbers m_j.

Let $n \geq n_f, n \neq m_j$ for all j. Choose j such that $n_j \leq n < n_{j+1}$. Then $j \geq f$. Since

$$r_{A^*}(n) = r_{A_j}(n) > cj > 0,$$

and since each element of F destroys at most c representations of n, it follows that

$$r_{A^* \setminus F}(n) > cj - cf \geq 0.$$

Thus, $A^* \setminus F$ is an asymptotic basis of order k, and so A^* is an $\aleph_0$-minimal asymptotic basis of order k. ∎

THEOREM 2. *Let A be a strictly increasing sequence of positive integers, and let $k \geq 2$. If*

(i) $\lim_{n\to\infty} r'_A(n) = \infty$,
(ii) $r'_A(n; a)$ *is bounded for all* $n \geq 1$, $a \in A$,
(iii) $|S'_A(m) \cap S'_A(n)|$ *is bounded for all* $m \neq n$,

then A contains

(a) *a minimal strict asymptotic basis of order k, and*
(b) *an $\aleph_0$-minimal strict asymptotic basis of order k.*

Proof. Let $r'_A(n; a) \leq c$ for all $n \geq 1$ and $a \in A$. It follows that if F is any finite subset of A and if $|F \cap S'_A(n)| \leq w$, then

$$r'_{A\setminus F}(n) \geq r'_A(n) - cw$$

for all n, since the removal of any one element of $S'_A(n)$ destroys at most c representations of n. Let $|S'_A(m) \cap S'_A(n)| \leq d$ for all $m \neq n$. If $F \subseteq S'_A(m)$, then

$$|F \cap S'_A(n)| \leq |S'_A(m) \cap S'_A(n)| \leq d,$$

and so

$$r'_{A\setminus F}(n) \geq r'_A(n) - cd$$

for all $n \neq m$.

We shall use induction to construct a decreasing sequence of sets $A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots$ such that $\widehat{A} = \bigcap_{j=0}^{\infty} A_j$ is a strict minimal asymptotic basis of order k. We shall also construct a second decreasing sequence of subsets of A whose intersection is an $\aleph_0$-minimal strict asymptotic basis of order k.

Let $A_0 = A$. Since $\lim_{n\to\infty} r'_A(n) = \infty$, we can choose an integer n_1 so that $r'_{A_0}(n) = r'_A(n) > c(1 + d)$ for all $n \geq n_1$. Choose k integers $a_1, b_{1,1}, b_{1,2}, \ldots, b_{1,k-1} \in A_0$ such that

$$a_1 \leq n_1 < kn_1 < b_{1,1} < b_{1,2} < \ldots < b_{1,k-1}.$$

Let

$$m_1 = a_1 + b_{1,1} + b_{1,2} + \ldots + b_{1,k-1}.$$

We shall construct a set $A_1 \subseteq A_0$ such that $r'_{A_1}(n) > 0$ for all $n \geq n_1$, and with the additional property that every representation of m_1 as a sum of k distinct elements of A_1 must include the integer a_1 as a summand.

We first determine a subset F_1 of A_0 that "destroys" every strict representation of m_1 that does not include a_1 as a summand. Every such representation is of the form

$$m_1 = a'_1 + a'_2 + \ldots + a'_t + b_{1,u_1} + b_{1,u_2} + \ldots + b_{1,u_{k-t}},$$

where $2 \leq t \leq k$, and $a'_i \in A_0, a'_i \neq a_1, b_{1,u}$ for $i = 1, 2, \ldots, t$ and $u = 1, \ldots, k-1$. Let $a'_1 < a'_2 < \ldots < a'_t$. Since $(k-1) - (k-t) = t - 1 \geq 1$ it follows that

$$(b_{1,1} + b_{1,2} + \ldots + b_{1,k-1}) - (b_{1,u_1} + b_{1,u_2} + \ldots + b_{1,u_{k-t}}) \\ = b_{1,v_1} + b_{1,v_2} + \ldots + b_{1,v_{t-1}} \geq b_{1,1}.$$

Then

$$m_1 = a_1 + b_{1,1} + b_{1,2} + \ldots + b_{1,k-1} \\ = a'_1 + a'_2 + \ldots + a'_t + b_{1,u_1} + b_{1,u_2} + \ldots + b_{1,u_{k-t}}$$

implies that

$$kn_1 < b_{1,1} < a_1 + b_{1,1} \leq a_1 + b_{1,v_1} + b_{1,v_2} + \ldots + b_{1,v_{t-1}} \\ = m_1 - (b_{1,u_1} + b_{1,u_2} + \ldots + b_{1,u_{k-t}}) = a'_1 + a'_2 + \ldots + a'_t < ta'_t \leq ka'_t$$

and so

$$a'_t > n_1.$$

Let F_1 be the set of all such integers a'_t, and let $A_1 = A_0 \backslash F_1$. Then $F_1 \subseteq [n_1 + 1, m_1]$. Since $a_1, b_{1,1}, b_{1,2}, \ldots, b_{1,k-1} \notin F_1$, it follows that $m_1 = a_1 + b_{1,1} + b_{1,2} + \ldots + b_{1,k-1}$ is a representation of m_1 as a sum of k distinct elements of A_1, and so $r'_{A_1}(m_1) > 0$. On the other hand, we have destroyed every representation of m_1 as the sum of k distinct elements of A_0 all different from a_1, and so $m_1 \notin k(A_0 \setminus \{a_1\})$.

Let $n \geq n_1, n \neq m_1$. Since $F_1 \subseteq S'_A(m_1)$, it follows that

$$r'_{A_1}(n) = r'_{A \backslash F_1}(n) \geq r'_A(n) - cd > c(1+d) - cd = c > 0.$$

This completes the first step of the induction.

Let $j \geq 2$. Suppose we have constructed sets $A = A_0 \supseteq A_1 \supseteq \ldots \supseteq A_{j-1}$ and integers n_i, a_i, m_i for $i = 1, \ldots, j-1$ with the following properties:

(i) $kn_1 < m_1 < n_2 < kn_2 < m_2 < n_3 < \ldots < kn_{j-1} < m_{j-1}$,
(ii) $F_i = A_{i-1} \setminus A_i \subseteq [n_i + 1, m_i]$ for $i = 1, \ldots, j-1$,
(iii) $a_1, \ldots, a_{j-1} \in A_{j-1}$,
(iv) $r'_{A_{j-1}}(n) > 0$ for $n \geq n_1$,
(v) $m_i \notin k(A_i \setminus \{a_i\})$ for $i = 1, \ldots, j-1$.

We now construct the set A_j and integers n_j, a_j, and m_j.

Let $G_j = A \setminus A_{j-1} \subseteq [1, m_{j-1}]$. Choose $n_j > m_{j-1}$ such that

$$r'_A(n) > c(j + d + |G_j|)$$

for all $n \geq n_j$. Choose $a_j, b_{j,1}, b_{j,2}, \ldots, b_{j,k-1} \in A_{j-1}$ such that

$$a_j \leq n_j < kn_j < b_{j,1} < b_{j,2} < \ldots < b_{j,k-1}.$$

Let

$$m_j = a_j + b_{j,1} + b_{j,2} + \ldots + b_{j,k-1}.$$

Exactly as in the first step of the induction, we shall determine a subset F_j of A_0 that "destroys" every representation of m_j as a sum of k distinct elements of A_{j-1} that does not include a_j as a summand.

Every such representation is of the form

$$m_j = a'_1 + a'_2 + \ldots + a'_t + b_{j,u_1} + b_{j,u_2} + \ldots + b_{j,u_{k-t}},$$

where $2 \leq t \leq k$, and $a'_i \in A_0, a'_i \neq a_j, b_{j,u}$ for $i = 1, 2, \ldots, t$ and $u = 1, 2, \ldots, k-1$. Let

$$a'_1 < a'_2 < \ldots < a'_t.$$

Since $(k-1) - (k-t) = t - 1 \geq 1$, it follows that

$$\begin{aligned}(b_{j,1} + b_{j,2} + \ldots + b_{j,k-1}) - (b_{j,u_1} + b_{j,u_2} + \ldots + b_{j,u_{k-t}})&\\ = b_{j,v_1} + b_{j,v_2} + \ldots + b_{j,v_{t-1}} \geq b_{j,1}&.\end{aligned}$$

Then

$$\begin{aligned}m_j &= a_j + b_{j,1} + b_{j,2} + \ldots + b_{j,k-1}\\ &= a'_1 + a'_2 + \ldots + a'_t + b_{j,u_1} + b_{j,u_2} + \ldots + b_{j,u_{k-t}}\end{aligned}$$

implies that

$$\begin{aligned}kn_j &< b_{j,1} < a_j + b_{j,1} \leq a_j + b_{j,v_1} + b_{j,v_2} + \ldots + b_{j,v_{t-1}}\\ &= m_j - (b_{j,u_1} + b_{j,u_2} + \ldots + b_{j,u_{k-t}}) = a'_1 + a'_2 + \ldots + a'_t < ta'_t \leq ka'_t\end{aligned}$$

and so

$$a'_t > n_j.$$

Let F_j be the set of all such integers a'_t, and let $A_j = A_{j-1} \setminus F_j$. Then $F_j \subseteq [n_j + 1, m_j]$. Since $a_j, b_{j,1}, b_{j,2}, \ldots, b_{j,k-1} \notin F_j$, it follows that $m_j = a_j + b_{j,1} + b_{j,2} + \ldots + b_{j,k-1}$ is a representation of m_j as a sum of k elements of A_j, and so $r'_{A_j}(m_j) > 0$. On the other hand, we have destroyed every representation of m_j as the sum of k distinct elements of A_{j-1} all different from a_j, and so $m_j \notin k(A_{j-1} \setminus \{a_j\})$. Let $n_1 \leq n \leq n_j$. Since $A_{j-1} \setminus A_j = F_j \subseteq [n_j + 1, m_j] \cap S'_A(m_j)$, it follows that $r'_{A_j}(n) = r'_{A_{j-1}}(n) > 0$. Let $n > n_j, n \neq m_j$. Since

$$A \setminus A_j = F_j \cup G_j$$

and

$$(F_j \cup G_j) \cap S'_A(n) \subseteq (F_j \cap S'_A(n)) \cup G_j \subseteq (S'_A(m_j) \cap S'_A(n)) \cup G_j,$$

it follows that

$$|(F_j \cup G_j) \cap S'_A(n)| \leq d + |G_j|$$

and so

$$r'_{A_j}(n) \geq r'_A(n) - c(d + |G_j|) > c(j + d + |G_j|) - c(d + |G_j|) = cj > 0.$$

This completes the induction.

Let $\widehat{A} = \bigcap_{j=1}^{\infty} A_j$. Let $n \geq n_1$. Choose $j \geq 1$ so that $n_j \leq n < n_{j+1}$. Since $A_j \setminus \widehat{A} \subseteq [n_{j+1} + 1, \infty)$, it follows that

$$r'_{\hat{A}}(n) = r'_{A_j}(n) > cj > 0,$$

and so $\widehat{A}$ is a strict asymptotic basis of order k. Moreover, for every $j \geq 1$, since $m_j \notin k(A_j \setminus \{a_j\})$, it follows that

$$m_j \notin k(\widehat{A} \setminus \{a_j\}).$$

Recall that at each step j of the induction, we chose an integer a_j. We had complete freedom to select this integer, subject only to the conditions that $a_j \in A_{j-1}$ and $a_j \leq n_j$. Let us choose these integers in such a way that every element $a \in \widehat{A}$ is chosen infinitely often, that is, if $a \in \widehat{A}$, then $a = a_j$ for infinitely many j. Then the set $\widehat{A}$ will be a minimal asymptotic basis of order k, since the deletion of any element a will destroy all representations of infinitely many integers m_j.

To construct an $\aleph_0$-minimal strict asymptotic basis, we choose the numbers a_j such that, if $a \in \widehat{A}$, then $a = a_j$ for exactly one integer j. If an infinite subset I is deleted from $\widehat{A}$, then there is an infinite increasing sequence of integers of the form m_j that cannot be written as the sum of k terms of $\widehat{A} \setminus I$, and so $\widehat{A} \setminus I$ is not a strict asymptotic basis of order k.

Let F be a finite subset of $\widehat{A}$, and let $|F| = f$. We shall show that $\widehat{A} \setminus F$ is a strict asymptotic basis of order k.

Since $a_j \in F$ for exactly f indices j, and since $b_{j,u} \in F$ for at most f double indices (j, u), it follows that $m_j \in k(\widehat{A} \setminus F)$ for all but at most $2f$ numbers m_j.

Let $n \geq n_f, n \neq m_j$ for all j. Choose j such that $n_j \leq n < n_{j+1}$. Then $j \geq f$. Since

$$r'_{\hat{A}}(n) = r'_{A_j}(n) > cj > 0,$$

and since each element of F destroys at most c representations of n, it follows that

$$r'_{\hat{A} \setminus F}(n) > cj - cf = c(j - f) \geq 0.$$

Thus, $\widehat{A} \setminus F$ is a strict asymptotic basis of order k, and so $\widehat{A}$ is an $\aleph_0$-minimal strict asymptotic basis of order k. ∎

3. Independence of solution sets. Let $\mathcal{S}$ be the asymptotic basis constructed in [7]. In this section we want to prove that $\mathcal{S}$ satisfies the conditions of Theorems 1 and 2. That is, we prove the following theorem.

THEOREM 3. *The asymptotic basis $\mathcal{S}$ contains the following*:

(a) *a minimal asymptotic basis of order k*,
(b) *a minimal strict asymptotic basis of order k*,
(c) *an $\aleph_0$-minimal asymptotic basis of order k*, *and*
(d) *an $\aleph_0$-minimal strict asymptotic basis of order k.*

Proof. In view of the previous section, it suffices to verify that $\mathcal{S}$ satisfies the hypotheses of Theorems 1 and 2. We first prove, in Lemma 1 below, that it suffices to verify that $\mathcal{S}$ satisfies the hypothesis of Theorem 2. The first criterion of the hypothesis of Theorem 2 is satisfied by $\mathcal{S}$, since $r'_{\mathcal{S}}(n) = \Theta(\log n)$, which is the main result of [7]. Lemmas 2 and 3 in the following show that the asymptotic basis $\mathcal{S}$ does in fact satisfy the rest of the hypothesis of Theorem 2. (In short, Lemmas 1–3 below constitute the proof of this theorem.) ∎

Suppose that $\mathcal{S}$ satisfies the hypothesis of Theorem 2. The following argument shows that $\mathcal{S}$ satisfies the hypothesis of Theorem 1 as well.

LEMMA 1. $r_{\mathcal{S}}(n) - r'_{\mathcal{S}}(n) < \infty$ *for all n.*

Proof. Consider the representations that contribute to $r_{\mathcal{S}}(n)$ but not to $r'_{\mathcal{S}}(n)$. The number of distinct elements in each such representation of n is at least one and at most $k-1$. Consider a representation of n with l distinct elements, where $1 \le l \le k-1$, i.e.

$$n = a_1 + \ldots + a_l + a_{l+1} + \ldots + a_k, \qquad a_i \in \mathcal{S},\ a_1 < \ldots < a_l.$$

We will be done by showing that there are only finitely many representations of this form for each n.

Consider $m = n - (a_{l+1} + \ldots + a_k) = a_1 + \ldots + a_l$. Equivalently, we want to show for each m, the number of representations (denoted by $r'_l(m)$) as a sum of l distinct elements from $\mathcal{S}$ is bounded.

By Lemma 10 of [7], we know that the number of representations of n as a sum of l distinct elements is bounded for $l < k$. Hence the lemma. ∎

With this lemma, for the rest of this section it suffices to consider only the *distinct* representations, and verify that $\mathcal{S}$ satisfies the hypothesis of Theorem 2. The second criterion in Theorem 2 asserts that the number of representations of n that use a be bounded, for every $n \in \mathbb{N}$, and $a \in \mathcal{S}$.

LEMMA 2. $r'_{\mathcal{S}}(n; a)$ *is bounded for all $a \in \mathcal{S}$.*

P r o o f. Note that $r'_{\mathcal{S}}(n;a)$ = the number of representations (in $\mathcal{S}$) of $n-a$ as a sum of $k-1$ terms. Once again this follows from Lemma 10 of [7].

Finally, the following lemma proves that $\mathcal{S}$ meets the third criterion in Theorem 2.

LEMMA 3. *$|S'_{\mathcal{S}}(m) \cap S'_{\mathcal{S}}(n)|$ is bounded for all $m < n$.*

Before we prove Lemma 3, we need a couple of technical lemmas. The idea is going to be similar to that of the proof of Lemma 10 of [7]; we first estimate the expected such number, and then bound the *disjoint* occurrences.

Let $R_l(n,m)$ represent the number of representations of n and m that overlap in l numbers. (Note that $l \in [1, k-1]$.) Further, let $R_l^*(n,m)$ represent a maximal collection of "disjoint overlaps" — each overlapping pair of representations for n and m is disjoint from the other overlapping pairs. Also, let $R(n,m)$ and $R^*(n,m)$ denote the corresponding terms when no restriction is made on the size (l) of the overlap.

LEMMA 4. $E[R(n,m)] \le n^{-l/(2k)+o(1)}$.

P r o o f. Without loss of generality, let $m < n$. Then, for fixed n and m, a typical overlapping pair of representations is of the following form:

$$z_1 + \ldots + z_l + x_1 + \ldots + x_{k-l} = n, \qquad z_1 + \ldots + z_l + y_1 + \ldots + y_{k-l} = m,$$

where

$$z_1 + \ldots + z_l = t, \qquad 1 \le t < m.$$

Thus the expected value of $R_l(n,m)$ equals

$$\begin{aligned}\sum_{1\le t<m} \sum_{\substack{z_1+\ldots+z_l=t\\ x_1+\ldots+x_{k-l}=n-t\\ y_1+\ldots+y_{k-l}=m-t}} &\Pr[z_1]\ldots\Pr[z_l]\\ &\times (\Pr[x_1]\ldots\Pr[x_{k-l}])(\Pr[y_1]\ldots\Pr[y_{k-l}])\\ &= \sum_t \Big(\sum_{z_1+\ldots+z_l=t} \Pr[z_1]\ldots\Pr[z_l]\Big)\\ &\quad\times \Big(\sum_{x_1+\ldots+x_{k-l}=n-t} \Pr[x_1]\ldots\Pr[x_{k-l}]\Big)\\ &\quad\times \Big(\sum_{y_1+\ldots+y_{k-l}=m-t} \Pr[y_1]\ldots\Pr[y_{k-l}]\Big)\\ &= \sum_t \mu_l(t)\mu_{k-l}(n-t)\mu_{k-l}(m-t) = \Delta \quad \text{(say)}.\end{aligned}$$

We are going to show that $\Delta \le n^{-l/(2k)+o(1)}$ by making use of the following estimates for $\mu_l(n)$ from [7] (Lemma 8, p. 252):

$$\mu_l(n) \le n^{-1+l/k+o(1)} \qquad \text{for } 2 \le l \le k-1.$$

For technical reasons, fix $\varepsilon = l/(4k)$. Now pick t_0 such that

$$\mu_l(t) \le t^{-1+l/k+\varepsilon} \qquad \text{for } t > t_0.$$

The proof that $\Delta \le n^{-l/(2k)+o(1)}$ gets quite technical, and can be omitted on the first reading without loss of understanding of the rest of the paper.

Case 1. Let us assume that $m = O(n^\delta)$ for $\delta < 1$.

Case 1(a). $t \le t_0$:

$$\begin{aligned}\Delta_1 &= \sum_{t\le t_0}(\mu_l(t)\mu_{k-l}(n-t)\mu_{k-l}(m-t))\\ &< n^{-1+(k-l)/k+o(1)}m^{-1+(k-l)/k+o(1)}\sum_{t\le t_0} H\\ &< n^{-1+(k-l)/k+o(1)} = n^{-l/k+o(1)}.\end{aligned}$$

Case 1(b). $m-t_0 < t \le m$:

$$\begin{aligned}\Delta_2 &= \sum_{m-t_0<t\le m}(\mu_l(t)\mu_{k-l}(n-t)\mu_{k-l}(m-t))\\ &< (m^{-1+l/k+o(1)}n^{-1+(k-l)/k+o(1)})\sum_{m-t_0<t\le m}\mu_{k-l}(m-t)\\ &< (n^{-1+(k-l)/k+o(1)})\sum_{m-t_0<t\le m} H\\ &< (n^{-1+(k-l)/k+o(1)}) = n^{-l/k+o(1)}.\end{aligned}$$

Case 1(c). $t_0 < t \le m-t_0$:

$$\begin{aligned}\Delta_3 &= \sum_{t_0<t\le m-t_0}(\mu_l(t)\mu_{k-l}(n-t)\mu_{k-l}(m-t))\\ &< (n^{-1+(k-l)/k+o(1)}m^{-1+(k-l)/k+o(1)})\sum_{t_0<t\le m-t_0} t^{-1+l/k+\varepsilon}.\end{aligned}$$

We can now estimate the sum by an integral over the full range $0 \le t \le m$:

$$\begin{aligned}\Delta_3 &< (n^{-1+(k-l)/k+o(1)}m^{-1+(k-l)/k+o(1)})\Big(\int_0^m t^{-1+l/k+\varepsilon} + O(1)\Big)\\ &= (n^{-1+(k-l)/k+o(1)}m^{-1+(k-l)/k+o(1)})(m^{l/k+\varepsilon} + O(1))\\ &< n^{-1+(k-l)/k+o(1)} = n^{-l/k+o(1)}.\end{aligned}$$

Case 2. In this case, we let $m = \Theta(n)$.

Case 2(a). $t \le t_0$:

$$\begin{aligned}
\Delta_1' &= \sum_{t\le t_0}(\mu_l(t)\mu_{k-l}(n-t)\mu_{k-l}(m-t)) \\
&< n^{-1+(k-l)/k+o(1)}m^{-1+(k-l)/k+o(1)}\sum_{t\le t_0}H \\
&< n^{-1+(k-l)/k+o(1)}m^{-1+(k-l)/k+o(1)} \\
&< n^{-2+2(k-l)/k+o(1)}, \quad \text{since } m=\Theta(n) \\
&= n^{-l/k+o(1)}.
\end{aligned}$$

Case 2(b). $m - t_0 < t \le m$:

$$\begin{aligned}
\Delta_2' &= \sum_{m-t_0<t\le m}(\mu_l(t)\mu_{k-l}(n-t)\mu_{k-l}(m-t)) \\
&< (m^{-1+l/k+o(1)})\sum_{m-t_0<t\le m}(n-t)^{-1+(k-l)/k+o(1)}H \\
&= (m^{-1+l/k+o(1)})\sum_{m-t_0<t\le m}(n-t)^{-1+(k-l)/k+o(1)} \\
&< (m^{-1+l/k+o(1)})(t_0\times(n-m)^{-1+(k-l)/k+o(1)}) \\
&= (m^{-1+l/k+o(1)})(n^{-1+(k-l)/k+o(1)}) \\
&= (n^{-1+l/k+o(1)})(n^{-l/k+o(1)}) \\
&< n^{-1+o(1)}.
\end{aligned}$$

Case 2(c). $t_0 < t \le m/2$:

$$\begin{aligned}
\Delta_3' &= \sum_{t_0\le t\le m/2}(\mu_l(t)\mu_{k-l}(n-t)\mu_{k-l}(m-t)) \\
&< (n^{-1+(k-l)/k+o(1)}m^{-1+(k-l)/k+o(1)})\sum_{t_0\le t\le m/2}t^{-1+l/k+\varepsilon}.
\end{aligned}$$

We can now estimate the sum by an integral over the full range $0 \le t \le m$:

$$\begin{aligned}
\Delta_3' &< (n^{-1+(k-l)/k+o(1)})(m^{-1+(k-l)/k+o(1)})\Big(\int_0^m t^{-1+l/k+\varepsilon}+O(1)\Big) \\
&= (n^{-1+(k-l)/k+o(1)})(m^{-1+(k-l)/k+o(1)})(m^{l/k+\varepsilon}+O(1)) \\
&= (n^{-l/k+o(1)}m^{\varepsilon+o(1)}) \\
&< n^{-l/k+\varepsilon+o(1)} = n^{-(3l)/(4k)+o(1)}.
\end{aligned}$$

Case 2(d). $m/2 < t \le m - t_0$:

$$\begin{aligned}\Delta_4' &= \sum_{m/2<t\le m-t_0} (\mu_l(t)\mu_{k-l}(n-t)\mu_{k-l}(m-t)) \\ &< (m^{-1+l/k+o(1)}) \sum_{m/2<t\le m-t_0} (n-t)^{-1+(k-l)/k+\varepsilon}(m-t)^{-1+(k-l)/k+\varepsilon} \\ &< (m^{-1+l/k+o(1)}) \sum_{m/2<t\le m-t_0} (m-t)^{-2l/k+2\varepsilon}.\end{aligned}$$

Once again, we estimate the sum by an integral over the full range $0 \le t \le m$:

$$\begin{aligned}\Delta_4' &< m^{-1+l/k+o(1)}\Big(\int_0^m (m-t)^{-2l/k+2\varepsilon} + O(1)\Big) \\ &< m^{-1+l/k+o(1)}(-(m-t)^{1-2l/k+2\varepsilon}|_0^m + O(1)) \\ &= m^{-l/k+2\varepsilon+o(1)} \\ &= n^{-l/k+2\varepsilon+o(1)} = n^{-l/(2k)+o(1)}.\end{aligned}$$

From Cases 1 and 2, we can conclude that

$$E[R_l(m,n)] \le n^{-l/(2k)+o(1)}.$$

This implies

$$E[R(m,n)] = \sum_{l=1}^{k-1} E[R_l(m,n)] \le n^{-l/(2k)+o(1)}.$$

Lemma 5. (i) $\Pr[R^*(m,n) > 8k] < n^{-4+o(1)}$.
(ii) *a.a.* $\exists c^*$ *such that* $R^*(m,n) < c^*$ *for all* $m < n$.

Proof. (i) We use the *disjointness lemma* from [7] to prove the first part; thus

$$\begin{aligned}\Pr[R^*(m,n) > 8k] &< \frac{(E[R(m,n)])^{8k}}{(8k)!} \\ &< \frac{1}{(8k)!}(n^{-l/(2k)+o(1)})^{8k} \\ &= n^{-4l+o(1)} < n^{-4+o(1)}, \quad \text{since } l \ge 1.\end{aligned}$$

(ii) Let A_{mn} denote the event that $R^*(m,n) > 8k$. Then the first part of this lemma implies that $\Pr[A_{mn}] < n^{-4+o(1)}$. There are at most n^2 pairs (m,n) such that $m < n$, and since $n^2\Pr[A(m,n)] < \infty$, by the Borel–Cantelli lemma (see e.g. [7]), this implies that

$$\text{a.a.} \quad \exists n^* \text{ such that } R^*(m,n) < 8k \text{ for all } m < n, \text{ whenever } n > n^*.$$

But for any finite n^*, $R^*(m, n^*)$ is certainly bounded for all $m < n^*$. Thus we conclude that

$$\text{a.a.}\quad \exists c^* \text{ such that } R^*(m,n) < c^* \text{ for all } m < n. \ \blacksquare$$

Proof of Lemma 3. Let us define the following equivalence relation "$\circ$" on the numbers in $|S_{\mathcal{S}}(m) \cap S_{\mathcal{S}}(n)|$: $x \circ y$ iff

$$x + a_1 + \ldots + a_{k-1} = m \quad \text{and} \quad y + a'_1 + \ldots + a'_{k-1} = n$$

and moreover,

$$\{a_1, \ldots, a_{k-1}\} \cap \{a'_1, \ldots, a'_{k-1}\} \neq \emptyset.$$

(Thus x and y are related iff x and y belong to some overlapping pair of representations for m and n.) The number of equivalence classes defined by $\circ$ is bounded since $R^*(m,n)$ is bounded. Moreover, for each $x \in \text{class}\, C_x$, there are at most a bounded number of $y \in C_x$, since both $r'_{\mathcal{S}}(m; a)$ and $r'_{\mathcal{S}}(n; a)$ are bounded. Thus each equivalence class is also bounded, and hence $|S'_{\mathcal{S}}(m) \cap S'_{\mathcal{S}}(n)|$ is bounded. $\blacksquare$

4. Conclusions. Theorems 1 and 2 along with Lemmas 1–3 imply that the asymptotic basis constructed in [7] contains a minimal (strict) and an $\aleph_0$-minimal (strict) asymptotic basis.

Erdős and Nathanson [3] obtained the following very simple criterion for an asymptotic basis A of order 2 to contain a minimal asymptotic basis.

THEOREM 4 (EN). *If there exists a constant $c > 1/\log(\frac{4}{3})$, such that $r'_A(n) > c \log n$ for all sufficiently large n, then A contains a minimal asymptotic basis of order* 2.

The combinatorial lemma at the heart of this theorem has since been generalized by Jia [9] and Nathanson [10]. However, the search for an analogue of Theorem [EN] remains open for bases of order $k > 2$. Clearly, this question requires some new ideas.

Another very interesting problem, which is open even for bases of order 2, is if the weaker condition that $r'_A(n) \to \infty$ is sufficient to imply that A must contain a minimal asymptotic basis. Perhaps this conjecture is too optimistic, but it is possible that $r'_A(n) > c \log n$, for every $c > 0$, is sufficient to imply that A must contain a minimal asymptotic basis.

References

[1] P. Erdős and M. B. Nathanson, *Oscillations of bases for the natural numbers*, Proc. Amer. Math. Soc. 53 (1975), 253–258.

[2] —,—, *Independence of solution sets in additive number theory*, in: Probability, Statistical Mechanics, and Number Theory, G.-C. Rota (ed.), Adv. Math. Suppl. Stud. 9 (1986), 97–105.

[3] P. Erdős and M. B. Nathanson, *Systems of distinct representatives and minimal bases in additive number theory*, in: Number Theory, Carbondale 1979, M. B. Nathanson (ed.), Lecture Notes in Math. 751, Springer, Heidelberg, 1979, 89–107.
[4] —,—, *Problems and results on minimal bases in additive number theory*, in: Number Theory, New York 1985–86, D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn, and M. B. Nathanson (eds.), Lecture Notes in Math. 1240, Springer, Heidelberg, 1987, 87–96.
[5] P. Erdős and R. Rado, *Intersection theorems for systems of sets*, J. London Math. Soc. 35 (1960), 85–90.
[6] P. Erdős and A. Rényi, *Additive properties of random sequences of positive integers*, Acta Arith. 6 (1960), 83–110.
[7] P. Erdős and P. Tetali, *Representations of integers as the sum of k terms*, Random Structures and Algorithms 1 (1990), 245–261.
[8] H. Halberstam and K. F. Roth, *Sequences*, Springer, Heidelberg, 1983.
[9] X.-D. Jia, *Simultaneous systems of representatives for finite families of finite sets*, Proc. Amer. Math. Soc. 104 (1988), 33–36.
[10] M. B. Nathanson, *Simultaneous systems of representatives for families of finite sets*, Proc. Amer. Math. Soc. 103 (1988), 1322–1326.

MATHEMATICAL INSTITUTE
HUNGARIAN ACADEMY OF SCIENCES
REÁLTANODA U. 13-15
H-1053 BUDAPEST
HUNGARY

AT&T BELL LABORATORIES
MURRAY HILL
NEW JERSEY 07974
U.S.A.
E-mail: PRASAD@RESEARCH.ATT.COM

DEPARTMENT OF MATHEMATICS
LEHMAN COLLEGE (CUNY)
BRONX, NEW YORK 10468
U.S.A.

Received on 15.11.1993 (2520)