PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 5, May 2009, Pages 1657–1661
S 0002-9939(08)09732-3
Article electronically published on December 17, 2008

ESSENTIALITIES IN ADDITIVE BASES

PETER HEGARTY

(Communicated by Ken Ono)

ABSTRACT. Let A be an asymptotic basis for $\mathbb{N}_0$ of some order. By an *essentiality* of A one means a subset P such that $A \backslash P$ is no longer an asymptotic basis of any order and such that P is minimal among all subsets of A with this property. A finite essentiality of A is called an *essential subset*. In a recent paper, Deschamps and Farhi asked the following two questions: (i) Does every asymptotic basis of $\mathbb{N}_0$ possess some essentiality? (ii) Is the number of essential subsets of size at most k of an asymptotic basis of order h (a number they showed to be always finite) bounded by a function of k and h only? We answer the latter question in the affirmative and answer the former in the negative by means of an explicit construction, for every integer $h \geq 2$, of an asymptotic basis of order h with no essentialities.

1. Introduction

Let $A \subseteq \mathbb{N}_0$ be such that $0 \in A$, and let $h \geq 2$ be an integer. The h-fold sumset of A, denoted by hA, is the subset of $\mathbb{N}_0$ consisting of all possible sums of h-tuples of elements of A, i.e.

$$hA = \{a_1 + \cdots + a_h : a_1, ..., a_h \in A\}. \tag{1.1}$$

We say that A is a *basis* (resp. *asymptotic basis*) for $\mathbb{N}_0$ of order h if the difference set $\mathbb{N}_0 \backslash hA$ is empty (resp. finite) or, in other words, if every (resp. every sufficiently large) non-negative integer can be expressed as a sum of at most h non-zero elements of A. This is a fundamental notion in additive number theory. In the rest of this article, we will be concerned only with asymptotic bases and we will refer to these simply as 'bases'. We hope no confusion arises for those who are acquainted with the classical terminology. It is important to note that much of what we discuss has also been the subject of investigation for ordinary bases, in which case many aspects actually become simpler.

In [4] Nathanson introduced the following idea: a subset P of a basis A of order h is said to be *necessary* if $A \backslash P$ is no longer a basis of order h. Nathanson was concerned with so-called *minimal bases*, that is, bases in which every element is necessary. There is by now an extensive literature on minimal bases: see e.g. [3] for a state-of-the-art result. The paper [1] provides a recent perspective on another popular line of research on necessary subsets of bases. A very similar notion was the subject of another recent paper of Deschamps and Farhi [2]. They call a subset P of

Received by the editors March 10, 2008, and, in revised form, August 19, 2008.
2000 *Mathematics Subject Classification.* Primary 11B13; Secondary 11B34.
Key words and phrases. Additive basis, essential subset.

a basis A (of some order) an *essentiality* if $A \backslash P$ is no longer a basis of any order and P is minimal, with respect to inclusion, among all subsets of A with this property. A finite essentiality is called an *essential subset* or, in the case of a singleton set, an *essential element*. The main difference between 'necessary' and 'essential' subsets of a basis is that removing one of the former need only increase the order of the basis, whereas removing one of the latter destroys the basis property entirely. The reader is invited to stop for a moment here and, to avoid later confusion, note the additional subtle differences between the meanings of the terms as employed by their various inventors.

The main result of [2], which improves on the work of earlier authors, provides a tight upper bound on the number of essential elements in a basis, purely in terms of the order of the basis. In particular, this number is always finite. Deschamps and Farhi also show that every basis possesses only finitely many essential subsets. To achieve this result, they first prove that for any basis A there exists a largest positive integer $a = a(A)$ such that A is contained, from some point onwards, in an arithmetic progression of common difference a. They then bound the number of essential subsets in terms of the so-called *radical* of a, that is, the number of distinct primes dividing it. In contrast to the situation with essential elements, this does not yield a bound purely in terms of the order of the basis, and they further give an example to show that no such bound is possible.

At the end of their paper, Deschamps and Farhi pose two problems. The first is whether one can find a universal bound on the number of essential subsets of size at most k, in a basis of order h, which is a function of k and h only. Their second problem concerns infinite essentialites. First note that it is easy to give examples of bases possessing no essential subsets whatsoever. As an extreme case, take $A = \mathbb{N}_0$ itself, which is a basis of order 1. Nevertheless, here we can still clearly identify infinite essentialities of A, namely the complements of the sets $p\mathbb{N}$, where p is any prime. The second problem posed in [2] is whether every basis for $\mathbb{N}_0$ must contain some essentiality, albeit possibly infinite. In fact, Deschamps and Farhi went further and asked more (though it is not important here to recall the exact details), suggesting that they believed the answer to the basic question was yes.

In this paper we solve both problems. In Section 2 we will prove a bound of the desired form on the number of essential subsets of bounded size in a basis of a given order. The proof uses ideas developed in [2] and is very short. In Section 3 we shall explicitly construct, for every $h \geq 2$, a basis for $\mathbb{N}_0$ of order h without essentialities.

2. The number of essential subsets in a basis

The following facts are proven in [2]:

Lemma 2.1. (i) *Let A be a basis (of some order) and P an essentiality of A. Let $d = d(P)$ be the largest integer such that $A \backslash P$ is contained in an arithmetic progression of common difference d. Then $d \geq 2$.*

(ii) *Let P_1 and P_2 be any two distinct essentialities of A such that $P_1 \cup P_2 \neq A$. Then $d(P_1)$ and $d(P_2)$ are relatively prime.*

We denote by $p_n\#$ the product of the first n prime numbers; this is fairly standard notation. We can now prove

Theorem 2.2. *Let k, h be two positive integers. There exists an integer $\phi(k,h)$ such that any basis for $\mathbb{N}_0$ of order h contains at most $\phi(k,h)$ essential subsets of size at most k.*

Proof. Let a basis A of order h be given. Let $P_1, ..., P_\phi$ be the complete list of its essential subsets of size at most k (we know from [2] that this list is finite). Let $d_i := d(P_i)$ be the integers defined in Lemma 2.1, for $i = 1, ..., \phi$. Since each P_i is a finite set, we conclude from the lemma that the integers $d_1, ..., d_\phi$ are pairwise relatively prime. Let $X := \bigcup_{i=1}^{\phi} P_i$ and $t := \prod_{i=1}^{\phi} d_i$. Then

$$|X| \leq k\phi, \tag{2.1}$$

$A \backslash X$ is contained in an arithmetic progression of common difference t and

$$t \geq p_\phi\#. \tag{2.2}$$

Let a_0 be any element of $A \backslash X$ and set $Y := X \cup \{a_0\}$. Now since A is a basis of order h, the h-fold sumset hY must meet all congruence classes mod t. At the very least this implies that

$$|Y| \geq t^{1/h}. \tag{2.3}$$

Equations (2.1)–(2.3) imply that

$$k\phi + 1 \geq (p_\phi\#)^{1/h}, \tag{2.4}$$

which clearly yields an upper bound on ϕ depending only on k and h. □

Remark 2.3. It follows from the prime number theorem that

$$p_n\# = \exp((1 + o(1)) \cdot n \log n). \tag{2.5}$$

From this and (2.4) we can easily deduce explicit upper bounds. For example, if h is fixed and $k \to \infty$, one easily shows that $\phi(k,h) = o(\log k)$. On the other hand, if k is fixed and $h \to \infty$, one gets a bound $\phi(k,h) \leq (1 + o(1))h$. It remains to investigate what the best possible bounds could be, for example, in these two situations. Notice that the latter bound is not optimal for $k = 1$ by the main result of [2].

3. Bases without any essentialities

The idea for our construction is quite simple. Let A be a basis for $\mathbb{N}_0$ of some order and suppose P is an essentiality of A. Then for every $x \in P$, the set $A_{x,P} := (A \backslash P) \cup \{x\}$ is once again a basis for $\mathbb{N}_0$. Thus x is an essential element of $A_{x,P}$. By Lemma 2.1(i), this means that the set $A \backslash P$ is contained in a non-trivial arithmetic progression; i.e. there exist integers $d > 1$ and $c \in \{0, 1, ..., d-1\}$ such that $a \equiv c \pmod{d}$ for every $a \in A \backslash P$. Thus, a basis A for $\mathbb{N}_0$ possesses no essentialities if it has the following property:

If $B \subseteq A$ is still a basis of some order, then for every $d \geq 2$ and $c \in \{0, 1, ..., d-1\}$, B contains infinitely many elements which are congruent to c modulo d.

For want of a better term, a basis with this property shall be called *devolved*. Thus it just remains to construct devolved bases, and this we shall now do.

Let $h \geq 2$ be given. We construct a devolved basis A of order h. The idea is to have

$$A = \mathcal{I} \sqcup \mathcal{J} \tag{3.1}$$

where

$$\mathcal{I} = \bigsqcup_{n=1}^{\infty} \mathcal{I}_n, \quad \mathcal{J} = \bigsqcup_{n=1}^{\infty} \mathcal{J}_n \tag{3.2}$$

and the following hold:

E1. Each $\mathcal{I}_n$ is a finite interval, say $\mathcal{I}_n = [r_n, R_n]$.

E2. Each $\mathcal{J}_n$ is a finite arithmetic progression, say $\mathcal{J}_n = [s_n, S_n] \cap (c_n + d_n\mathbb{Z})$.

E3. $r_1 = 0$ and, for every $n \geq 1$, $r_n < R_n < s_n < S_n < r_{n+1}$.

E4. For every $d \geq 2$ and $c \in \{0, 1, ..., d-1\}$, there are infinitely many $n \geq 1$ such that $J_n \subseteq c + d\mathbb{Z}$.

We need to show that an appropriate choice of the parameters r_n, R_n, s_n, S_n yields a set A which is a devolved basis of order h. First of all, let $\mathbb{X}$ be the set of all ordered integer pairs (c, d), where $d \geq 2$ and $c \in \{0, 1, ..., d-1\}$. This is a countable set, so let $\mathscr{O}$ be any well-ordering of it. We have quite a lot of freedom in the choices of the above parameters, but something specific that works is the following recursive recipe:

Step 1. $n := 1$, $r_1 := 0$, $R_1 := 2$, $\mathbb{X}_1 := \{\}$.

Step 2. Let (c_n, d_n) be the least element of $\mathbb{X}\backslash\mathbb{X}_1$, as defined by the ordering $\mathscr{O}$, such that $d_n \leq (h-1)(R_n - r_n) + 1$. Take s_n to be the smallest number greater than R_n satisfying $s_n \equiv c_n \pmod{d_n}$, and take $\mathcal{J}_n := [s_n, S_n] \cap (c_n + d_n\mathbb{Z})$, where S_n is the smallest number greater than $(h+n)s_n$ such that $S_n \equiv c_n \pmod{d_n}$.

Step 3. Update $n := n + 1$. Take $r_n := S_{n-1} + 1$ and $R_n := hr_n$. Put $\mathbb{X}_n := \mathbb{X}_{n-1} \cup \{(c_{n-1}, d_{n-1})\}$ and go to Step 2.

It is straightforward to check that our choices ensure that the set A given by (3.1) and (3.2) satisfies the properties **E1** through **E4**. Note specifically that **E4** will be satisfied since $c + kd\mathbb{Z} \subseteq c + d\mathbb{Z}$ for every positive integer k. It remains to verify the following two claims:

Claim 1. A is a basis of order h.

Claim 2. A is devolved.

Proof of Claim 1. For each $n \geq 1$ let

$$A_n := \left(\bigsqcup_{k=1}^{n} \mathcal{I}_k\right) \sqcup \left(\bigsqcup_{k=1}^{n-1} \mathcal{J}_k\right). \tag{3.3}$$

Clearly, $hA_1 = [0, hR_1]$. Suppose for some $n \geq 1$ that $hA_n = [0, hR_n]$. The choice of s_n guarantees that there is at least one representation

$$hR_n + 1 = s_n + \alpha_1 + \cdots + \alpha_{h-1}, \tag{3.4}$$

where $\alpha_1, ..., \alpha_{h-1} \in \mathcal{I}_n$. Then the choice of d_n ensures that, at least for every $x \in (hR_n, S_n + (h-1)R_n]$, there is at least one representation

$$x = \beta_0 + \beta_1 + \cdots + \beta_{h-1}, \tag{3.5}$$

where $\beta_0 \in \mathcal{J}_n$ and $\beta_1, ..., \beta_{h-1} \in \mathcal{I}_n$. Finally, then, the choices of r_{n+1} and R_{n+1} ensure that for every $x \in (S_n + (h-1)R_n, hR_{n+1}]$, there is at least one representation

$$x = \gamma_1 + + \cdots + \gamma_h, \tag{3.6}$$

where each $\gamma_i \in \mathcal{I}_{n+1} \cup \mathcal{I}_n$. Thus $hA_{n+1} = [0, hR_{n+1}]$, which completes the proof of our first claim. □

Proof of Claim 2. Let $n \geq 1$. Since $S_n > (h+n)s_n$, any representation of the number S_n as a sum of at most $h+n$ elements of A must contain an element from $\mathcal{J}_n$. Now let B be a subset of A which is still a basis of some order. It follows immediately that B must intersect all the sets $\mathcal{J}_n$ except finitely many of them. But then, by property **E4**, A must be devolved. □

Acknowledgement

I thank the referee for a very careful reading of the manuscript as originally submitted.

References

[1] J. Cassaigne and A. Plagne, *Grekos' S function has a linear growth*, Proc. Amer. Math. Soc. **132** (2004), no. 10, 2833–2840 (electronic). MR2063100 (2005b:11011)

[2] B. Deschamps and B. Farhi, *Essentialité dans les bases additives* (French), J. Number Theory **123** (2007), 170–192. MR2295438 (2008g:11016)

[3] P. Erdős, M. B. Nathanson and P. Tetali, *Independence of solution sets and minimal asymptotic bases*, Acta Arith. **69**, no. 3 (1995), 243–258. MR1316478 (96e:11014)

[4] M. B. Nathanson, *Minimal bases and maximal nonbases in additive number theory*, J. Number Theory **6** (1974), 324–333. MR0347764 (50:265)

Department of Mathematical Sciences, Division of Mathematics, Chalmers University of Technology and University of Gothenburg, SE-41296 Gothenburg, Sweden

E-mail address: hegarty@math.chalmers.se