ISSN 2220-5438

Moscow Journal

of **Combinatorics** and Number Theory





МФТИ

2016

Volume 6 • Issue 4



Moscow Journal of Combinatorics and Number Theory 2016, vol. 6, iss. 4 pp. 33–42, [pp. 437–446]



Every finite set of integers is an asymptotic approximate group

Melvyn B. Nathanson (New York)

Abstract: A set A is an (r, ℓ) -approximate group in the additive abelian group G if A is a nonempty subset of G and there exists a subset X of G such that $|X| \leq \ell$ and $rA \subseteq X + A$. The set A is an asymptotic (r, ℓ) -approximate group if the sumset hA is an (r, ℓ) -approximate group for all sufficiently large integers h. It is proved that every finite set of integers is an asymptotic (r, r + 1)-approximate group for every positive integer r.

Keywords: Sums of finite sets of integers, approximate group, asymptotic approximate group, additive number theory

AMS Subject Classification: 11B13, 05A17, 11B75, 11P99

Received: 21.11.2015; revised: 06.04.2016

1. Asymptotic approximate groups

Let A be a nonempty subset of an additive abelian group G. We do not assume that A is finite, nor that A contains the identity, nor that A is symmetric in the sense that -A = A, where $-A = \{-a : a \in A\}$. Let $x \in G$. The *translate of* A by x is the set $x + A = \{x + a : a \in A\}$. If A_1, A_2, \ldots, A_h are nonempty subsets of G, then their sumset is

 $A_1 + A_2 + \dots + A_h = \{a_1 + a_2 + \dots + a_h : a_i \in A_i \text{ for } i = 1, 2, \dots, h\}.$

If $A_i = A$ for all i = 1, ..., h, then we denote the sumset $A_1 + A_2 + \cdots + A_h$ by hA.

Let r and ℓ be positive integers. The set A is an (r, ℓ) -approximate group if there exists a subset X of G such that

$$|X| \le \ell \quad \text{and} \quad rA \subseteq X + A. \tag{1}$$

In this paper we consider only abelian groups because the subject is approximate groups of integers. Our definition of approximate group is more general than the original definition, which is due to Tao [1, 2, 7] and which has been extensively investigated.

We begin with some simple observations. Let A and X be subsets of G that satisfy (1). Let $y \in G$, and let

$$A' = y + A$$
 and $X' = (r-1)y + X$

Then

 $|X'| = |X| \leq \ell$

and

$$egin{aligned} rA' &= r(y+A) = ry+rA \ &\subseteq ry+X+A \ &= (r-1)y+X+(y+A) \ &= X'+A'. \end{aligned}$$

Thus, every translate of an (r, ℓ) -approximate group is an (r, ℓ) -approximate group.

Let A and X be subsets of G that satisfy (1), and let $a_0 \in A$. For $r' \in \{1, 2, ..., r-1\}$, let

$$X_{r^{\prime}}=-(r-r^{\prime})a_{0}+X.$$

We have

$$|X_{r'}| = |X| \leq \ell$$

and

$$(r-r')a_0+r'A\subseteq rA\subseteq X+A.$$

It follows that

$$r'A\subseteq (-(r-r')a_0+X)+A=X_{r'}+A$$

and so A is also a (r', ℓ) -approximate group.

An (r, ℓ) -approximate group is not necessarily an (r', ℓ) -approximate group for r' > r. If A and X are finite subsets of G that satisfy (1), then

$$|rA| \le |X+A| \le \ell |A|.$$

Equivalently, if $|rA| > \ell |A|$, then A is not an (r, ℓ) -approximate group. For example, $\{0, 1, 2, 3\}$ is a (2, 2)-approximate group of integers, but not a (3, 2)-approximate group.

In this paper we study asymptotic approximate groups. The set A is an *asymptotic* (r, ℓ) -approximate group if hA is an (r, ℓ) -asymptotic group for every sufficiently large integer h. This means that, for every integer $h \ge h_1(A)$, there exists a subset X_h of G such that

$$|X_h| \le \ell \quad \text{and} \quad rhA \ \subseteq X_h + hA. \tag{2}$$

The purpose of this paper is to prove that every nonempty finite set of integers is an asymptotic (r, r + 1)-approximate group for every positive integer r.

2. Approximate groups of integers

Let Z and N denote, respectively, the additive group of integers and the additive semigroup of positive integers. For $A \subseteq Z$ and $d \in Z$, we define the *dilation*

$$d * A = \{ da : a \in A \}.$$

For $u, v \in \mathbf{Z}$, the set

$$[u,v]=\{n\in {f Z}: u\leq n\leq v\}$$

is an *interval of integers*. The interval of integers [u, v] is a *maximal subinterval* of A if $u - 1 \notin A$, $v + 1 \notin A$, and $[u, v] \subseteq A$.

We recall the following well-known result.

THEOREM 2.1. Let A be a nonempty finite set of integers. For every integer $r \ge 2$,

$$|rA| \geq r|A| - r + 1 = |A| + (r-1)(|A| - 1)$$

and

$$|rA| = r|A| - r + 1$$

if and only if A is an arithmetic progression.

PROOF. See [5, Theorem 1.3].

THEOREM 2.2. A nonempty finite set A of integers is an (r, 1)-approximate group for some integer $r \ge 2$ if and only if |A| = 1 if and only if A is an (r, 1)-approximate group for all $r \ge 2$.

PROOF. If A is an (r, 1)-approximate group, then there is a set X with |X| = 1 such that $rA \subseteq X + A$, and so

$$|rA| \le |X+A| \le |X||A| = |A|.$$

Theorem 2.1 implies that that |rA| > |A| if $r \ge 2$ and $|A| \ge 2$. It follows that if $r \ge 2$ and A is an (r, 1)-approximate group, then |A| = 1.

If |A| = 1 and $A = \{a_0\}$, then

$$rA = \{ra_0\} = \{(r-1)a_0\} + \{a_0\} = X + A$$

where $X = \{(r-1)a_0\}$ and |X| = 1. Thus, if |A| = 1, then A is an (r, 1)-approximate group for all $r \ge 2$. This completes the proof.

THEOREM 2.3. Let A be a finite set of integers with $|A| \ge 2$. The set A is an (r, 2)-approximate group for some integer $r \ge 2$ if and only if either r = 2 and A is an arithmetic progression, or r = 3 and |A| = 2.

PROOF. Let $|A| = k \ge 2$. If $r \ge 2$ and A is an (r, 2)-approximate group, then there is a set X with |X| = 2 such that

$$rA \subseteq X + A.$$

By Theorem 2.1,

$$|rk-r+1\leq |rA|\leq |X+A|\leq |X||A|=2k$$

and so

$$(r-2)(k-1) \le 1,$$

If $r \ge 3$, then r = 3 and k = 2. Otherwise, r = 2 and A is a (2, 2)-approximate group.

Note that if r = 3 and if k = 2 and $A = \{a_0, a_1\}$ with $a_0 < a_1$, then

$$3A = \{3a_0, 2a_0 + a_1, a_0 + 2a_1, 3a_1\} = \{2a_0, 2a_1\} + \{a_0, a_1\} = X + A$$

where $X = \{2a_0, 2a_1\}$. Thus, every set A with |A| = 2 is a (3, 2)-approximate group.

Suppose that A is a (2, 2)-approximate group, and that $2A \subseteq X + A$, where |X| = 2. If A is not an arithmetic progression, then, by Theorem 2.1,

$$2k \le |2A| \le |X+A| \le |X||A| = 2k$$

and so |2A| = |X + A| = 2k. Let $X = \{x_0, x_1\}$, where $x_0 < x_1$. Then

$$2A = X + A = (x_0 + A) + (x_1 + A)$$

and

$$(x_0 + A) \cap (x_1 + A) = \varnothing.$$

Let $a_0 = \min(A)$ and $a_{k-1} = \max(A)$. Then

$$2a_0 = \min(2A) = \min(X + A) = x_0 + a_0$$

and so $a_0 = x_0$. Similarly,

$$2a_{k-1} = \max(2A) = \max(X+A) = x_1 + a_{k-1}$$

and so $x_1 = a_{k-1}$. It follows that

$$a_0+a_{k-1}\in (x_0+A)\cap (x_1+A)=arnothing$$

which is absurd. Therefore, if the finite set A is a (2, 2)-approximate group, then A is an arithmetic progression.

We shall prove that every finite arithmetic progression is a (2, 2)-approximate group. If

$$A = \{a_0 + id : i = 0, 1, \dots, k-1\}$$

$$egin{aligned} &2A = \{2a_0+id:i=0,\,1,\ldots,2k-2\}\ &= \{2a_0+id:i=0,\,1,\ldots,k-1\}\cup\{2a_0+id:i=k-1,\ldots,2k-2\}\ &= (\{a_0\}+A)\cup(\{a_0+(k-1)d\}+A)\ &= X+A \end{aligned}$$

where

$$X = \{a_0, a_0 + (k-1)d\}$$

and so A is a 2-approximate group. This completes the proof.

THEOREM 2.4. Let u_0, u, v, v_0 be integers such that

$$u_0 \leq u \leq v \leq v_0$$

and let A be a set of integers such that

$$\{u_0,v_0\}\cup [u,v]\subseteq A\subseteq [u_0,v_0].$$

Let $r \geq 2$. If the integer ℓ satisfies

$$\ell \ge \frac{r(v_0 - u_0) + 1}{v - u + 1} \tag{3}$$

and if

$$X_\ell = \{ru_0 - u + i(v - u + 1): i = 0, 1, 2, \dots, \ell - 1\}$$

then

$$rA \subseteq X_{\ell} + A$$

and A is an (r, ℓ) -approximate group.

PROOF. For $i = 0, 1, \ldots, \ell - 1$ we have

$$ru_0 + v - u + i(v - u + 1) = ru_0 + (i + 1)(v - u + 1) - 1$$

and so

$$X_\ell + [u,v] = igcup_{i=0}^{\ell-1} (ru_0 - u + i(v-u+1)) + [u,v]$$

$$egin{aligned} &= igcup_{i=0}^{\ell-1} [ru_0 + i(v-u+1), ru_0 + v - u + i(v-u+1)] \ &= igcup_{i=0}^{\ell-1} [ru_0 + i(v-u+1), ru_0 + (i+1)(v-u+1) - 1] \ &= [ru_0, ru_0 + \ell(v-u+1) - 1]. \end{aligned}$$

Because

 $X_\ell + [u,v] \subseteq X_\ell + A$

it follows that

$$rA\subseteq [ru_0,rv_0]\subseteq X_\ell+[u,v]$$

if

$$ru_0+\ell(v-u+1)-1\geq rv_0.$$

This completes the proof.

3. Asymptotic approximate groups of integers

The following is a fundamental result of additive number theory [3, 4, 8-10].

THEOREM 3.1. If A is a nonempty finite set of nonnegative integers with

$$\min(A) = 0$$
, $\max(A) = a^*$, and $\gcd(A) = 1$

then there is a positive integer $h_0(A)$ and there are nonnegative integers C and D and finite sets $C \subseteq [0, C-2]$ and $D \subseteq [0, D-2]$ such that $[C, ha^* - D]$ is a maximal subinterval of hA and

$$\{0,ha^*\}\cup [C,ha^*-D]\subseteq hA=\mathcal{C}\cup [C,ha^*-D]\cup (ha^*-\mathcal{D})\subseteq [0,ha^*]$$

for all $h \geq h_0(A)$.

Note that $0 \in \mathcal{C}$ if $\mathcal{C} \neq \emptyset$ and $0 \in \mathcal{D}$ if $\mathcal{D} \neq \emptyset$.

PROOF. See [5, Theorem 1.1].

39

THEOREM 3.2. Every nonempty finite set of integers is an asymptotic (r, r + 1)-approximate group for every positive integer r.

PROOF. We begin with a simple observation. Let $A^{(N)}$ be an (r, ℓ) -approximate group, and let X' be a set of integers such that $|X'| = \ell$ and

$$rA^{(N)} \subseteq X' + A^{(N)}.$$

For $d \in \mathbf{N}$ and $a_0 \in \mathbf{Z}$, let

$$A=d*A^{(N)}+a_0$$

and

$$X=d*X'+(r-1)a_0.$$

Then $|X| = |X'| = \ell$, and

$$egin{aligned} rA &= r(d*A^{(N)}+a_0) = d*rA^{(N)}+ra_0 \ &\subseteq d*(X'+A^{(N)})+ra_0 = d*X'+d*A^{(N)}+ra_0 \ &= d*X'+(r-1)a_0+d*A^{(N)}+a_0 \ &= X+A. \end{aligned}$$

It follows that A is an (r, ℓ) -approximate group.

Let A be a nonempty finite set of integers, and let $a_0 = \min(A)$ and $d = \gcd(A - a_0)$. The finite set

$$A^{(N)}=\left\{rac{a-a_0}{d}:a\in A
ight\}$$

satisfies $\min(A^{(N)}) = 0$, $gcd(A^{(N)}) = 1$, and

$$hA = d * hA^{(N)} + ha_0$$

for all $h \in \mathbb{N}$ By the previous remark, it suffices to prove that $A^{(N)}$ is an asymptotic (r, r + 1)-approximate group.

Let a^* , C, D, and $h_0(A^{(N)})$ be the integers defined by Theorem 3.1, and let

$$h_1(A^{(N)}) = \max\left(h_0(A^{(N)}), rac{(r+1)(C+D)-r}{a^*}
ight).$$

Let $h \ge h_1(A^{(N)})$. Applying Theorem 2.4 to the set $hA^{(N)}$ with $u_0 = 0$, u = C, $v = ha^* - D$, and $v_0 = ha^*$, we satisfy inequality (3) with $\ell = r + 1$ and obtain a set

$$X_{h,r+1} = ig\{ -C + i(ha^* - C - D + 1) : i = 0, 1, 2, \dots, r ig\}$$

such that $|X_{h,r+1}| = r+1$ and

$$rhA^{(N)} \subseteq X_{h,r+1} + hA^{(N)}.$$

Thus, $A^{(N)}$ is an asymptotic (r, r + 1)-approximate group. This completes the proof.

Remark. Using results about convex polytopes, Nathanson [6] proved that every finite set of lattice points is an asymptotic approximate group, and, more generally, that every finite subset of an abelian group is an asymptotic approximate group.

Acknowledgments

Supported in part by a grant from the PSC-CUNY Research Award Program.

Bibliography

- 1. *E. Breuillard, A brief introduction to approximate groups*, Thin groups and superstrong approximation, Math. Sci. Res. Inst. Publ., Cambridge Univ. Press, Cambridge, **61** (2014), 23–50.
- 2. **B. Green**, What is ... an approximate group?, Notices Amer. Math. Soc. **59**(5) (2012), 655–656.
- R. K. Mistri, R. K. Pandey, A generalization of sumsets of set of integers, J. Number Theory 143 (2014), 334–356.
- 4. *M. B. Nathanson, Sums of finite sets of integers*, Amer. Math. Monthly **79** (1972), 1010–1012.
- M. B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Graduate Texts in Mathematics, vol. 165, Springer-Verlag, New York, 1996.
- 6. *M. B. Nathanson,* Every finite subset of an abelian group is an asymptotic approximate group, arXiv:1512.03130, 2015.
- 7. **T. Tao**, Product set estimates for non-commutative groups, Combinatorica **28**(5) (2008), 547–594.

- 8. Jian-Dong Wu, Feng-Juan Chen, Yong-Gao Chen, On the structure of the sumsets, Discrete Math. 311(6) (2011), 408–412.
- 9. Quan-Hui Yang, Another proof of Nathanson's theorems, J. Integer Seq. 14(8) (2011), Article 11.8.4, 5.
- Quan-Hui Yang, Yong-Gao Chen, On the cardinality of general h-fold sumsets, European J. Combin. 47 (2015), 103–114.

MELVYN B. NATHANSON

Department of Mathematics Lehman College (CUNY) Bronx, NY 10468 melvyn.nathanson@lehman.cuny.edu