12

Long arithmetic progressions in sum sets

12.1 Introduction

One general theme throughout this book is that sum sets $A + B$ are more structured than arbitrary sets A, B, and in particular that iterated sum sets such as $lA = \{a_1 + \cdots + a_l : a_i \in A_i\}$ should get increasingly structured as l gets larger. One example of this phenomenon is Lemma 4.13, which shows that if A has small Fourier bias then lA quickly fills out the entire ambient group. (See also Exercise 4.3.12 for related demonstration of special structure of sum sets.) For another example, let A be a subset of $[1, n]$ for some large n and consider (as a measure of structure) the longest progression contained inside A. If A has no structure other than density, e.g. $|A| \geq 0.99n$, then there is not much we can say. Even the powerful quantitative version (11.23) of Szemerédi's theorem due to Gowers can only obtain an arithmetic progression of length $\Omega(\log\log\log\log\log n)$. For cubes the situation is somewhat better (and simpler); Lemma 10.49 guarantees that A contains a proper cube of dimension $\Omega(\log\log n)$, though this is still far from the maximal dimension $\Theta(\log n)$ of the cubes inside $[1, n]$.

The situation improves markedly with taking sum sets, though. First, if $A \subset [1, n]$ has cardinality at least $0.99n$, then it is easy to see that $A + A$ or $A - A$ contains an arithmetic progression of length $0.98n$. This is of course a rather extreme case, but more generally if $A \subset [1, n]$ is such that $|A| \geq \delta n$, then Bourgain's theorem (Theorem 4.47) shows that $A + A$ and $A - A$ contain proper arithmetic progressions of length at least $\exp(\Omega_\delta(\log^{1/3} n))$. For $3A$ and $2A - A$, Exercise 4.7.1 shows that these sets in fact contain proper arithmetic progressions of length $\Omega_\delta(n^{\Omega_\delta(1)})$, while Theorem 4.43 shows that these sets contain proper generalized arithmetic progressions of rank $O_\delta(1)$ and volume $\Theta_\delta(n)$. For $2A - 2A$, Chang's theorem (Theorem 4.42) gives similar results but with better dependence on δ.

These results however require A to be rather dense inside the ambient interval $[1, n]$; even Chang's theorem requires A to have density $\Omega(\frac{\log\log n}{\log n})$ in order to be

non-trivial. If A is sparser than this, one can still ask what happens to sum sets such as lA when l gets large. One can show fairly easily (see exercises) that for fixed $A \subset \mathbf{Z}$ and l very large, lA essentially coalesces into a single long arithmetic progression, plus some negligible terms at the boundary. For other groups, the situation is slightly different (again, see exercises); note that unlike the situation with small l, Freiman homomorphisms are much rarer when l gets very large and one cannot identify the asymptotic behavior of lA as $l \to \infty$ for non-isomorphic ambient groups. See [260], [261] for some more advanced results in this direction.

Now we ask a more quantitative question. Suppose we are given positive integers l, m, n with $2 \leq m \leq n$ (the case $m = 1$ will be too degenerate to consider). If A is an arbitrary subset of $[1, n]$ with cardinality $|A| = m$, what can we say about the structure of lA, and more precisely, what is the largest arithmetic progression (or generalized arithmetic progression) one can find inside A? From the above discussion we expect to find quite a large progression when l is large. For instance, from the work of Lev [226] one has the following result:

Theorem 12.1 *[226] Let $A \subset [1, n]$ be such that $|A| > 2$ and A is not contained in any progression of step greater than 1. Let l be such that $l \geq 2(n-1)/(|A|-2)$. Then lA contains an interval $[m+1, m+n]$ for some integer m.*

In fact more precise statements are available; see [227]. An earlier result of Sárközy [307] established the following weaker result:

Theorem 12.2 *[226] There exists an absolute constant $C > 0$ such that the following holds. Let $A \subset [1, n]$ and $l \geq 1$ be such that $|A| \geq 2$ and $l|A| \geq Cn$. Then lA contains a proper arithmetic progression of length $\Omega(l|A|)$.*

We shall prove this theorem as a special case of more general results below.

We can phrase the above theorems in a different way. For any l, m, n with $2 \leq m \leq n$, we define $f(m, l, n)$ to be the largest integer such that, for every subset $A \subset [1, n]$ of cardinality $|A| \geq m$, lA contains a proper arithmetic progression of length $f(m, l, n)$. The question is now to determine the size of $f(m, l, n)$ for various values of m, l, n. Theorem 12.2 asserts that $f(m, l, n) = \Omega(lm)$ whenever $lm \geq Cn$. In fact we have $f(m, l, n) = \Theta(lm)$ in this case, as can be seen by considering the set $A = [1, m]$.

This gives a satisfactory answer to the question when m is large compared to n/l. It is now natural to ask whether this threshold n/l is sharp, and what happens to $f(m, l, n)$ for m below this threshold. It turns out in this case that the upper bound for $f(m, l, n)$ drops dramatically:

Lemma 12.3 (Upper bound on f) *Let $d \geq 1$ be an integer, and let l, m, n be positive integers such that $l \geq 2$ and $n \geq 2^d l^{d-1} m^d$. Then $f(m^d, l, n) \leq lm - l + 1$.*

Proof Let A be the rank d progression

$$A := [1, m]^d \cdot (1, 2lm, \ldots, (2lm)^{d-1}),$$

thus

$$lA = [l, lm]^d \cdot (1, 2lm, \ldots, (2lm)^{d-1}),$$

Then by summing the geometric series we see that $A \subseteq [1, n]$. From the base $2lm$ representation of the integers we see that the map $\phi : [l, lm]^d \to lA$ defined by $\phi(x_0, \ldots, x_{d-1}) = \sum_{j=0}^{d-1} x_j (2lm)^j$ is a Freiman homomorphism of order 2. The same argument shows that A is proper, so that $|A| = m^d$. From Proposition 5.24 we thus see that the length of the longest arithmetic progression in lA is the same as the length of the longest arithmetic progression in $[l, lm]^d$, which is clearly $lm - l + 1$. The claim follows. □

From this lemma (and the trivial observation that $f(m, l, n)$ is monotone increasing in m) we see that there exist constants c_d for $d = 1, 2, 3, \ldots$ such that $f(m, l, n) = O(lm^{1/d})$ whenever $m \leq c_d \frac{n}{l^{d-1}}$. Thus the upper bounds for $f(m, l, n)$ exhibit a thresholding behavior in m near the points $n/l, n/l^2, n/l^3, \ldots$. Somewhat remarkably, these thresholds are sharp up to constants:

Theorem 12.4 *[350] Let $d \geq 1$. Then there exists a constant $C_d > 0$ such that for any $l \geq 1$ and $A \subset [1, n]$ with $|A| \geq C_d \frac{n}{l^d}$ and $|A| \geq 2$, lA contains a proper arithmetic progression of length $\Omega_d(l|A|^{1/d})$.*

Note that Theorem 12.2 already gives the $d = 1$ case of this theorem. Combining this with the preceding discussion, we see that $f(m, l, n) = \Theta_d(lm^{1/d})$ whenever $C_d \frac{n}{l^d} \leq m \leq c_d \frac{n}{l^{d-1}}$. This settles the question of determining the magnitude of $f(m, l, n)$ as long as m is well away from the thresholds $n/l, n/l^2$, etc. and is not too small. The precise behavior near these thresholds is still unclear, and may be difficult to resolve.

We will prove Theorem 12.4 (and hence Theorem 12.2) in the following sections. A key observation is that up to constants, one only needs to consider the case when l is a power of 2, in which case one can view lA as an iteration of the doubling operation $A \mapsto A + A$. This gives the problem a certain dynamic flavor, in which we analyze the evolution of a set under the doubling map. We then discuss extensions and variants, in particular to restricted sum sets

$$l^*A := \{a_1 + \cdots + a_l : a_1, \ldots, a_l \in A, \text{ distinct}\}$$

and finite sum sets

$$FS(A) := \bigcup_{l=0}^{\infty} l^*(A) = \left\{ \sum_{x \in B} x : B \subset A, 0 \leq |B| < \infty \right\},$$