where we now allow A to possibly be infinite. This in particular will be used to resolve some conjectures of Erdős and Folkman on complete sequences; we also present some other applications.

Exercises

12.1.1 Let A be an additive set in a cyclic group $\mathbf{Z}_p$ of prime order. Show that $lA = \mathbf{Z}_p$ whenever $l(|A| - 1) \geq p - 1$, and that this condition is best possible. (Hint: use the Cauchy–Davenport inequality, Theorem 5.4.) Thus when $|A| \geq 2$, the iterated sum sets stabilize to the entire group after at most $(p-1)/(|A|-1)$ summations.

12.1.2 Let A be an additive set in a finite additive group Z. Show that there exists a subgroup G of Z such that lA is a coset of G for all sufficiently large l. If A contains 0, show that we in fact have $lA = \langle A \rangle$ whenever $l|A| \geq 2|\langle A \rangle|$, where $\langle A \rangle$ is the group generated by A. (Hint: quotient out by the symmetry group $\mathrm{Sym}_1(lA)$ and then apply Kneser's theorem, Theorem 5.5.) Thus in this case the iterated sum sets stabilize to a group after at most $2|Z|/|A|$ summations.

12.1.3 Let A is an additive set of integers. Show that if l is sufficiently large depending on A, then lA is a proper arithmetic progression of length $\Theta_A(l)$ together with at most $O_A(1)$ additional elements. (Hint: this statement is only non-trivial for very large l. Use the Chinese remainder theorem. It may be useful to reduce to the case when A has smallest element zero, and has no common divisor.)

12.1.4 Prove Theorem 12.2 in the case when l is extremely large compared to A and n.

12.1.5 Let A be an additive set in $\mathbf{Z}^d$ that contains the origin 0. Let B be the convex hull of A in $\mathbf{R}^d$, and let Γ be the sub-lattice of $\mathbf{Z}^d$ spanned by A. Show that for all large l we have

$$((1 - o_{l\to\infty;A}(1)) \cdot B) \cap \Gamma \subseteq lA \subseteq ((1 + o_{l\to\infty;A}(1)) \cdot B) \cap \Gamma.$$

How is this statement modified when A does not contain the origin?

12.1.6 Show that $f(m, l, n) \leq lm - l + 1$ for all $l \geq 1$ and $2 \leq m \leq n$.

12.1.7 Show that $f(m, l, n) = l$ whenever $n \geq (2l)^{m-1}$. (Hint: for the upper bound, consider $A = 2l\hat{}[0, m-1] = \{1, 2l, (2l)^2, \ldots, (2l)^{m-1}\}$.)

12.2 Proof of Theorem 12.4

To prove Theorem 12.4 it turns out to be convenient to prove a stronger result. Observe in the example given in Lemma 12.3 not only contains an arithmetic

progression, it in fact contains a much larger *generalized* arithmetic progression. This phenomenon turns out to be quite general:

Theorem 12.5 *[350] For any fixed positive integer d there is a constants $C_d > 0$ such that the following holds. For any positive integers n and l and any set $A \subset [1,n]$ satisfying $l^d|A| \geq C_d n$, lA contains a proper progression of rank d' and volume at least $\Omega_d(l^{d'}|A|)$, for some integer $1 \leq d' \leq d$.*

It is easy to see that this implies Theorem 12.4, and we leave this as an exercise. The example in Lemma 12.3 shows that one can have $d' = d$; the simple example $A = [1,m]$ also shows that one can have $d' = 1$. Of course intermediate values of d' are also possible.

We now prove Theorem 12.5. We begin with a version of this theorem for progressions.

Lemma 12.6 (Coalescence of progressions) *Let P be a proper progression of integers of rank at most d, and let $l \geq 1$ be an integer. Then lP contains a proper progression of rank d' and volume at least $\Omega_d(l^{d'}|P|)$ for some $1 \leq d' \leq d$.*

Remark 12.7 It is instructive to experiment with the sum sets lP for a proper progression P of rank d as $l \to \infty$, e.g. the progression $P = [1,m]^4 \cdot (1, N_1, N_1N_2, N_1N_2N_3)$ where $m < N_1 < N_2 < N_3$. At first, the sum sets lP will remain proper of rank d (and grow polynomially in size, like l^d). But at some point there will be a "collision", causing the sum set to essentially "coalesce" into a progression of rank $d-1$ or less (and thus grow somewhat more slowly in l). After a finite number of collisions, the sum set will coalesce into a single arithmetic progression (plus negligible terms), at which point it only grows linearly in l. The proof of Lemma 12.6 below can be used to formalize this intuitive picture but we will not do so here as the notation required is somewhat complicated. This result is also closely related to Minkowski's second theorem (Theorem 3.30), as well as the other machinery in Section 3.5.

Proof We shall induce on d. The case $d = 1$ is obvious (indeed, lP is now an arithmetic progression of length $l|P| - l + 1$), so suppose $d > 1$ and the claim has already been proven for $d-1$. We may assume that l is large depending on d since the claim is trivial otherwise (since lP contains a translate of P).

Let $C_d > 1$ be a large constant to be chosen later. Now let $k \geq 1$ be the largest integer such that $2^k \leq l/C_d$. If $2^k P$ is proper, then $|2^k P| = \Omega_d(2^{kd}|P|) = \Omega_d(l^d|P|/C_d^d)$ and the claim follows with $d' = d$ since lP contains a translate of $2^k P$. Now suppose that $2^k P$ is not proper. Let $1 \leq k' \leq k$ be the first integer such that $2^{k'} P$ is improper, then by arguing as before we see that $|2^{k'} P| \geq |2^{k'-1} P| = \Omega_d(2^{k'd}|P|)$. Applying Theorem 3.40 we see that $O_d(1)2^{k'} P$ contains a proper

progression Q of rank $d-1$ and volume $\Omega_d(|2^{k'}P|) = \Omega_d(2^{k'd}|P|)$. Applying the induction hypothesis we see that $2^{k-k'}Q$ contains a proper progression of rank d' and volume at least

$$\Omega_d\big(2^{(k-k')d'}|2^{k'}P|\big) = \Omega_d\big(2^{(k-k')d'}2^{k'd}|P|\big) = \Omega_d(2^{kd'}|P|) = \Omega_d\big(l^{d'}|P|/C_d^{d'}\big)$$

for some $1 \leq d' \leq d-1$. If C_d is large enough, then lP will contain a translate of $2^{k-k'}O_d(1)2^{k'}P$ and hence a translate of $2^{k-k'}Q$. The claim follows. □

The above lemma allows us to split the problem of finding a progression of small rank in lA into two parts. First, we find a progression P of large rank in $l'A$ for some $l' < l$, and then use the above lemma to find a progression of small rank in kP, where $kl' \leq l$. More precisely, we have

Proof of Theorem 12.5 Note from the hypotheses $l^d|A| \geq C_d n$ and $A \subset [1,n]$ that we can ensure that l is large depending on d, simply by choosing C_d large depending on d.

Let k be the largest integer such that $2^k \leq l$. Thus

$$2^{kd}|A| \geq l^d|A|/2^d \geq C_d n/2^d.$$

On the other hand we have $2^kA \subset [1, 2^k n]$ and hence

$$|2^kA| \leq 2^k n \leq \frac{2^d}{C_d}2^{k(d+1)}|A|.$$

Now let $k' \geq 1$ be the smallest positive integer such that

$$|2^{k'}A| < 2^{k'(d+3/2)}|A|$$

then for C_d large enough we have $k' \leq k$, and in fact

$$k' \leq k - \Omega_d(\log C_d).$$

Set $A' := 2^{k'-1}A$. By construction of k', we have

$$|2^{k'-1}A'| \geq 2^{(k'-1)(d+3/2)}|A|$$

and hence

$$|A'+A'| \leq 2^{d+3/2}|A'|.$$

By Exercise 2.3.14, we can find a subset $F \subset A'$ which is symmetric around some point $x/2$ such that $|F| = \Theta_d(|A'|)$ with doubling constant $O_d(1)$. Applying the Ruzsa–Chang theorem (Theorem 5.30), we see that $2F-2F$ contains a proper progression of rank $O_d(1)$ and volume $\Omega_d(|A'|)$. By the symmetry of F, we see that $2F-2F$ is a translate of $4F$, which is contained in $4A'$. Thus $4A' = 2^{k'+1}A$ contains a proper progression Q of rank $O_d(1)$ and volume $\Omega_d(|A'|)$. Now lA

contains a translate of $2^k A$, which in turn contains $2^{k-k'-1}Q$. Applying Lemma 12.6 we conclude that lA contains a proper progression P of rank d' and volume

$$|P| = \Omega_d\big(2^{(k-k')d'}|Q|\big) = \Omega_d\big(2^{(k-k')d'}|A'|\big) = \Omega_d\big(2^{(k-k')d'}2^{k'(d+3/2)}|A|\big)$$

for some $d' = O_d(1)$. On the other hand, since $lA \subseteq [1, ln]$, we have

$$|lA| \leq ln \leq 2^{k+1}n \leq \frac{2^{d+1}}{C_d}2^{k(d+1)}|A|.$$

Since $|P| \leq |lA$, we conclude that

$$2^{(k-k')d'}2^{k'(d+3/2)}|A| \leq O_d\left(\frac{1}{C_d}2^{k(d+1)}|A|\right)$$

and thus

$$2^{(k-k')(d'-d-1)} \leq O_d\left(\frac{1}{C_d}2^{-k'/2}\right).$$

Thus implies (for C_d large enough) that $d' < d+1$, and thus $1 \leq d' \leq d$ since d' is an integer. Since

$$|P| = \Omega_d\big(2^{(k-k')d'}2^{k'(d+3/2)}|A|\big) = \Omega_d(2^{kd'}|A|) = \Omega_d(l^{d'}|A|)$$

and the claim follows. □

Remark 12.8 The key trick here was to split up the long sum lA by expressing it as a binary tree of binary sums $2^kA + 2^kA = 2^{k+1}A$. The bounds we had on $|lA|$ forced one of the binary sums to have small doubling constant, at which point we could use an inverse theorem, in this case the Freiman cube lemma and the Ruzsa–Chang theorem. A similar trick was employed in Theorem 2.35; see also [42]. This method is sometimes referred to as the *tree argument*.

Remark 12.9 The above proof made use of some rather powerful theorems, including Theorem 3.40 and the Ruzsa–Chang theorem. However, it is possible to prove the above results without using such deep facts from additive geometry and Fourier analysis, instead relying on more elementary inverse theorems such as the $3k-3$ theorem (Theorem 5.11) and the Freiman cube lemma (Theorem 5.20). See [351], and the exercises below. This latter approach turns out to be more robust, in particular being able to deal with restricted sum sets l^*A.

Exercises

12.2.1 Show that Theorem 12.5 implies Theorem 12.4. (Hint: use Exercise 3.2.5.)

12.2.2 Using only the $3k-3$ theorem and the tree argument, show that if P is an arithmetic progression of integers and $A \subset P$ is such that $|A| \geq \delta|P|$,