3.5.8 Let A be a bounded open subset of $\mathbf{R}^d$, and let B, C be open subsets of A. Prove that

$$\mathrm{mes}((B-B)\cap(C-C)) \geq \frac{\mathrm{mes}(B)\mathrm{mes}(C)\mathrm{mes}(A)}{\mathrm{mes}(A-B)\mathrm{mes}(A-C)}.$$

(Hint: use the volume-packing argument to locate a large set of the form $(x+B)\cap(y+C)$ where $x \in A-B$ and $y \in A-C$.)

3.5.9 Let B the the unit ball in $\mathbf{R}^5$, and let Γ be the lattice generated by the five basis vectors $e_1, \ldots, e_5$ and by $\frac{1}{2}(e_1 + \cdots + e_5)$. Show that in this case the directional basis for Γ does not actually generate Γ.

3.6 Progressions and proper progressions

In this section we work in a fixed additive group Z, which may or may not be torsion-free.

Recall from Definition 0.2 that a progression $P = a + [0, N] \cdot v$ is *proper* if the map $n \mapsto n \cdot v$ is injective on $[0, N]$. Not all progressions are proper; however it turns out that, just as John's theorem (Theorem 3.13) shows that all convex sets are in some sense comparable to ellipsoids, all progressions are comparable to proper progressions. This is most obvious in the rank 1 case, in which every arithmetic progression is equal (as a set) to a proper arithmetic progression:

Lemma 3.37 *Let $a + [0, N] \cdot v$ be an arithmetic progression in an additive group Z. Then there exists an $n > 0$ such that $a + [0, n) \cdot v$ is a proper arithmetic progression and $a + [0, n) \cdot v = a + [0, N] \cdot v$.*

Proof If $a + [0, N] \cdot v$ is already proper, then we are done. Otherwise, there exist distinct $n_1, n_2 \in [0, N]$ such that $a + n_1 \cdot v = a + n_2 \cdot v$. In particular, there exists $n \in [1, N]$ such that $n \cdot v = 0$. Let n be the least integer in $[1, N]$ with this property. Then $a + [0, n) \cdot v$ is necessarily proper, and by the Euclidean algorithm it is clear that $a + [0, n) \cdot v = a + [0, N] \cdot v$. □

We now consider the higher rank case; as with John's theorem, the constants will deteriorate worse than exponentially in d. We first show the easier of the two containments, namely that every progression contains a large proper progression of equal or lesser rank.

Theorem 3.38 *Let P be a progression of rank d in an additive group Z. Then P contains a proper progression of rank at most d and volume at least $O(d)^{-5d}|P|$.*

Remark 3.39 For a result of similar flavor (but proven by completely different methods), see Theorem 4.42 below. Note that the $d = 1$ case already follows from Lemma 3.37 (with a constant of 1 instead of $O(d)^{-5d}$).

Proof The idea is to pass to a convex body, apply Lemma 3.32 to obtain a "proper" subset of this body, and then use Lemma 3.33 to pass back to a progression.

By translating and enlarging P slightly we may assume $P = [-N, N] \cdot v$. We may assume that none of the components N_j of N are equal to 0 or 1, since otherwise we could refine P by at worst a factor of 3^d to eliminate those dimensions. Now consider the set $\Gamma := \{n \in \mathbf{Z}^d : n \cdot v = 0\}$, which is clearly a sub-lattice of $\mathbf{Z}^d$, and let A be the symmetric convex box

$$A := \{(x_1, \ldots, x_d) \in \mathbf{R}^d : -N_j \leq x_j \leq N_j \text{ for all } 1 \leq j \leq d\}.$$

By Lemma 3.32, we may find a symmetric convex subset A' of A such that $A' - A'$ is disjoint from $\Gamma - \{0\}$, and such that $A \subset O(d)^{3/2} \cdot A' + \Gamma$ for some $x \in \mathbf{R}^d$. From Corollary 3.15, we thus see that A can be covered by $O(d)^{3d/2}$ translates of $\frac{1}{2} \cdot A' + \Gamma$. Since $[-N, N] = A \cap \mathbf{Z}^d$ and $\Gamma \subseteq \mathbf{Z}^d$, we conclude that $[-N, N]$ can be covered by $O(d)^{3d/2}$ sets of the form $[(\frac{1}{2} \cdot A' + x) \cap \mathbf{Z}^d] + \Gamma$. Taking inner products with v, we conclude that $P = [-N, N] \cdot v$ can be covered by $O(d)^{3d/2}$ sets of the form $[(\frac{1}{2} \cdot A' + x) \cap \mathbf{Z}^d] \cdot v$. By the pigeonhole principle, there must thus exist an x such that

$$\left|\left(\frac{1}{2} \cdot A' + x\right) \cap \mathbf{Z}^d\right| \geq \Omega\left(\frac{1}{d}\right)^{3d/2} |P|$$

and hence by (3.9)

$$|A' \cap \mathbf{Z}^d| \geq \Omega\left(\frac{1}{d}\right)^{3d/2} |P|.$$

We now apply Lemma 3.33 to find a proper progression $\tilde{P} \subseteq A' \cap \mathbf{Z}^d \subseteq [0, N]$ of rank at most d such that

$$|\tilde{P}| \geq O(d)^{-7d/2} |A' \cap \mathbf{Z}^d| \geq \Omega\left(\frac{1}{d}\right)^{5d} |P|.$$

The set $\tilde{P} \cdot v$ is then clearly a progression of rank at most d contained in P; it is proper since $A' - A'$ is disjoint from $\Gamma - \{0\}$, so in particular $|\tilde{P} \cdot v| = |\tilde{P}|$). The claim follows. □

Now we show the more difficult containment, that every progression can be contained inside a proper progression of equal or lesser rank, but somewhat larger volume.

Theorem 3.40 *Let P be a progression of rank d in an additive group Z. Then P is contained in a proper progression Q of rank at most d and volume at most $d^{C_0 d^3}|P|$ for some absolute constant $C_0 > 0$. Also, Q is contained in a translate of $d^{C_0 d^2} P$. If $d \geq 2$ and P is not proper, then Q can be chosen to have rank at most $d-1$. Finally, if Z is torsion-free and P is symmetric, then one can ensure that Q is symmetric also.*

Remark 3.41 Theorems of this type first appeared in the literature in [26], and later in some unpublished work of Gowers–Walters and Ruzsa. The version we give here is taken from [365].

Comparison with Theorem 3.38 suggests that the factor $d^{C_0 d^3}$ is probably not best possible, but we do not know what the correct constant here should be. This theorem can be thought of as the analogue of Corollary 3.8 or Corollary 3.9, but for progressions rather than finitely generated additive groups.

Proof This claim is analogous to the basic linear algebra statement that every linear space spanned by d vectors is equal to a linear space with a *basis* of at most d vectors. Recall that the proof of that fact proceeds by a descent argument, showing that if the d spanning vectors were linearly dependent, then one could exploit that dependence to "drop rank" and span the same linear space with $d-1$ vectors. Our proof of Theorem 3.40 shall be based on a similar strategy.

We shall work only in the case when Z is torsion-free; the general case is proven similarly but contains a few additional technicalities, and we leave it as an exercise (Exercise 3.6.3).

We induce on d. When $d = 1$ the claim follows from Lemma 3.37. Now suppose inductively that $d \geq 2$, and the claim has already been proven for $d-1$ (for arbitrary groups Z and arbitrary progressions P). Let $P = a + [0, N] \cdot v$ be a progression in Z of rank d, where $N = (N_1, \ldots, N_d)$ and $v = (v_1, \ldots, v_d)$; we may translate P so that the base point a equals 0. If P is proper, then we are done. Similarly, if one of the N_j is equal to zero, then we are done by induction hypothesis. Suppose instead that P is not proper and all the N_j are at least 1; then there exist distinct $n, n' \in [0, N]$ such that $n \cdot v = n' \cdot v$. If we then let $\Gamma_0 \subseteq \mathbf{Z}^d$ denote the lattice $\{m \in \mathbf{Z}^d : m \cdot v = 0\}$, then we see that $\Gamma_0 \cap [-N, N]$ contains at least one non-zero element, namely $n' - n$.

Let $m = (m_1, \ldots, m_d)$ be a non-zero element of $\Gamma_0 \cap [-N, N]$, thus

$$m_1 \cdot v_1 + \cdots + m_d \cdot v_d = 0. \tag{3.22}$$

We may assume without loss of generality that m is irreducible in Γ_0. Since Z is torsion-free, this also implies that m is irreducible in $\mathbf{Z}^d$ (i.e. that the $m_1, \ldots, m_d$ have no common divisor) unless Z is torsion-free. The strategy shall be to contain

P inside a progression Q of rank $d-1$ and size

$$|Q| \leq d^{O(d^2)}|P|, \tag{3.23}$$

such that Q is contained in a translate of $d^{O(d)}P$. If we can achieve this, then by the induction hypothesis we can contain Q inside a proper progression R of rank at most $d-1$ and cardinality

$$|R| \leq (d-1)^{C_0(d-1)^3}(O(d))^{O(d^2)}|P|$$

and which is contained in a translate of $d^{C_0(d-1)^2}d^{O(d)}P$. If C_0 is sufficiently large, we will have completed the induction.

It remains to cover P by a progression of rank at most $d-1$ with the bound (3.23) and contained in a translate of $d^{O(d)}P$. Observe that m lies in $[-N, N]$, so the rational numbers $m_1/N_1, \ldots, m_d/N_d$ lie between -1 and 1. Without loss of generality we may assume that m_d/N_d has the largest magnitude, thus

$$|m_d|/N_d \geq |m_j|/N_j \tag{3.24}$$

for all $1 \leq j \leq d$. By replacing v_d with $-v_d$ if necessary, we may also assume that m_d is positive.

To exploit the cancellation in (3.22) we introduce the rational vector $q \in \frac{1}{m_d} \cdot \mathbf{Z}^{d-1}$ by the formula

$$q := \left(-\frac{m_1}{m_d}, \ldots, -\frac{m_{d-1}}{m_d}\right).$$

Since m is irreducible in $\mathbf{Z}^d$, we see, for any integer n, that $n \cdot q$ lies in $\mathbf{Z}^{d-1}$ if and only if n is a multiple of m_d, because $(m_1, \ldots, m_d)$ is irreducible in $\mathbf{Z}^d$.

Next, let $\Gamma \subset \mathbf{R}^{d-1}$ denote the lattice $\Gamma := \mathbf{Z}^{d-1} + \mathbf{Z} \cdot q$. Since q is rational, this is indeed a lattice; since it contains $\mathbf{Z}^{d-1}$, it is certainly full rank. We define the homomorphism $f : \Gamma \to Z$ by the formula

$$f((n_1, \ldots, n_{d-1}) + n_d q) := (n_1, \ldots, n_d) \cdot v;$$

the condition (3.22) ensures that this homomorphism is indeed well defined, in the sense that different representations $v = (n_1, \ldots, n_{d-1}) + n_d q$ of the same vector $v \in \Gamma$ give the same value of $f(v)$. We also let $B \subseteq \mathbf{R}^{d-1}$ denote the convex symmetric body

$$B := \{(t_1, \ldots, t_{d-1}) \in \mathbf{R}^{d-1} : -3N_j < t_j < 3N_j \text{ for all } 1 \leq j \leq d-1\}.$$

We now claim the inclusions

$$P \subseteq f(B \cap \Gamma) \subseteq 5P - 5P.$$

To see the first inclusion, let $n \cdot v \in P$ for some $n \in [0, N]$, then we have $n \cdot v = f((n_1, \ldots, n_{d-1}) + n_d q)$; from (3.24) we see that the jth coefficient of $(n_1, \ldots, n_{d-1}) + n_d q$ has magnitude at most $3N_j$, and thus $n \cdot v$ lies in $f(B \cap \Gamma)$ as claimed. To see the second inclusion, let $(n_1, \ldots, n_{d-1}) + n_d q$ be an element of $B \cap \Gamma$. By subtracting if necessary an integer multiple of m_d from n_d (and thus adding integer multiples of $m_1, \ldots, m_{d-1}$ to $n_1, \ldots, n_{d-1}$) we may assume that $|n_d| \leq |m_d|/2$. By (3.24) and the definition of B, this forces $|n_j| \leq 5N_j$ for all $1 \leq j \leq d$, and hence

$$f((n_1, \ldots, n_{d-1}) + n_d q) = (n_1, \ldots, n_d) \cdot v \subseteq [-5N, 5N] \cdot v = 5P - 5P.$$

Next, we apply Theorem 3.36 to find vectors $w_1, \ldots, w_{d-1} \in \Gamma$ and $M_1, \ldots, M_{d-1}$ such that

$$(-M, M) \cdot w \subseteq B \cap \Gamma \subseteq (-d^{O(d)}M, d^{O(d)}M) \cdot w.$$

Applying the homomorphism f, we obtain

$$(-M, M) \cdot f(w) \subseteq f(B \cap \Gamma) \subseteq (-d^{O(d)}M, d^{O(d)}M) \cdot f(w)$$

where $f(w) := (f(w_1), \ldots, f(w_{d-1}))$. Observe that $(-d^{O(d)}M, d^{O(d)}M) \cdot f(w)$ is a progression of rank $d-1$ which contains $f(B \cap \Gamma)$ and hence contains P. Furthermore, by two applications of Lemma 3.10 we have

$$\begin{aligned} |(-d^{O(d)}M, d^{O(d)}M) \cdot f(w)| &\leq (O(d))^{O(d^2)} |f(B \cap \Gamma)| \\ &\leq (O(d))^{O(d^2)} |5P - 5P| \\ &\leq (O(d))^{O(d^2)} O(1)^d |P| \end{aligned}$$

which proves (3.23). Also, since $(-M, M) \cdot f(w)$ is contained in $f(B \cap \Gamma)$, which is contained in $5P - 5P$, which is a translate of $10P$, we see that $(-d^{O(d)}M, d^{O(d)}M) \cdot f(w)$ is contained in a translate of $d^{O(d)}P$. This completes the induction and proves the theorem. When P is symmetric, one can easily modify the above argument to ensure that all progressions in the above construction are also symmetric; we leave this modification to the interested reader. □

Exercises

3.6.1 Let $P = a + [0, N] \cdot v$ be a progression of rank d in some additive group Z, and let $\Gamma := \{n \in \mathbf{Z}^d : n \cdot v = 0\}$ be the associated sub-lattice of $\mathbf{Z}^d$. Prove the inequalities

$$\frac{|[0, N]|}{|P|} \leq |[-N, N] \cap \Gamma| \leq 3^d \frac{|[0, N]|}{|P|}.$$

Thus the ratio between the volume and cardinality of a progression P is essentially controlled by the quantity $|[-N, N] \cap \Gamma|$. (Hints: for the lower

bound, first use Cauchy–Schwarz to obtain a lower bound for $\{(n, n') \in [0, N] : n \cdot v = n' \cdot v\}$. For the upper bound, consider the multiplicity of the map $f : [-N, 2N] \to Z$ defined by $f(n) := n \cdot v$.)

3.6.2 Let $[0, N]$ be a box in $\mathbf{Z}^d$, and let Γ be a sub-lattice of $\mathbf{Z}^d$. Show that $|[-kN, kN] \cap \Gamma| \leq (2k)^d |[-N, N] \cap \Gamma|$ for all integers $k \geq 1$.

3.6.3 Prove Theorem 3.40 in the case when Z is not necessarily torsion-free. (The main new difficulty is that the vector m is not always irreducible in $\mathbf{Z}^d$; in such a case one will have to "quotient out" a finite cyclic group from P before proceeding with the rest of the argument. However, this will only introduce additional factors of C^d into the inductive bound (3.23), which is acceptable.) Note that the second part of the Theorem does not extend to the torsion case, as can already be seen by considering $P = Z = \mathbf{Z}_2$.

3.6.4 Prove an extension of Theorem 3.40 in the torsion-free case in which one requires that kQ is also proper for some fixed constant $k \geq 1$ (of course, the bounds on Q will depend on k). Note that the torsion-free hypothesis is now essential, as can be seen by considering the case when $P = [1, N] \cdot 1$ in $\mathbf{Z}_N$.

3.6.5 [349] Let N_1, N_2, a_1, a_2 be positive integers such that $0 < a_2 < N_1/5$ and $0 < a_1 < N_2/5$, and a_1, a_2 are coprime. Use the Chinese remainder theorem to show the inclusion

$$\left[\frac{1}{5}(a_1 N_1 + a_2 N_2), \frac{4}{5}(a_1 N_1 + a_2 N_2)\right] \subseteq [0, (N_1, N_2)] \cdot (a_1, a_2).$$

Conclude that if P is any progression of rank 2 in the integers of dimensions N_1, N_2 and steps v_1, v_2 with $0 < v_2 < N_1/5$ and $0 < v_1 < N_2/5$, then P contains a proper arithmetic progression of length $3(N_1 v_1 + N_2 v_2)/5\gcd(v_1, v_2)$ and spacing $\gcd(v_1, v_2)$.

3.6.6 [349] Let A be an additive set in an ambient group Z. Show that there exists $d = O(\log |A|)$ and distinct elements $v_1, \ldots, v_d \in A$ such that the cube $[0, 1]^d \cdot (v_1, \ldots, v_d)$ has cardinality at least $\frac{1}{4}|A|$. (Hint: Using (2.21), show that if S is any additive set in Z such that $|S| < \frac{1}{4}|A|$, then there exists $a \in A$ such that $|S \cup (S + a)| \geq \frac{3}{2}|S|$. Then use the greedy algorithm.)