is absolutely necessary, as can be seen by considering the case when $A = \mathbf{Z}_N$).

6.2.4 Let $S \subset [1, n]$ be a maximal Sidon set in $[1, n]$. Show that $2S - S$ contains $[1, n]$, and conclude that $|S| = \Omega(n^{1/3})$.

6.2.5 [339] Let $S = \{1, 2, 4, 8, 13, 21, 31, \ldots\}$ be the Sidon set of positive integers constructed by the greedy algorithm (this set is sometimes known as the *Mian–Chowla sequence*). Show that the kth element of S does not exceed $(k-1)^3 + 1$, and hence $|S \cap [1, n]| = \Omega(n^{1/3})$ as $n \to \infty$.

6.2.6 (Minkowski's bound for sphere packing) A *sphere packing* P in $\mathbf{R}^n$ is a collection of non-intersecting open spheres with equal radii, and its density $\Delta(P)$ is the fraction of space covered by their interior. Define Δ_n to be the supremum of $\Delta(P)$ taken over all packings in $\mathbf{R}^n$. Prove that $\Delta_n = \Omega(2^{-n})$. (This is a special case of the Hlawka–Minkowski problem of packing convex sets in $\mathbf{R}^n$.)

6.2.7 [218] Let the notation be as in the previous exercise. Prove that $\Delta_n = \Omega(n2^{-n})$. (Hint: Discretize the problem, convert the sphere packing problem to one of finding a large independent set, and apply Ajtai et al.'s theorem.) Up to a constant this is the best bound known for sphere packing.

6.2.8 Prove the following extension of Theorem 6.4. Let $G = G(V, E)$ be a triangle-free graph on n vertices with maximum degree d and T triangles. Then G contains an independent set of size $\Omega(\frac{n}{d} \log \frac{dn^{1/2}}{n^{1/2}+T^{1/2}})$. (Hint: Apply Theorem 6.4 to a properly defined random subgraph of G.)

6.3 Ramsey theory

We now briefly consider another application of graph theory, or more precisely *Ramsey theory*, to additive combinatorics. This theory typically can produce results of the following form: if an explicit set (such as $[1, N]$) is colored into finitely many colors, then at least one of the color classes contains a specific arithmetic structure (e.g. an arithmetic progression). The simplest example of this is the *pigeonhole principle*: if we color an n-element set by fewer than n colors, then there exists two elements with the same color. Indeed one can view Ramsey theory as the study of generalizations and repeated applications of the pigeonhole principle. We will focus on only two results in this field, namely Schur's theorem and the Hales–Jewett theorem (a generalization of van der Waerden's theorem); for a more thorough treatment of these topics, see [143].

We say that a graph G is *complete* if every pair of distinct vertices $v, w \in G$ is connected by exactly one edge. A *edge k-coloring* of a graph $G(V, E)$ is a partition of the edge set E into k classes $E_1, \ldots, E_k$. We say that a subgraph G' of G is E_j*-monochromatic* if all of its edges lie in E_j.

Theorem 6.9 (Ramsey's theorem for two colors) *[276] Let $n, m \geq 1$ be integers, and let $G = (V, E)$ be a complete graph with at least $\binom{n+m-2}{n-1}$ vertices. Then for any edge 2-coloring $E = E_{\text{blue}} \cup E_{\text{red}}$, there either exists a blue-monochromatic complete subgraph G_{blue} with n vertices, or a red-monochromatic complete subgraph G_{red} with m vertices.*

Example 6.10 Any two-coloring of a complete graph with six or more vertices into red and blue edges will contain either a blue triangle or a red triangle.

Proof We shall induce on the quantity $n + m$. When $n + m = 2$ (i.e. $n = m = 1$) the claim is vacuously true. Now suppose that $n + m > 2$ and the claim has already been proven for all smaller values of $n + m$. If $n = 1$ then the claim is again vacuoust (with $R(1, m) = 1$), and similarly when $m = 1$. Thus we shall assume $n, m \geq 2$.

Let $G = (V, E)$ be a complete graph with at least $\binom{n+m-2}{n-1}$ vertices, and let $v \in V$ be an arbitrary vertex. This vertex is adjacent to at least

$$\binom{n+m-2}{n-1} - 1 = \binom{n+m-3}{n-2} + \binom{n+m-3}{n-1} - 1$$

many edges, each of which is either blue or red. Thus by the pigeonhole principle, either v is adjacent to at least $\binom{n+m-3}{n-2}$ blue edges, or is adjacent to at least $\binom{n+m-3}{n-1}$ red edges. Suppose first that we are in the former case. Then we can find a complete subgraph G' of G with at least $\binom{n+m-3}{n-2}$ edges such that every vertex of G' is connected to v by a blue edge. By the induction hypothesis (with (n, m) replaced by $(n-1, m)$), G' either contains a blue-monochromatic complete subgraph G'_{blue} with $n-1$ vertices, or a red-monochromatic complete subgraph G'_{red} with m vertices. In the latter case we are already done by taking $G_{\text{red}} := G_{\text{red}}$, and in the latter case we can find a blue-monochromatic complete subgraph G_{blue} of G with n vertices by adjoining v to G'_{blue} (and adding in all the edges connecting v and G'_{blue}, which are all blue by construction). This disposes of the case when v is adjacent to at least $\binom{n+m-3}{n-2}$ blue edges; the case when v is connected to at least $\binom{n+m-3}{n-1}$ red edges is proven similarly (now using the inductive hypothesis at $(n, m-1)$ instead of $(n-1, m)$). □

Remark 6.11 The bound $\binom{n+m-2}{n-1}$ is sharp for very small values of n and m, but can be improved for larger values of n and m, although computing the precise constants is very difficult (for instance, when $n = m = 5$ the best constant is only known to be somewhere between 43 and 49 inclusive). On the other hand, lower bounds are known (see Exercise 6.3.6).

One can iterate this theorem to arbitrary number of colors:

Corollary 6.12 (Ramsey's theorem for many colors) *[276] Given any positive integers $n_1, \ldots, n_m$, there exists a number $R(n_1, \ldots, n_m; m)$ such that given any complete graph $G = (V, E)$ with at least $R(n_1, \ldots, n_m; m)$ vertices, and any edge m-coloring $E = E_1 \cup \cdots \cup E_m$, there exists a $1 \leq j \leq m$ and a E_j-monochromatic complete subgraph G_j of G with n_j vertices.*

Proof We induce on m. The case $m = 1$ is trivial, and the case $m = 2$ is just Theorem 6.9. Now suppose inductively that $m > 2$ and the claim has already been proven for all smaller values of m. We set

$$R(n_1, \ldots, n_m; m) := R(R(n_1, \ldots, n_{m-1}; m-1), n_m; 2).$$

Suppose we color the edges of $K_{R(n_1,\ldots,n_m;m)}$ into m color classes $E_1, \ldots, E_m$. We coarsen this edge m-coloring into an edge 2-coloring $E_1 \cup \cdots \cup E_{m-1}, E_m$. By the induction hypothesis, we see that with respect to the coarsened coloring, either G contains a E_m-monochromatic complete subgraph G_m with n_m elements, or G contains a $E_1 \cup \cdots \cup E_{m-1}$-monochromatic complete subgraph $G_{1,\ldots,m-1}$ with $R(n_1, \ldots, n_{m-1}; m-1)$ elements. In the first case we are done; in the second case we are done by applying the induction hypothesis once again, this time to the complete graph $G_{1,\ldots,m-1}$. This complete the induction and than the proof. □

We now give an immediate application of Ramsey's theorem to an arithmetic setting.

Theorem 6.13 (Schur's theorem) *[315] If m, k are positive integers, there exists a positive integer $N = N(m, k)$ such that, given any partition of $[1, N]$ into m sets $[1, N] = A_1 \cup \cdots \cup A_m$, at least one of the A_j contains a subset of the form $\{x_1, \ldots, x_k, x_1 + \cdots + x_k\}$. In fact we can choose $N := R(k+1, \ldots, k+1; m) - 1$, using the notation of Corollary 6.12.*

Remarks 6.14 Schur's theorem (in the $k = 2$ case) is equivalent to the assertion that the set $[1, N]$ cannot be covered by m sum-free sets if N is sufficiently large depending on m; in particular, the integers cannot be partitioned into any finite number of sum-free sets. Even when $k = 2$, the value of N given by the above arguments grows double-exponentially in m (Exercise 6.3.4); this is not best possible. For instance, it is known that given any 2-coloring of $[1, N]$, there exist at least $\frac{1}{22}N^2 - \frac{7}{22}N$ monochromatic triples of the form $(x, y, x + y)$, and that this bound is sharp [280], [313] (see also [142]).

Proof Let $G = G(V, E)$ be the complete graph on the $N + 1$ vertices $V := [1, N + 1]$, and let us edge m-color this graph as $E = E_1 \cup \cdots \cup E_m$ where E_j is the set of those edges (a, b) for which $|a - b| \in A_j$. By Corollary 6.12, the graph G

must contain a complete subgraph G' of $k+1$ vertices which is E_r monochromatic for some r. If we list the vertices of G' in order as $v_0 < v_1 < \cdots < v_k$, then the quantities $\mathbf{c}(v_i - v_j)$ for $i > j$ are all equal to each other. The claim then follows by setting $x_j := v_j - v_{j-1} \in A_r$. □

We now give the Hales–Jewett theorem, which we state in an "arithmetic" format. While not strictly a theorem about graphs, it is certainly close in spirit to Ramsey's theorem.

Theorem 6.15 (Hales–Jewett theorem) *[169] Let $m \geq 1$ and $n \geq 1$. Then there exists an integer $d = d(|A|, m) \geq 1$ such that if $[0, n-1]^d \subset \mathbf{Z}^d$ is partitioned into m non-empty sets $[0, n-1]^d = E_1 \cup \cdots \cup E_m$, then at least one of the sets E_j contains a proper arithmetic progression $a + [0, n-1] \cdot v$ of length n, for some $a \in [0, n-1]^d$ and $v \in [0, 1]^d$.*

This theorem can be proven by a double induction. It is a special case of the following more technical proposition, in which one either locates a single monochromatic progression of length n, or several linked monochromatic progressions of length $n-1$ (with each progression being monochromatic with a different color).

Proposition 6.16 *Let $m \geq 1$, $n \geq 1$, and $1 \leq s \leq m$. Then there exists an integer $\tilde{d} = \tilde{d}(n, m, s) \geq 1$ such that if $[0, n-1]^{\tilde{d}} \subset \mathbf{Z}^d$ is partitioned into m non-empty sets $[0, n-1]^{\tilde{d}} = E_1 \cup \cdots \cup E_m$, then either at least one of the sets E_j contains a proper arithmetic progression $a + [0, n-1] \cdot v$, or there exists distinct classes $E_{j_1}, \ldots, E_{j_s}$ and $a \in [0, n-1]^{\tilde{d}}$ and $v_1, \ldots, v_s \in [0, 1]^{\tilde{d}}$ such that $a + [1, n-1] \cdot v_i \subseteq E_{j_i}$ for all $1 \leq i \leq s$.*

Indeed, applying Proposition 6.16 with $s := m$ one can conclude Theorem 6.15, since if one has m distinct monochromatic progressions $a + [1, n-1] \cdot v_i$, then one of the progressions $a + [0, n-1] \cdot v_i$ must also be monochromatic by the pigeonhole principle.

Proof of Proposition 6.16 To abbreviate notation, we shall use "arithmetic progression" in this proof to denote any proper arithmetic progression $a + [0, n-1] \cdot v$ or $a + [1, n-1] \cdot v$ in a lattice $\mathbf{Z}^d$ where $a \in [0, n-1]^d$ and $v \in [0, 1]^d$.

We use two induction loops. For the outer loop, we induce on n. The claim is trivial when $n = 1$, so we assume that $n > 1$ and the claim has already been proven for $n-1$ (and for arbitrary m, s). In particular, by the above discussion we see that we may assume Theorem 6.15 for $n-1$.

Now we begin our inner loop, inducing on s. When $s = 1$ the claim follows from Theorem 6.15 for $n-1$ (shifting $[1, n-1]$ to $[0, n-2]$), so assume that $2 \leq s \leq m$ and the claim has already been proven for $s-1$ (and the same value of n, but with arbitrary m). We set $\tilde{d} := \tilde{d}(n, m, s) := d_1 + d_2$, where $d_1 := \tilde{d}(n, m, s-1)$

and $d_2 := d(n-1, m^s n^{sd_1})$. Let $[0, n-1]^{\tilde{d}} = E_1 \cup \cdots \cup E_m$ be a partition of $[0, n-1]^{\tilde{d}}$ into m distinct color classes. Suppose that none of the E_j contain any arithmetic progressions of length n. Our task is then to show that there are s distinct classes $E_{j_1}, \ldots, E_{j_s}$, $a \in [0, n-1]^{\tilde{d}}$, and $v_1, \ldots, v_s \in [0, 1]^{\tilde{d}}$ such that $a + [1, n-1] \cdot v_i \subseteq E_{j_i}$ for all $1 \leq i \leq s$.

We write $[0, n-1]^{\tilde{d}} = [0, n-1]^{d_1} \times [0, n-1]^{d_2}$, and for each $x \in [0, n-1]^{d_2}$ we consider the partition $[0, n-1]^{d_1} = E_{1,x} \cup \cdots \cup E_{m,x}$, where $E_{j,x} := \{y \in [0, 1]^{d_1} : (y, x) \in E_j\}$. Since none of the E_j contain an arithmetic progression of length n, neither do the $E_{j,x}$. By definition of d_1 and the inner induction hypothesis, we conclude that for each x there exist distinct color classes $j_{1,x}, \ldots, j_{s-1,x}, a_x \in [0, n-1]^{d_1}$ and $v_{1,x}, \ldots, v_{s-1,x} \in [0, 1]^{d_1}$ such that

$$a_x + [1, n-1] \cdot v_{i,x} \in E_{j_{i,x}} \tag{6.1}$$

for all $1 \leq i \leq s-1$. Note that a_x itself must then belong to another color class $j_{s,x}$ distinct from $j_{1,x}, \ldots, j_{s-1,x}$, otherwise one of the classes $E_{j,x}$ would contain an arithmetic progression of length n. If we set $v_{s,x} := 0$ then we see that (6.1) now holds for $i = s$ also, although in that case the progression $a_x + [1, n-1] \cdot v_{i,x}$ is not proper. This will however be rectified by means of the d_2 coordinates.

The map $x \mapsto (j_{1,x}, \ldots, j_{s,x}, a_x, v_{1,x}, \ldots, v_{s-1,x})$ is a map from $[0, n-1]^{d_2}$ to a set of cardinality at most $m^s n^{sd_1}$. Thus it induces a partition $[0, n-1]^{d_2} = F_1 \cup \cdots \cup F_{m^s n^{sd_1}}$ into $m^s n^{sd_1}$ color classes (some of which may be empty). By definition of d_2 and the outer induction hypothesis (again shifting $[1, n-1]$ to $[0, n-2]$), we conclude that one of the color classes F_t contains an arithmetic progression $a_* + [1, n-1] \cdot v_*$ with $a_* \in [0, n-1]^{d_2}$ and $v \in [0, 1]^{d_2}$. This means that there exist distinct $j_{1,(t)}, \ldots, j_{s,(t)} \in [1, m]$, $a_{(t)} \in [0, n-1]^{d_1}$, and $v_{1,(t)}, \ldots, v_{s,(t)} \in [0, 1]^{d_1}$ (with $v_{s,(t)} = 0$) such that $a_{(t)} + [1, n-1] \cdot v_{i,(t)} \in E_{j_{i,x}}$ for all $x \in a_* + [1, n-1] \cdot v_*$ and $1 \leq i \leq s$. But if we now set $a := (a_{(t)}, a_*) \in [0, n-1]^{\tilde{d}}$ and $v_i := (v_{i,(t)}, v_*) \in [0, 1]^{\tilde{d}}$, we see that $a + [1, n] \cdot v_i \in E_{j_i}$ for all $1 \leq j \leq s$, and that each of the $a + [1, n] \cdot v_i$ are *proper* arithmetic progressions of length $n-1$. This closes the induction loop, and the claim follows. □

This theorem has a number of consequences, the most notable being perhaps van der Waerden's theorem.

Theorem 6.17 *(van der Waerden, [371]) Let $k, m \geq 1$ be integers. Then there exists an integer $N = N(k, m) \geq 1$ such that given any proper arithmetic progression P of length at least N (in an arbitrary additive group Z), and any partition $P = E_1 \cup \cdots \cup E_m$ of P into m color classes, at least one of these classes E_j contains a monochromatic proper arithmetic sub-progression P' of P of length $|P'| = k$.*

We leave the proof as an exercise. Let us, however, remark that if we fix k then the bound on m which follow from Hales–Jewett's theorem are very poor, being of growing as fast as the infamous Ackermann function. One can use Gowers' theorem [138] and the pigeonhole principle to deduce a much better bound.

Remark 6.18 In the case of $k = 3$, Solymosi observed (private communication) that one can obtain a rather good bound (which is comparable to the bound one gets from Roth's theorem) by a simple argument which does not involve Fourier analysis. For simplicity, let us assume that we color a group Z of cardinality N by k colors. We now show that there is a monochromatic arithmetic progression of length 3, assuming that k is sufficiently small compared with N. Let C_1 be the most popular color and let $a_1, \ldots, a_{m_1}$ be the elements colored by C_1. Clearly $m_1 \geq n/k$. By the pigeonhole principle, there is an element $x \in Z$ such that there are at least $\binom{m_1}{2}/n$ pairs (a_i, a_j), $i < j$ such that $a_j - a_i = x$. If there is no monochromatic arithmetic progression of length 3, then $b_j = a_j + x$ is not colored by C_1. Thus we end up with a set S_1 of at least

$$\binom{m_1}{2}\Big/n \geq n/3k^2 = n_1$$

elements which are not colored by C_1. Now repeat the argument with the set S_1; we end up with a set S_2 of size at least $\binom{n_1}{2}/n \geq n/27k^4 = n_2$ elements which are not colored by either C_1 or C_2 (Exercise 6.3.8). Iterating this argument k times, we end up with a set of $n_k = n/3^{2^k-1}k^{2^k}$ elements which cannot be colored by any color. This is a contradiction if $n \geq 3^{2^k-1}k^{2^k}$.

Exercises

6.3.1 Using Schur's theorem, show that if the positive integers $\mathbf{Z}^+$ are finitely colored and $k \geq 1$ is arbitrary, then there exist infinitely many monochromatic sets in $\mathbf{Z}^+$ of the form $\{x_1, \ldots, x_k, x_1 + \cdots + x_k\}$. (Hint: Schur's theorem can easily produce *one* such set; now color all the elements of that set by new colors and repeat.) Conversely, show that if the previous claim is true, then it implies Schur's theorem.

6.3.2 Show that if the positive integers $\mathbf{Z}^+$ are finitely colored then there exist infinitely many *distinct* integers x and y such that $\{x, y, x + y\}$ are monochromatic. (Hint: refine the coloring so that x and $2x$ always have different colors.) A more challenging problem is to establish a similar result for general k, i.e. to find infinitely many distinct $x_1, \ldots, x_k$ such that $\{x_1, \ldots, x_k, x_1 + \cdots + x_k\}$ is monochromatic.

6.3.3 Show that if the positive integers $\mathbf{Z}^+$ are finitely colored and $k \geq 1$ is arbitrary, then there exist infinitely many monochromatic sets of the form $\{x_1, \ldots, x_k, x_1 \ldots x_k\}$. Thus Schur's theorem can be adapted to products instead of sums. However, nothing is known about the situation when one has both sums *and* products; for instance, it is not even known that if one finitely colors the positive integers that one can find even a single monochromatic set of the form $\{x + y, xy\}$ for some positive integers x, y (not both equal to 1).

6.3.4 Show that the quantity $N(m, k)$ in Schur's theorem can be taken to be $O(1)^{k^m}$.

6.3.5 Let k be an integer, and let A be an additive set in an ambient group Z such that $|A| \geq \binom{2k-2}{k-1}$, and let C be an arbitrary subset of Z. Show that there exists a set $B \subseteq A$ of cardinality $|B| = k$ such that either $B + B \subseteq C$ or $B + B$ is disjoint from C.

6.3.6 [84] Show that if $n \geq 3$ and $N \leq 2^{n/2}$ then there exists a two-coloring of the edges of the complete graph on N vertices which does not contain a monochromatic complete subgraph of n vertices. (Hint: color the graph randomly.)

6.3.7 Prove van der Waerden's theorem. (Hint: set $N = k^d$ for a large d, and identify P with $[0, k-1]^d$. Then apply Theorem 6.15.)

6.3.8 Consider Remark 6.18. Show that if after the ith step we get an element y which is colored by C_j for some $j < i$, then $y, y - (d_i + \cdots + d_j), y - 2(d_i + \cdots + d_j)$ are all of color C_j, where d_l is the "popular" difference in step l.

6.3.9 Let Z be an arbitrary finite additive group, partitioned into m color classes $E_1 \cup \cdots \cup E_m$. Show that for any $k \geq 1$ there exists a color class E_j such that

$$\mathbf{P}_{a,r\in Z}(a, a + r, \ldots, a + (k-1)r \in E_j) = \Omega_{k,m}(1).$$

(Hint: apply Theorem 6.17 to a random progression in Z of a suitable length $N(k, m)$ and use the first moment method.) This is a weak form of Varnavides' version of Szemerédi's theorem, see Theorem 11.1.

6.3.10 Let A be an additive set, and let $P(n)$ be a statement pertaining to an element $n \in A$. Let us say that the property P is *k-choosable* for some $k \geq 1$ if, given every proper arithmetic progression of length k in A, at least one element n of that progression obeys the property $P(n)$. Show that if the properties $P_1(n), \ldots, P_m(n)$ are k-choosable, then the joint property $P_1(n) \wedge \cdots \wedge P_m(n)$ is $O_{k,m}(1)$-choosable. (This statement is in fact equivalent to van der Waerden's theorem, and plays a key role in the original proof [345] of Szemerédi's theorem.)

6.3.11 (Multi-dimensional Hales–Jewett theorem) [169] Let $n, m, r \geq 1$. Show that there exists an integer $d = d(n, m, r) \geq 1$ such that, given any partition of $[0, n-1]^d$ into m color classes $E_1, \ldots, E_m$, then at least one of