Combinatorial Number Theory

Lecture Notes

Contents

Chapter 1

Ramsey's Theorem

1.1. Ramsey's Theorem for graphs

Definition 1. A *graph* $G = (V, E)$ is a set V of points, called *vertices*, and a set E of distinct pairs of vertices, called *edges*.

Definition 2. A *subgraph* $G' = (V', E')$ of a graph $G = (V, E)$ is a graph such that $V' \subseteq V$ and $E' \subseteq E$.

Figure 1.1 below depicts a graph G with four vertices $V = \{V_1, V_2, V_3, V_4\}$ and four edges $E = \{e_1, e_2, e_3, e_4\}$, where $e_1 = \{V_1, V_2\}$, $e_2 = \{V_2, V_3\}$, $e_3 = \{V_3, V_4\}$, and $e_4 = \{V_2, V_4\}$. Note that edges are *unordered* pairs of vertices, meaning that $\{V_1, V_2\}$ and $\{V_2, V_1\}$ refer to the same edge. Next to it is a graph $G' = (V', E')$ with $V' = V = \{V_1, V_2, V_3, V_4\}$ and $E' = \{e_1, e_3\}$. Since $V' \subseteq V$ and $E' \subseteq E$, we deduce that G' is a subgraph of G.

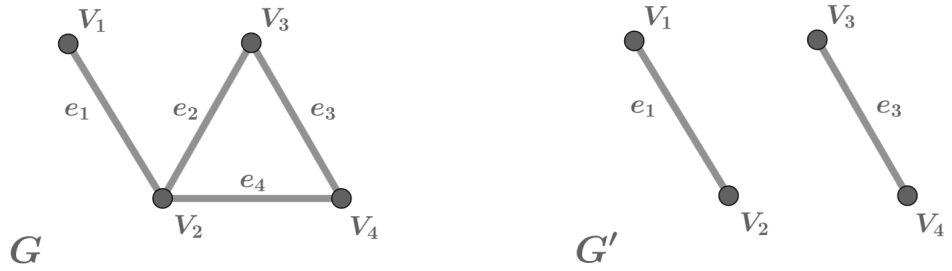

Figure 1.1: A graph G and one of its subgraphs G'.

Definition 3. Given $n \in \mathbb{N}$, a *complete graph on n vertices*, denoted by K_n, is a graph with n vertices and the property that every pair of distinct vertices is connected by an edge.

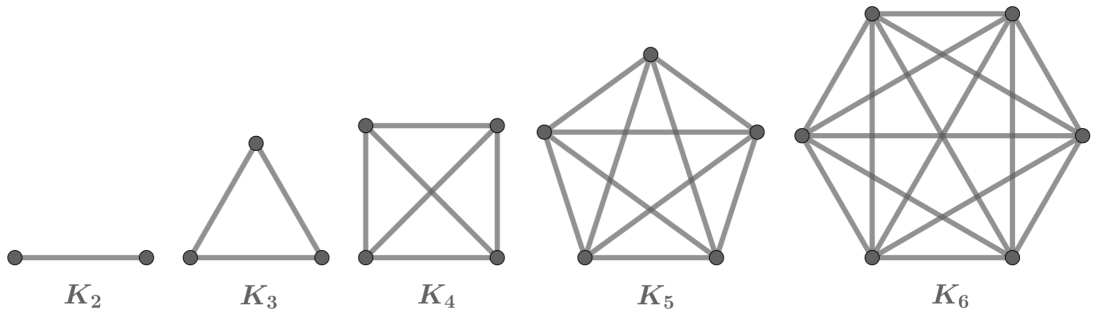

Figure 1.2: A depiction of K_n for $n = 2, 3, 4, 5$, and 6.

Definition 4. An *edge-coloring* of a graph $G = (V, E)$ is an assignment of a color to each edge of the graph. A graph that has been edge-colored is called *monochromatic* if all of its edges are the same color.

An edge-coloring of a graph can also be viewed as a function where the domain is the set of edges of the graph and the codomain is the set of colors. For example, suppose one has a graph with edges $E = \{e_1, e_2, e_3\}$ and a set of colors $C = \{\text{red}, \text{blue}\}$. A valid coloring of this graph can be seen as a function $\chi : E \to C$, where, for instance, $\chi(e_1) = \text{red}$, $\chi(e_2) = \text{blue}$, and $\chi(e_3) = \text{red}$.

Ramsey's Theorem for graphs. *For any $n, m \in \mathbb{N}$ there exists $R = R(n, m) \in \mathbb{N}$ such that any edge-coloring of K_R with at most m colors contains a monochromatic copy of K_n as a subgraph.*

Let us illustrate the content of Ramsey's Theorem for graphs by looking at an example. If the edge-coloring consists only of two colors, say red and blue, and we assume $n = 3$, then Ramsey's Theorem asserts that there exists a number $R(3, 2)$ such that any edge-coloring of a complete graph on $R(3, 2)$ vertices admits a monochromatic triangle. Note that $R(3, 2)$ cannot equal 5, because Figure 1.3 below shows a 2-coloring of K_5 containing no monochromatic triangle. However, taking

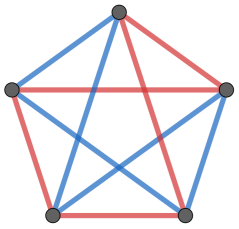

Figure 1.3: An edge-coloring of K_5 containing no monochromatic copy of K_3.

$R(3,2) = 6$ already works. Indeed, through some trial-and-error, one quickly realizes that it is impossible to find an edge-coloring of K_6 using only 2 colors that avoids monochromatic triangles. For instance, Figure 1.4 below shows a complete graph on 6 vertices where all but one edge have been colored either red or blue. As can be seen from the picture, it is impossible to complete the coloring without creating either a red or a blue triangle.

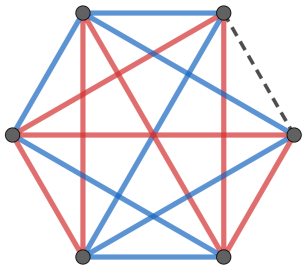

Figure 1.4: An almost-complete edge-coloring of K_6 that cannot be completed without creating a monochromatic copy of K_3. This example illustrates that it is impossible to color K_6 using two colors without producing a monochromatic copy of K_3.

The best possible value for $R(n,m)$ is called the *Ramsey number* for (n,m). Below is a list of Ramsey numbers known to date:

(n,m)	Ramsey Number
$(3,2)$	6
$(4,2)$	18
$(3,3)$	17
$(3,4)$	30
$(5,2)$	unknown
$(3,5)$	unknown
$(4,3)$	unknown
$\vdots$	

1.2. Ramsey's Theorem for 2-sets

Definition 5. A 2-*set* is a set consisting of exactly two elements. Given a set X, a 2-*subset* of X is any subset of X that is a 2-set. We will use $X^{(2)}$ to denote the set of all 2-subsets of X.

We have already seen examples of 2-subsets in the previous section. Indeed, the set of edges E of a graph $G = (V,E)$ consists of 2-subsets of the set of vertices V. In other words, $E \subseteq V^{(2)}$. Note that a graph $G = (V,E)$ is a complete graph if and only if $E = V^{(2)}$.

Definition 6. Let X be a set. A *coloring of* $X^{(2)}$ is an assignment of a color to each 2-subset of X. We call $X^{(2)}$ *monochromatic* if all elements in $X^{(2)}$ have the same color.

The following can be viewed as an "infinitary" version of Ramsey's Theorem for graphs.

Ramsey's Theorem for 2-sets. *Let X be an infinite set. Then for any finite coloring of $X^{(2)}$ there exists an infinite subset $Y \subseteq X$ such that $Y^{(2)}$ is monochromatic.*

Proof. Fix an arbitrary element $x_1 \in X$ and note that any 2-set of the form $\{x_1, x\}$ for $x \in X \backslash \{x_1\}$ has a certain color. Since the number of colors is finite but the set $X \backslash \{x_1\}$ is infinite, there exists an infinite subset $X_1 \subseteq X \backslash \{x_1\}$ such that all 2-sets of the form $\{x_1, x\}$ for $x \in X_1$ have the same color. Now fix an arbitrary element $x_2 \in X_1$ and let us repeat the same procedure. Any 2-set of the form $\{x_2, x\}$ for $x \in X_1 \backslash \{x_2\}$ has a certain color. For the same reason as before, since the number of colors is finite but the set $X_1 \backslash \{x_2\}$ is infinite, there exists an infinite subset $X_2 \subseteq X_1 \backslash \{x_1\}$ such all 2-sets of the form $\{x_2, x\}$ for $x \in X_2$ have the same color. Continuing this procedure produces an infinite sequence of distinct elements $x_1, x_2, x_3, \ldots$ and a nested family of infinite sets $X \supseteq X_1 \supseteq X_2 \supseteq X_3 \supseteq \ldots$ such that for all $i \in \mathbb{N}$ we have $x_{i+1} \in X_i$ and the set $\{\{x_i, x\} : x \in X_i\}$ is monochromatic.

Let c_i denote the color of elements in the set $\{\{x_i, x\} : x \in X_i\}$. Then $c_1, c_2, c_3, \ldots$ is an infinite sequence of colors. Since there are only finitely many different colors, one color must appear infinitely often in this sequence. In other words, there exists a color c and an infinite sequence $i_1 < i_2 < i_3 < \ldots \in \mathbb{N}$ such that $c_{i_k} = c$ for all $k \in \mathbb{N}$.

To finish the proof, define $Y = \{x_{i_k} : k \in \mathbb{N}\}$ and observe that any 2-subset of Y is of the form $\{x_{i_k}, x_{i_\ell}\}$ for $k < \ell \in \mathbb{N}$. Since $x_{i_\ell} \in X_{i_\ell - 1}$ and $X_{i_\ell - 1} \subseteq X_{i_k}$, the 2-set $\{x_{i_k}, x_{i_\ell}\}$ has the color c. Hence all 2-subsets of Y have the color c, which proves that $Y^{(2)}$ is monochromatic. □

Proposition 7. *Ramsey's Theorem for 2-sets implies Ramsey's Theorem for graphs.*

Proof. We shall prove the contrapositive. Suppose $V_1, V_2, \ldots$ is an infinite sequence of distinct vertices and let K_R denote the complete graph on the vertices $V_1, \ldots, V_R$. If Ramsey's Theorem for graphs is false then for some $n, m \in \mathbb{N}$ and every $R \in \mathbb{N}$ there exists an edge-coloring $\chi_R : \{V_1, \ldots, V_R\}^{(2)} \to \{1, \ldots, m\}$ of K_R admitting no monochromatic copy of K_n.

If $s \leqslant R$ then any edge-coloring of K_R induces an edge-coloring of K_s, because K_s is a subgraph of K_R. In particular, we can restrict χ_R to K_s and obtain an edge-coloring of K_s with at most m colors admitting no monochromatic copy of K_n. Let us denote this restriction of χ_R to K_s by $\chi_{R,s}$.

Set $\mathscr{R}_1 = \mathbb{N}$. Consider the sequence of colors $(\chi_{R,2})_{R \in \mathscr{R}_1}$, all of which are edge-colorings of K_2. Since there are only finitely many possibilities of coloring the edges of K_2 with m colors and $\mathscr{R}_1$ is infinite, there exists an infinite subset $\mathscr{R}_2 \subseteq \mathscr{R}_1$ such that $(\chi_{R,2})_{R \in \mathscr{R}_2}$ all yield the same edge-coloring of K_2. Next, we can repeat the same

argument with $\mathscr{R}_2$ in place of $\mathscr{R}_1$ and $\chi_{R,3}$ in place of $\chi_{R,2}$. Indeed, since there are only finitely many possibilities of coloring the edges of K_3 with m colors and $(\chi_{R,3})_{R\in\mathscr{R}_2}$ is an infinite sequence of edge-colorings of K_3, there exists an infinite subset $\mathscr{R}_3 \subseteq \mathscr{R}_2$ such that all colorings in $(\chi_{R,3})_{R\in\mathscr{R}_3}$ are identical. By continuing this procedure we end up with an infinite family of nested sets $\mathscr{R}_1 \supseteq \mathscr{R}_2 \supseteq \mathscr{R}_3 \supseteq \dots$ such that all edge-colorings in $\{\chi_{R,s} : R \in \mathscr{R}_s\}$ are identical. In other words, for all $R_1, R_2 \in \mathscr{R}_s$ and all distinct $i, j \in \{1,\dots,s\}$ the edge $\{V_i, V_j\}$ has the same color with respect to χ_{R_1} and χ_{R_2}.

Next define a finite coloring of $\mathbb{N}^{(2)}$ by assigning to each 2-subset $\{i,j\} \in \mathbb{N}^{(2)}$ the same color as the edge $\{V_i, V_j\}$ under the coloring χ_R, where R is any element in $\mathscr{R}_s$ and s is any number bigger than both i and j. Due to our construction, the choice of the color does not depend on which $R \in \mathscr{R}_s$ or which s bigger than i and j we choose. To finish the proof, note that with this coloring of $\mathbb{N}^{(2)}$ there does not exist a subset $Y \subseteq \mathbb{N}$ with $|Y| \geqslant n$ and such that $Y^{(2)}$ is monochormatic, because the existence of such a set would imply the existence of a monochromatic copy of K_n with respect to the coloring χ_R for sufficiently large R, which we know is not possible. This also means that there exists no infinite subset $Y \subseteq \mathbb{N}$ such that $Y^{(2)}$ is monochormatic, thus contradicting Ramsey's Theorem for 2-sets.

□

1.3. Schur's Theorem

Fermat's Last Theorem states that for $m \geqslant 3$ the equation

$$x^m + y^m = z^m \tag{1.3.1}$$

has no positive integer solutions $x, y, z \in \mathbb{N}$. For centuries, this remained one of the biggest open problems in mathematics, and one whose intriguing nature captivated many mathematicians. Among them was also Issai Schur, who investigated a natural, localized version of Fermat's Last Theorem. More precisely, he wondered whether for any $m \geqslant 2$ the congruence equation

$$x^m + y^m \equiv z^m \pmod{p} \tag{1.3.2}$$

possesses non-trivial solutions for all but finitely many primes p. Note that any non-trivial solution to Fermat's equation $x^m + y^m = z^m$ also offers a non-trivial solution to Schur's equation $x^m + y^m \equiv z^m \pmod{p}$ for all primes p satisfying $p > z^m$, but not the other way around. In order to address (1.3.2), Schur proved a theorem that is often regarded as the earliest result in Ramsey Theory:

Schur's Theorem ([Sch17]). *For any $m \in \mathbb{N}$ there exists $S = S(m) \in \mathbb{N}$ such that if the set $\{1,\dots,S\}$ is colored using at most m colors then there exist monochromatic $x, y, z \in \{1,\dots,S\}$ with $x + y = z$.*

Proof. Take $S = R(3,m)$, where $R(3,m)$ is the Ramsey number for $(3,m)$. Let K_S denote the complete graph on S vertices and denote the vertices of K_S by $V_1, V_2, \ldots, V_S$. Any coloring of the set $\{1,\ldots,S\}$ induces an edge-coloring on K_S by assigning to each edge $\{V_i, V_j\}$ the color of the number $|i-j| \in \{1,\ldots,S\}$. According to Ramsey's Theorem for graphs, K_S contains a monochromatic triangle. Let V_a, V_b, and V_c, for $a < b < c$, be the vertices of this monochromatic triangle. By setting

$$x = b-a, \qquad y = c-b, \qquad \text{and} \qquad z = c-a,$$

it is then easy to check that x, y, z have the same color and satisfy $x + y = z$. □

The smallest possible positive integer $S(m)$ for which the conclusion of Schur's Theorem holds is referred to as the *Schur number* for m. The known Schur numbers to date are:

m	Schur Number
2	5
3	14
4	45
5	161
6	unknown
7	unknown
⋮	

Here is an example from Schur's original paper [Sch17] of a 3-coloring of $\{1,\ldots,13\}$ admitting no monochromatic solution to the equation $x + y = z$:

color 1: $\{2,3,11,12\}$

color 2: $\{5,6,8,9\}$

color 3: $\{1,4,7,10,13\}$

More examples along these lines can be found here: https://oeis.org/A030126.

The proof that the Schur number for 5-colorings equals 161 took up 2 petabytes of space. Even though every 5-coloring of $\{1,\ldots,161\}$ admits a monochromatic solution to $x + y = z$, there are 2447113088 many 5-colorings of $\{1,\ldots,160\}$ admitting no monochromatic solution to $x + y = z$.

With the help of the above theorem, Schur was able to show that, contrary to Fermat's equation (1.3.1), its "local" counterpart (1.3.2) does possess non-trivial solutions.

Theorem 8. *Let $m \in \mathbb{N}$. There exists $F = F(m)$ such that for all prime numbers $p > F$ there exist $x, y, z \in \{1,\ldots,p-1\}$ with $x^m + y^m \equiv z^m \pmod{p}$.*

For the proof of Theorem 8, we will need the following basic fact from algebra, the proof of which is left to the interested reader.

Lemma 9. *Let $(K,+,\cdot)$ be a field and $f(x)\in K[x]$ a polynomial of degree $\deg(f)=m$ with coefficients in K. Then the number of roots of $f(x)$ is at most m.*

Let us now see the proof of Theorem 8.

Proof of Theorem 8. Take $F=S(m)$, where $S(m)$ is as guaranteed by Schur's Theorem. Let p be any prime number bigger than F. The set $\mathbb{F}_p=\{0,1,\dots,p-1\}$ of congruence classes modulo p naturally forms a field $(\mathbb{F}_p,+,\cdot)$ under the modular arithmetic operations $+$ and $\cdot$. Let $\mathbb{F}_p^\times=\mathbb{F}_p\setminus\{0\}$ and consider the set

$$C:=\{x^m : x\in\mathbb{F}_p^\times\}.$$

Note that C is a subgroup of the multiplicative group $(\mathbb{F}_p^\times,\cdot)$. This means that $\mathbb{F}_p^\times$ can be covered by cosets of C. More precisely, there exist coset representatives $g_1,g_2,\dots,g_r\in\mathbb{F}_p^\times$ such that

$$\mathbb{F}_p^\times=g_1C\cup g_2C\cup\ldots\cup g_rC. \tag{1.3.3}$$

It follows from Lemma 9 that for any $y\in\mathbb{F}_p^\times$ the equation $x^m\equiv y \pmod p$ has at most m solutions, because the polynomial x^m-y can have no more than m roots. So any $y\in\mathbb{F}_p^\times$ admits at most m representation of the form x^m, which implies that that $m|C|\geqslant|\mathbb{F}_p^\times|$. It follows that C can have at most m cosets, or in other words, $r\leqslant m$. Since $p>F$, the set $\{1,\dots,F\}$ is a subset of $\mathbb{F}_p^\times=\{1,\dots,p-1\}$ and hence (1.3.3) yields a partition of the set $\{1,\dots,F\}$ involving r disjoint cells. We can think of this partition as a coloring of $\{1,\dots,F\}$ using r colors. Since $F=S(m)$ and $r\leqslant m$, it follows from Schur's Theorem that there exist monochromatic $\tilde{x},\tilde{y},\tilde{z}\in\{1,\dots,F\}$ for which $\tilde{x}+\tilde{y}=\tilde{z}$. Since $\tilde{x},\tilde{y},\tilde{z}$ have the same color, they all belong to the same coset. In other words, there exists a coset representative $g_i\in\{g_1,\dots,g_r\}$ such that $\tilde{x},\tilde{y},\tilde{z}\in g_iC$. Take any $x,y,z\in\mathbb{F}_p^\times$ for which

$$\tilde{x}\equiv g_ix^m \pmod p,\qquad \tilde{y}\equiv g_iy^m \pmod p,\qquad \text{and}\qquad \tilde{z}\equiv g_iz^m \pmod p,$$

which is possible because $\tilde{x},\tilde{y},\tilde{z}\in g_iC$. Then we have

$$g_ix^m+g_iy^m\equiv g_iz^m \pmod p,$$

from which it follows that

$$x^m+y^m\equiv z^m \pmod p,$$

because $g_i\not\equiv 0 \pmod p$. □

1.4. Ramsey's Theorem for k-sets

Definition 10. A *k-set* is a set consisting of exactly k elements. Given a set X, a *k-subset* of X is any subset of X that is a k-set. We will use $X^{(k)}$ to denote the set of all k-subsets of X.

We have already seen Ramsey's Theorem for 2-sets. Here is Ramsey's result in full generality.

Ramsey's Theorem for k-sets ([Ram30]). *Let X be an infinite set and $k \geqslant 2$. Then for any finite coloring of $X^{(k)}$ there exists an infinite subset $Y \subseteq X$ such that $Y^{(k)}$ is monochromatic.*

Proof. Let us use a proof by induction on k. The base case of the induction, when $k = 2$, follows from Ramsey's Theorem for 2-sets established in Section 1.2. To prove the inductive step, assume $k \geqslant 3$ and Ramsey's Theorem has already been proven for $(k-1)$-sets. Let $Y_0 = X$ and fix an arbitrary element $y_1 \in Y_0$. Note that any k-set of the form $\{y_1, x_2, \ldots, x_k\}$ for $\{x_2, \ldots, x_k\} \in (Y_0 \backslash \{y_1\})^{(k-1)}$ has a certain color, which induces a finite coloring on $(Y_0 \backslash \{y_1\})^{(k-1)}$. Applying Ramsey's Theorem for $(k-1)$-sets, we can find an infinite subset $Y_1 \subseteq Y_0 \backslash \{y_1\}$ such that all k-sets of the form $\{y_1, x_2, \ldots, x_k\}$ for $\{x_2, \ldots, x_k\} \in Y_1^{(k-1)}$ are monochromatic. Next, fix an arbitrary element $y_2 \in Y_1$ and repeat the same procedure. The given coloring of k-sets of the form $\{y_2, x_2, \ldots, x_k\}$ for $\{x_2, \ldots, x_k\} \in (Y_1 \backslash \{y_2\})^{(k-1)}$ induces a finite coloring of $(Y_1 \backslash \{y_2\})^{(k-1)}$. Applying Ramsey's Theorem for $(k-1)$-sets once more yields an infinite subset $Y_2 \subseteq Y_1 \backslash \{y_2\}$ such that all k-sets of the form $\{y_2, x_2, \ldots, x_k\}$ for $\{x_2, \ldots, x_k\} \in Y_2^{(k-1)}$ are monochromatic. Continuing this procedure produces an infinite sequence of distinct elements $y_1, y_2, y_3, \ldots$ and a nested family of infinite sets $X = Y_0 \supseteq Y_1 \supseteq Y_2 \supseteq Y_3 \supseteq \ldots$ such that for all $i \in \mathbb{N}$ the set $\{\{y_i, x_2, \ldots, x_k\} : \{x_2, \ldots, x_k\} \in Y_i^{(k-1)}\}$ is monochromatic. Moreover, we have $y_{i+1} \in Y_i$ for all $i \in \mathbb{N}$.

Let c_i denote the color of elements in the set $\{\{y_i, x_2, \ldots, x_k\} : \{x_2, \ldots, x_k\} \in Y_i^{(k-1)}\}$. Since the sequence $c_1, c_2, c_3, \ldots$ is infinite but the number of colors is finite, one color must appear infinitely often in this sequence. In other words, there exists a color c and an infinite subsequence $c_{i_1}, c_{i_2}, c_{i_3}, \ldots \in \mathbb{N}$ such that $c_{i_\ell} = c$ for all $\ell \in \mathbb{N}$. To finish the proof, define $Y = \{y_{i_k} : k \in \mathbb{N}\}$ and observe that any k-subset of Y is of the form $\{y_{i_{\ell_1}}, \ldots, y_{i_{\ell_k}}\}$ for $\ell_1 < \ldots < \ell_k \in \mathbb{N}$. Since $\{y_{i_{\ell_2}}, \ldots, y_{i_{\ell_k}}\} \in Y_{i_{\ell_1}}$ because $\ell_1 < \ell_2 < \ldots < \ell_k$, the k-set $\{y_{i_{\ell_1}}, \ldots, y_{i_{\ell_k}}\}$ has the color c. Hence all k-subsets of Y have the color c, which proves that $Y^{(k)}$ is monochromatic. □

1.5. The compactness principle for colorings

Compactness Theorem for finite colorings. *Let Y be an infinite set, let $m \in \mathbb{N}$, and let $\mathscr{F}$ be a collection of finite subsets of Y. The following are equivalent:*

(i) For any coloring of Y using no more than m colors there exists $F \in \mathscr{F}$ such that all elements in F have the same color.

(ii) There exists a finite set $Z \subseteq Y$ such that for any finite coloring of Z using no more than m colors there exists $F \in \mathscr{F}$ with $F \subseteq Z$ and such that all elements in F have the same color.

Proof. The implication (ii) $\Longrightarrow$ (i) is immediate, so it only remains to prove (i) $\Longrightarrow$ (ii). We can view a coloring of Y that uses no more than m colors as a function $\chi\colon Y \to \{1,\dots,m\}$ simply by associating a number from 1 to m with each color. This means the space of all possible colorings of Y can be identified with the product space $\{1,\dots,m\}^Y$. Note that the finite set $\{1,\dots,m\}$, endowed with the discrete topology, is a compact Hausdorff space. By Tychonoff's theorem, $\{1,\dots,m\}^Y$ endowed with the product topology is therefore also a compact Hausdorff space.

For any finite non-empty set $Z \subseteq Y$ let $\mathscr{C}_Z$ be the set of all colorings in $\{1,\dots,m\}^Y$ for which there is monochromatic $F \in \mathscr{F}$ with $F \subseteq Z$. Then $\mathscr{C}_Z$ is an open set in the product topology on $\{1,\dots,m\}^Y$. Moreover, in light of statement (i), we have

$$\bigcup_{\substack{Z\subseteq Y\\ 0<|Z|<\infty}} \mathscr{C}_Z = \{1,\dots,m\}^Y.$$

By compactness, it follows that there is some finite non-empty set $Z \subseteq Y$ such that $\mathscr{C}_Z = \{1,\dots,m\}^Y$, completing the proof. □

1.6. Ramsey's Theorem for hypergraphs

A hypergraph is a generalization of a graph in which an edge can join multiple vertices at once.

Definition 11. Let $k \in \mathbb{N}$. A *k-uniform hypergraph* is a pair $G = (V,E)$ where V is a set of points, called *vertices*, and $E \subseteq V^{(k)}$ is a set of k-subsets of V, called *hyperedges*.

Given $k,n \in \mathbb{N}$ with $k \leqslant n$, a *complete k-uniform hypergraph on n vertices* is a k-uniform hypergraph $G = (V,E)$ where the set of vertices has cardinality n and where every set of k distinct vertices in V is connected by an edge. In other words, $G = (V,E)$ is a complete k-uniform hypergraph on n vertices if $|V| = n$ and $E = V^{(k)}$.

Ramsey's Theorem for hypergraphs. *For any $n,m,k \in \mathbb{N}$ there exists a number $R = R_k(n,m) \in \mathbb{N}$ such that any edge-coloring of a complete k-uniform hypergraph on R vertices with at most m colors admits a monochromatic copy of a complete k-uniform hypergraph on n vertices.*

Proof. Let $n,m,k \in \mathbb{N}$ be given. If follows from Ramsey's Theorem for k-sets that for any m-coloring of $\mathbb{N}^{(k)}$ there exists a set $S \subseteq \mathbb{N}$ with $|S| = n$ such that $S^{(k)}$ is monochromatic. If we now apply the Compactness Theorem for finite colorings to this statement (with $Y = \mathbb{N}^{(k)}$ and $\mathscr{F} = \{S^{(k)} : S \subseteq \mathbb{N},\ |S| = n\}$), it follows that there exists some integer $R = R_k(n,m)$ such that for any m-coloring of $\{1,\dots,R\}^{(k)}$ exists a set $S \subseteq \{1,\dots,R\}$ with $|S| = n$ such that $S^{(k)}$ is monochromatic. But note that $\{1,\dots,R\}^{(k)}$ can be identified with a complete k-uniform hypergraph on R vertices, and $S^{(k)}$ with a complete k-uniform hypergraph on n vertices. This finishes the proof. □

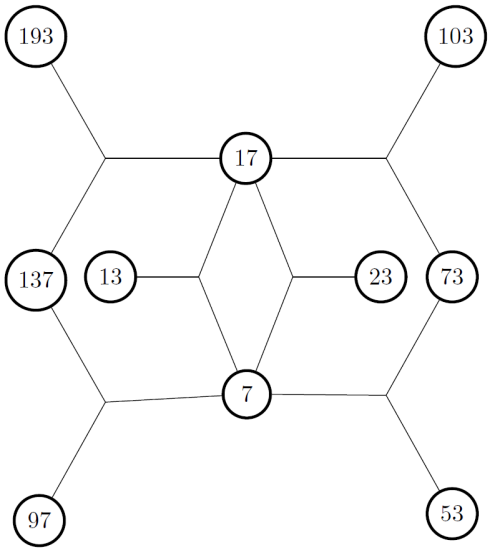

Figure 1.5: Here is an example of a 3-uniform hypergraph with vertices $V = \{7,13,17,23,53,73,97,103,137,193\}$, where three vertices are connected by a hyperedge if and only if their squares form a 3-term arithmetic progression. For example, $\{7,13,17\}$ is an edge, because $7^2, 13^2, 17^2$ are in an arithmetic progression.

1.7. Erdős-Szekeres' Theorem on convex polygons

Definition 12. A non-empty set $C \subseteq \mathbb{R}^2$ is called *convex* if for any $\vec{x}, \vec{y} \in C$ and $\lambda \in [0,1]$ one has $\lambda\vec{x} + (1-\lambda)\vec{y} \in C$.

The point $\lambda\vec{x} + (1-\lambda)\vec{y}$ is usually referred to as a *convex combination* of the points $\vec{x}$ and $\vec{y}$. Also observe that the set $\{\lambda\vec{x} + (1-\lambda)\vec{y} : \lambda \in [0,1]\}$ is just an algebraic description for the line segment joining the points $\vec{x}$ and $\vec{y}$.

Figure 1.6: A convex polygon (left) and a non-convex polygon (right).

Definition 13. The *convex hull* of a non-empty set $K \subseteq \mathbb{R}^2$ is the smallest convex set that contains K.

Since the intersection of convex sets is again a convex set, it follows that the convex hull of K equals the intersection of all convex sets that contain K. The convex hull can also be described algebraically as the set of all finite convex combinations of elements in the set. More precisely, if K is a subset of $\mathbb{R}^2$ and we use $\mathrm{conv}(K)$ to denote its convex hull, then

$$\mathrm{conv}(K) = \{w_1\vec{z}_1 + \ldots + w_\ell\vec{z}_\ell : \ell \in \mathbb{N},\ \vec{z}_1,\ldots,\vec{z}_\ell \in K,\ w_1,\ldots,w_\ell \in [0,1],\ w_1+\ldots+w_\ell = 1\}. \tag{1.7.1}$$

Mind that the convex hull of K should not be confused with the *closed convex hull* of K, which is defined as the smallest closed convex set that contains K, and is usually denoted by $\overline{\mathrm{conv}}(K)$ instead of $\mathrm{conv}(K)$.

Definition 14. A non-empty set of points $K \subseteq \mathbb{R}^2$ is said to be in *convex position* if no point $\vec{x} \in K$ belongs to the convex hull of $K\backslash\{\vec{x}\}$.

For example, a finite set $K \subseteq \mathbb{R}^2$ is in convex position if and only if its elements are the corners of a convex polygon.

Definition 15. A set $K \subseteq \mathbb{R}^2$ is called *discrete* if it has no accumulation points.

Erdős-Szekeres' Theorem on points in convex position. *Let K be an infinite discrete set of points in $\mathbb{R}^2$. Then either there is an infinite subset of K whose points lie on a straight line or there is an infinite subset of K whose points are in convex position.*

For the proof of Erdős-Szekeres' Theorem on points in convex position we will need the following classical result from convex geometry.

Carathéodory's theorem. *Let $K \subseteq \mathbb{R}^2$ with $|K| \geqslant 4$ be given. Then K is in convex position if and only if any four distinct points from K form a convex quadrilateral.*

Proof. Clearly, if K is in convex position then any quadrilateral formed using points from K is convex. To prove the converse, we will show that if K is not in convex position then there exist four points in K such that one of these points lies within the triangle spanned by the others.

Suppose K is not in convex position. Then there exists a point $\vec{x} \in K$ lying in the convex hull of $K' = K\backslash\{\vec{x}\}$. In light of (1.7.1), this means that we can write $\vec{x}$ as

$$\vec{x} = w_1\vec{z}_1 + \ldots + w_\ell\vec{z}_\ell, \tag{1.7.2}$$

where $\vec{z}_1,\ldots,\vec{z}_\ell \in K'$ and $w_1,\ldots,w_\ell \in [0,1]$ with $w_1+\ldots+w_\ell = 1$. Note that we can assume without loss of generality that $\vec{z}_1,\ldots,\vec{z}_\ell$ are in convex position. Indeed, if for example $\vec{z}_\ell$ belongs to the convex hull of $\vec{z}_1,\ldots,\vec{z}_{\ell-1}$ then we can express $\vec{z}_\ell$ as a convex combination of $\vec{z}_1,\ldots,\vec{z}_{\ell-1}$ and substitute this representation in (1.7.2), allowing us to represent $\vec{x}$ as a convex combination of $\vec{z}_1,\ldots,\vec{z}_{\ell-1}$ instead of $\vec{z}_1,\ldots,\vec{z}_\ell$. Thus, invoking induction on ℓ, we may assume that $\vec{z}_1,\ldots,\vec{z}_\ell$ are in convex position. This implies that $\vec{z}_1,\ldots,\vec{z}_\ell$ form the corners of a convex polygon. Since $\vec{x}$ lies inside this polygon and since convex polygons decompose into triangles (as illustrated in

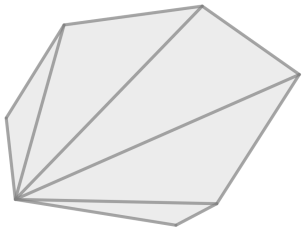

Figure 1.7: A convex polygon divided into triangles.

Figure 1.7), there exists $i < j < k \in \{1, \dots, \ell\}$ such that $\vec{x}$ lies in the triangle spanned by $\vec{z}_i, \vec{z}_j, \vec{z}_k$, finishing the proof. □

Proof of Erdős-Szekeres' Theorem on points in convex position. Let $K \subseteq \mathbb{R}^2$ be infinite. We begin by coloring $K^{(3)}$ by assigning the color red to $\{\vec{x}, \vec{y}, \vec{z}\} \in K^{(3)}$ if the points $\vec{x}, \vec{y}, \vec{z}$ are collinear and the color blue otherwise. According to Ramsey's Theorem for k-sets, there exists an infinite set $L \subseteq K$ such that all 3-sets in $L^{(3)}$ have the same color. If this color is red, then any three distinct points in L are collinear. This can only happen if all the points in L lie on a straight line, in which case we are done.

It remains to deal with the case when all elements in $L^{(3)}$ are blue, i.e., when no three points in L are collinear. In this situation, we need to apply Ramsey's Theorem one more time. Note that L is a discrete set. This implies that for any three points $\vec{x}, \vec{y}, \vec{z} \in L$ the triangle $\triangle\vec{x}\vec{y}\vec{z}$ contains only finitely many points from L. Color all elements in $L^{(3)}$ by assigning the color red to the 3-set $\{\vec{x}, \vec{y}, \vec{z}\} \in L^{(3)}$ if the triangle $\triangle\vec{x}\vec{y}\vec{z}$ contains an even number of points from L, and the color blue otherwise. By Ramsey's Theorem for k-sets there exists an infinite set $C \subseteq L$ such that $C^{(3)}$ is monochromatic. We claim that C is in convex position. Indeed, if C were not in convex position then, in view of Carathéodory's theorem, there exist four points $\vec{w}, \vec{x}, \vec{y}, \vec{z} \in C$ such that $\vec{w}$ lies inside the triangle $\Delta_0 = \triangle\vec{x}\vec{y}\vec{z}$. Note that Δ_0 splits into three smaller triangles, $\Delta_1 = \triangle\vec{w}\vec{y}\vec{z}$, $\Delta_2 = \triangle\vec{w}\vec{x}\vec{z}$, and $\Delta_3 = \triangle\vec{w}\vec{x}\vec{y}$, as seen in Figure 1.8. For $i = 0, 1, 2, 3$ let $\#\Delta_i$ denote the number of points from L inside the

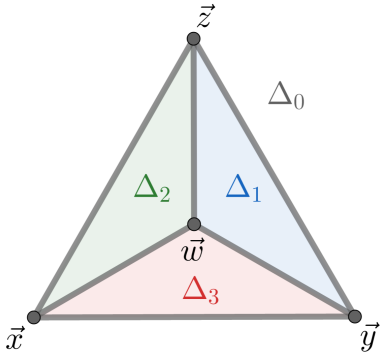

Figure 1.8

triangle Δ_i. Since no three points from L are collinear, there are no points on the boundary of any of these triangles aside from their corners. This means that the number of points from L inside Δ_0 equals the combined number of points inside the three smaller triangles plus the point $\vec{w}$, or in other words,

$$\#\Delta_0 = \#\Delta_1 + \#\Delta_2 + \#\Delta_3 + 1. \tag{1.7.3}$$

Recall that $C^{(3)}$ is monochromatic. If all elements in $C^{(3)}$ are red then the quantities $\#\Delta_0$, $\#\Delta_1$, $\#\Delta_2$, and $\#\Delta_3$ are even numbers. This would imply that the left hand side of (1.7.3) is an even number whereas the right hand side is an odd number, a contradiction. Similarly, if all elements in $C^{(3)}$ are blue then $\#\Delta_0$, $\#\Delta_1$, $\#\Delta_2$, $\#\Delta_3$ are odd numbers, implying that the left hand side of (1.7.3) is odd whereas the right hand side is even. Either way, we have obtained a contradiction, which means that C is in convex position. □

The following is a big open conjecture at the interface of convex geometry and Ramsey theory, posed by Erdős and Szekeres in 1960.

Conjecture (Erdős-Szekeres convex polygon problem). *Let $n \geqslant 3$. Any set of $2^{n-2}+1$ points in the plane, no three of which are collinear, contains a subset of n points in convex position.*

1.8. Erdős-Szekeres' Theorem on monotone paths

Erdős-Szekeres' Theorem on monotone paths. *Fix $n, m \in \mathbb{N}$. Any sequence of distinct real numbers of length at least $nm+1$ admits either a monotonically increasing subsequence of length $n+1$ or a monotonically decreasing subsequence of length $m+1$.*

Proof. Let $x_1, x_2, \ldots, x_{nm+1}$ be a sequence of real numbers of length $nm+1$. Label each element x_i in the sequence with the pair (a_i, b_i), where a_i is the length of the longest monotonically increasing subsequence ending with x_i and b_i is the length of the longest monotonically decreasing subsequence ending with x_i. Note that any two elements in the sequence are labeled with a different pair: if $i < j$ and $x_i < x_j$ then $a_i < a_j$, and on the other hand if $x_i > x_j$ then $b_i < b_j$. If $a_i \leqslant n$ and $b_i \leqslant m$ for all i then there are only nm possible labels, contradicting the fact that there are $nm+1$ elements in the sequence each with a unique label. It follows that either $a_i > n$ or $b_i > m$ for some i, yielding either an increasing sequence of length at least $n+1$ or a decreasing sequence of length at least $m+1$. □

Chapter 2

van der Waerden's Theorem

2.1. Notions of largeness

The goal of this section is to develop a general framework for dealing with notions of largeness for sets. In what follows, let X be a set and $\mathscr{P}$ a family of subsets of X. Since any reasonable notion of largeness is closed under supersets, the following definition will be very useful for our purposes.

Definition 16. We call $\mathscr{P}$ *upward closed* if for all $A \subseteq B \subseteq X$ we have $A \in \mathscr{P} \implies B \in \mathscr{P}$.

Natural examples of upward closed families include the set of all infinite subsets and the set of all cofinite subsets of a given infinite set X,

$$\mathscr{P}_{\text{inf}} = \{A \subseteq X : A \text{ is infinite}\} \qquad \text{and} \qquad \mathscr{P}_{\text{cofin}} = \{A \subseteq X : A \text{ is cofinite}\}.$$

Another example of an upward closed family is the collection of all sets that share a common point,

$$\mathscr{P}_{\{x\}} = \{A \subseteq X : x \in A\}$$

where $x \in X$ is fixed.

Definition 17. The *dual family* of $\mathscr{P}$, denoted by $\mathscr{P}^*$, is defined as

$$\mathscr{P}^* = \{A \subseteq X : A \cap B \neq \emptyset \text{ for all } B \in \mathscr{P}\}.$$

The families $\mathscr{P}_{\text{inf}}$ and $\mathscr{P}_{\text{cofin}}$ are mutually dual, meaning that $\mathscr{P}_{\text{inf}}^* = \mathscr{P}_{\text{cofin}}$ and $\mathscr{P}_{\text{cofin}}^* = \mathscr{P}_{\text{inf}}$, whereas the family $\mathscr{P}_{\{x\}}$ is self-dual in the sense that $\mathscr{P}_{\{x\}} = \mathscr{P}_{\{x\}}^*$. Note that if $\mathscr{P}$ is upward closed then its dual $\mathscr{P}^*$ is also upward closed. Also, if $\mathscr{P}$ is upward closed then we have the following two convenient properties:

- For any set $A \subseteq X$,

$$A \in \mathscr{P}^* \iff A^c \notin \mathscr{P}, \tag{2.1.1}$$

where $A^c = X \setminus A$ denotes the complement of A in X.

- $\mathscr{P}^{**} = \mathscr{P}$.

Definition 18. The family $\mathscr{P}$ is called *partition regular* if for any finite coloring of a set $A \in \mathscr{P}$ there exists a monochromatic subset of A that belongs to $\mathscr{P}$.

Using a standard "color blindness" argument, we deduce that any upward closed family $\mathscr{P}$ is partition regular if and only if for any disjoint $A, B \subseteq X$ with $A \cup B \in \mathscr{P}$ either $A \in \mathscr{P}$ or $B \in \mathscr{P}$. With some additional work, one can even remove the word disjoint from this statement.

Definition 19. We say a family of sets $\mathscr{P}$ is *closed under finite intersections* if for any $A_1, \ldots, A_k \in \mathscr{P}$ we have $A_1 \cap \ldots \cap A_k \in \mathscr{P}$.

Coming back to our previous examples, we see that the family $\mathscr{P}_{\text{inf}}$ is partition regular but not closed under finite intersections, whereas the family $\mathscr{P}_{\text{cofin}}$ is not partition regular but closed under finite intersections. In contrast, the family $\mathscr{P}_{\{x\}}$ is simultaneously partition regular and closed under finite intersections. These observations are explained by the next proposition.

Proposition 20. *Let $\mathscr{P}$ be an upward closed family of subsets of a set X. Then $\mathscr{P}$ is partition regular if and only if $\mathscr{P}^*$ is closed under finite intersections.*

Proof. ($\Rightarrow$) Suppose $\mathscr{P}$ is partition regular, let $A_1, \ldots, A_k \in \mathscr{P}^*$, and define $C_i = A_i^c$ for $i = 1, \ldots, k$. In view of (2.1.1) we have $C_1, \ldots, C_k \notin \mathscr{P}$. As $\mathscr{P}$ is partition regular, it follows from $C_1, \ldots, C_k \notin \mathscr{P}$ that $\bigcup_{i=1}^k C_i \notin \mathscr{P}$. Using (2.1.1) once more we get

$$\left(\bigcup_{i=1}^k C_i\right)^c = \bigcap_{i=1}^k A_i \notin \mathscr{P}^*.$$

This proves that $\mathscr{P}^*$ is closed under finite intersections.

($\Leftarrow$) Assume $\mathscr{P}^*$ is closed under finite intersections, let $C_1, \ldots, C_k \in \mathscr{P}$, and assume $\bigcup_{i=1}^k C_i \in \mathscr{P}$. Define $A_i = C_i^c$ for $i = 1, \ldots, k$ and note that from (2.1.1) and $\bigcup_{i=1}^k C_i \in \mathscr{P}$ we have

$$\bigcap_{i=1}^k A_i \notin \mathscr{P}^*.$$

Since $\mathscr{P}^*$ is closed under finite intersections, it follows that for some $i \in \{1, \ldots, k\}$ we must have $A_i \notin \mathscr{P}^*$. By (2.1.1) we conclude that $C_i \in \mathscr{P}$, showing that $\mathscr{P}$ is partition regular. □

Proposition 21. *Let $\mathscr{P}$ be upward closed. Then the family $\mathscr{P} \wedge \mathscr{P}^* = \{A \cap B : A \in \mathscr{P},\ B \in \mathscr{P}^*\}$ is partition regular.*

Proof. Suppose $C \in \mathscr{P} \wedge \mathscr{P}^*$. It suffices to show that if $C = C_1 \cup C_2$ with $C_1 \cap C_2 = \emptyset$ then either $C_1 \in \mathscr{P} \wedge \mathscr{P}^*$ or $C_2 \in \mathscr{P} \wedge \mathscr{P}^*$. Pick $A \in \mathscr{P}$ and $B \in \mathscr{P}^*$ such that $C = A \cap B$, and define $D = C_1 \cup A^c$. If $D \in \mathscr{P}^*$ then $C_1 = A \cap D$ belongs to $\mathscr{P} \wedge \mathscr{P}^*$ and we are

done. On the other hand, if $D \notin \mathscr{P}^*$ then $D^c \in \mathscr{P}$ (by (2.1.1)) and $C_2 = D^c \cap B$, which implies $C_2 \in \mathscr{P} \wedge \mathscr{P}^*$ and we are also done. □

2.2. Syndetic sets and thick sets

In what follows, let $A - n = \{m \in \mathbb{N} : m + n \in A\}$.

Definition 22. A set of positive integers $S \subseteq \mathbb{N}$ is called *syndetic* if there exists $h \in \mathbb{N}$ such that $S \cup (S-1) \cup \ldots \cup (S-h) = \mathbb{N}$.

Observe that syndetic sets are characterised by the property that the distance between consecutive elements is bounded. In other words, if $s_1 < s_2 < \ldots$ is an increasing enumeration of elements in S then S is syndetic if and only if $\sup_{k\in\mathbb{N}}(s_{k+1} - s_k) < \infty$. For this reason, syndetic sets are sometimes also referred to as *sets with bounded gaps*.

Definition 23. A set of positive integers $T \subseteq \mathbb{N}$ is called *thick* if for every $h \in \mathbb{N}$ the intersection $T \cap (T-1) \cap \ldots \cap (T-h)$ is non-empty.

Thick sets are characterized by the property that they contain arbitrarily long blocks of consecutive integers, i.e., a set $T \subseteq \mathbb{N}$ is thick if and only if for every $h \in \mathbb{N}$ there exists $n \in \mathbb{N}$ such that $\{n, n+1, \ldots, n+h\} \subseteq T$.

Let us use $\mathscr{P}_{\text{syn}}$ to denote the family of all syndetic subsets of $\mathbb{N}$ and $\mathscr{P}_{\text{thick}}$ for the family of all thick subsets of $\mathbb{N}$.

Proposition 24. *The families $\mathscr{P}_{\text{syn}}$ and $\mathscr{P}_{\text{thick}}$ are dual, i.e., $\mathscr{P}^*_{\text{syn}} = \mathscr{P}_{\text{thick}}$ and $\mathscr{P}^*_{\text{thick}} = \mathscr{P}_{\text{syn}}$.*

Proof. Since any syndetic set has bounded gaps, it must have non-empty intersection with any thick set, because thick sets contain arbitrarily long intervals. From this, it follows that $\mathscr{P}_{\text{syn}} \subseteq \mathscr{P}^*_{\text{thick}}$. On the other hand, if a set intersects every thick set then its complement cannot be thick. If the complement is not thick then the set itself must have bounded gaps, i.e., it is syndetic. This implies $\mathscr{P}^*_{\text{thick}} \subseteq \mathscr{P}_{\text{syn}}$. In conclusion, we have $\mathscr{P}_{\text{syn}} = \mathscr{P}^*_{\text{thick}}$, which implies $\mathscr{P}^*_{\text{syn}} = \mathscr{P}^{**}_{\text{thick}} = \mathscr{P}_{\text{thick}}$ as desired. □

Definition 25. Sets belonging to $\mathscr{P}_{\text{syn}} \wedge \mathscr{P}_{\text{thick}}$ are called *piecewise syndetic* sets.

Piecewise syndetic sets are characterized by the property that they have bounded gaps on arbitrarily large intervals. Here is a more intuitive explanation of what this means. Let A be a subset of $\mathbb{N}$ and let a_n denote the n-th element of A, so that $a_1, a_2, a_3, \ldots$ becomes an increasing enumeration of elements in A. Then A is piecewise syndetic if and only if there exists some number $h \in \mathbb{N}$ with the following property: Somewhere in $A = \{a_1, a_2, a_3, \ldots\}$ there are two consecutive elements a_n, a_{n+1} whose distance $a_{n+1} - a_n$ is at most h. Somewhere else in A there are three consecutive elements a_m, a_{m+1}, a_{m+2} such that the distance between

the first and the second $a_{m+1}-a_m$ and the distance between the second and the third $a_{m+2}-a_{m+1}$ are at most h. Then, somewhere else in the set, there exist four consecutive elements $a_k, a_{k+1}, a_{k+2}, a_{k+3}$ such that the distances $a_{k+1}-a_k$, $a_{k+2}-a_{k+1}$, $a_{k+3}-a_{k+2}$ are all at most h. And so on. This is another way of characterizing piecewise syndeticity.

Corollary 26. *Piecewise syndetic sets are partition regular.*

Proof. This follows by combining Proposition 21 and Proposition 24. □

Proposition 27. *Let $A \subseteq \mathbb{N}$ be piecewise syndetic. Then there exists a syndetic set L such that for any finite, non-empty $F \subseteq L$ the intersection*

$$\bigcap_{n\in F}(A-n) \tag{2.2.1}$$

is piecewise syndetic.

Proof. Since A is piecewise syndetic, there exist a syndetic set S and a thick set T so that $A = S \cap T$. Any thick set contains arbitrarily long intervals. Hence, by passing to a subset of T if necessary, we can assume without loss of generality that

$$T = [a_1, b_1] \cup [a_2, b_2] \cup [a_3, b_3] \cup \dots$$

where $a_1 < b_1 < a_2 < b_2, \dots \in \mathbb{N}$ with $b_n - a_n \to \infty$ as $n \to \infty$. Since S is syndetic, there exists $h \in \mathbb{N}$ for which $S \cup (S-1) \cup \dots \cup (S-h+1) \supseteq \mathbb{N}$. Our goal is to construct a sequence $l_0 < l_1 < l_2 < \dots \in \mathbb{N}$ such that $l_{n+1} - l_n \leqslant h$ for all $n \in \mathbb{N}$ and

$$\bigcap_{k=0}^{n}(A-l_k) \text{ is piecewise syndetic} \tag{2.2.2}$$

for all $n \in \mathbb{N}$. Once this task has been accomplished, we can take $L = \{l_n : n \in \mathbb{N}\}$ and we are done. Indeed L is syndetic because it has gaps bounded by h and (2.2.2) implies (2.2.1).

Let us now proceed with the construction of the sequence $l_0 < l_1 < l_2 < \dots$, for which we use induction. Define $l_0 = 0$. If $l_0, l_1, \dots, l_n$ have already been found, then l_{n+1} is constructed as follows: Define $A_n = \bigcap_{k=0}^{n}(A-l_k)$ and note that $A_n \subseteq A \subseteq T$. Since $S \cup (S-1) \cup \dots \cup (S-h+1) \supseteq \mathbb{N}$, we also have $(S-l_n-1) \cup (S-l_n-2) \cup \dots \cup (S-l_n-h) \supseteq \mathbb{N}$. In particular, by defining $A_{n,i} = A_n \cap (S-l_n-i)$ we get

$$A_n = A_{n,1} \cup \dots \cup A_{n,h}.$$

Using Corollary 26, it follows from the fact that A_n is piecewise syndetic that for some $i \in \{1, \dots, h\}$ the set $A_{n,i}$ is also piecewise syndetic. Define $l_{n+1} = l_n + i$ and note that

$$A_{n,i} = A_n \cap (S - l_{n+1}).$$

To finish the proof, let $T_{remainder} = T \setminus (T - l_{n+1})$ and note that

$$A_{n,i} = \big(A_{n,i} \cap (T - l_{n+1})\big) \cup \big(A_{n,i} \cap T_{remainder}\big),$$

because $A_{n,i} \subseteq T$. Since $A_{n,i}$ is piecewise syndetic, and the set

$$T_{remainder} \subseteq [b_1 - l_{n+1} + 1, b_1] \cup [b_2 - l_{n+1} + 1, b_2] \cup [b_3 - l_{n+1} + 1, b_3] \cup \dots$$

is clearly not piecewise syndetic, we conclude from Corollary 26 that $A_{n,i} \cap (T - l_{n+1})$ must be piecewise syndetic. Thus the set

$$\begin{aligned} \bigcap_{k=0}^{n+1} (A - l_k) &= A_n \cap (A - l_{n+1}) \\ &= A_n \cap (S - l_{n+1}) \cap (T - l_{n+1}) \\ &= A_{n,i} \cap (T - l_{n+1}) \end{aligned}$$

is piecewise syndetic, finishing the proof. □

From Proposition 27 we immediately obtain the following interesting corollary.

Corollary 28. *For any piecewise syndetic $A \subseteq \mathbb{N}$ there exist infinitely many $n \in \mathbb{N}$ such that $A \cap (A - n)$ is piecewise syndetic.*

2.3. van der Waerden's Theorem – equivalent forms

van der Waerden's Theorem is one of the key results in Combinatorial Number Theory.

van der Waerden's Theorem ([vdW28]). *For any $k \in \mathbb{N}$ and any finite coloring of $\mathbb{N}$ there exists a monochromatic k-term arithmetic progression.*

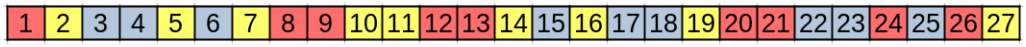

Figure 2.1: An example of a 3-coloring of the set $\{1, \dots, 27\}$. Can you find a monochromatic arithmetic progression of length 3?

Proposition 29. *Fix $k \in \mathbb{N}$. The following are equivalent:*

(i) (van der Waerden's Theorem – infinitary version). For any finite coloring of $\mathbb{N}$ there exists a monochromatic k-term arithmetic progression.

(ii) (van der Waerden's Theorem – finitary version). For any $r \in \mathbb{N}$ there exists $W = W(r,k) \in \mathbb{N}$ such that if the set $\{1, \dots, W\}$ is colored using at most r colors then there exists a monochromatic k-term arithmetic progression in $\{1, \dots, W\}$.

(iii) Any syndetic set $S \subseteq \mathbb{N}$ contains a k-term arithmetic progression.

(iv) For any piecewise syndetic $A \subseteq \mathbb{N}$ there exists $d \in \mathbb{N}$ and a piecewise syndetic set $B \subseteq \mathbb{N}$ such that for all $b \in B$ we have $\{b + d, b + 2d, \dots, b + kd\} \subseteq A$.

Let us now provide a proof of Proposition 29.

Proof of (i) $\Longleftrightarrow$ (ii). This equivalence follows immediately from the Compactness Theorem for finite colorings (see Section 1.5) applied to the set $Y = \mathbb{N}$ and the family $\mathscr{F} = \{\{a, a+d, \ldots, a+(k-1)d\} : a, d \in \mathbb{N}\}$. □

Proof of (i) $\Longrightarrow$ (iii). Let $S \subseteq \mathbb{N}$ be syndetic. By definition, this means there exists $h \in \mathbb{N}$ such that $S \cup (S-1) \cup \ldots \cup (S-h)$ covers $\mathbb{N}$. We can interpret this finite partitioning of $\mathbb{N}$ as a finite coloring of $\mathbb{N}$ using at most h colors. According to (i), one of the cells of the partition, say $S-j$, contains a k-term arithmetic progression. But if $S-j$ contains a k-term arithmetic progression then shifting this progression by j shows that S also contains a k-term arithmetic progression. □

Proof of (iii) $\Longrightarrow$ (iv). Let $A \subseteq \mathbb{N}$ be piecewise syndetic. Using Proposition 27 we can find a syndetic set L such that for any finite, non-empty $F \subseteq L$ the intersection

$$\bigcap_{n \in F} (A - n) \tag{2.3.1}$$

is piecewise syndetic. According to part (iii), the syndetic set L contains a k-term arithmetic progression, i.e., there exist $a, d \in \mathbb{N}$ such that $\{a, a+d, \ldots, a+(k-1)d\} \subseteq L$. In view of (2.3.1), the set $B' = (A-a) \cap (A-a-d) \cap \ldots \cap (A-a-(k-1)d)$ is piecewise syndetic. This implies that the set

$$B = (A-d) \cap \ldots \cap (A-kd)$$

is also piecewise syndetic, because $B = B' - d + a$. It is now easy to check that for all $b \in B$ we have $\{b+d, b+2d, \ldots, b+kd\} \subseteq A$ as desired. □

Proof of (iv) $\Longrightarrow$ (i). If $\mathbb{N}$ is colored using finitely many colors then, according to Corollary 26, there exists a monochromatic piecewise syndetic set. By part (iv), any piecewise sydnetic set contains a k-term arithmetic progression. It follows that there exists a monochromatic k-term arithmetic progression. □

The smallest possible number $W(r,k)$ in part (ii) of Proposition 29 is called the *van der Waerden number* for (r,k). Below is a table of known van der Waerden numbers (or best known lower bounds):

k/r	2 Colors	3 Colors	4 Colors	5 Colors	6 Colors
$3-$Term	9	27	76	> 170	$> \mathbf{225}$
$4-$Term	35	293	$> 1,048$	$> 2,254$	$> 9,778$
$5-$Term	178	$> 2,173$	$> 17,705$	$> 98,740$	$> 98,748$
$6-$Term	1132	$> 11,191$	$> 91,331$	$> 540,025$	$> 816,981$
$7-$Term	$> 3,703$	$> 48,811$	$> 420,217$	$> \mathbf{2,941,519}$	$> \mathbf{20,590,633}$
$8-$Term	$> 11,495$	$> 238,400$	$> 2,388,317$	$> \mathbf{16,718,219}$	$> \mathbf{117,027,533}$
$9-$Term	$> 41,265$	$> 932,745$	$> 10,898,729$	$> 79,706,009$	$> \mathbf{557,942,063}$
$10-$Term	$> 103,474$	$> 4,173,724$	$> 76,049,218$	$> 542,694,970$	$> \mathbf{3,798,864,790}$
$11-$Term	$> 193,941$	$> 18,603,731$	$> 329,263,781$	$> \mathbf{3,621,901,591}$	$> \mathbf{39,840,917,501}$
$12-$Term	$> 638,727$	$> 79,134,144$	$> 1,536,435,264$	$> \mathbf{16,900,787,904}$	$> \mathbf{185,908,666,944}$
$13-$Term	$> 1,642,309$	$> 251,282,317$	$> 5,683,410,589$	$> \mathbf{73,884,37,657}$	$> \mathbf{960,496,389,541}$

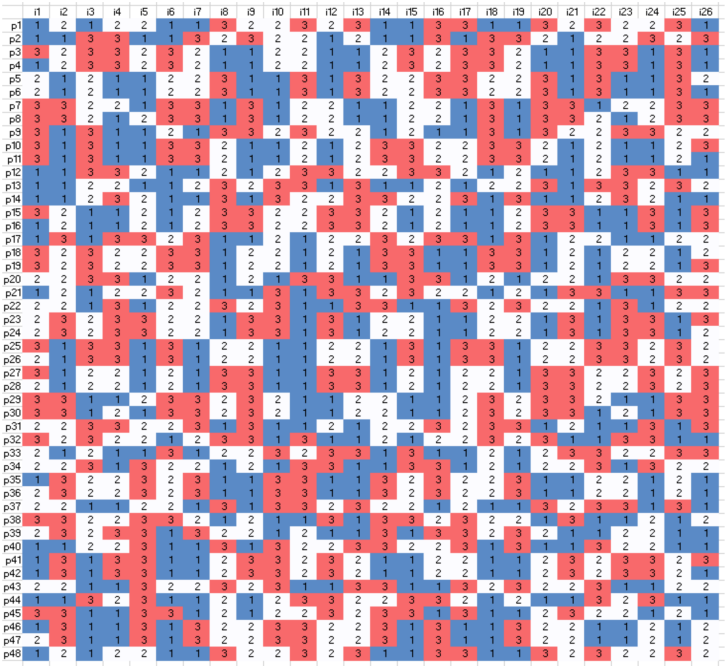

Figure 2.2: Since $N(3,3) = 27$, there exists no 3-coloring of the set $\{1,\dots,27\}$ without a monochromatic 3-term arithmetic progression. But there exist 48 distinct colorings of the set $\{1,\dots,26\}$ without a monochromatic 3-term arithmetic progression. A complete list of these 48 colorings, denoted by $p1,\dots,p48$, is depicted above.

The best known upper bound on van der Waerden numbers that holds for all $r,k \geqslant 2$ is

$$W(r,k) \leqslant 2^{2^{r^{2^{2^{k+9}}}}}.$$

2.4. Proof of van der Waerden's Theorem

Color Focusing Lemma. *Let $k \in \mathbb{N}$ and suppose van der Waerden's Theorem has already been proven for k. Then for any finite coloring of $\mathbb{N}$ and any $r \in \mathbb{N}$ there exist monochromatic piecewise syndetic sets $A_0, A_1, \dots, A_r \subseteq \mathbb{N}$ such that for all $0 \leqslant i < j \leqslant r$ there exists $u \in \mathbb{N}$ with*

$$\{a+u, a+2u, \dots, a+ku : a \in A_j\} \subseteq A_i. \tag{2.4.1}$$

Proof. We proceed by induction on r. It follows from Corollary 26 that there exists a monochromatic piecewise syndetic set $A_0 \subseteq \mathbb{N}$. If $A_0,\dots,A_{r-1}$ have already been found then A_r is constructed as follows. According to part (iv) of Proposition 29, there exists a piecewise syndetic set $B \subseteq \mathbb{N}$ and some $d \subseteq \mathbb{N}$ such that for all $b \in B$

we have $\{b+d, b+2d, \ldots, b+kd\} \subseteq A_{r-1}$. The finite coloring of $\mathbb{N}$ induces a finite partition of B. Hence, using Corollary 26 once more, we can find a monochromatic piecewise syndetic set $A_r \subseteq B$. Thus

$$\{a+d, a+2d, \ldots, a+kd : a \in A_r\} \subseteq A_{r-1}. \tag{2.4.2}$$

Let $0 \leqslant i < j \leqslant r$. If $j < r$ then (2.4.1) follows from the induction hypothesis. If $j = r$ then we can first use the induction hypothesis to find some $\tilde{u} \in \mathbb{N}$ such that

$$\{a+\tilde{u}, a+2\tilde{u}, \ldots, a+k\tilde{u} : a \in A_{r-1}\} \subseteq A_i. \tag{2.4.3}$$

Then, by defining $u = \tilde{u} + d$ and combining (2.4.2) and (2.4.3), we obtain $\{a+u, a+2u, \ldots, a+ku : a \in A_r\} \subseteq A_i$ as desired. □

Proof of van der Waerden's Theorem. We proceed by induction on k. If $k = 2$ then van der Waerden's Theorem is trivial. So let us assume that $k \geqslant 2$ and that van der Waerden's Theorem has already been proven for k. We want to show that any finite coloring of $\mathbb{N}$ admits a monochromatic $(k+1)$-term arithmetic progression.

Suppose $\mathbb{N}$ is colored using m colors. By applying the Color Focusing Lemma with $r = m$ we can find monochromatic piecewise syndetic sets $A_0, A_1, \ldots, A_m \subseteq \mathbb{N}$ such that for all $0 \leqslant i < j \leqslant m$ there exists $u \in \mathbb{N}$ with

$$\{a+u, a+2u, \ldots, a+ku : a \in A_j\} \subseteq A_i. \tag{2.4.4}$$

Since there are $m+1$ sets $A_0, A_1, \ldots, A_m$ but only m colors, two of the sets must have the same color. In other words, there exist $0 \leqslant i < j \leqslant m$ such that A_i and A_j have the same color. Take any $u \in \mathbb{N}$ for which (2.4.4) is satisfied and take any $a \in A_j$. Then the $(k+1)$-term arithmetic progression $a, a+u, \ldots, a+ku$ is monochromatic, finishing the proof. □

2.5. Gallai's Theorem

What if instead of finitely coloring the positive integers $\mathbb{N}$ as in Schur's Theorem or van der Waerden's Theorem, one colors the integer lattice points in the plane $\mathbb{N}^2$. This begs the following natural quesiton.

Question 30. Is it possible to find for any finite coloring of $\mathbb{N}^2$ a monochromatic square $(a,b), (a+h,b), (a,b+h), (a+h,b+h)$?

An affirmative answer to Question 30 is provided by Gallai's Theorem, which can the viewed as a higher-dimensional generalization of van der Waerden's Theorem. We need the following definition.

Definition 31. Let $V, W \subseteq \mathbb{Z}^d$. We say that W is *homothetic* to V if V can be shifted and dilated to become W, i.e., there exist $\vec{u} \in \mathbb{Z}^d$ and $\lambda \in \mathbb{Z} \setminus \{0\}$ such that $W = \lambda V + \vec{u}$.

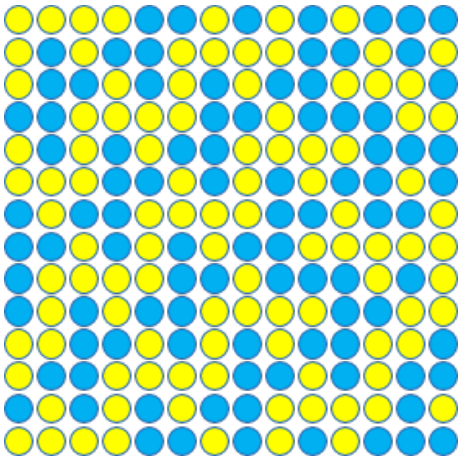

Figure 2.3: Can you find a monchromatic square in this two-coloring of the 14×14 grid?

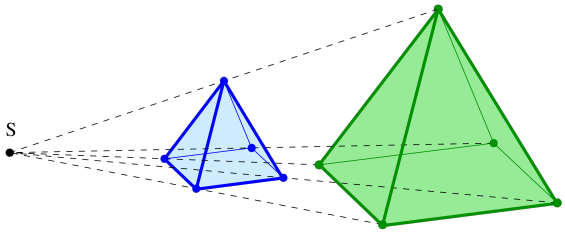

Figure 2.4: Two homothetic pyramids.

Gallai's Theorem. *Let V be a finite subset of $\mathbb{Z}^d$. For any finite coloring of $\mathbb{Z}^d$ there exists a monochromatic set of points homothetic to V.*

We can reduce Gallai's Theorem to the following.

Theorem 32. *For any finite coloring of $\mathbb{Z}^d$ there exist $(a_1,\ldots,a_d) \in \mathbb{Z}^d$ and $h \in \mathbb{N}$ such that the d-dimensional "cube"*

$$\{(a_1+\varepsilon_1 h,\ldots,a_d+\varepsilon_d h) : \varepsilon_1,\ldots,\varepsilon_d \in \{0,1\}\}$$

is monochromatic.

Proof that Theorem 32 implies Gallai's Theorem. Let $V = \{\vec{v}_1,\ldots,\vec{v}_r\}$ be a finite subset of $\mathbb{Z}^d$ and suppose $\chi\colon \mathbb{Z}^d \to \{1,\ldots,m\}$ is a coloring of $\mathbb{Z}^d$ using at most m colors. Define a coloring $\tilde{\chi}\colon \mathbb{Z}^r \to \{1,\ldots,m\}$ of $\mathbb{Z}^r$ as

$$\tilde{\chi}(n_1,\ldots,n_r) = \chi(n_1\vec{v}_1+\ldots+n_r\vec{v}_r), \qquad \forall (n_1,\ldots,n_r) \in \mathbb{Z}^r.$$

By Theorem 32, there exist $(a_1,\ldots,a_r) \in \mathbb{Z}^r$ and $h \in \mathbb{N}$ such that $\{(a_1+\varepsilon_1 h,\ldots,a_r+\varepsilon_r h) : \varepsilon_1,\ldots,\varepsilon_r \in \{0,1\}\}$ is monochromatic. Define

$$\vec{u} = a_1\vec{v}_1+\ldots+a_r\vec{v}_r \qquad \text{and} \qquad \lambda = h.$$

Then the set $\lambda V + \vec{u}$ is homothetic to V and monochromatic with respect to the coloring χ. □

Proof that Gallai's Theorem implies Theorem 32. Suppose $\chi\colon \mathbb{Z}^d \to \{1,\dots,m\}$ is a finite coloring of $\mathbb{Z}^d$. Let

$$H = \{(\varepsilon_1,\dots,\varepsilon_d) : \varepsilon_1,\dots,\varepsilon_d \in \{0,1\}\}$$

denote the unit cube in $\mathbb{Z}^d$. By Gallai's Theorem, we can find a homothetic image of H that is monochromatic with respect to χ, finishing the proof. □

The proof of Gallai's Theorem is omitted.

Chapter 3

Hindman's Theorem

3.1. Filters and Ultrafilters

Definition 33. Let X be a non-empty set. A family $\mathscr{F}$ of subsets of X is called a *filter* on X if

(i) $\emptyset \notin \mathscr{F}$ and $X \in \mathscr{F}$;
(ii) $\mathscr{F}$ is upward closed (see Definition 16);
(iii) $\mathscr{F}$ is closed under finite intersections (see Definition 19).

We call $\mathscr{F}$ an *ultrafilter* if it satisfies (i)–(iii) and, additionally,

(iv) $\mathscr{F}$ is *maximal*, i.e., no other filter on X contains $\mathscr{F}$ as a proper subset.

Example 34.
- Recall from Section 2.1 that $\mathscr{P}_{\text{cofin}} = \{A \subseteq X : A^c \text{ is finite}\}$ denotes the family of all cofinite subsets of X. This family forms a filter, called the *Fréchet filter* on X.
- If (X, τ) is a topological space with topology τ, then the *neighbourhood system* $\mathscr{U}(x) = \{U \subseteq X : \exists O \in \tau \text{ with } O \subseteq U \text{ and } x \in O\}$ is the collection of all neighbourhoods of a point $x \in X$ and forms a filter.
- If $(X, \mathscr{A}, \mu)$ is a probability space with sigma-algebra $\mathscr{A}$ and probability measure μ then the collection of measurable conull sets $\mathscr{N} = \{A \in \mathscr{A} : \mu(A) = 1\}$ is a filter on X.

Proposition 35. *Let $\mathscr{F}$ be a filter on X. Then $\mathscr{F}$ is an ultrafilter if and only if it is partition regular (see Definition 18).*

Proof. Let us first show that if $\mathscr{F}$ is an ultrafilter then it is also partition regular. Let $A \in \mathscr{F}$ be arbitrary and suppose $A = A_1 \cup A_2$. Our goal is to prove that either $A_1 \in \mathscr{F}$ or $A_2 \in \mathscr{F}$. Suppose $A_1 \notin \mathscr{F}$. Then we must have $B \cap A_2 \neq \emptyset$ for all $B \in \mathscr{F}$, because if there exists $B \in \mathscr{F}$ with $B \cap A_2 = \emptyset$ then $A_1 \supseteq A \cap B \in \mathscr{F}$, contradicting $A_1 \notin \mathscr{F}$. It follows that the family $\{B \cap A_2 : B \in \mathscr{F}\}$ does not contain the empty set

and hence

$$\mathcal{G} = \{C \subseteq X : \exists B \in \mathcal{F},\ B \cap A_2 \subseteq C\}$$

is a filter. Since $\mathcal{F}$ is maximal and $\mathcal{F} \subseteq \mathcal{G}$, we get $\mathcal{F} = \mathcal{G}$. Finally, since $A_2 \in \mathcal{G}$ we conclude $A_2 \in \mathcal{F}$ as desired.

It remains to show that if $\mathcal{F}$ is partition regular then it is an ultrafilter. Suppose $\mathcal{G}$ is a filter on X with $\mathcal{F} \subseteq \mathcal{G}$. For any $A \in \mathcal{G}$ we must have $A^c \notin \mathcal{G}$, because otherwise filter property (iii) would imply $A \cap A^c = \emptyset \in \mathcal{G}$, which would contradict filter property (i). Since $A^c \notin \mathcal{G}$, it also follows that $A^c \notin \mathcal{F}$ because $\mathcal{F} \subseteq \mathcal{G}$. Since $\mathcal{F}$ is partition regular and $A^c \notin \mathcal{F}$, we conclude that $A \in \mathcal{F}$. This proves that $\mathcal{F} = \mathcal{G}$ and hence $\mathcal{F}$ is an ultrafilter. □

Corollary 36. *A filter $\mathcal{F}$ on X is an ultrafilter if and only if for any $A \subseteq X$ either $A \in \mathcal{F}$ or $A^c \in \mathcal{F}$.*

Proof. This is an immediate consequence of the statement of Proposition 35. □

3.2. The Stone-Čech Compactification of $\mathbb{N}$

Definition 37. Ultrafilters of the form $\delta_n = \{A \subseteq \mathbb{N} : n \in A\}$ for $n \in \mathbb{N}$ are called *principal*. All other ultrafilters are called *non-principal*.

Proposition 38. *There exists a non-principal ultrafilter.*

Proof. Consider the Fréchet filter on $\mathbb{N}$, $\mathcal{P}_{\text{cofin}} = \{A \subseteq \mathbb{N} : A^c \text{ is finite}\}$, and order all filters $\mathcal{F}$ that contain $\mathcal{P}_{\text{cofin}}$ as a subset under set-inclusion. Since an arbitrary union of nested filters is again a filter, we see that any chain in this partial ordering has an upper bound. Thus, by Zorn's Lemma, there exists a maximal element p with respect to this partial ordering. By maximality, p must be an ultrafilter. Moreover, since p contains $\mathcal{P}_{\text{cofin}}$ as a subset, it cannot be a principal ultrafilter. □

Henceforth, let $\beta\mathbb{N}$ denote the set of all ultrafilters on $\mathbb{N}$ and, for $A \subseteq \mathbb{N}$, write $\overline{A} = \{p \in \beta\mathbb{N} : A \in p\}$. We observe that sets of the form $\overline{A}$ are closed under intersections, because $\overline{A} \cap \overline{B} = \overline{A \cap B}$. In particular, $\{\overline{A} : A \subseteq \mathbb{N}\}$ forms the basis for a topology on $\beta\mathbb{N}$.

Definition 39. The space $\beta\mathbb{N}$, endowed with the topology generated by $\{\overline{A} : A \subseteq \mathbb{N}\}$, is called the *Stone-Cech compactification* of $\mathbb{N}$.

Proposition 40. *The topology on $\beta\mathbb{N}$ is compact Hausdorff.*

Proof. To show that the topology on $\beta\mathbb{N}$ is compact, it suffices to show that for any cover of $\beta\mathbb{N}$, consisting of elements from the basis of the topology $\{\overline{A} : A \subseteq \mathbb{N}\}$, there exists a finite subcover. Let $(\overline{A}_i)_{i\in I}$ be such a cover of $\beta\mathbb{N}$. Consider

$$\mathscr{F} = \{B \subseteq \mathbb{N} : \exists i_1, \ldots, i_k \in I \text{ with } A_{i_1}^c \cap \ldots \cap A_{i_k}^c \subseteq B\},$$

and note that $\mathscr{F}$ satisfies properties (ii) and (iii) of the definition of a filter.

We now distinguish two cases, the case $\emptyset \notin \mathscr{F}$ and the case $\emptyset \in \mathscr{F}$. If $\emptyset \notin \mathscr{F}$ then $\mathscr{F}$ also satisfies property (i) of the definition of a filter and hence $\mathscr{F}$ is a filter. As we have seen in the proof of Proposition 38, any filter can be extended to an ultrafilter using Zorn's Lemma. Let $p \in \beta\mathbb{N}$ be an ultrafilter that extends $\mathscr{F}$, i.e., $\mathscr{F} \subseteq p$. Then $A_i^c \in p$ for all $i \in I$ by construction. This implies $p \notin \overline{A}_i$ for all $i \in I$, which contradicts the fact that $(\overline{A}_i)_{i\in I}$ covers all of $\beta\mathbb{N}$. We conclude that $\emptyset \notin \mathscr{F}$ cannot happen.

So we must be in the second case, when $\emptyset \in \mathscr{F}$. This means there exist $i_1, \ldots, i_k \in I$ with $A_{i_1}^c \cap \ldots \cap A_{i_k}^c = \emptyset$. But then $\overline{A}_{i_1}, \ldots, \overline{A}_{i_k}$ is a finite subcover and we are done with the proof that $\beta\mathbb{N}$ is compact.

To prove that the topology on $\beta\mathbb{N}$ is Hausdorff, let $p, q \in \beta\mathbb{N}$ be two distinct ultrafilters. Since $p \neq q$, there must either be a set in p that is not in q or there must be a set in q that is not in p (because otherwise p and q would contain the same sets and hence would be the same). Suppose there is a set A with $A \in p$ and $A \notin q$. By Corollary 36 we have $A^c \notin p$ and $A^c \in q$. We have found two disjoint open sets $\overline{A}$ and $\overline{A^c}$ that separate p and q, proving that the topology on $\beta\mathbb{N}$ is Hausdorff. □

An embedding of a topological space as a dense subset of a compact space is called a *compactification*.

Corollary 41. *$\beta\mathbb{N}$ is a compactification of $\mathbb{N}$.*

Proof. The map $\iota : n \mapsto \delta_n$ that sends a positive integer n to the principal ultrafilter $\delta_n = \{A \subseteq \mathbb{N} : n \in A\}$ is an embedding of $\mathbb{N}$ into $\beta\mathbb{N}$. Since $\overline{\{\delta_n : n \in \mathbb{N}\}} = \overline{\mathbb{N}} = \beta\mathbb{N}$, we see that $\mathbb{N}$ embeds as a dense set in $\beta\mathbb{N}$, proving that $\beta\mathbb{N}$ is a compactification of $\mathbb{N}$. □

3.3. Ellis-Numakura Lemma

Definition 42. If S is a set and $\cdot : S \times S \to S$ a binary operation on S satisfying the associative property

$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \qquad \forall a, b, c \in S,$$

then $(S, \cdot)$ is called a *semigroup*.

Perhaps the most well-known semigroup is $(\mathbb{N}, +)$, but other semigroups also show up naturally in various different settings. For instance, the set X^X of all functions from X to X is a semigroup under composition $\circ : X^X \times X^X \to X^X$, because composition of functions is always associative.

Definition 43. Suppose $(S,\cdot)$ is a semigroup and τ_S is a topology on S. If for any fixed $b \in S$ the map $a \mapsto a \cdot b$ is continuous then $(S,\cdot)$ is called *right-topological*.

Ellis-Numakura Lemma ([Ell58, Num52]). *Any right-topological compact Hausdorff semigroup $(S,\cdot)$ contains an idempotent element, i.e., an element $p \in S$ satisfying $p \cdot p = p$.*

Proof. Order all non-empty closed sub-semigroups of $(S,\cdot)$ under set-inclusion. By compactness, any nested family of such subgroups has non-empty intersection, from which it follows that any chain in this partial ordering possesses a lower bound. Thus, by Zorn's Lemma, there exists a minimal non-empty closed sub-semigroup, which we call $(G,\cdot)$. Let $p \in G$ be arbitrary. Observe that the set $Gp = \{a \cdot p : a \in G\}$ is compact, because the map $a \mapsto a \cdot p$ is continuous, and closed under the semigroup operation $\cdot : G \times G \to G$, because $(a \cdot p) \cdot (b \cdot p) = (a \cdot p \cdot b) \cdot p$. In other words, $(Gp,\cdot)$ is a non-empty closed sub-semigroup of $(G,\cdot)$. By minimiality, it follows that $G = Gp$. In particular, there exists some element $q \in G$ such that $q \cdot p = p$.

Next, consider the set $V = \{a \in G : a \cdot p = p\}$. Since $q \in V$, we know that V is non-empty. Also, V is compact because $a \mapsto a \cdot p$ is continuous and the topology is Hausdorff, and V is closed under the semigroup operation $\cdot : G \times G \to G$, because if $a \cdot p = p$ and $b \cdot p = p$ then $(a \cdot b) \cdot p = p$. Hence V is a non-empty closed sub-semigroup of G. Invoking the minimality assumption on G once more, we conclude that $V = G$. In particular, $p \in V$, which implies $p \cdot p = p$. □

3.4. Algebra on the Stone-Čech compactification of $\mathbb{N}$

Our next goal is to lift the additive arithmetic structure on $\mathbb{N}$ to its Stone-Čech compactification $\beta\mathbb{N}$. As a preparatory step, let us define the shift of a subset of $\mathbb{N}$ by an element in $\beta\mathbb{N}$.

Recall that for any set $A \subseteq \mathbb{N}$ and any positive integer n the *shift of A by n* is defined as

$$A - n = \{m \in \mathbb{N} : n + m \in A\}.$$

There is a natural way of extending this shift operation from integers to ultrafilters. Given a set $A \subseteq \mathbb{N}$ and an ultrafilter $q \in \beta\mathbb{N}$, we define the *shift of A by q* as

$$A - q = \{n \in \mathbb{N} : A - n \in q\}.$$

Note that if $\delta_n = \{A \subseteq \mathbb{N} : n \in A\}$ is the principal ultrafilter supported on n then the shift of A by δ_n coincides with the shift of A by n, that is,

$$A - \delta_n = A - n.$$

The ultrafilter-shift is a set function on $\mathbb{N}$ and interacts nicely with other set functions, such as unions, intersections, or set-theoretic complements. More precisely, it is straightforward to check that for any $A,B \subseteq \mathbb{N}$ and any $p,q \in \beta\mathbb{N}$ the following properties are satisfied:

1. $(A \cap B) - q = (A - q) \cap (B - q)$;
2. $(A \cup B) - q = (A - q) \cup (B - q)$;
3. $A^c - q = (A - q)^c$;
4. $A \subseteq B \implies A - q \subseteq B - q$.

We are now ready to define addition on $\beta\mathbb{N}$. Given two ultrafilters $p,q \in \beta\mathbb{N}$, define their sum $p+q$ as

$$p + q = \{A \subseteq \mathbb{N} : A - q \in p\}.$$

Lemma 44. *If p and q are ultrafilters on $\mathbb{N}$ then $p+q$ is an ultrafilter on $\mathbb{N}$.*

Proof. Let us first establish that $p+q$ is a filter by showing that it satisfies the three filter conditions:

- We begin by proving that $\emptyset \notin p+q$. By definition, we have $\emptyset - n = \emptyset$ for all $n \in \mathbb{N}$. It follows that $\emptyset - q = \emptyset$, and hence $\emptyset - q \notin p$. This shows that $\emptyset \notin p+q$.
- Next, let us verify that $p+q$ is upward closed. Let $A \subseteq B \subseteq \mathbb{N}$ be given. From $A \subseteq B$ it follows that $A - q \subseteq B - q$ and, since p is upward closed, we conclude $A - q \in p \implies B - q \in p$. By definition, this means $A \in p+q \implies B \in p+q$.
- Finally, let us verify that $p+q$ is closed under finite intersections. Suppose both A and B belong to $p+q$. This means that both $A-q$ and $B-q$ belong to p. Since p is closed under finite intersections, it follows that $(A-q)\cap(B-q) = (A\cap B)-q$ belongs to p. We get that $A \cap B \in p+q$ as desired.

Now that we have established that $p+q$ is a filter, we can use Corollary 36 to show that $p+q$ is an ultrafilter. Let $A \subseteq \mathbb{N}$. Since p is an ultrafilter, we either have $A - q \in p$ or $(A-q)^c \in p$. Since $(A-q)^c = A^c - q$, it follows that either $A - q \in p$ or $A^c - q \in p$. By the definition of $p+q$, we thus have $A \in p+q$ or $A^c \in p+q$. In view of Corollary 36, this proves that $p+q$ is an ultrafilter. □

Usually, the symbol + is reserved for commutative operations. It is therefore important to note that addition on $\beta\mathbb{N}$ is not commutative, despite the fact that the symbol + is used. This means that in general $p+q \neq q+p$. The reason why we use + to denote this operation on $\beta\mathbb{N}$ is because it naturally extends addition on $\mathbb{N}$: If δ_m and δ_n are the principal ultrafilters supported on m and n respectively then

$$\delta_m + \delta_n = \delta_{m+n}.$$

This also implies that the canonical map $\iota\colon n \mapsto \delta_n$ described in the proof of Corollary 41 is not just a continuous embedding of $\mathbb{N}$ into $\beta\mathbb{N}$, it is in fact a homomorphic continuous embedding of $(\mathbb{N},+)$ into $(\beta\mathbb{N},+)$.

Proposition 45. $(\beta\mathbb{N},+)$ *is a right-topological compact Hausdorff semigroup.*

Proof. It follows from Proposition 40 that $\beta\mathbb{N}$ is compact Hausdorff. To verify that $(\beta\mathbb{N},+)$ is a semigroup, we need to show that addition on $\beta\mathbb{N}$ is associative, i.e., for all $p,q,r\in\beta\mathbb{N}$ one has $(p+q)+r=p+(q+r)$. Note that for any $A\subseteq\mathbb{N}$ and $n\in\mathbb{N}$ we have

$$\begin{aligned}(A-n)-r&=\{m\in\mathbb{N}:(A-n-m)\in r\}\\&=\{m\in\mathbb{N}:(A-m)\in r\}-n\\&=(A-r)-n.\end{aligned}$$

Using this observation, we get

$$\begin{aligned}(A-r)-q&=\{n\in\mathbb{N}:(A-r)-n\in q\}\\&=\{n\in\mathbb{N}:(A-n)-r\in q\}\\&=\{n\in\mathbb{N}:(A-n)\in q+r\}\\&=A-(q+r).\end{aligned}$$

It follows that $A\in(p+q)+r$ if and only if $A\in p+(q+r)$, which proves that $(p+q)+r=p+(q+r)$.

It remains to prove that $(\beta\mathbb{N},+)$ is right-topological. Fix $q\in\beta\mathbb{N}$. In order to prove that $p\mapsto p+q$ is continuous, it suffices to show that for any $A\subseteq\mathbb{N}$ the preimage of $\overline{A}$ is open, because sets of this form generate the topology on $\beta\mathbb{N}$. By definition, the pre-image of $\overline{A}$ under $p\mapsto p+q$ equals $\{p\in\beta\mathbb{N}:p+q\in\overline{A}\}$. We have

$$\begin{aligned}\{p\in\beta\mathbb{N}:p+q\in\overline{A}\}&=\{p\in\beta\mathbb{N}:A\in p+q\}\\&=\{p\in\beta\mathbb{N}:A-q\in p\}\\&=\overline{A-q}.\end{aligned}$$

Since $\overline{A-q}$ is open, we are done. □

With Proposition 45 at hand, we can think of $+:\beta\mathbb{N}\times\beta\mathbb{N}\to\beta\mathbb{N}$ as a continuous (right-topological) lift of $+:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ from $\mathbb{N}$ to its Stone-Čech compactification.

3.5. Idempotent Ultrafilters and IP sets

Theorem 46. $(\beta\mathbb{N},+)$ *contains an idempotent element, i.e., there exists an ultrafilter* $p\in\beta\mathbb{N}$ *satisfying* $p+p=p$.

Proof. The existence of an idempotent ultrafilter follows directly by combining Proposition 45 with the Ellis-Numakura Lemma. □

Connecting different realms of mathematics is both beautiful and powerful. Idempotent ultrafilters are a perfect example of this phenomenon. Their shier existence is hard to comprehend, yet they from an astounding bridge between the topological group structure on $\beta\mathbb{N}$ and the additive group structure on $\mathbb{N}$.

Definition 47. Given $D \subseteq \mathbb{N}$, the set of *finite sums* of D is

$$\mathrm{FS}(D) = \left\{ \sum_{n \in F} n : F \subseteq D \text{ finite and non-empty} \right\}.$$

For example,

- if $D = \{x\}$ then $\mathrm{FS}(D) = \{x\}$;
- if $D = \{x, y\}$ then $\mathrm{FS}(D) = \{x, y, x+y\}$;
- if $D = \{x, y, z\}$ then $\mathrm{FS}(D) = \{x, y, z, x+y, x+z, y+z, x+y+z\}$
- if $D = \{x_1, x_2, x_3, \ldots\}$ then $\mathrm{FS}(D) = \{x_{i_1} + \ldots + x_{i_k} : k \in \mathbb{N},\ i_1 < \ldots < i_k \in \mathbb{N}\}$.

Definition 48. A set $A \subseteq \mathbb{N}$ is called an *IP-set* if there exists $x_1, x_2, x_3, \ldots \in \mathbb{N}$ with $\mathrm{FS}(\{x_1, x_2, x_3, \ldots\}) \subseteq A$.

Theorem 49. *If $p = p + p$ is an idempotent ultrafilter on $\mathbb{N}$ then any $A \in p$ is an IP-set.*

Proof. Using $p = p + p$, we get $(A - p) \in p$, and hence $A \cap (A - p) \in p$, because ultrafilters are closed under finite intersections. Let x_1 be an arbitrary element in $A \cap (A - p)$ and observe that $A \cap (A - x_1) \in p$ by the definition of $A - p$.

Next, define $A_1 = A \cap (A - x_1)$. As before, we have $A_1 \cap (A_1 - p) \in p$. Thus, taking x_2 to be any element in $A_1 \cap (A_1 - p)$ with $x_2 > x_1$, we have $A_1 \cap (A_1 - x_2) \in p$. So far, we have $\mathrm{FS}(\{x_1, x_2\}) = \{x_1, x_2, x_1 + x_2\} \subseteq A$.

Once again, letting $A_2 = A_1 \cap (A_1 - x_2)$, we have $A_2 \cap (A_2 - p) \in p$. Taking $x_3 \in A_2 \cap (A_2 - p)$ with $x_3 > x_2$, we have $A_2 \cap (A_2 - x_3) \in p$ as well as $\mathrm{FS}(\{x_1, x_2, x_3\}) = \{x_1, x_2, x_3, x_1 + x_2, x_1 + x_3, x_2 + x_3, x_1 + x_2 + x_3\} \subseteq A$.

Following this procedure, we can construct an infinite sequence $x_1 < x_2 < x_3 < \ldots \in \mathbb{N}$ such that $\mathrm{FS}(\{x_1, x_2, x_3, \ldots\}) \subseteq A$ as desired. □

3.6. Hindman's Finite Sums Theorem

Recall Schur's Theorem, which asserts that for any finite coloring of $\mathbb{N}$ there exists $\{x, y\} \subseteq \mathbb{N}$ such that $\mathrm{FS}(\{x, y\}) = \{x, y, x + y\}$ is monochromatic. The following result is one of the cornerstones of Ramsey Theory and offers an infinitary generalization of Schur's result.

Hindman's Finite Sums Theorem ([Hin74]). *For any finite coloring of $\mathbb{N}$ there exists an infinite set $D \subseteq \mathbb{N}$ such that $\mathrm{FS}(D)$ is monochromatic.*

Proof. Suppose $\mathbb{N}$ is colored using finitely many colors. Let $p = p + p$ be an idempotent ultrafilter on $\mathbb{N}$, which exists due to Theorem 46. Since ultrafilters are partition regular (cf. Proposition 35), there exists a monochromatic set $A \subseteq \mathbb{N}$ with $A \in p$. By Theorem 49, A contains $\mathrm{FS}(D)$ for an infinite set $D \subseteq \mathbb{N}$, finishing the proof. □

3.7. Hindman's Finite Unions Theorem

Definition 50. Let $\mathscr{F}(\mathbb{N})$ denote the set of all finite non-empty subsets of $\mathbb{N}$. Given $\alpha_1, \alpha_2, \alpha_3, \ldots \in \mathscr{F}(\mathbb{N})$, the *set of finite unions* of $\{\alpha_1, \alpha_2, \alpha_3, \ldots\}$ is

$$\mathrm{FU}(\{\alpha_1, \alpha_2, \alpha_3, \ldots\}) = \left\{ \alpha_{n_1} \cup \ldots \cup \alpha_{n_k} : k \in \mathbb{N},\ n_1, \ldots, n_k \in \mathbb{N} \right\}.$$

Hindman's Finite Unions Theorem ([Hin74]). *For any finite coloring of $\mathscr{F}(\mathbb{N})$ there exist mutually disjoint $\alpha_1, \alpha_2, \alpha_3, \ldots \in \mathscr{F}(\mathbb{N})$ such that $\mathrm{FU}(\{\alpha_1, \alpha_2, \alpha_3, \ldots\})$ is monochromatic.*

For the proof of Hindman's Finite Unions Theorem, we need a short technical lemma.

Lemma 51. *Let $D \subseteq \mathbb{N}$ be infinite. For any $m \in \mathbb{N}$ there exists $n \in \mathrm{FS}(D)$ such that $n \equiv 0 \bmod m$.*

Proof. By the pigeonhole principle, the infinite set D contains m numbers $x_1, x_2, \ldots, x_m$ belonging to the same residue class modulo m. Then $n = x_1 + \ldots + x_m$ is a number in $\mathrm{FS}(D)$ divisible by m. □

Proof of Hindman's Finite Unions Theorem. Recall that any positive integer n possesses a unique binary expansion,

$$n = \sum_{i=0}^{\infty} \varepsilon_i 2^{i-1}$$

where $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots \in \{0, 1\}$ are called the digits in the binary expansion of n and all but finitely many of them are equal to 0. Using the binary expansion, we can find a natural correspondence between elements in $\mathbb{N}$ and elements in $\mathscr{F}(\mathbb{N})$. Indeed, we can associate the digits of a natural number n with the indicator function of a finite set. More formally, we have the map $\phi \colon \mathbb{N} \to \mathscr{F}(\mathbb{N})$ given by

$$n \mapsto \phi(n) = \{i \in \mathbb{N} : \text{the } i\text{-th digit in the binary expansion of } n \text{ is } 1\}.$$

By uniqueness of the binary expansion, ϕ is a bijection between $\mathbb{N}$ and $\mathscr{F}(\mathbb{N})$.

Now suppose we are given a finite coloring of $\mathscr{F}(\mathbb{N})$. We can pull back this finite coloring to a finite coloring of $\mathbb{N}$ via the map ϕ. By Hindman's Finite Sums Theorem, there exist $x_1 < x_2 < \ldots \in \mathbb{N}$ such that $\mathrm{FS}(\{x_1, x_2, \ldots\})$ is monochromatic. Our hope is that this monochromatic finite sums set in $\mathbb{N}$ corresponds to a monochromatic finite unions set in $\mathscr{F}(\mathbb{N})$. However, this is not true on the nose because $\phi(x_i + x_j)$ is not necessarily equal to $\phi(x_i) \cup \phi(x_j)$, which in turn means that the image of $\mathrm{FS}(\{x_1, x_2, \ldots\})$ under ϕ is not necessarily a finite unions set. But this problem can be fixed by passing to a subset of $\mathrm{FS}(\{x_1, x_2, \ldots\})$. More precisely, our goal is to find

$y_1, y_2, \ldots$ such that $\mathrm{FS}(\{y_1, y_2, \ldots\}) \subseteq \mathrm{FS}(\{x_1, x_2, \ldots\})$ and such that $\phi(y_1), \phi(y_2), \ldots$ are pairwise disjoint. It then follows that for all $i_1, \ldots, i_k \in \mathbb{N}$ we have

$$\phi(y_{i_1} + \ldots + y_{i_k}) = \phi(y_{i_1}) \cup \ldots \cup \phi(y_{i_k})$$

and hence $\phi(\mathrm{FS}(\{y_1, y_2, \ldots\})) = \mathrm{FU}(\phi(y_1), \phi(y_2), \ldots)$. Since $\mathrm{FS}(\{x_1, x_2, \ldots\})$ is monochromatic and $\mathrm{FS}(\{y_1, y_2, \ldots\}) \subseteq \mathrm{FS}(\{x_1, x_2, \ldots\})$, the finite unions set $\mathrm{FU}(\phi(y_1), \phi(y_2), \ldots)$ is monochromatic too and the proof is complete. It remains to construct $y_1, y_2, \ldots$ with these properties.

Take $y_1 = x_1$. If $y_1 < \ldots < y_n$ have already been found then let $m \in \mathbb{N}$ be any number with $2^m > y_n$. Also, choose r sufficiently large such that $y_1, \ldots, y_n \in \mathrm{FS}(\{x_1, \ldots, x_r\})$. According to Lemma 51, we can find $y_{n+1} \in \mathrm{FS}(\{x_{r+1}, x_{r+2}, \ldots\})$ such that 2^m divides y_{n+1}. Note that with this choice of y_{n+1} we have

$$\mathrm{FS}(\{y_1, \ldots, y_{n+1}\}) = \mathrm{FS}(\{y_1, \ldots, y_n\}) \cup \big(\mathrm{FS}(\{y_1, \ldots, y_n\}) + y_{n+1}\big) \subseteq \mathrm{FS}(\{x_1, x_2 \ldots\}).$$

Moreover, since $2^m \mid y_{n+1}$, the first m digits in the binary expansion of y_{n+1} are zero. Contrarily, since $y_i < 2^m$ for all $i = 1, \ldots, n$, the only non-zero digits in the binary expansion of y_i are among the first m digits. This proves that $\phi(y_{n+1})$ and $\phi(y_i)$ are disjoint for all $i = 1, \ldots, n$. □

Corollary 52. *Any finite coloring of the semigroup $(\mathscr{F}(\mathbb{N}), \cup)$ admits a monochromatic isomorphic image of itself.*

Chapter 4

Roth's Theorem

4.1. Natural density on $\mathbb{N}$

Consider the following two sets of integers,

$$A = \{n \in \mathbb{N} : n \text{ is even}\} \qquad \text{and} \qquad B = \{n^2 : n \in \mathbb{N}\}.$$

How do the "sizes" of A and B compare to one another? Both sets have the same cardinality (they are both countably infinite), and neither one is a subset of the other. So from a set-theoretic point of view there seems to be no way of differentiating the largess of A from the largeness of B. Yet, intuitively, it seems as if A contains more numbers than B, because it is "more likely" for a positive integer to be an even number than it is for it to be a perfect square. In other words, A occupies a bigger proportion of the positive integers than B. This intuitive concept of comparative size in the positive integers is formalized using the notion of natural density, which measures the relative proportion of a set with respect to all of $\mathbb{N}$. With the help of this notion, we can turn vague statements such as "almost no integer is the sum of two squares" or "the probability for two integers to be coprime is $\frac{6}{\pi^2}$" into meaningful mathematical theorems.

Definition 53. The *lower density* and *upper density* of a set $A \subseteq \mathbb{N}$ are defined respectively as

$$\underline{d}(A) = \liminf_{N\to\infty} \frac{|A \cap \{1,\dots,N\}|}{N} \qquad \text{and} \qquad \overline{d}(A) = \limsup_{N\to\infty} \frac{|A \cap \{1,\dots,N\}|}{N}.$$

Observe that $\underline{d}(A) \leqslant \overline{d}(A)$ always. If $\underline{d}(A) = \overline{d}(A)$ then the limit

$$d(A) = \lim_{N\to\infty} \frac{|A \cap \{1,\dots,N\}|}{N}$$

exists and we call this number the *density* of A. In the literature, the density of a set is sometimes also referred to as the *natural density* or *asymptotic density*, but for

simplicity we will stick to the simpler term.

We start by mentioning some basic properties of upper and lower density functions. Let $A, B \subseteq \mathbb{N}$:

- **(Unit Range).** $0 \leqslant \underline{d}(A) \leqslant \overline{d}(A) \leqslant 1$.
- **(Monotonicity).** If $A \subseteq B$ then $\underline{d}(A) \leqslant \underline{d}(B)$ and $\overline{d}(A) \leqslant \overline{d}(B)$.
- **(Super- and Sub-Additivity).** If A and B are disjoint then $\underline{d}(A) + \underline{d}(B) \leqslant \underline{d}(A \cup B)$ and $\overline{d}(A \cup B) \leqslant \overline{d}(A) + \overline{d}(B)$.
- **(Complement Property).** $\overline{d}(A^c) = 1 - \underline{d}(A)$ and $\underline{d}(A^c) = 1 - \overline{d}(A)$.
- **(Shift Invariance).** For $n \in \mathbb{N}$ we have $\underline{d}(A - n) = \underline{d}(A)$ and $\overline{d}(A - n) = \overline{d}(A)$.

The following proposition is often helpful when calculating the density of sets that admit a natural enumeration or parametrization, such as for example $\{f(n) : n \in \mathbb{N}\}$ where $f : \mathbb{N} \to \mathbb{N}$ is an increasing function.

Proposition 54. *If $A = \{a_1 < a_2 < a_3 < \ldots\} \subseteq \mathbb{N}$ then*

$$\underline{d}(A) = \liminf_{n\to\infty} \frac{n}{a_n} \qquad \text{and} \qquad \overline{d}(A) = \limsup_{n\to\infty} \frac{n}{a_n}.$$

Proof. Since

$$\frac{|A \cap \{1, \ldots, a_n\}|}{a_n} = \frac{n}{a_n},$$

we immediately see that $\underline{d}(A) \leqslant \liminf_{n\to\infty} \frac{n}{a_n}$. For the other direction, note that if $N \in \mathbb{N}$ is arbitrary and n is the smallest integer satisfying $a_n > N$ then

$$\frac{|A \cap \{1, \ldots, N\}|}{N} = \frac{n-1}{N} > \frac{n-1}{a_n}.$$

This proves that $\underline{d}(A) \geqslant \liminf_{n\to\infty} \frac{n-1}{a_n}$. Since $\liminf_{n\to\infty} \frac{n-1}{a_n} = \liminf_{n\to\infty} \frac{n}{a_n}$, we have that $\underline{d}(A) \geqslant \liminf_{n\to\infty} \frac{n}{a_n}$, which finishes the proof that $\underline{d}(A) = \liminf_{n\to\infty} \frac{n}{a_n}$. The proof for the statement on upper density follows an analogous argument to the one that we have just seen for the lower density. □

4.2. Arithmetic progressions in sets of positive density

The following strengthening of van der Waerden's Theorem was conjectured by Erdős and Turán in 1936 and eventually proved by Szemerédi in 1975 using ingenious techniques from graph theory.

Szemerédi's Theorem ([Sze75]). *Let $k \in \mathbb{N}$. Any set $A \subseteq \mathbb{N}$ with positive upper density contains a k-term arithmetic progressions.*

The cases $k = 1$ and $k = 2$ of Szemerédi's Theorem are trivial. The purpose of this section is to present a proof of the first non-trivial case, which is $k = 3$. This special case was first established by Roth in 1953 and the proof relies on ideas from Fourier analysis.

Roth's Theorem. *Any set $A \subseteq \mathbb{N}$ with positive upper density contains a 3-term arithmetic progressions.*

Szemerédi's Theorem has been generalized in many different ways. One of the most striking results in this direction is the following landmark theorem.

Green-Tao Theorem. *The prime numbers $\mathbb{P} = \{2,3,5,7,11,\ldots\}$ contain a k-term arithmetic progression for every $k \in \mathbb{N}$.*

The following is a famous open conjecture in combinatorial number theory and offers a simultaneous generalization of both Szemerédi's Theorem and the Green-Tao Theorem.

Erdős' conjecture. *Let $k \in \mathbb{N}$. Any set $A \subseteq \mathbb{N}$ with $\sum_{n \in A} \frac{1}{n} = \infty$ contains a k-term arithmetic progression.*

4.3. Fourier Analysis of finite cyclic groups

For every $N \in \mathbb{N}$ let $\mathbb{Z}_N = \{0,1,\ldots,N-1\}$ denote the set of integers modulo N. When endowed with modular addition, $\mathbb{Z}_N$ forms a finite cyclic group of order N. Let $e(x)$ be shorthand for $e^{2\pi i x}$, $x \in \mathbb{R}$.

Definition 55. The *Fourier transform* of a function $f : \mathbb{Z}_N \to \mathbb{C}$ is defined for all $\xi \in \mathbb{Z}_N$ as

$$\hat{f}(\xi) = \frac{1}{N} \sum_{n \in \mathbb{Z}_N} f(n) e\big(-\tfrac{\xi n}{N}\big).$$

Proposition 56. *The Fourier transform on $\mathbb{Z}_N$ has the following properties:*

- *The* **Fourier Inversion Formula** *tells us that any function $f : \mathbb{Z}_N \to \mathbb{C}$ can be fully recovered from its Fourier coefficients using the formula*

$$f(n) = \sum_{\xi \in \mathbb{Z}_N} \hat{f}(\xi) e\big(\tfrac{\xi n}{N}\big).$$

- **Parseval's Identity** *says that the Fourier transform is a unitary operator in the sense that*

$$\frac{1}{N} \sum_{n \in \mathbb{Z}_N} f(n)\overline{g(n)} = \sum_{\xi \in \mathbb{Z}_N} \hat{f}(\xi)\overline{\hat{g}(\xi)};$$

- *An important special case of Parseval's Identity is* **Plancherel's Identity**, *which asserts that*

$$\frac{1}{N}\sum_{n\in\mathbb{Z}_N}|f(n)|^2=\sum_{\xi\in\mathbb{Z}_N}|\hat{f}(\xi)|^2;$$

- *Given* $f,g\colon\mathbb{Z}_N\to\mathbb{C}$, *the* **Convolution Formula** *states that the Fourier transform of the convolution* $(f*g)(n)=\frac{1}{N}\sum_{m\in\mathbb{Z}_N}f(n-m)g(m)$ *equals the product of the Fourier transforms of* f *and* g, *i.e.,*

$$\widehat{(f*g)}(\xi)=\hat{f}(\xi)\hat{g}(\xi),\qquad\forall\xi\in\mathbb{Z}_N.$$

Proof of the Fourier Inversion Formula. Using the definition of $\hat{f}(\xi)$, we have for any $n\in\mathbb{Z}_N$,

$$\sum_{\xi\in\mathbb{Z}_N}\hat{f}(\xi)e\big(\tfrac{\xi n}{N}\big)=\sum_{\xi\in\mathbb{Z}_N}\left(\frac{1}{N}\sum_{m\in\mathbb{Z}_N}f(m)e\big(-\tfrac{\xi m}{N}\big)\right)e\big(\tfrac{\xi n}{N}\big)$$

change order of summation

$$=\frac{1}{N}\sum_{m\in\mathbb{Z}_N}f(m)\left(\sum_{\xi\in\mathbb{Z}_N}e\big(\tfrac{\xi(n-m)}{N}\big)\right).$$

Since $\sum_{\xi\in\mathbb{Z}_N}e(\xi k/N)=0$ for any non-zero $k\in\mathbb{Z}_N$, it follows that

$$\sum_{\xi\in\mathbb{Z}_N}e\big(\tfrac{\xi(n-m)}{N}\big)=\begin{cases}N, & \text{if } n=m,\\ 0, & \text{otherwise.}\end{cases}$$

Hence $\frac{1}{N}\sum_{m\in\mathbb{Z}_N}f(m)\big(\sum_{\xi\in\mathbb{Z}_N}e(\xi(n-m)/N)\big)=f(n)$, finishing the proof. □

Proof of Parseval's Identity. Using the Fourier Inversion Formula, we obtain

$$\frac{1}{N}\sum_{n\in\mathbb{Z}_N}f(n)\overline{g(n)}=\frac{1}{N}\sum_{n\in\mathbb{Z}_N}\left(\sum_{\xi\in\mathbb{Z}_N}\sum_{\zeta\in\mathbb{Z}_N}\hat{f}(\xi)\overline{\hat{g}(\zeta)}e\big(\tfrac{(\xi-\zeta)n}{N}\big)\right)$$

change order of summation

$$=\sum_{\xi\in\mathbb{Z}_N}\sum_{\zeta\in\mathbb{Z}_N}\hat{f}(\xi)\overline{\hat{g}(\zeta)}\left(\frac{1}{N}\sum_{n\in\mathbb{Z}_N}e\big(\tfrac{(\xi-\zeta)n}{N}\big)\right).$$

Similar to what we observed above, we have

$$\frac{1}{N}\sum_{n\in\mathbb{Z}_N}e\big(\tfrac{(\xi-\zeta)n}{N}\big)=\begin{cases}1, & \text{if } \xi=\zeta,\\ 0, & \text{otherwise.}\end{cases}$$

Therefore, we obtain $\sum_{\xi\in\mathbb{Z}_N}\sum_{\zeta\in\mathbb{Z}_N}\hat{f}(\xi)\overline{\hat{g}(\zeta)}\big(\frac{1}{N}\sum_{n\in\mathbb{Z}_N}e((\xi-\zeta)n/N)\big)=\sum_{\xi\in\mathbb{Z}_N}\hat{f}(\xi)\overline{\hat{g}(\xi)}$ and the claim follows. □

Proof of Plancherel's Identity. This follows immediately by taking $f=g$ in Parseval's Identity . □

Proof of the Convolution Formula. This is a straightforward calculation. Indeed,

$$\widehat{(f*g)}(\xi)=\frac{1}{N}\sum_{n\in\mathbb{Z}_N}(f*g)(n)e\big(-\tfrac{\xi n}{N}\big)$$

$$= \frac{1}{N} \sum_{n \in \mathbb{Z}_N} \left(\frac{1}{N} \sum_{m \in \mathbb{Z}_N} f(n-m) g(m) \right) e\left(-\tfrac{\xi n}{N}\right)$$

change order of summation

$$= \frac{1}{N} \sum_{m \in \mathbb{Z}_N} g(m) \left(\frac{1}{N} \sum_{n \in \mathbb{Z}_N} f(n-m) e\left(-\tfrac{\xi n}{N}\right) \right).$$

Using the substitution $m + k = n$, we can write

$$\begin{aligned} &\frac{1}{N} \sum_{m \in \mathbb{Z}_N} g(m) \left(\frac{1}{N} \sum_{n \in \mathbb{Z}_N} f(n-m) e\left(-\tfrac{\xi n}{N}\right) \right) \\ &\qquad = \left(\frac{1}{N} \sum_{m \in \mathbb{Z}_N} g(m) e\left(-\tfrac{\xi m}{N}\right) \right) \left(\frac{1}{N} \sum_{k \in \mathbb{Z}_N} f(k) e\left(-\tfrac{\xi k}{N}\right) \right) \\ &\qquad = \hat{f}(\xi) \hat{g}(\xi), \end{aligned}$$

completing the proof. □

Interpretation of discrete Fourier transform. Let $\mathbb{C}^{\mathbb{Z}_N} = \{f : \mathbb{Z}_N \to \mathbb{C}\}$ denote the space of all functions from $\mathbb{Z}_N$ to $\mathbb{C}$. It is easy to see that $\mathbb{C}^{\mathbb{Z}_N}$ is an $\mathbb{N}$-dimensional complex vector space (i.e., isomorphic to $\mathbb{C}^N$). There are two natural orthogonal bases to consider for this vector space. The first basis arises from the canonical basis vectors $\delta_0, \delta_1, \ldots, \delta_{N-1}$, where

$$\delta_m(n) = \begin{cases} 1 & \text{if } n = m, \\ 0 & \text{otherwise.} \end{cases}$$

It is clear that any $f : \mathbb{Z}_N \to \mathbb{C}$ can be expressed uniquely as a linear combination of Dirac delta functions δ_m. This is the usual, canonical representation. Yet there is another, equally natural orthogonal basis for $\mathbb{C}^{\mathbb{Z}_N}$ to consider: The character basis $e_0, e_1, \ldots, e_{N-1}$ where

$$e_\xi(n) = e\left(\tfrac{\xi n}{N}\right).$$

The discrete Fourier transform defined in Definition 55 is nothing more than a change of basis from the canonical basis to the character basis.

4.4. Linear homogeneous equations in 3 variables

Let $a, b, c \in \mathbb{Z} \backslash \{0\}$ and let $N \in \mathbb{N}$ be a large positive integer. In this section we investigate the following basic question: What sets $A \subseteq \{0, 1, \ldots, N-1\}$ contain a solution (or perhaps even many solutions) to the linear homogeneous equation

$$ax + by + cz = 0. \tag{4.4.1}$$

In other words, what are necessary and/or sufficient conditions on a set $A \subseteq \{0,1,\dots,N-1\}$ such that there exist $x,y,z \in A$ satisfying (4.4.1).

Example 57.

- Schur's Theorem tells us that if N is sufficiently large then for any set $A \subseteq \{1,\dots,N\}$ either A or its complement $\{1,\dots,N\}\backslash A$ contains a solution to $x+y=z$. Note the "Schur's equation" $x+y=z$ corresponds to equation (4.4.1) with $a=b=1$ and $c=-1$.
- As we will see below (see Proposition 63), Roth's Theorem tells us that if $\delta > 0$ and N is sufficiently large then any set $A \subseteq \{1,\dots,N\}$ with $|A| \geqslant \delta N$ contains a 3-term arithmetic progression, which is equivalent to containing a solution to the equation $x+y=2z$. This corresponds to a solution of equation (4.4.1) with $a=b=1$ and $c=-2$.

Given $N \in \mathbb{N}$ and $a,b,c \in \mathbb{Z}\backslash\{0\}$, we are interested in estimating the number of solutions to the equation $ax+by+cz=0$, i.e., the cardinality of the set

$$\{(x,y,z) \in A \times A \times A : ax+by+cz=0\}.$$

Proposition 58. *Let $N,N' \in \mathbb{N}$ and $a,b,c \in \mathbb{Z}\backslash\{0\}$ with $N(|a|+|b|+|c|) \leqslant N'$. Then for any triple $x,y,z \in \{0,1,\dots,N-1\}$ the following are equivalent:*

(i) $ax+by+cz=0$;

(ii) $ax+by+cz \equiv 0 \bmod N'$.

Proof. If there are $x,y,z \in A$ with $ax+by+cz=0$ then we also have $ax+by+cz \equiv 0 \bmod N'$. On the other hand, if there exist $x,y,z \in A$ with $ax+by+cz \equiv 0 \bmod N'$ then we must have $ax+by+cz=0$ because the assumption $N(|a|+|b|+|c|) \leqslant N'$ implies $|ax+by+cz| < N'$. □

In what follows, if $N < N'$ then we identify $\mathbb{Z}_N = \{0,1,\dots,N-1\}$ with a subset of $\mathbb{Z}_{N'} = \{0,1,\dots,N'-1\}$ in the obvious manner. In particular, if $A \subseteq \{0,1,\dots,N-1\}$ then we can think of A as a subset of both $\mathbb{Z}_N$ and $\mathbb{Z}_{N'}$.

Corollary 59. *Let $N,N' \in \mathbb{N}$ and $a,b,c \in \mathbb{Z}\backslash\{0\}$ with $N(|a|+|b|+|c|) \leqslant N'$. Then for any set $A \in \{0,1,\dots,N-1\}$, the number of solutions from A to the equation $ax+by+cz=0$ in $(\mathbb{Z},+)$ is the same as the number of solutions from A to the congruence equation $ax+by+cz \equiv 0 \bmod N'$ in $(\mathbb{Z}_{N'},+)$.*

Proof. This follows straightaway from Proposition 58. □

Proposition 60. *Let $N \in \mathbb{N}$ and $a,b,c \in \mathbb{Z}\backslash\{0\}$. Suppose N is coprime to abc. Then for all $A_1,A_2,A_3 \subseteq \{0,1,\dots,N-1\}$ we have*

$$\big|\{(x,y,z) \in A_1 \times A_2 \times A_3 : ax+by+cz \equiv 0 \bmod N\}\big| = N^2 \sum_{\xi \in \mathbb{Z}_N} \hat{A}_1(a\xi)\hat{A}_2(b\xi)\hat{A}_3(c\xi),$$

where $\hat{A}_i : \mathbb{Z}_N \to \mathbb{C}$ denotes the Fourier transform of the indicator function 1_{A_i} of A_i.

Proof. We begin by showing that $\widehat{aA_1}(\xi) = \hat{A}_1(a\xi)$. Using the definition of the Fourier transform, we get

$$\widehat{aA_1}(\xi) = \frac{1}{N} \sum_{n \in \mathbb{Z}_N} 1_{aA_1}(n) e\left(-\tfrac{n\xi}{N}\right).$$

Since a and N are coprime, the map $n \mapsto an$ is a bijection from $\mathbb{Z}_N$ to $\mathbb{Z}_N$. We can thus substitute an for n and get

$$\widehat{aA_1}(\xi) = \frac{1}{N} \sum_{n \in \mathbb{Z}_N} 1_{aA_1}(an) e\left(-\tfrac{an\xi}{N}\right).$$

Using once more that a and N are coprime, we get $1_{aA_1}(an) = 1_{A_1}(n)$ and so

$$\begin{aligned}\widehat{aA_1}(\xi) &= \frac{1}{N} \sum_{n \in \mathbb{Z}_N} 1_{aA_1}(an) e\left(-\tfrac{an\xi}{N}\right) \\ &= \frac{1}{N} \sum_{n \in \mathbb{Z}_N} 1_{A_1}(n) e\left(-\tfrac{an\xi}{N}\right) \\ &= \hat{A}_1(a\xi).\end{aligned}$$

An analogous argument proves $\widehat{bA_2}(\xi) = \hat{A}_2(b\xi)$ and $\widehat{cA_3}(\xi) = \hat{A}_3(c\xi)$.

Next, using the Fourier Inversion Formula, we get

$$\begin{aligned}1_{aA_1}(n) &= \sum_{\xi_1 \in \mathbb{Z}_N} \hat{A}_1(a\xi_1) e\left(\tfrac{\xi_1 n}{N}\right). \\ 1_{bA_2}(n) &= \sum_{\xi_2 \in \mathbb{Z}_N} \hat{A}_2(b\xi_2) e\left(\tfrac{\xi_2 n}{N}\right), \\ 1_{cA_3}(n) &= \sum_{\xi_3 \in \mathbb{Z}_N} \hat{A}_3(c\xi_3) e\left(\tfrac{\xi_3 n}{N}\right).\end{aligned}$$

We now obtain

$$\begin{aligned}&\left|\{(x,y,z) \in A_1 \times A_2 \times A_3 : ax + by + cz \equiv 0 \bmod N\}\right| \\ &\qquad = \sum_{n,m \in \mathbb{Z}_N} 1_{aA_1}(n) 1_{bA_2}(m) 1_{cA_3}(-n-m) \\ &\qquad = \sum_{n,m \in \mathbb{Z}_N} \sum_{\xi_1,\xi_2,\xi_3 \in \mathbb{Z}_N} \hat{A}_1(a\xi_1) \hat{A}_2(b\xi_2) \hat{A}_3(c\xi_3) e\left(\tfrac{\xi_1 n + \xi_2 m - \xi_3(n+m)}{N}\right) \\ &\qquad = \sum_{\xi_1,\xi_2,\xi_3 \in \mathbb{Z}_N} \hat{A}_1(a\xi_1) \hat{A}(b\xi_2)_2 \hat{A}_3(c\xi_3) \sum_{n,m \in \mathbb{Z}_N} e\left(\tfrac{\xi_1 n + \xi_2 m - \xi_3(n+m)}{N}\right).\end{aligned}$$

Note that the inner sum in m vanishes unless $\xi_2 = \xi_3$, whereas the inner sum in n vanishes unless $\xi_1 = \xi_3$. Thus the only non-zero contribution arises when $\xi_1 = \xi_2 = \xi_3$, yielding

$$\left|\{(x,y,z) \in A_1 \times A_2 \times A_3 : ax + by + cz \equiv 0 \bmod N\}\right| = N^2 \sum_{\xi \in \mathbb{Z}_N} \hat{A}_1(a\xi) \hat{A}_2(b\xi) \hat{A}_3(c\xi),$$

as desired. □

4.5. Pseudorandom sets

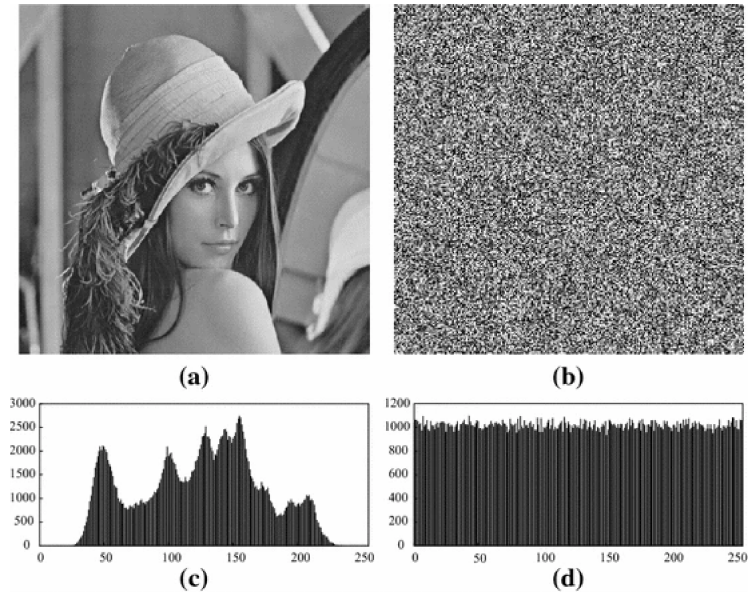

Figure 4.1: Depicted above are two grayscale images labeled (a) and (b). If each image has a resolution of N pixels, we can use the set $\{0,1,\ldots,N-1\}$ to index the pixels in a linear order, typically from left to right and top to bottom. If we also associate each pixel's intensity with a value between 0 (black) and 1 (white), a grayscale image can be thought of as a function $f:\{0,1,\ldots,N-1\}\to[0,1]$. This point of view allows us to associate to each grayscale image a Fourier transform using Definition 55. For the images (a) and (b), their respective Fourier transforms are depicted in (c) and (d). We observe that image (a), which has a clear structure with meaningfully arranged pixels, exhibits a Fourier transform where certain frequencies are dominant while others are less pronounced. In contrast, image (b), often referred to as "white noise", shows no bias among frequencies; its Fourier transform gives roughly equal value to all frequencies, with a flat power spectral density.

Definition 61. Let $A\subseteq\{0,1,\ldots,N-1\}$ and $\varepsilon>0$. We say that A is *ε-pseudorandom* if $|\hat{A}(\xi)|\leqslant\varepsilon$ holds for all $\xi\in\mathbb{Z}_N\backslash\{0\}$.

Proposition 62. *Let $N\in\mathbb{N}$, $a,b,c\in\mathbb{Z}\backslash\{0\}$, and $\varepsilon,\delta>0$. Suppose N is coprime to abc and $A_1,A_2,A_3\subseteq\{0,1,\ldots,N-1\}$ satisfy $|A_i|\geqslant\delta N$. If at least one of the A_i is ε-pseudorandom then $A_1\times A_2\times A_3$ contains at least $\delta N^2(\delta^2-\varepsilon)$ many solutions to the congruence equation $ax+by+cz\equiv 0 \bmod N$.*

Proof. Without loss of generality, let us assume that A_1 is ε-pseudorandom; if one of

the other two sets is the one that is ε-pseudorandom then by symmetry the argument of the proof remains the same, just with the order switched.

In view of Proposition 60, we have

$$\big|\{(x,y,z)\in A_1\times A_2\times A_3 : ax+by+cz\equiv 0 \bmod N\}\big| = N^2\sum_{\xi\in\mathbb{Z}_N}\hat{A}_1(a\xi)\hat{A}_2(b\xi)\hat{A}_3(c\xi)$$

Note that $\hat{A}_i(0)=\frac{|A_i|}{N}$. Hence, splitting the sum over ξ into the zero term and the non-zero terms and applying the triangle inequality yields

$$\begin{aligned}
&\big|\{(x,y,z)\in A_1\times A_2\times A_3 : ax+by+cz\equiv 0 \bmod N\}\big| \\
&\qquad = \frac{|A_1||A_2||A_3|}{N} + N^2\sum_{\substack{\xi\in\mathbb{Z}_N\\ \xi\neq 0}}\hat{A}_1(a\xi)\hat{A}_2(b\xi)\hat{A}_3(c\xi) \\
&\qquad \geqslant \frac{|A_1||A_2||A_3|}{N} - N^2\sum_{\substack{\xi\in\mathbb{Z}_N\\ \xi\neq 0}}\big|\hat{A}_1(a\xi)\hat{A}_2(b\xi)\hat{A}_3(c\xi)\big| \\
&\qquad \geqslant \frac{|A_1||A_2||A_3|}{N} - N^2\underbrace{\Big(\sup_{\xi\in\mathbb{Z}_N\setminus\{0\}}\big|\hat{A}_1(a\xi)\big|\Big)}_{\substack{\text{controlled by}\\ \text{pseudorandomness}}}\underbrace{\Big(\sum_{\xi\in\mathbb{Z}_N}\big|\hat{A}_2(b\xi)\hat{A}_3(c\xi)\big|^2\Big)}_{\substack{\text{controlled by}\\ \text{Plancherel}}}.
\end{aligned}$$

Due to the pseudorandomness assumption on the set A_1, we can estimate

$$\sup_{\xi\in\mathbb{Z}_N\setminus\{0\}}\big|\hat{A}_1(a\xi)\big|\leqslant\varepsilon.$$

According to the Cauchy-Schwarz inequality and Plancherel's Identity, we have the upper bound

$$\begin{aligned}
\sum_{\xi\in\mathbb{Z}_N}|\hat{A}_2(b\xi)\hat{A}_3(c\xi)| &\leqslant \Big(\sum_{\xi\in\mathbb{Z}_N}|\hat{A}_2(b\xi)|^2\Big)^{\frac{1}{2}}\Big(\sum_{\xi\in\mathbb{Z}_N}|\hat{A}_3(c\xi)|^2\Big)^{\frac{1}{2}} \\
&= \Big(\sum_{\xi\in\mathbb{Z}_N}|\hat{A}_2(\xi)|^2\Big)^{\frac{1}{2}}\Big(\sum_{\xi\in\mathbb{Z}_N}|\hat{A}_3(\xi)|^2\Big)^{\frac{1}{2}} \\
&= \Big(\frac{1}{N}\sum_{n\in\mathbb{Z}_N}|1_{A_2}(n)|^2\Big)^{\frac{1}{2}}\Big(\frac{1}{N}\sum_{n\in\mathbb{Z}_N}|1_{A_3}(n)|^2\Big)^{\frac{1}{2}} \\
&= \frac{|A_2|^{\frac{1}{2}}|A_3|^{\frac{1}{2}}}{N}.
\end{aligned}$$

Putting everything together and using $|A_i|\geqslant\delta N$ leaves us with the estimate

$$\begin{aligned}
\big|\{(x,y,z)\in A_1\times A_2\times A_3 : ax+by+cz\equiv 0 \bmod N\}\big| &\geqslant \frac{|A_1||A_2||A_3|}{N} - \varepsilon N|A_2|^{\frac{1}{2}}|A_3|^{\frac{1}{2}} \\
&\geqslant \delta N(\delta^2-\varepsilon).
\end{aligned}$$

□

4.6. Roth's Theorem – equivalent forms

Proposition 63. *The following are equivalent:*

(i) (Roth's Theorem – infinitary version). Any $A \subseteq \mathbb{N}$ with positive upper density contains a 3-term arithmetic progressions.

(ii) (Roth's Theorem – finitary version). For every $\delta > 0$ there exists $N(\delta) \in \mathbb{N}$ such that if $N \geqslant N(\delta)$ then any set $A \subseteq \{1,\dots,N\}$ with $|A| \geqslant \delta N$ contains a 3-term arithmetic progression.

Proof. The implication (ii) $\Longrightarrow$ (i) is obvious. For the reverse implication (i) $\Longrightarrow$ (ii), we shall prove the contrapositive. Suppose there exists some $\delta > 0$ and a sequence $N_1 < N_2 < \ldots \in \mathbb{N}$ such that for every $k \in \mathbb{N}$ there is a set $A_k \subseteq \{1,\dots,N_k\}$ with $|A_k| \geqslant \delta N_k$ admitting no 3-term arithmetic progression. By refining the sequence $N_1 < N_2 < \ldots$ if necessary, we can assume without loss of generality that $N_{k+1} > 8N_k$. Consider the set

$$A = \bigcup_{k=1}^{\infty} (A_k + 3N_k).$$

Note that $\overline{d}(A) > 0$ because

$$\begin{aligned}
\overline{d}(A) &= \limsup_{N\to\infty} \frac{|A \cap \{1,\dots,N\}|}{N} \\
&\geqslant \limsup_{k\to\infty} \frac{|A \cap \{1,\dots,4N_k\}|}{4N_k} \\
&\geqslant \limsup_{k\to\infty} \frac{|A_k + 3N_k|}{4N_k} \\
&= \frac{1}{4}\left(\limsup_{k\to\infty} \frac{|A_k|}{N_k}\right) \\
&\geqslant \delta/4.
\end{aligned}$$

Also, A contains no 3-term arithmetic progression. Indeed, if there were $a, b \in \mathbb{N}$ for which $\{a, a+b, a+2b\} \in A$ then, in particular, we would have $a + b \in A_k + 3N_k$ for some $k \in \mathbb{N}$. Since $b \leqslant a + b \leqslant 4N_k$, we get $a + 2b \leqslant 8N_k$. Hence $a + 2b \in A_k + 3N_k$ because $N_{k+1} > 8N_k$. But from $a + b, a + 2b \in A_k + 3N_k$ it follows that $b \leqslant N_k$ and hence $a \geqslant 2N_k$. Therefore $a \in A_k + 3N_k$ as well. This would imply that $A_k + 3N_k$ contains a 3-term arithmetic progression, a contradiction to the assumption that A_k does not contain a 3-term arithmetic progression. In conclusion, A is a set with positive upper density containing no 3-term arithmetic progression, finishing the proof of the contrapositive. □

4.7. Proof of Roth's Theorem

This section presents a proof of Roth's Theorem. The core idea, known as the density increment argument, involves iteratively increasing the density until the presence of three-term arithmetic progressions becomes evident. In what follows, let $R(\delta)$ refer to the statement:

$R(\delta)$: *"There exists $N(\delta) \in \mathbb{N}$ such that if $N \geqslant N(\delta)$, any set $A \subseteq \{0,1,\dots,N-1\}$ with $|A| \geqslant \delta N$ contains a 3-term arithmetic progression."*

Density Increment Lemma. *For every $\delta \in (0,1]$, if $R(\delta)$ is false then $R(\delta + \delta^2/16)$ is also false.*

Proof of Roth's Theorem assuming the Density Increment Lemma. Define

$$\Delta = \inf\{\delta \in (0,1] : R(\delta) \text{ is true}\}.$$

In light of Proposition 63, Roth's Theorem is equivalent to the assertion that $\Delta = 0$. By way of contradiction, assume $\Delta > 0$. Then $R(\delta)$ is true for $\delta > \Delta$ and false for $\delta < \Delta$. Choose some $\delta_* \in (0,1]$ for which $\delta_* < \Delta$ and $\delta_* + \delta_*^2/16 > \Delta$. Then $R(\delta_* + \delta_*^2/16)$ is true and $R(\delta_*)$ is false. However, by the Density Increment Lemma, if $R(\delta_*)$ is false then $R(\delta_* + \delta_*^2/16)$ is false. Since $R(\delta_* + \delta_*^2/16)$ cannot be true and false at the same time, we have reached a contradiction. □

Lemma 64. *For all $\delta > 0$, all sufficiently large odd $N \in \mathbb{N}$, and all $A \subseteq \{0,1,\dots,N-1\}$ with $|A| \geqslant \delta N$ the following holds: If A is $\frac{\delta^2}{5}$-pseudorandom then A contains a 3-term arithmetic progression.*

Proof. Let B be either all even numbers in A or all odd numbers in A, whichever is larger. It follows from the assumption that N is odd and parity considerations that a triple $(x,y,z) \in B \times A \times B$ satisfies the congruence equation $x + z \equiv 2y \bmod N$ if and only if it satisfies the integral equation $x + z = 2y$. Hence, to prove that A contains a 3-term arithmetic progression it suffices to show that $B \times A \times B$ contains a non-trivial solution to $x + z \equiv 2y \bmod N$.

Since A is $\frac{\delta^2}{5}$-pseudorandom and $|A|, |B| \geqslant \frac{\delta}{2}N$, it follows from Proposition 62 that $B \times A \times B$ contains at least $\frac{\delta N^2}{2}(\frac{\delta^2}{4} - \frac{\delta^2}{5}) = \frac{\delta^3}{40}$ many solutions to $x + z \equiv 2y \bmod N$. But this number also includes trivial solutions of the form $x = y = z$. Since there are at most N trivial solutions, the number of non-trivial solutions to $x + z \equiv 2y$ is at least $\frac{\delta^3 N^2}{40} - N$. So as long as N is larger than $\frac{40}{\delta^3}$, there is at least one non-trivial solution. It is worth pointing out that if N is much larger than $\frac{40}{\delta^3}$, then this method gives in fact *many* non-trivial solutions. □

For the proof of the Density Increment Lemma, we need the following classical result on Diophantine approximation.

Dirichlet's Approximation Theorem. *For any real number α and any $Q \geqslant 1$ there exist integers p and q with $1 \leqslant q \leqslant Q$ and*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ}.$$

Proof of the Density Increment Lemma. Suppose $R(\delta)$ is false. This means there exists arbitrarily large $N \in \mathbb{N}$ and a set $A \subseteq \{0,1,\dots,N-1\}$ with $|A| \geqslant \delta N$ admitting no 3-term arithmetic progression. From this we want to show that there exist arbitrarily large $N' \in \mathbb{N}$ and a set $A' \subseteq \{0,1,\dots,N'-1\}$ with $|A'| \geqslant (\delta + \delta^2/16)N'$ admitting no 3-term arithmetic progression.

First, by replacing N with $N+1$ if necessary, we can assume without loss of generality that N is odd. Then, using Lemma 64, we deduce that A cannot be $\delta^2/5$-pseudorandom, because if it were then it would contain a 3-term arithmetic progression. Since A is not $\delta^2/5$-pseudorandom, this means there exists $\xi \in \mathbb{Z}_N \setminus \{0\}$ such that $|\hat{A}(\xi)| > \delta^2/5$. Recall that

$$\hat{A}(\xi) = \frac{1}{N} \sum_{n \in \mathbb{Z}_N} 1_A(n) e\left(-\tfrac{n\xi}{N}\right).$$

Since $\xi \neq 0$, we have $\frac{1}{N}\sum_{n \in \mathbb{Z}_N} e\left(-\frac{n\xi}{N}\right) = 0$, and hence $|\hat{A}(\xi)| > \delta^2/5$ implies

$$\left|\frac{1}{N} \sum_{n \in \mathbb{Z}_N} \left(1_A(n) - \delta\right) e\left(-\tfrac{n\xi}{N}\right)\right| > \frac{\delta^2}{5}.$$

Next, we use Dirichlet's Approximation Theorem (with $\alpha = \xi/N$ and $Q = \sqrt{N}$) to find integers p and q with $1 \leqslant q \leqslant \sqrt{N}$ and

$$\left|\frac{\xi}{N} - \frac{p}{q}\right| < \frac{1}{q\sqrt{N}}. \tag{4.7.1}$$

We now divide $\{0,1,\dots,N-1\}$ into progressions mod q. There are q such progressions each with approximately N/q elements. (In fact, each progression has more than $N/q - 1$ and less than $N/q + 1$ elements, but this small rounding error will not make any difference.) We now subdivide these progressions into M intervals each, where M is to be chosen later. Thus there are qM such intervals in all, and each interval contains approximately $N/(qM)$ elements. Let I denote a typical such interval. We claim that on I the function $n \mapsto e(n\xi/N)$ is close to being constant. Indeed, if n_1, n_2 are two arbitrary elements in I then

$$\left|e\left(\tfrac{n_1\xi}{N}\right) - e\left(\tfrac{n_2\xi}{q}\right)\right| = \left|e\left(\tfrac{(n_1-n_2)\xi}{N}\right) - 1\right| = \left|e\left(\tfrac{(n_1-n_2)\xi}{N} - \tfrac{(n_1-n_2)p}{q}\right) - 1\right| \leqslant 2\pi|n_1 - n_2|\left|\frac{\xi}{N} - \frac{p}{q}\right|,$$

where the second to last equality follows because n_1 and n_2 belong to the same residue class mod q and hence $n_1 - n_2$ is divisible by q. Using (4.7.1) and $|n_1 - n_2| \leqslant N/M$ we conclude that

$$\left|e\left(\tfrac{n_1\xi}{N}\right) - e\left(\tfrac{n_2\xi}{q}\right)\right| \leqslant \frac{2\pi\sqrt{N}}{qM}.$$

Combined with the above, we find that

$$\frac{\delta^2 N}{5} < \Big|\sum_{n\in Z_N} (1_A(n)-\delta)e\big(-\tfrac{n\xi}{N}\big)\Big| \leqslant \sum_I \Big|\sum_{n\in I} (1_A(n)-\delta)e\big(-\tfrac{n\xi}{N}\big)\Big|$$
$$\leqslant \sum_I \Big|\sum_{n\in I} (1_A(n)-\delta)\Big| + \frac{2\pi N^{\frac{3}{2}}}{qM}.$$

So if we pick $M = \frac{40\pi\sqrt{N}}{\delta^2 q}$ then

$$\frac{\delta^2 N}{8} < \sum_I \Big|\sum_{n\in I} (1_A(n)-\delta)\Big|.$$

Since $\sum_I \sum_{n\in I}(1_A(n)-\delta) = 0$ and there are qM intervals, it follows that there exists some I with

$$\sum_{n\in I} (1_A(n)-\delta) \geqslant \frac{\delta^2 N}{16qM}.$$

Recall that I contains $N/(qM)$ elements, and so the relative density of A within I is at least $\delta + \frac{\delta^2}{16}$. Now we take $N' = |I|$ and translate and dilate the set I so that it corresponds to the set $\{0,1,\dots,N'-1\}$. The image of the set $A\cap I$ under this translation and dilation we call A'. Note that arithmetic progressions are preserved under translation and dilation; in particular, since A contained no 3-term arithmetic progressions, the same is true for A'. We have thus extracted a set A' of density at least $\delta + \frac{\delta^2}{8}$ lying in $\{0,1,\dots,N'-1\}$ containing no 3-term arithmetic progressions. Since I has size about $\frac{N}{qM} = \frac{\delta^2\sqrt{N}}{40\pi}$ and N can be made arbitrarily large, we see that N' can be made arbitrarily large. This shows that $R(\delta+\delta^2/16)$ is false. □

4.8. Behrend's Example

Roth's Theorem addresses the question of how small a set can be whilst still admitting 3-term arithmetic progressions. On the flip side of the coin, one can ask about how large a set can be whilst avoiding 3-term arithmetic progressions. Even though these two questions are formally equivalent, they still offer contrasting perspectives on the problem. The following construction is due to Behrend and provides a surprisingly large subset of $\{1,\dots,N\}$ avoiding 3-term arithmetic progressions.

Behrend's Theorem. *For all but finitely many $N\in\mathbb{N}$ there is a set $A\subseteq\{1,\dots,N\}$ which contains no 3-term arithmetic progressions and satisfies $|A| \geqslant N\exp(-c\sqrt{\log N})$. Here c is an absolute positive constant.*

Proof. Consider points $(x_1,\dots,x_K)$ with $x_i\in\{0,1,\dots,d\}$; there are $(d+1)^K$ of them. For each such point, the number $\sum_{i=1}^K x_i^2$ belongs to the interval $[0,Kd^2]$. Since there are

only (Kd^2+1) integers in the interval $[0,Kd^2]$ but $(d+1)^K$ many tuples $(x_1,\dots,x_K)$, there exists $n \leqslant Kd^2$ such that $n = \sum x_i^2$ for more than $(d+1)^K/\left(Kd^2+1\right)$ tuples. That is, there is a sphere containing many points $(x_1,\dots,x_K)$ with $x_i \in \{0,1,\dots,d\}$. The argument rests on the fact that any line can intersect the sphere in at most two points.

Let A be the set of numbers $\sum_{i=1}^K x_i(2d+1)^{i-1}$ where $(x_1,\dots,x_K)$ is a point on our sphere. Note that $A \subseteq \{1,\dots,(2d+1)^K\}$ and $|A| \geqslant (d+1)^K/\left(Kd^2+1\right)$. We claim that A has no 3-term arithmetic progression. For, if

$$\sum x_i(2d+1)^{i-1} \; + \; \sum z_i(2d+1)^{i-1} \; = \; \sum 2y_i(2d+1)^{i-1}$$

then $x_i + z_i = 2y_i$, as x_i, y_i, and z_i are all smaller than or equal to d. In other words the points $(x_1,\dots,x_K)$, $(y_1,\dots,y_K)$, and $(z_1,\dots,z_K)$ all lie on a line, which is impossible because they lie on the surface of a sphere.

To finish the proof, take K about size $\sqrt{\log N}$, and d about size $e^{\sqrt{\log N}}$. Then A is a subset of $\{1,\dots,N\}$ with $|A| \geqslant N\exp(-c\sqrt{\log N})$ admitting no 3-term progressions. □

In a surprising breakthrough, it was proven in February 2023 that for all but finitely many $N \in \mathbb{N}$, any set $A \subseteq \{1,\dots,N\}$ with $|A| \geqslant N\exp(-c(\log N)^{\frac{1}{11}})$ contains a 3-term arithmetic progression.

Chapter 5

Sárközy's Theorem

5.1. Intersective sets

One of the goals of additive combinatorics is to study the arithmetic and combinatorial properties of difference sets $A-A$. In this section, we investigate difference sets of sets with positive density. In particular, we focus on the following question:

> *If $A \subseteq \mathbb{N}$ has positive density then how large is $A-A$ and what arithmetic structure does it contain?*

The next definition offers one way to explore the above question.

Definition 65. A set $R \subseteq \mathbb{N}$ is *intersective* if for all sets $A \subseteq \mathbb{N}$ with $\overline{d}(A) > 0$, there exists $n \in R$ with $n \in A-A$.

Note that if R is an intersective set then one can remove a finite amount of elements from R and it remains an intersective set. It follows that a set R is intersective if and only if for all sets A of positive upper density the intersection $R \cap (A-A)$ has infinite cardinality.

Example 66. For any $k \in \mathbb{N}$ the set $k\mathbb{N} = \{kn : n \in \mathbb{N}\}$ is intersective because any set A of positive upper desnity contains two numbers of the same residue class mod k. This and other examples and non-examples of intersective sets are summarized in the following list:

Intersective	Non-intersective
$\mathbb{N}$	Any finite set
$k\mathbb{N}$	$k\mathbb{N}+1$
$\{n^2 : n \in \mathbb{N}\}$	$\{n^2+1 : n \in \mathbb{N}\}$
$\mathbb{P}-1$	$\mathbb{P}$
$D-D$ for any infinite $D \subseteq \mathbb{N}$	$\{2^n : n \in \mathbb{N}\}$

5.2. The compactness principle for density

The purpose of this section is to prove the following density analogue of the Compactness Theorem for finite colorings that we have seen in Section 1.5.

Compactness Theorem for positive density. *Let $\delta > 0$, and let $\mathcal{F}$ be a shift-invariant collection of finite subsets of $\mathbb{N}$. (Here, shift-invariant means that if $F \in \mathcal{F}$ then $F + t \in \mathcal{F}$ for all $t \in \mathbb{N}$.) The following are equivalent:*

(i) For any set $A \subseteq \mathbb{N}$ with $\overline{d}(A) \geqslant \delta$ there exists $F \in \mathcal{F}$ with $F \subseteq A$.

(ii) There exists $N(\delta) \in \mathbb{N}$ such that for any $N \geqslant N(\delta)$ and any set $A \subseteq \{1,\dots,N\}$ with $|A| \geqslant \delta N$ one can find $F \in \mathcal{F}$ with $F \subseteq A$.

For the proof we will need two technical lemmas. For the reminder of this section, given two sets $A, B \subseteq \mathbb{N}$, we say that *a shift of A is a subset of B* if there exists $t \in \mathbb{N} \cup \{0\}$ such that $A + t \subseteq B$.

Lemma 67. *Suppose $N \in \mathbb{N}$, $\delta > 0$, and $A \subseteq \{1,\dots,N\}$ with $|A| \geqslant \delta N$. For all $\varepsilon \in (0,1)$ there exist $M > \varepsilon N$ and a set $A' \subseteq \{1,\dots,M\}$ such that a shift of A' is a subset of A, and*

$$\min_{1 \leqslant m \leqslant M} \frac{|A' \cap \{1,\dots,m\}|}{m} \geqslant \delta - \varepsilon.$$

Proof. If $|A \cap \{1,\dots,m\}| \geqslant (\delta - \varepsilon)m$ holds for all $m = 1,\dots,N$ then we can simply take $M = N$ and $A' = A$ and are done. Otherwise, let x be the largest number in $\{1,\dots,N\}$ for which $|A \cap \{1,\dots,x\}| < (\delta - \varepsilon)x$. Pick $M = N - x$ and $A' = \{n \in \mathbb{N} : n + x \in A\}$. Clearly, $A' + x \subseteq A$. Note that

$$\delta - \varepsilon > \frac{|A \cap \{1,\dots,x\}|}{x} \geqslant \frac{|A \cap \{1,\dots,N\}| - (N - x)}{N} \geqslant \delta - \frac{N - x}{N} = \delta - \frac{M}{N},$$

which implies that $M > \varepsilon N$. Finally, we have

$$|A' \cap \{1,\dots,m\}| = |A \cap \{x+1,\dots,x+m\}| = \underbrace{|A \cap \{1,\dots,x+m\}|}_{\geqslant (\delta-\varepsilon)(x+m)} - \underbrace{|A \cap \{1,\dots,x\}|}_{< (\delta-\varepsilon)x} \geqslant (\delta - \varepsilon)m,$$

completing the proof. □

Lemma 68. *Let $\delta > 0$. Suppose we have $N_1 < N_2 < \ldots \in \mathbb{N}$ and for every $k \in \mathbb{N}$ a set $A_k \subseteq \{1,\dots,N_k\}$ with $|A_k| \geqslant \delta N_k$. Then there exists a set $A \subseteq \mathbb{N}$ with $\underline{d}(A) \geqslant \delta$ and with the property that for any finite set $F \subseteq A$ there exists some $k \in \mathbb{N}$ such that a shift of F is a subset of A_k.*

Proof. Define $\varepsilon_k = N_k^{-\frac{1}{2}}$. By Lemma 67, for every k we can find $M_k \geqslant \sqrt{N_k}$ and a set $A_k' \subseteq \{1,\dots,M_k\}$ such that a shift of A_k' is a subset of A_k and $|A_k' \cap \{1,\dots,x\}| \geqslant (\delta - \varepsilon_k)x$ for all $x = 1,\dots,M_k$. We can identify the indicator functions $1_{A_k'}$ with elements in

$\{0,1\}^{\mathbb{N}}$. Note that the finite set $\{0,1\}$, endowed with the discrete topology, is a compact metric space. By Tychonoff's theorem, $\{0,1\}^{\mathbb{N}}$ endowed with the product topology is therefore also a compact metric space. Since in compact metric spaces, sequences possess converging subsequences, there exists $k_1 < k_2 < \ldots \in \mathbb{N}$ and $A \subseteq \mathbb{N}$ such that $1_{A'_{k_i}}$ converges to $1_A \in \{0,1\}^{\mathbb{N}}$ as $i \to \infty$. By the nature of the topology we have for every $x \in \mathbb{N}$ that the equality

$$A \cap \{1,\ldots,x\} = A'_{k_i} \cap \{1,\ldots,x\} \tag{5.2.1}$$

holds for all but finitely many $i \in \mathbb{N}$. From this it follows that a shift of $A \cap \{1,\ldots,x\}$ is a subset of A_{k_i} and that

$$\frac{|A \cap \{1,\ldots,x\}|}{x} \geqslant \delta - \varepsilon_{k_i}$$

and hence $\underline{d}(A) \geqslant \delta$. □

Proof of Compactness Theorem for positive density. The implication (ii) $\implies$ (i) is obvious, so we focus on the implication in the other direction. By way of contradiction, suppose (ii) is false. This means there exists $\delta > 0$, a sequence $N_1 < N_2 < N_3 < \ldots \in \mathbb{N}$, and sets $A_k \subseteq \{1,\ldots,N_k\}$ such that $|A_k| \geqslant \delta N_k$ and no set $F \in \mathscr{F}$ satisfies $F \subseteq A_k$. By Lemma 68, there exists a set $A \subseteq \mathbb{N}$ with $\underline{d}(A) \geqslant \delta$ and with the property that for any finite set $F \subseteq A$ there exists some $k \in \mathbb{N}$ such that a shift of F is a subset of A_k. In view of (i), there exists $F \in \mathscr{F}$ with $F \subseteq A$. This means a shift of F appears in A_k for some $k \in \mathbb{N}$. Since shifts of F also belong to $\mathscr{F}$, this directly contradicts that A_k does not contain an element of $\mathscr{F}$ as a subset. □

Corollary 69 (Compactness theorem for intersective sets)**.** *For any set $R \subseteq \mathbb{N}$ the following are equivalent:*

(i) R is intersective.

(ii) For every $\delta > 0$ there exists $N(\delta) \in \mathbb{N}$ such that for any $N \geqslant N(\delta)$ and any set $A \subseteq \{1,\ldots,N\}$ with $|A| \geqslant \delta N$ one can find $n \in R$ with $n \in A - A$.

Proof. Simply apply the Compactness Theorem for positive density to the family of sets $\mathscr{F} = \{\{a,b\} \subseteq \mathbb{N} : b - a \in R\}$ and the statement follows readily. □

5.3. Sárközy's Theorem – equivalent forms

Sárközy's Theorem. *For any $A \subseteq \mathbb{N}$ with $\overline{d}(A) > 0$ the set of differences $A - A$ contains a perfect square.*

Proposition 70 (Compactness theorem for Sárközy's Theorem)**.** *The following are equivalent:*

(i) (Sárközy's Theorem – infinitary version). Any $A \subseteq \mathbb{N}$ with positive upper density contains $\{n, n+r^2\}$ for some $n, r \in \mathbb{N}$.

(ii) (Sárközy's Theorem – finitary version). For every $\delta > 0$ there exists $N(\delta) \in \mathbb{N}$ such that if $N \geqslant N(\delta)$ then any set $A \subseteq \{1, \dots, N\}$ with $|A| \geqslant \delta N$ contains $\{n, n+r^2\}$ for some $n, r \in \mathbb{N}$.

Proof. This follows from Corollary 69 applied to the set $R = \{n^2 : n \in \mathbb{N}\}$. □

5.4. Coboundaries

Throughout this section, we identity the set $\{0, 1, \dots, N-1\}$ with the cyclic group $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ and the set of all functions $f : \mathbb{Z}_N \to \mathbb{R}$ with the N-dimensional real vector space $\mathbb{R}^N$. For every $p > 0$, the associated p-norm $\|.\|_p$ is

$$\|f\|_p = \left(\frac{1}{N} \sum_{n \in \mathbb{Z}_N} |f(n)|^p \right)^{\frac{1}{p}}.$$

An important tool in the estimation of averages and norms of arithmetic functions is the Cauchy-Schwarz inequality, which asserts that for all $f, g : \mathbb{Z}_N \to \mathbb{R}$ we have

$$\left| \frac{1}{N} \sum_{n=1}^{N} f(n) g(n) \right| \leqslant \|f\|_2 \|g\|_2. \tag{5.4.1}$$

It will also be convenient to introduce the shift operator T on $\mathbb{Z}_N$. Given a function $f : \mathbb{Z}_N \to \mathbb{R}$, let $T^m f : \mathbb{Z}_N \to \mathbb{R}$ denote the shift of the function f by $m \in \mathbb{N} \cup \{0\}$, i.e.,

$$T^m f(n) = f(n+m).$$

Observe that $T^{m_1}(T^{m_2} f) = T^{m_1+m_2} f$ holds for all $m_1, m_2 \in \mathbb{N} \cup \{0\}$.

Definition 71. Let $Q \in \mathbb{N}$. We say that $g : \mathbb{Z}_N \to \mathbb{R}$ is a *Q-step coboundary on $\mathbb{Z}_N$* if there exists $f : \mathbb{Z}_N \to \mathbb{R}$ such that $g = \frac{1}{2}(f - T^Q f)$.

Lemma 72. *Let $H, Q, M, N \in \mathbb{N}$ and assume that $2h \mid Q$ for all $h = 1, \dots, H$. If $g = \frac{1}{2}(f - T^Q f)$ is a Q-step coboundary on $\mathbb{Z}_N$ then*

$$\left\| \frac{1}{M} \sum_{m=1}^{M} T^{m^2} g \right\|_2 \leqslant \|f\|_2 \cdot \left(\frac{2Q}{M} + \frac{1}{H} \right).$$

Proof. Note that for any $h = 1, \dots, H$ we have

$$\frac{1}{M} \sum_{m=1}^{M} T^{m^2} g = \frac{1}{M} \sum_{m=1}^{M} T^{(m+h)^2} g + \frac{1}{M} \sum_{j=1}^{h} T^{j^2} g - \frac{1}{M} \sum_{j=1}^{h} T^{(M+j)^2} g,$$

from which it follows that

$$\left\| \frac{1}{M} \sum_{m=1}^{M} T^{m^2} g \right\|_2 \leqslant \left\| \frac{1}{H} \sum_{h=1}^{H} \left(\frac{1}{M} \sum_{m=1}^{M} T^{(m+h)^2} g \right) \right\|_2 + \frac{2H\|g\|_2}{M}.$$

Changing the order of summation, applying the triangle inequality, and afterwards using the Cauchy-Schwarz inequality, we have

$$\begin{aligned} \left\| \frac{1}{H} \sum_{h=1}^{H} \left(\frac{1}{M} \sum_{m=1}^{M} T^{(m+h)^2} g \right) \right\|_2 &= \left\| \frac{1}{M} \sum_{m=1}^{M} \left(\frac{1}{H} \sum_{h=1}^{H} T^{(m+h)^2} g \right) \right\|_2 \\ &\leqslant \frac{1}{M} \sum_{m=1}^{M} \left\| \frac{1}{H} \sum_{h=1}^{H} T^{(m+h)^2} g \right\|_2 \\ &\leqslant \left(\frac{1}{M} \sum_{m=1}^{M} \left\| \frac{1}{H} \sum_{h=1}^{H} T^{(m+h)^2} g \right\|_2^2 \right)^{\frac{1}{2}}. \end{aligned}$$

We can now expand the square to find that

$$\begin{aligned} \frac{1}{M} \sum_{m=1}^{M} \left\| \frac{1}{H} \sum_{h=1}^{H} T^{(m+h)^2} g \right\|_2^2 &= \frac{1}{H^2} \sum_{h_1,h_2=1}^{H} \frac{1}{M} \sum_{m=1}^{M} \left\langle T^{(m+h_1)^2} g, T^{(m+h_2)^2} g \right\rangle \\ &= \frac{1}{H^2} \sum_{h_1,h_2=1}^{H} \frac{1}{M} \sum_{m=1}^{M} \left\langle g, T^{2m(h_2-h_1)+h_2^2-h_1^2} g \right\rangle \\ &\leqslant \|g\|_2 \cdot \left(\frac{1}{H^2} \sum_{h_1,h_2=1}^{H} \left\| \frac{1}{M} \sum_{m=1}^{M} T^{2m(h_2-h_1)} g \right\|_2 \right). \end{aligned}$$

Recall that $g = f - T^Q f$. Let $d = 2(h_2 - h_1)$ and $b = Q/d$. If $h_1 \neq h_2$ then the sum $\frac{1}{M} \sum_{m=1}^{M} T^{2m(h_2-h_1)} g$ is telescoping and we have

$$\left\| \frac{1}{M} \sum_{m=1}^{M} T^{2m(h_2-h_1)} g \right\|_2 = \left\| \frac{1}{M} \sum_{m=1}^{M} T^{dm} f - \frac{1}{M} \sum_{m=1}^{M} T^{d(m+b)} f \right\|_2 \leqslant \frac{2b\|f\|_2}{M} \leqslant \frac{Q\|f\|_2}{M}.$$

On the other hand, if $h_1 = h_2$ then

$$\left\| \frac{1}{M} \sum_{m=1}^{M} T^{2m(h_2-h_1)} g \right\|_2 = \|g\|_2.$$

We conclude that

$$\frac{1}{H^2} \sum_{h_1,h_2=1}^{H} \left\| \frac{1}{M} \sum_{m=1}^{M} T^{2m(h_2-h_1)} g \right\|_2 \leqslant \frac{\|g\|_2}{H} + \frac{Q\|f\|_2}{M}.$$

Combining all estimates above yields

$$\begin{aligned} \left\| \frac{1}{M} \sum_{m=1}^{M} T^{m^2} g \right\|_2 &\leqslant \frac{2H\|g\|_2}{M} + \|g\|_2^{\frac{1}{2}} \cdot \left(\frac{\|g\|_2}{H} + \frac{Q\|f\|_2}{M} \right)^{\frac{1}{2}} \\ &\leqslant \frac{2H\|g\|_2}{M} + \frac{\|g\|_2}{H} + \frac{Q\|g\|_2^{\frac{1}{2}}\|f\|_2^{\frac{1}{2}}}{M} \end{aligned}$$

$$\leqslant \|f\|_2 \cdot \left(\frac{2Q}{M} + \frac{1}{H}\right).$$

where in the last step we used $2H \leqslant Q$ and $\|g\|_2 \leqslant \|f\|_2$. □

Bibliography

[Ell58] R. ELLIS, Distal transformation groups, *Pacific J. Math.* **8** (1958), 401–405. MR 0101283. http://dx.doi.org/10.2140/pjm.1958.8.401.

[Hin74] N. HINDMAN, Finite sums from sequences within cells of a partition of N, *J. Combinatorial Theory Ser. A* **17** (1974), 1–11. http://dx.doi.org/10.1016/0097-3165(74)90023-5.

[Num52] K. NUMAKURA, On bicompact semigroups, *Math. J. Okayama Univ.* **1** (1952), 99–108. MR 0048467. Available at https://www.math.okayama-u.ac.jp/mjou/mjou-01.html.

[Ram30] F. P. RAMSEY, On a Problem of Formal Logic, *Proceedings of the London Mathematical Society* **s2-30** (1930), 264–286. http://dx.doi.org/10.1112/plms/s2-30.1.264.

[Sch17] I. SCHUR, Über die Kongruenz $x^m + y^m \equiv z^m$ (mod. p), *Jahresbericht der Deutschen Mathematiker-Vereinigung* **25** (1917), 114–116. Available at http://eudml.org/doc/145475.

[Sze75] E. SZEMERÉDI, On sets of integers containing k elements in arithmetic progression, *Acta Arithmetica* **27** (1975), 199–245 (eng). Available at http://eudml.org/doc/205339.

[vdW28] B. L. VAN DER WAERDEN, Beweis einer Baudetschen Vermutung, *Nieuw. Arch. Wisk.* **15** (1928), 212–216.