# Lecture 8: Ramsey Theory Continued and Additive Combinatorics

Combinatorial Methods (Winter 2023)
University of Toronto
Swastik Kopparty
Scribes: Xinyu Huo and Asha McMullin

## 1 First half of the lecture

**Theorem 1** (Van der Waerden's theorem)**.** *Suppose* $\mathbb{N}$ *is partitioned into* $c$ *colors. Then for every* $k$*, there is a monochromatic* $k$*-AP (an arithmetic progression of length* $k$*.*

**Example 2.** *Consider the case* $c = 2$ *and* $k = 3$*:*

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| B | R | R | B | B | R | R | B | ? |

*For the first 8 integers, no three integers of the same color form a monochromatic* 3*-AP. However, you cannot add a ninth integer without creating a monochromatic* 3*-AP. If you add a red 9, then, the red 3,6,9 forms a monochromatic* 3*-AP; if you add a blue 9, then the blue 1, 5, and 9 forms a monochromatic* 3*-AP.*

In order to prove the Van der Waerden's theorem, it is enough to prove:

**Claim 3.** $\forall c, k$, $\exists n_0$ *such that any* $c$*-coloring of* $[n_0]$ *has monochromatic* $k$*-AP.*

Let us take a detour before coming to the proof of Theorem 1.

**Lemma 4.** *Theorem 1 implies Claim 3.*

*Proof.* We will prove by contraposition. Suppose for a certain $c$ and $k$, there does not exist $n_0$ such that any $c$-coloring of $[n_0]$ has a monochromatic $k$-AP, i.e. $\forall n_0$, $\exists$ $c$-coloring of $[n_0]$ without monochromatic $k$-APs.

For each $n_0$. we have coloring of $[n_0]$. Let $S = \{\text{all these colorings}\}$. It is obvious that $|S| = \infty$, and we will maintain this. We want to prove it will produce a $c$-coloring of $\mathbb{N}$ without monochromatic $k$-APs and here is our algorithm:

Step 1: let $i = 1$.

Step 2: amongst all coloring in $S$, look at the color that they give to $i$. For some color $\alpha$, it appears as the color of $i$ infinitely many times in $S$ since $|S| = \infty$. Remove all colorings from $S$ that do not give color $\alpha$ to $i$. Define $\text{color}(i) = \alpha$.

Step 3: let $i = i + 1$, and repeat Step 2. Note that this algorithm will run forever.

We claim that the $c$-coloring of $\mathbb{N}$ we get from the above algorithm does not have a monochromatic $k$-AP. Assume there is a monochromatic $k$-AP, saying $a_0, a_1, \ldots, a_{k-1}$. Note that some coloring in the original $S$ is consistent with the coloring of $\mathbb{N}$ we get from the above algorithm on $\{a_0, a_1, \ldots, a_{k-1}\}$, and there are no monochromatic $k$-APs in the original $S$ by assumption. Contradiction. □

We will use the notion of rainbow fans as our main tool to prove Theorem 1.

**Definition 5** (Rainbow Fan)**.** *A rainbow fan with degree $d$, radius $l$, center $b \in \mathbb{N}$ is a set $A_1 \cup A_2 \cup \cdots \cup A_d$ such that*

- *each $A_i$ is an $l$-AP with $l+1^{st}$ member equal to $b$.*
- *all elements of any given $A_i$ are colored the same color $\alpha_i$.*
- *$\alpha_1, \alpha_2, \ldots, \alpha_d$ are pairwise distinct.*

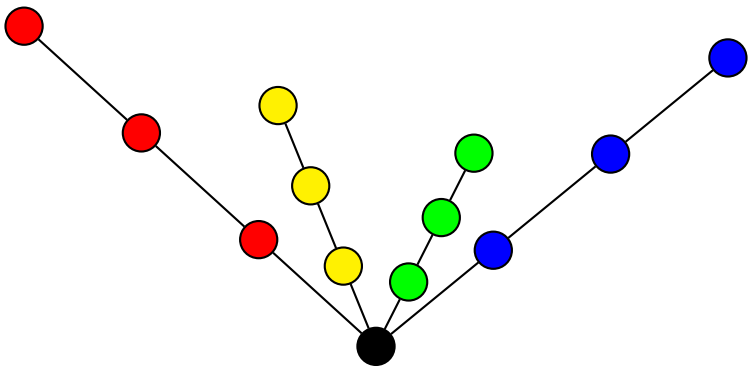

Figure 1: A rainbow fan with degree 4, raidus 3

We will use the following claim to prove Claim 3 and then Theorem 1 follows.

**Claim 6.** *$\forall c, d \leq c, l$, $\exists$ $n_0$ such that any $c$-coloring of $[n_0]$ has a rainbow fan with degree $d$ and radius $l$.*

Define $R(c, d, l)$ to be the smallest $n_0$ in Claim 2, i.e. any $c$-coloring of $[R(c, d, l)]$ has a rainbow fan with degree $d$ and radius $l$ but for any $n < R(c, d, l)$, such a rainbow fan does not exsit for some $c$-coloring of $[n]$.

*Proof.* Induction on $c, d, l$. Given any $(c, d, l)$, assume we have already proved it for $(a, b, l-1)$ where $a, b \in \mathbb{N}$ and $a \geq b$ and $(c, d-1, l)$. We want to prove the claim for $(c, d, l)$.

Let $N = R(c^{n_0}, c^{n_0}, l-1) \cdot n_0$, where $n_0 = R(c, d-1, l)$. Note that $R(c^{n_0}, c^{n_0}, l-1)$ and $R(c, d-1, l)$ both exist by our assumption. Consider $c$-coloring of $[N]$. Break $[N]$ into blocks of size $n_0$, which also exists by our assumption. Each block has rainbow fan with radius $l$, degree $d-1$, or a monochromatic $l+1$-AP.

If any block has a $l+1$-AP, we are done.

If not, consider a coloring of $[N/n_0]$ with $c^{n_0}$ colors, where color of $i$ is the sequence of colors assigned to $\{j \cdot n_0 + 1, j \cdot n_0 + 2, \ldots, j \cdot n_0 + n_0\}$. Since $N_0/n_0 \geq R(c^{n_0}, c^{n_0}, l-1)$, there is a monochromatic $l$-AP in this coloring. Suppose the $l$-AP we found was blocks $j_1, j_2, \ldots, j_l$. By the way we construct the monochromatic $l$-AP, each block $j_i$ has the same color pattern for all $n_0$ elements inside it and $j_i \cdot n_0 + A_1 \cup A_2 \cup \cdots A_{d-1}$ is a degree $d-1$, radius $l$ rainbow fan in the block $j_i$. Let $j_i n_0 + b$ denote the centers of these fans. For $s \in [d-1]$, $A_s$ has a monochromatic $l$-AP; there exists some $d_s$ such that $A_s = \{b + d_s, b + 2d_s, \ldots, b + l \cdot d_s\}$. Since we have $l$ blocks, we have $l$ such rainbow fans. Notice that $j_i n_0 + b + w d_s$ has the same color for all $i$, we denote the color $\alpha_s$. Let $B_s = \{j_i n_0 + b + (l + 1 - i)d_s : i \in [l]\}$, which is a monochromatic $l$-AP and every element of $B_s$ is colored by $\alpha_s$. Let $B_0 = \{j_i n_0 + b : i \in [l]\}$, which is also a monochromatic $l$-AP. Then, $B_0 \cup B_1 \cup \ldots B_{d-1}$ is a rainbow fan with degree $d$, radius $l$, center $j_{l+1} \cdot n_0 + b$.

□

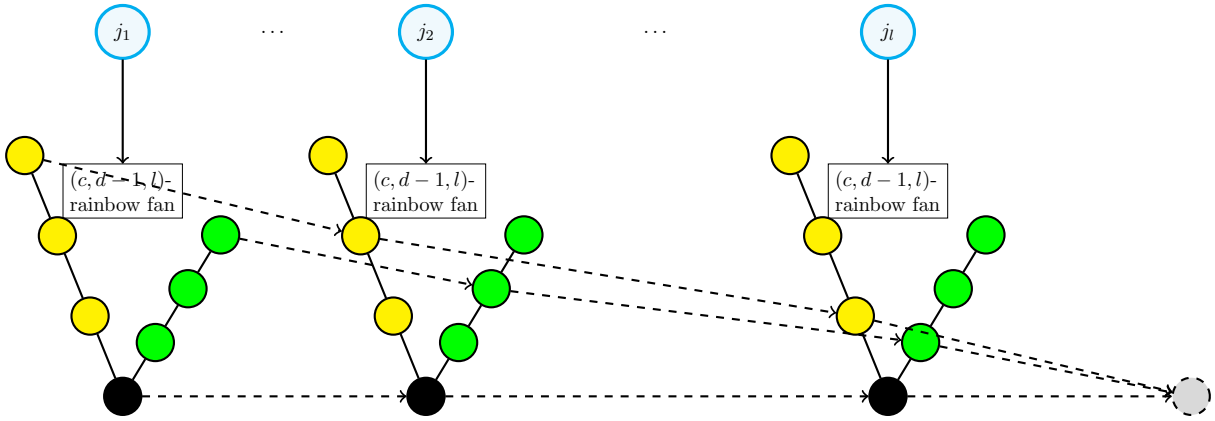


Figure 2: Construction of a $(c, d, l)$-rainbow fan

Claim 3 follows from Claim 6, and thus proves Theorem 1.

## 2 Second half of the lecture

The second part of Feb 28 covered four theorems in additive combinatorics (combinatorics with an additive structure). The first two involve sums in coloured sets of natural numbers. The last two are about adding subsets of an abelian group.

### 2.1 Colouring Continues

A **$c$-colouring** of a set X is a map "colour($x$)" from X to a set of $c$ distinct colours. A set of points is **monochromatic** if all points in the set are assigned the same colour.

The first theorem says that for any $c$ and a large enough $n$, every $c$-colouring of $\mathbb{Z}/n\mathbb{Z}$ has some $x, y, z$ all the same colour with $x+y=z$. Both the colouring theorems from this part of the lecture work on $\{1, 2, ..., n\}$ with regular addition just as well as on $\mathbb{Z}/n\mathbb{Z}$.

**Theorem 7** (Schur's Theorem)**.** *$\forall c \in \mathbb{N}, \exists n_0 \in \mathbb{N}$ so that $\forall n > n_0$ if we $c$-colour $\mathbb{Z} \mod n$ (also known as the additive group $\mathbb{Z}/n\mathbb{Z}$), then there are monochromatic $x, y, z \in \mathbb{Z}/n\mathbb{Z}$ such that $x + y = z$.*

This proof is much easier than the proof from part 1 of today's class! It's graph-theory based and uses the Graph-Ramsey theorem.

*Proof.* Take a $c$-colouring of $\mathbb{Z}/n\mathbb{Z}$.

Create a $c$-coloured graph as follows: The vertices of our graph are $\mathbb{Z}/n\mathbb{Z}$, and every pair of vertices are connected, making the graph complete. Colour the edge $(i, j)$ with the colour of the vertex $j-i$ if $j > i$. Otherwise use the colour of $i - j$.

Graph-Ramsey says that for large enough $N$ relative to $c$, there is a monochromatic triangle in this graph. That is, $\exists n_0$, so that $n > n_0$ implies there are some $i, j, k$ with $i < j < k$ and $\text{colour}(j - i) = \text{colour}(k - j) = \text{colour}(k - i)$.

Let $x = j - i$, $y = k - j$ and $z = k - i$.

$$\begin{aligned} x + y &= j - i + k - j \\ &= k - i \\ &= z \end{aligned}$$

□

Now to one-up Schur's Theorem: we show the same thing for $x + y = z + w$.

**Theorem 8** (Schur++)**.** *$\forall c, \exists n_0$ so that $\forall n > n_0$, if we $c$-colour $\mathbb{Z}/n\mathbb{Z}$ then there are distinct $x, y, z, w$ monochromatic with $x + y = z + w$.*

*Proof.* Construct a complete coloured graph on $\mathbb{Z}/n\mathbb{Z}$ as in Schur's Theorem. Some colour class must contain at least $\frac{n}{c}$ edges.

Within this colour class, there are at least $\binom{\frac{1}{c}n}{2}$ sums of distinct elements, but at most $2n$ results of these sums.

By the pidgeonhole principle, when $\binom{\frac{1}{c}n}{2} > 2n$, some pair of sums must give the same result, so there are some $x, y, z, w$ so that $x + y = z + w$.

Note that $x, y, z, w$ are automatically distinct: If $x = z$ then $y = w$ so $x + y$ and $z + w$ are not two distinct sums, and would never have been considered by our process.

You can compute this bound but we didn't do it in class: $n_0 = 10c^2$ is sufficiently large for any $c$.

□

## 2.2 SumSets

**Definition 9** (SumSet)**.** *If $A, B \subset G$ where $G$ is an abelian group.*

*we define the* ***SumSet*** $A + B = \{a + b, a \in A, b \in B\}$

From here forward, $A$ and $B$ always denote subsets of some abelian group $G$.

**Question 10.** *If $|A| = m$ and $|B| = n$, what can we say about $|A + B|$?*

Some ideas:

1. It's at most $|A| \cdot |B|$, since there are at most that many distinct sums.

2. When both $A$ and $B$ are non-empty, $|A + B| \geq \max(|A|, |B|)$, because $A + b$ for any $b \in B$ is a coset of A, so has the same size. The same is true for B.

3. If $A = B$ and $B$ is a **subgroup** of $G$, $|A + B|$ achieves the lower bound above.

4. When A,B are small relative to G, if they are chosen at random, it seems likely that $|A + B|$ will be closer to $|A| \cdot |B|$, since it is unlikely for any sums in $A + B$ to be equal.

Turns out that we aren't the first people to ask this question. Cauchy, Davenport, and their baby, already have it figured out!

**Theorem 11** (Baby Cauchy Davenport Theorem)**.** *If $A, B \subset \mathbb{R}$ with $|A| = m$ and $|B| = n$, then $|A + B| \geq m + n - 1$.*

This bound is actually tight. You can consider the sets $A = \{1, ..., m\}$ and $B = \{1, ..., n\}$. Then $A + B = \{2, ..., m + n\}$.

*Proof.* Write $A = \{a_1, ..., a_m\}$ and $B = \{b_1, ..., b_n\}$ with $a_1 < a_2 < ... < a_m$ and $b_1 < b_2 < ... < b_n$.

The ordering of the elements tells us that

$$a_1 + b_1 < a_1 + b2 < ... < a_1 + b_n < a_2 + b_n ... a_m + b_n$$

There are $n$ elements up to $a_1 + b_n$ and $m - 1$ after that, for a total of $n + m - 1$ distinct sums.

□

This proof used order heavily, but we don't actually need it. A similar theorem holds in $\mathbb{Z}/n\mathbb{Z}$. This proof was too hard for the baby, so the theorem got renamed.

**Theorem 12** (Cauchy Davenport)**.** *If $A, B \subset \mathbb{Z}/p\mathbb{Z}$ for **prime** $p$, $|A| = m$ and $|B| = n$, then*

$$|A + B| \geq \min(m + n - 1, p)$$

We get to keep our bound from Baby Cauchy-Davenport unless we run out of elements in the surrounding group! That's pretty nice.

**Reader's Note:** This proof will use polynomials and the fact that $\mathbb{Z}/p\mathbb{Z} = F_p$, the finite field with $p$ elements. It doesn't work with just any group that is also a finite field. It also requires that $\mathbb{Z}/n\mathbb{Z}$ has no subgroups.

First, we do two lemmas that work for on polynomials over any field. They're called "Combinatorial Nullstensatz", which means "statements about zeroes".

**Lemma 13** (Combinatorial Nullstensatz 1 – CN1)**.** *Let F(X,Y) be a polynomial over any field that vanishes on $A \times B$. Define $Z_A(X) = \pi_{a \in A}(x - a)$ and $Z_B(Y) = \pi_{b \in B}(Y - b)$. Then*

$$F(X, Y) = U(X, Y) \cdot Z_A(x) + V(X, Y) \cdot Z_B(y)$$

*Where* $\deg(U) \leq \deg(F) - |A|$,*and* $\deg(V) \leq \deg(F) - |B|$.

We will use CN1 in our proof of Cauchy Davenport to reduce the degree of $F$ while keeping its values the same.

**Lemma 14** (Combinatorial Nullstensatz 2 – CN2)**.** *Suppose F(X,Y) has X-degree $< |A|$ and Y-degree $< |B|$ and vanishes on $A \times B$. Then $F(X, Y) \equiv 0$.*

We will prove CN2 first, and use it to prove the CN1.

*Proof of CN2.* Recall: For any polynomial $p$ over a field, if $p(x)$ has has $k$ roots and degree $< k$, then $p(x)$ is the zero polynomial.

The form of $F$ is $F(X, Y) = \sum_{i=0}^{|A|-1} u_i(Y)X^i$ with $\deg(u_i) < |B|$. Since $F(X, b)$ has $|A|$ zeroes, we know $u_i(b) = 0$ for all $i$ and all $b \in B$. This means $u_i(Y)$ has at least $|B|$ zeroes, so the same argument shows the $u_i \equiv 0$ for all $i$.

□

Now we go back to prove CN1.

*Proof of CN1.* $Z_A(X) = X^{|A|} - g(X)$, where $g(X)$ has degree less than $|A|$. This means we can replace $X^{|A|} = Z_A + g(X)$, and similarly for $Y^{|B|}$ and $Z_B(Y)$.

We can replace all monomials $X|A|$ in $F$ like this until we get something of the form.

$F(X,Y) = U(X,Y) \cdot Z_A(X) + V(X,Y) \cdot Z_B(Y) +$polynomial with X-degree ¡ —A—, and Y-degree ¡ —B—

$F$, $Z_A$ and $Z_B$ are all zero on $A \times B$, so the polynomial at the end must be as well. By CN2, the polynomial at the end must be zero everywhere. This gives us

$$F(X,Y) = U(X,Y) \cdot Z_A(X) + V(X,Y) \cdot Z_B(Y)$$

We didn't show that $U$ and $V$ have the required degrees in class, but it follows from the process. □

Now we prove Cauchy Davenport

*Proof of Cauchy Davenport.* Suppose $p < m + n - 1$. Since $A + B \subset F_p$, $|A + B| < p$ so we are done. Therefore, we only need to work on the case that $m + n - 1 \leq p$.

Let $C = A + B$. Suppose for the sake of contradiction that $|C| \leq m + n - 2$.

Consider $Q(X,Y) \in F_p[X,Y]$ given by $Q(X,Y) = \prod_{c \in C}(X + Y - c)$. The degree of $Q$ is $|C|$ and $Q$ vanishes on $A \times B$. The highest degree part of $Q(X,Y)$ is

$$\begin{aligned}(X+Y)^{|C|} &= (X+Y)^{m+n-2} \\ &= (X+Y)^{(m-1)(n-1)} \\ &= \binom{m+n-2}{m-1} X^{m-1} Y^{n-1}\end{aligned}$$

The coefficient $\binom{m+n-2}{m-1}$ is non-zero because $p$ is prime and $m+n-2 < p$. (This is where the proof fails in other finite fields.)

By CN1,

$$Q(X,Y) = U(X,Y) \cdot Z_A(X) + V(X,Y) \cdot Z_B(Y)$$

where $\deg(U) \leq n - 2$ and $\deg(V) \leq m - 2$. A term of order $X^{m-1}Y^{n-1}$ is therefore impossible. This is a contradiction, so $|C| > m + n - 2$.

□