Arithmetic Progressions

Tibor Szabó

Extremal Combinatorics, FU Berlin, WiSe 2017–18

1 The Erdős-Turán Conjecture

In this section we return to the very origins of the Regularity Lemma. The story can be traced back to a number theoretic conjecture of Erdős and Turán, whose motivation was to find "structured" subsets within the set of positive natural numbers. What would be a natural first candidate for a concept describing a "structured subset of the integers"? The set $\mathbb{N}$ has two quite different arithmetic operations on it: addition and multiplication. Here we will deal with additive structures; questions concerning multiplicative struture and the interplay of the two strutures also provide a rich terrain of attractive problems.

The concept inherent to the additive structure of integers is the one of an *arithmetic progression*. For given $k \in \mathbb{N}$, a k-element subset $S \subseteq \mathbb{Z}$ of the integers is called a *k-term arithmetic progression* or *k-AP*, if there is an integer $a \in \mathbb{Z}$ and positive integer $d \in \mathbb{N}$ such that $S = \{a, a+d, a+2d, \dots, a+(k-1)d\}$. Note that for our treatment here we require that $d \neq 0$, i.e., that an arithmetic progression is not constant.

Being thoroughly trained in extremal combinatorics, we are immediately ready to ask the very first question about the concept: how many integers would definitely force the existence of a large additive substructure among them? Quantitatively, for integers $k \leq n$, what is the smallest integer $s \in \mathbb{N}$, such that every s-subset of $[n]$ contains an arithmetic progression of length k. Or, fomulated in the negated language, we define

$$s_k(n) := \max\{|S| : S \subseteq [n] \text{ is } k\text{-AP-free}\}.$$

Note that $s_k(n)$ is monotone increasing in k: $s_3(n) \leq s_4(n) \leq \cdots \leq s_k(n) \leq \cdots$.

Erdős and Turán came up with the following construction of a large 3-AP-free set: the set $R \subseteq \mathbb{N}_0$ of those numbers whose ternary expansion does not contain the digit 2. To see that this set is 3-AP-free, let $a, b, c \in R$, such that $a + b = 2c$. So a, c, b, in this order, form a 3-AP. The crucial observation is that when we perform the addition $a + b$ and $c + c$ of the numbers in their ternary expansion, there is no "carry-over", since all digits are 0 or 1. In $2c$ all digits are 0 or 2, while if a and b are different, then in at least one digit we add a 0 to a 1, so the result is 1. In conlcusion $a + b$ can only be equal to $2c$ if $a = b = c$, hence R is 3-AP-free.

How large is $R \cap [n]$? Among the $n = 3^\ell$ integers between 0 and $3^\ell - 1$ there are 2^ℓ members of S, so the size of S is $2^{\log_3 n} = n^{\log_3 2} \geq n^{0.63}$.

HW Show that R is the 3-AP-free set we obtain with the following greedy procedure. Consider the integers in increasing order and place the next integer into R if this does not create a 3-AP with the elements that are already in R.

In terms of upper bounds Erdős and Turán strongly believed that $s_3(n)$ should be less than linear in n, but were only able to show that $s_3(n) \leq \left(\frac{3}{8} + \epsilon\right) n$. In other words they conjectured that an arbitrary tiny, but positive constant fraction of the integers up to a large enough n should contain an arithmetic progression of length 3 (and in fact of length k).[1]

[1] In their paper Erdős and Turán mention that George Szekeres went that far as to conjecture that the greedy set of the Homework *is* the largest possible 3-AP-free set. This conjecture would have implied the existence of infinitely many 3-APs consisting of prime numbers, but it turned out to be false.

Conjecture 1.1 (Erdős-Turán, 1936). *For every $k \in \mathbb{N}$,*

$$s_k(n) = o(n).$$

While at the time of its posing the conjecture seemed just a modest request to say a somewhat more meaningful upper bound, soon it turned out that nothing significantly better will ever be possible. The following construction of Behrend improves the greedy construction above and obtains a 3-AP-free sets whose size is larger than n to any constant power strictly less than 1 (say $n^{0.999}$).

Construction (Behrend, 1946)

$$s_3(n) \geq n^{1-O\left(\frac{1}{\sqrt{\log N}}\right)}.$$

The idea is to use the "no-carry-over" property in the addition of two numbers with small digits—but use it for some large b-ary expansion instead of the ternary (the one we used in the greedy construction). For given integers n, b, and ℓ such that $n = b^\ell$ we consider the set S of numbers whose b-ary expansion is of length at most ℓ and only contains digits less than $b/2$.

This set $S \subseteq [0, n-1]$ is then in a canonical one-to-one correspondence with the set of vectors

$$V := \left\{0, 1, 2, \ldots, \left\lfloor \frac{b-1}{2} \right\rfloor\right\}^\ell.$$

For a vector $\vec{x} = (x_0, x_1, \ldots, x_{\ell-1}) \in [0, b-1]^\ell$ we define the integer $n_{\vec{x}} := \sum_{i=0}^{\ell-1} x_i b^i < n$. Because there is no carry-over in addition of two numbers from S, for any two vectors $\vec{x}, \vec{y} \in V$ we have $n_{\vec{x}} + n_{\vec{y}} = n_{\vec{x}+\vec{y}}$. So if three numbers from S form a 3-AP, i.e. $n_{\vec{x}} + n_{\vec{y}} = 2n_{\vec{z}}$, then we can conlcude that $n_{\vec{x}+\vec{y}} = n_{2\vec{z}}$ and in turn for the corresponding vectors we have $\vec{x} + \vec{y} = 2\vec{z}$. Hence our goal will be to give a 3-AP-free subset of vectors, which will then translate back to a 3-AP-free subset of integers.

In the greedy construction of Erdős and Turán $\vec{x} + \vec{y} = 2\vec{z}$ was enough to conclude the equality of the vectors $\vec{x}, \vec{y}, \vec{z}$ and hence the equality of the numbers $n_{\vec{x}}, n_{\vec{y}}, n_{\vec{z}}$. Here this is not true anymore. For example, in base 5, we can take $\vec{x} = (1, 0)$, $\vec{y} = (1, 2)$ and $\vec{z} = (1, 1)$ (so $n_{\vec{x}} = 5$, $n_{\vec{y}} = 7$ and $n_{\vec{z}} = 6$). To this end we will not be able to keep the whole set V of vectors, but will need to select a subset of it that is 3-AP-free. If three vectors form a 3-AP, then one is the midpoint of the segment between the other two, in particular the three vector is on the same line. Our limited geometric intuition suggests that a sphere for example intersects any line in at most two points, so in particular it will also not contain a non-trivial 3-AP of vectors.

Let $S_r := \{n_{\vec{x}} \in S : \|\vec{x}\| = r\}$ be the intersection of S with the sphere of radius r. Then S_r is 3-AP-free, because if $n_{\vec{x}} + n_{\vec{y}} = 2n_{\vec{z}}$ for some $\vec{x}, \vec{y}, \vec{z} \in S_r$, then $\vec{x} + \vec{y} = 2\vec{z}$ and

$$\|2\vec{z}\| = 2\|\vec{z}\| = 2\sqrt{r} = \|\vec{x}\| + \|\vec{y}\| \geq \|\vec{x} + \vec{y}\| = \|2\vec{z}\|.$$

Equality happens only if $\vec{x}$ and $\vec{y}$ are parallel. Since they are of the same length, we conclude $\vec{x} = \vec{y}$.

We will take the radius r for which S_r is the largest and bound its size by averaging. Since $\vec{x} \in [0, b-1]^\ell$, we have $\|\vec{x}\|^2 < \ell b^2$,
so there is a radius r for which

$$|S_r| \geq \frac{|\bigcup_i S_i|}{\sqrt{\ell} b} = \frac{(b/2)^l}{\sqrt{\ell} b} = \frac{b^{\ell-1}}{2^\ell \sqrt{\ell}}$$

For a given n, choose $\ell = \sqrt{\log n}$ and $b = n^{\frac{1}{\ell}}$.

2 Roth's Theorem and Szemerédi's Theorem

Eventually the Erdős-Turán Conjecture was proved 1952 for 3-AP by Klaus Roth and was one of the results in the citation[2] of his awarding of the Fields Medal in 1958.

[2]The other result was Roth's solution of the famous Thue-Siegel problem concerning the approximation to algebraic numbers by rational numbers.

Theorem 2.1 (Roth's Theorem). *For all $\epsilon > 0$ there exists a positive integer $N = N(\epsilon)$ such that for any $n \geq N$ and $S \subseteq [n]$, $|S| \geq \epsilon n$, there is a 3-AP in S.*

Roth used the Hardy-Davenport circle method from analytic number theory for his proof. Here we present a fully combinatorial proof that transfers the number theoretic problem into one in graph theory.

Proof. Let $S \subseteq [n]$ be a 3-AP-free set of size $|S| \geq \epsilon n$.

We create a three-partite graph $H = H(S)$ from S and use the Triangle Removal Lemma for it.

$V(H) = A \cup B \cup C$, where $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_{2n}\}$, $C = \{c_1, \ldots, c_{3n}\}$. Edges are defined as follows: $a_i b_j \in E(H)$ if $j - i \in S$, $b_j c_k \in E(H)$ if $k - j \in S$, and $a_i c_k \in E(H)$ if $k - i \in 2S = \{2s : s \in S\}$.

There is a large family of pairwise edge-disjoint trinagles in H: the triangles a_i, b_{i+s}, c_{i+2s} are pairwise disjoint for any $i \in [n]$ and $s \in S$. Hence at least $|[n]| \cdot |S| \geq \epsilon n^2 \geq \frac{\epsilon}{36} v(H)^2$ edges must be removed from H to make it triangle-free.

Let us apply the Triangle Removal Lemma for H with $\gamma = \frac{\epsilon}{36}$ and receive a $\delta = \delta(\gamma)$. From what we showed above there has to be at least $\delta\binom{|V(H)|}{3}$ triangles in H. However the triangles shown above are all that there is in H. Indeed, if a_i, b_j and c_k form a triangle, then $j - i =: s_1 \in S$, $k - j = s_2 \in S$ and $\frac{s_1+s_2}{2} = \frac{k-i}{2} = s_3 \in S$ form a 3-AP in S. So they must all be equal and consequently $i = j = k$. Therefore the number of triangles in H is at most $n|S| \leq n^2$. This number is less than $36\delta n^3 = \delta(v(H))^3$ providing a contradiction for $n \geq \frac{1}{36\delta}$.

Hence the choice $N(\epsilon) = \frac{1}{36\delta(\epsilon/36)}$ will be a good one.

□

Remark. The quantitative dependence of $N(\epsilon)$ on ϵ in the above proof is horrendously large, as at the bottom there is the Regularity Lemma that we used to show the Triangle Removal Lemma. From the Fourier analityc proof proof of Roth much better estimate follows.

Endre Szemerédi proved the conjecture for $k = 4$ in 1969 using combinatorics and Roth followed up with a proof extending his analytic number theoretic method to 4-APs.

The full conjecture, for every $k \in \mathbb{N}$ was settled by Szemerédi in 1975 using combinatorial ideas.

Theorem 2.2 (Szemerédi's Theorem, 1975). *For any integer $k \geq 1$ and $\epsilon > 0$ there is an integer $N = N(k, \epsilon)$ such that any subset $S \subseteq \{1, \ldots, N\}$ with $|S| \geq \epsilon N$ contains an arithmetic progression of length k.*

Unlike many other famous conjecture, the story of this one did not end with its resolution. Szemerédi's Theorem inspired a lot of great new ideas and research in various, seemingly unrelated fields of mathematics. In 1977 Furstenberg gave a proof using ergodic theory (which provided no quantitative bounds). A third proof was given Gowers who managed to greatly extend the analytic number theoretic method of Roth, using Fourier analysis together with combinatorics. In the process he developed several important tools both in combinatorics and number theory that later found many other applications. An extension of the combinatorial proof we have just seen to arbitrary k, using an appropriate hypergraph regularity lemma and removal lemma, was given by Rödl and Schacht and by Gowers in 2007. A fifth proof, using measure theory, was published in 2012 by Elek and Szegedy.

The non-trivial methods that had to be developed in each of these disparate fields, to solve the very same problem, underline the centrality of the orginal question. The whole story supports what I would idealistically want to believe about the intrinsic unity of mathematics.

Szemerédi's Theorem also had tremendous effect on further research in combinatorics and number theory. It is for example a basic building block in the proof of Green and Tao that the sequence of primes contains arithmetic progressions of arbitrary finite length.

Unfortunately the proof of Szemerédi's Theorem, even for arithmetic progressions of length 4, is waaay out of the league for our lectures. In the next section we will settle for something more manageable, but still substantial and, most importantly, beautiful!

3 Van der Waerden's Theorem

3.1 Ramsey- vs. Turán-type problems

In a typical Turán-type problem we are looking for the largest subset of the base set, which does *not* contain the sub-structure that we care not to have. This was the case in graph Turán-theory when we were looking for the largest subset of $E(K_n)$ which does not contain a copy of $E(K_k)$ or some other fixed graph $E(H)$. And this was the case above in Szemerédi's theorem when we were looking for the largest subset of $[n]$ which did not contain a k-AP.

In a typical Ramsey-type problem we are looking for *partition*s of our base set such that *none* of the partition classes contain the substructure we care not to have. This was the case in graph Ramsey theory, when we tried to partition (i.e. color) the edges of $E(K_n)$ such that there is no $E(K_k)$ in any of the partition classes (i.e., there is no monochromatic K_k).

What is the Ramsey counterpart of Szemerédi's theorem? It should talk about partitionings (colorings) of $[n]$ such that no part (color class) contains a k-AP. There is an obvious way how a Turán type statement could somtimes imply a Ramsey-type statement. If the base set is colored by r colors, then the largest color class is at least $\frac{1}{r}$-fraction of the whole set. If the Turán number of the structure is less then this, then it is sure that the largest color class does contain a monochromatic forbidden substructure. In particular Szemerédi's Theorem proves that for any finite $r \in \mathbb{N}$ and $k \in \mathbb{N}$, in any r-coloring of $[n]$, where n is large enough that $\frac{1}{r} > \frac{s_k(n)}{n}$ (which certainly will be the case for all large enough n), there is a monochromatic k-AP in the *largest* color class.

Next we will show the weaker statement that claims the existence of a monochromatic k-AP in *some* color class (not necessarily the largest).

Note that not every Turán-type statement implies the corresponding Ramsey statement. For example in the K_k-problem the Turán result does not give any useful information about the Ramsey result. Indeed, the Tur'an number of K_k is more than $\binom{n}{2}/2$, and from this we cannot even conclude that any 2-colorings of $E(K_n)$ contain a K_3!

Recall our definition of the $\binom{k}{2}$-uniform "Subgraph"-hypergraph $\mathcal{SG}^{(2)}(n, K_k) = \mathcal{SG}(n, K_k)$, defined on the set $E(K_n) =: V(\mathcal{SG}(n, K_k))$ of edges of an n-clique as its vertex set and containing a hyperedge corresponding to each k-clique in K_n. That is, formally,

$$\mathcal{SG}(n, K_k) = \left\{ \binom{K}{2} : K \subseteq [n], |K| = k \right\}.$$

With this notion in hand, the questions about symmetric Ramsey numbers could be expressed as questions about the chromatic number of this special hypergraph. For example, $R(k, k) \leq n$ if and only if $\chi\left(\mathcal{SG}(n, K_k)\right) > 2$.

A moment of thought reveals that he Turán number can be expressed as the independence number of this hyper graph

$$\alpha(\mathcal{SG}(n, K_k)) = \mathrm{ex}(n, K_k).$$

The relationship between Ramsey- and Turán-type problems is just the familiar inequality between chromatic number and independence number:

$$\chi(\mathcal{SG}(n, H)) \geq \frac{\binom{n}{2}}{\alpha(\mathcal{SG}(n, H))}.$$

Hence an upper bound on the Turán-number (the independence number) leades to a lower bound on the chromatic number, that translates to an upper bound on the Ramsey-number.

The hypergraph $\mathcal{AP}(n, k)$ of Szemerédi's Theorem is defined on the vertex set $V(\mathcal{AP}(n, k) = [n]$. Edges are the k-APs:

$$\mathcal{AP}(n, k) := \{\{a, a + d, \ldots, a + (k - 1)d\} \subseteq [n] : a, d \in [n]\}.$$

The extremal function $s_k(n)$ is just the independence number and Szemerédi's Theorem states that for every $k \in \mathbb{N}$ we have $\alpha(\mathcal{AP}(n, k)) = o(n)$.

This implies an lower bound the chromatic number:

$$\chi(\mathcal{AP}(n,k)) \geq \frac{n}{\alpha(\mathcal{AP}(n,k))} \to \infty.$$

This implication is what we will show next.

3.2 Van der Waerden's theorem

The Ramsey problem: if we r-color $[n]$ will one of the color classes contain a k-AP?

In the children's game TicTacToe the players two-color the three-by-three board. Labelling the squares with integeres 1 through 9 appropriately, every winning set is a 3-AP (123, 456, 789,147, 258, 369, 159, 357), however not every 3-AP is a win.

Definition 3.1. *Given $r, k \in \mathbb{N}$, the van der Waerden number is defined as*

$$W(r,k) := \min\{n : \textit{any } r\textit{-colouring of } [n] \textit{ contains a monochromatic } k\textit{-AP}\}$$

Exmaples: $W(r,1) = 1$ and $W(r,2) = r+1$ by the Pigeonhole Principle.

The finiteness of $W(r,k)$ is not clear a priori. Before proving it let us see a lower bound for $r = 2$.

Proposition 3.2. $W(2,k) > \sqrt{2}^k k^{\frac{1}{4}-o(1)}$.

Proof. We use our investigations about Property B for the hypergraph $\mathcal{AP}(k,n)$. For that we need count its edges. An arithmetic progression is fully determined by its first element and difference, each of which must be selected from $[n]$. So $|\mathcal{AP}(n,k)| \leq n^2$. We can apply the Radhakrisnan-Srinivasan bound (that we proved by the method of Charkashin and Kozik). Since $\mathcal{AP}(n,k)$ is k-uniform if its number of edges is less than $2^k k^{\frac{1}{2}-o(1)}$ then the hypergraph is two-colorable. □

Remarks

1. The correct asymptotics for the number of k-APs in $[n]$ is $\frac{n^2}{2(k-1)}$ for any fixed k.

2. One can easily prove that $W(r,k) > r^{\frac{k-1}{2}}$ for any r, in a direct way, by considering a random r-coloring of $[n]$.

Theorem 3.3 (Van der Waerden, 1927)**.** *For every $r, k \in \mathbb{N}$, the number $W(r,k)$ is finite.*

Remark This is the last highlight of our tour of Ramsey- and Turán-theory. After starting out with Ramsey's Theorem for cliques and studying hypergraph Ramsey-theory, we went on to investigate Turán-numbers of graphs. Armed with our graph theoretic tools, we discussed a Turán-type conjecture about arithmetic progressions. Now we come back a full circle and prove its Ramsey-theoretic counterpart, van der Waerden's Theorem, which, incidentally, is even older than Ramsey's Theorem we started with.

First we motivate the proof with an informal attempt to prove the case with two colors, `red` and `blue`. Starting out slowly: to find a monochromatic 2-AP it is enough to consider the colors of 1, 2, and 3. Indeed, either 2 has the same color as 1, producing a monochromatic 2-AP or it is different, in which case the number 3 will form a monochromatic 2-AP either with 1 or 2. Let us say the color of the monochromatic 2-AP $a, a+d_1$ we found in $\{1,2,3\}$ is `red`. To find a monochromatic 3-AP, we first check what is the color of the integer $a+2d_1$, extending our monochromatic `red` 2-AP into a 3-AP. If this color is also `red`, then $a+2d_1$ completes a monochromatic 3-AP in `red`. Otherwise we have found a 3-AP in $\{1,2,3,4,5\}$ with the color pattern `red`, `red`, `blue`. If we were able to find the same color pattern on a disjoint translate of our 3-AP, then we could use some of these six numbers to find a *monochromatic* 3-AP we are seeking. Let us say that at distance d from our original 3-AP the disjoint 3-AP $a+d, a+d_1+d, a+2d_1+d$ also has color pattern `red`, `red`, `blue`. Then, depending on the color of the integer $a+2d_1+2d$, we either have a `blue` 3-AP of difference d starting with $a+2d_1, a+2d_1+d$ or a `red` 3-AP of difference d_1+d starting with $a, a+d_1+d$. The Pigeonhole Principle ensures that among the first 2^5+1 disjoint

blocks of five consecutive integers there are two with identical color patterns and hence also the appropriate translates of the appropriately colored 3-AP. So we find the monochromatic 3-AP in the first $5 \cdot (2^5 + 1) + 5 \cdot 2^5 = 325$ integers.

To find a monochromatic arithmetic progression of length 4, we can start by finding a monochromatic 3-AP $\{a, a + d_1, a + 2d_1\}$ in any interval of 325, and check the color of the integer $a + 3d_1$ that extends it to a 4-AP. If this integer is of the same color than the 3-AP, we are done. Otherwise, we find a 4-AP, with color pattern of the form, say, `red, red, red, blue` in an interval of length $\left\lfloor \frac{3}{2} \cdot 325 \right\rfloor = 488$. To be able to use the previous trick, we need not just one, but *two* further pairwise disjoint translates of the very same 4-AP with the very same color pattern such that these three copies of the 4-APs are regularly spaced, i.e. form a 3-AP (say with difference d). Then we could again look at the color of the integer $a + 3d_1 + 3d$ and in both cases find a monochromatic 4-AP ending on it. To find a 3-AP of identically colored blocks the Pigeonhole Principle will not anymore do, but we need to use the van der Waerden number for 3-APs with 2^{488} colors. So before going on to attack the 4-AP theorem for two colors we need to settle the 3-AP theorem for many colors. Therefore the multicolor version of the van der Waerden Theorem is not only a generalization for its own sake, but a necessity for this proof idea to go through.

Proof of van der Waerden's Theorem. We proceed by induction on k to show that for *every* $r \in \mathbb{N}$, the van der Waerden number is finite. As we mentioned above $W(r, 1) = 1$ and $W(r, 2) = r + 1$ for every $r \in \mathbb{N}$.

Let $k \geq 3$ and let $r \geq 1$ be arbitrary. By induction we can assume that $W(r^*, k - 1) < \infty$ for any $r^* \in \mathbb{N}$. To handle not only two, but r colors we will need not only two but r $(k-1)$-APs that extend to a k-AP with the same integer. This motivates the following definition. We say that s monochromatic $(k - 1)$-AP's $P_i = \{a_i + jd_i : j \in [0, k - 2]\}$, $i \in [s]$, are *colour-focused on* $x \in \mathbb{Z}$, if their colors are pairwise distinct and if $x = a_i + (k - 1)d_i$ for every $i \in [s]$. Note that that this means that the integer x extends each $(k - 1)$-AP into a k-AP. The pairwise different colors of the monochromatic $(k - 1)$-APs guarantee that either x extends one of them to a monochromatic k-AP or a new colour to be used at x.

Definition 3.4. *For positive integers $r, k,$ and $s \leq r$ let*

$$W(r, k, s) := \min\{n \in \mathbb{N} : \textit{any } r\textit{-coloring of } [n] \textit{ contains a monochromatic } k\textit{-AP or } s \textit{ color-focused } (k-1)\textit{-APs}\}.$$

Observe that $W(r, k, 1) = W(r, k-1)$, since color-focussing does not pose any extra restriction on a single monochromatic $(k - 1)$-AP.

Furthermore, $\frac{k}{k-1}W(r, k, r) \geq W(r, k)$, since one of the r monochromatic $(k-1)$-APs that are color focussed on $x \leq \frac{k}{k-1}W(r, k, r)$ will have the same color as x and hence forms a monochromatic k-AP with it.

We use induction on s to show that $W(r, k, s)$ is finite for every $s \leq r$. This will imply our inductive statement for k since then $\frac{k}{k-1}W(r, k, r) \geq W(r, k)$ is finite.

For $s = 1$ we have $W(r, k, 1) = W(r, k - 1)$, which is finite by our induction on k.

We will show that for any $s \geq 1$,

$$W(r, k, s + 1) \leq 2W(r, k, s)W\left(r^{2W(r,k,s)}, k - 1\right) =: n_{s+1}.$$

This number is finite by our induction on s and by our induction on k (used for a huge number of colors). Take any r-colouring of $[n_{s+1}]$ and split $[n_{s+1}]$ into $W\left(r^{2W(r,k,s)}, k - 1\right)$ intervals of length $2W(r, k, s) = 2n_s$. Each block can be coloured in one of r^{2n_s} ways. By the definition of the van der Waerden number there are $k - 1$ blocks with the same color pattern, that form a $(k - 1)$-AP. Let these blocks be $[2an_s+1, 2an_s+2n_s]$, $[2(a+d)n_s+1, 2(a+d)n_s+2n_s], \ldots, [2(a+(k-2)d)n_s+1, 2(a + (k - 2)d)n_s + 2n_s]$. Now consider the first half of the first block: $[2an_s + 1, 2an_s + n_s]$. This is an r-coloured interval of length $n_s = W(r, k, s)$. By the definition of this number, if we have no monochromatic k-AP, then we must have s color-focused $(k-1)$-APs in it. Say for $j \in [s]$, let $P_j = \{2an_s + a_j, 2an_s + a_j + d_j, \ldots, 2an_s + a_j + (k - 2)d_j\}$ be monochromatic $(k - 1)$-AP in

color c_j for $j \in [s]$, such that the c_js are pairwise distinct and the P_j focus on the integer x, that is $x = 2an_s + a_j + (k-1)d_j$ for every $j \in [s]$. Observe that $x \in [2an_s + 1, 2an_s + 2n_s]$ is still in the first block.

If the color of x is equal to any of the c_j then x completes a monochromatic k-AP in that color. Otherwise the color of x is a new color c_{s+1}. Using the fact that in the other $k-2$ blocks the color pattern is the same, we find the translates of the P_j and x in each of these blocks, in the same color as in the first one. We can now produce $(s+1)$ monochromatic $(k-1)$-APs that are color focussed on the integer $x + (k-1)d$. Indeed, there is a monochromatic $(k-1)$-AP in color c_j when we take the ith element from the jth AP in the ith block: $a2n_s + a_j, a2n_s + a_j + d_j + d, a2n_s + a_j + d_j + 2d, \ldots, a2n_s + a_j + (k-2)d_j + (k-2)d$ is a monochromatic $(k-1)$-AP in color c_j with difference $d_j + d$, and its subsequent term $a2n_s + a_j + (k-1)(d_j + d)$ is equal to $x + (k-1)d$ for every $j \in [s]$. Finally there is a monochromatic $(k-1)$-AP in color c_{s+1} and with difference d when we take the foci $x + id$ of the color focused $(k-1)$-APs in each of the $k-1$ blocks.

This completes the induction step and hence the proof of our theorem. □

Let us end this section with a couple of remarks on the bounds of the Van der Waerden numbers. The above double-induction proof gives **terrible** bounds. For example:

$$W(2,3) \leq 2W(2,3,2) \leq 2[2W(2,3,1)(2^{2W(2,3,1)}+1) = 2[2W(2,2)(2^{2W(2,2)}+1)]] = 2[2{\cdot}3(2^{2\cdot 3}+1)] = 780$$

when we know that in reality $W(2,3) = 9$. Furthermore the proof gives $W(3,3) \leq 10^{50099}$, but $W(3,3) = 27$.
In general, the obtained bound on $W(2,k)$ grows faster than any tower. To have a sense how large it is let us define the Grzegorczyk hierarchy of primitive recursive functions.

- $g_1(n) := 2n$,
- $g_{i+1}(n) := \underbrace{g_i(g_i(\cdots g_i(g_i(1))\cdots))}_{n\text{-times}}$

Example: $g_2(n) = 2^n$, $\quad g_3(n) = \underbrace{2^{2^{\cdot^{\cdot^{\cdot^2}}}}}_{n\text{-times}}$

The upper bound one obtains from van der Waerden's proof is roughly $g_k(k)$. It was considered a breakthrough when Saharon Shelah in 1988 came up with a proof that provided a primitive recursive upper bound: $g_4(k)$. In 2001 Timothy Gowers, as a corollary to his new analytic number theoretic proof of Szemerédi's Theorem, improved the upper bound to $2^{2^{2^{2^{2^{k+9}}}}}$. Ron Graham offers 1000$ to prove $W(2,k) \leq 2^{k^2}$.

In terms of lower bounds Berlekamp in 1968 gave a monochromatic k-AP-free coloring of $[(k-1)2^{k-1}]$ whenever k is a prime. The best general lower bound, valid for *every* large enough k, is due to Zoltán Szabó (1990), who showed that for every $\epsilon > 0$ and every $k > k_0(\epsilon)$, $W(2,k) > \frac{2^k}{k^\epsilon}$.