

Van der Waerden's Theorem

Lecturer: Michel Goemans

We're going to use our knowledge of probability to prove a statement that doesn't seem to have any relation to probability at all! It's an example of the *probabilistic method*; it has become a staple tool in combinatorics.

We're only going to deal with natural numbers in what follows. Recall the concept of an *arithmetic progression*; a subset of "equally spaced" numbers. For our purposes, a *k-term arithmetic progression* is a subset

$$\{a, a + b, a + 2b, \dots, a + (k - 1)b\}$$

of \mathbb{N} , for some $a, b \in \mathbb{N}$. So for example, 1, 3, 5, 7 and 7, 11, 15, 19 are both 4-term arithmetic progressions.

Next, we define the idea of a *coloring* of a subset. Let S be a subset of \mathbb{N} (e.g., $\{1, 2, \dots, 100\}$). A 2-coloring of S simply assigns each element of S either "red" or "blue". (More formally, a 2-coloring is a map $\chi : S \rightarrow \{1, 2\}$, where 1 and 2 represent red and blue.)

The following theorem is known as "[Van der Waerden's Theorem](#)"; it's an example of a result in Ramsey Theory.

Theorem 1. *For every $k \in \mathbb{N}$, there exists an $n \in \mathbb{N}$ such that for every 2-coloring of $\{1, 2, \dots, n\}$, there exists some k -term arithmetic progression which is monochromatic (i.e., whose elements all have the same color).*

We won't prove this theorem; it doesn't need a lot of background though, so you could try to read the proof if you're interested.

Now let $W(k)$ be the smallest possible choice of n in the theorem, for a particular value of k ; the $W(k)$'s are known as Van der Waerden numbers. In other words, $W(k)$ is such that any 2-coloring of $\{1, 2, \dots, W(k)\}$ contains a monochromatic k -term arithmetic progression; but there exists some coloring of $\{1, 2, \dots, W(k) - 1\}$ with *no* monochromatic k -term arithmetic progression. For example, $W(2) = 3$; this is easy to see just by trying all the possible colorings. It turns out that $W(3) = 9$; that's not as easy to prove, though it's not hard to find a coloring of $\{1, \dots, 8\}$ with no k -term arithmetic progressions:

1 2 3 4 5 6 7 8.

If you try to color one more, you'll find you get stuck, no matter what you do! These van der Waerden numbers have received lots of interest; we don't know too much about them, and in particular we only have exact values for $W(k)$ for fairly small values of k .

We are going to prove a *lower bound* for $W(k)$:

Theorem 2. *For any $k \in \mathbb{N}$,*

$$W(k) \geq \sqrt{k-1} \cdot 2^{(k-1)/2}.$$

Proof. Let n be the largest integer strictly smaller than $\sqrt{k-1} \cdot 2^{(k-1)/2}$. Our goal is to show that there exists a “good” coloring of $\{1, 2, \dots, n\}$: in other words, a coloring with *no* monochromatic k -term arithmetic progressions. However, we will not explicitly construct a good coloring. Instead, we are going to prove that a certain *randomly chosen* coloring has a positive probability of being good. This implies that there exists a good coloring; if there was no good coloring, the chance of getting a good coloring would have to be zero!

So define a random coloring of $\{1, 2, \dots, n\}$ as follows: for each i between 1 and n , color i red with probability $1/2$, and color it blue with probability $1/2$, and do this independently for each i . In other words, we toss an unbiased coin n times, one for each position, to determine the colors. Now define the random variable

$$f = \#\text{monochromatic } k\text{-term arithmetic progressions in } \{1, \dots, n\}.$$

Our goal is to show that $\mathbb{P}(f = 0) > 0$. Our strategy to prove that is to show that $\mathbb{E}(f) < 1$; this is sufficient, by the following Lemma:

Lemma 1. *Let g be any random variable taking on only nonnegative integer values, and satisfying $\mathbb{E}(g) < 1$. Then $\mathbb{P}(g = 0) > 0$.*

Proof. We have

$$\begin{aligned} \mathbb{E}(g) &= \sum_{i=0}^{\infty} \mathbb{P}(g = i)i \\ &\geq \sum_{i=1}^{\infty} \mathbb{P}(g = i) \quad (\text{note the change in summation index}) \\ &= 1 - \mathbb{P}(g = 0); \end{aligned}$$

the last line follows since $\sum_{i=0}^{\infty} \mathbb{P}(g = i) = 1$. Rearranging,

$$\mathbb{P}(g = 0) \geq 1 - \mathbb{E}(g) > 0.$$

□

(If you think about it a bit, the lemma should seem quite intuitive; if the average is less than 1, and the random variable is nonnegative, it had better be less than 1 at least some of the time; since it’s integral, it must be zero some of the time.)

In order to get a handle on $\mathbb{E}(f)$, we will use linearity of expectation. Define, for any $a, b \in \mathbb{N}$,

$$Q_{a,b} = \{a, a + b, \dots, a + (k - 1)b\}.$$

Then define for any a, b such that $Q_{a,b} \subseteq \{1, \dots, n\}$ the indicator random variable

$$I_{a,b} = \begin{cases} 1 & \text{if } Q_{a,b} \text{ is monochromatic} \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$f = \sum_{(a,b): Q_{a,b} \subseteq \{1, \dots, n\}} I_{a,b};$$

every monochromatic k -term arithmetic progression will be counted once in the right hand side. Thus, using linearity of expectation,

$$\begin{aligned}\mathbb{E}(f) &= \sum_{(a,b):Q_{a,b}\subseteq\{1,\dots,n\}} \mathbb{E}(I_{a,b}) \\ &= \sum_{(a,b):Q_{a,b}\subseteq\{1,\dots,n\}} \mathbb{P}(Q_{a,b} \text{ is monochromatic}).\end{aligned}$$

Now it's not hard to see that for any a, b ,

$$\mathbb{P}(Q_{a,b} \text{ is monochromatic}) = \frac{1}{2^k} \cdot 2 = \frac{1}{2^{k-1}};$$

$Q_{a,b}$ has k elements, each red with probability $1/2$; so the probability that they are all red is $1/2^k$, and the same for all blue. So to get a bound on $\mathbb{E}(f)$, we just need to bound the number of terms in the sum.

So how many k -term arithmetic progressions are there, roughly? Well certainly a is between 1 and n (actually it can't be more than $n - k$, but we just want a rough bound). The final term of the arithmetic progression must be at most n , and so $a + (k - 1)b \leq n$. Thus certainly $b \leq n/(k - 1)$. Since each k -term arithmetic progression is determined by the pair (a, b) , there are at most $n^2/(k - 1)$ of them.

So all in all, we have

$$\mathbb{E}(f) \leq \frac{n^2}{k - 1} \cdot \frac{1}{2^{k-1}};$$

considering how we defined n , we see that we have reached our goal: $\mathbb{E} f < 1$. Thus, by the Lemma, $\mathbb{P}(f = 0) > 0$, and there must exist a good coloring. □

The bound of the above theorem could be improved slightly, by doing a more precise count of the number of k -term arithmetic progressions.

Again, note that this proof does not tell us *how* to find a good coloring (except perhaps by trying random colorings until we find one that works), and doesn't tell us what these good colorings look like. There are many examples of situations where we can prove that a certain structure exists, using the probabilistic method, but have no explicit deterministic construction!

MIT OpenCourseWare
<http://ocw.mit.edu>

18.310 Principles of Discrete Applied Mathematics
Fall 2013

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.