MAT 307: Combinatorics

Lecture 11: The probabilistic method

Instructor: Jacob Fox

Very often, we need to construct a combinatorial object satisfying properties, for example to show a counterexample or a lower bound for a certain statement. In situations where we do not have much a priori information and it's not clear how to define a concrete example, it's often useful to try a *random construction.*

1 Probability basics

A *probability space* is a pair $(\Omega, \Pr)$ where Pr is a normalized measure on Ω, i.e. $\Pr(\Omega) = 1$. In combinatorics, it's mostly sufficient to work with finite probability spaces, so we can avoid a lot of the technicalities of measure theory. We can assume that Ω is a finite set and each *elementary event* $\omega \in \Omega$ has a certain probability $\Pr[\omega] \in [0, 1]$; $\sum_{\omega \in \Omega} \Pr[\omega] = 1$.

Any subset $A \subseteq \Omega$ is an *event*, of probability $\Pr[A] = \sum_{\omega \in A} \Pr[\omega]$. Observe that a union of events corresponds to OR and an intersection of events corresponds to AND.

A *random variable* is any function $X : \Omega \to R$. Two important notions here will be *expectation* and *independence.*

Definition 1. *The expectation of a random variable X is*

$$\mathbf{E}[X] = \sum_{\omega \in \Omega} X(\omega) \Pr[\omega] = \sum_{a} a \Pr[X = a].$$

Definition 2. *Two events $A, B \subseteq \Omega$ are independent if*

$$\Pr[A \cap B] = \Pr[A] \Pr[B].$$

Two random variables X, Y are independent if the events $X = a$ and $Y = b$ are independent for any choices of a, b.

Lemma 1. *For independent random variables X, Y, we have $\mathbf{E}[XY] = \mathbf{E}[X]\mathbf{E}[Y]$.*

Proof.

$$\mathbf{E}[XY] = \sum_{\omega \in \Omega} X(\omega)Y(\omega) \Pr[\omega] = \sum_{a,b} ab \Pr[X = a, Y = b] = \sum_{a} a \Pr[X = a] \sum_{b} b \Pr[Y = b] = \mathbf{E}[X]\mathbf{E}[Y].$$

□

The two most elementary tools that we will use are the following.

1.1 The union bound

Lemma 2. *For any collection of events $A_1, \ldots, A_n$,*

$$\Pr[A_1 \cup A_2 \cup \ldots \cup A_n] \leq \sum_{i=1}^{n} \Pr[A_i].$$

An equality holds if the events A_i are disjoint.

This is obviously true by the properties of a measure. This bound is very general, since we do not need to assume anything about the independence of $A_1, \ldots, A_n$.

1.2 Linearity of expectation

Lemma 3. *For any collection of random variables $X_1, \ldots, X_n$,*

$$\mathbf{E}[X_1 + X_2 + \ldots + X_n] = \sum_{i=1}^{n} \mathbf{E}[X_i].$$

Again, we do not need to assume anything about the independence of $X_1, \ldots, X_n$.

Proof.

$$\mathbf{E}[\sum_{i=1}^{n} X_i] = \sum_{\omega \in \Omega} \sum_{i=1}^{n} X_i(\omega) \Pr[\omega] = \sum_{i=1}^{n} \sum_{\omega \in \Omega} X_i(\omega) \Pr[\omega] = \sum_{i=1}^{n} \mathbf{E}[X_i].$$

□

2 2-colorability of hypergraphs

Our first application is the question of 2-colorability of hypergraphs. We call a hypergraph 2-colorable, if its vertices can be assigned 2 colors so that every hyperedge contains both colors. An example which is *not* 2-colorable is the complete r-uniform hypergraph on $2r-1$ vertices, $K^{(r)}_{2r-1}$. This is certainly not 2-colorable, because for any coloring there is a set of r vertices of the same color. The number of hyperedges here is $\binom{2r-1}{r} \simeq 4^r/\sqrt{r}$.

A question is whether a number of edges exponential in r is necessary to make a hypergraph non-2-colorable. The probabilistic method shows easily that this is true.

Theorem 1. *Any r-uniform hypergraph with less than 2^{r-1} hyperedges is 2-colorable.*

Proof. Consider a random coloring, where every vertex is colored independently red/blue with probability 1/2. For each hyperedge e, the probability that e is monochromatic is $2/2^r$. By the union bound,

$$\Pr[\exists \text{monochromatic edge}] \leq \sum_{e \in E} \frac{2}{2^r} = \frac{2|E|}{2^r} < 1$$

by our assumption that $|E| < 2^{r-1}$. If every coloring contained a monochromatic edge, this probability would be 1; therefore, for at least one coloring this is not the case and therefore the hypergraph is 2-colorable. □

3 A tournament paradox

A tournament is a directed graph where we have an arrow in exactly one direction for each pair of vertices. A tournament can represent the outcome of a competition where exactly one game is played between every pair of teams. A natural notion of k winning teams would be such that there is no other team, beating all these k teams. Unfortunately, such a notion can be ill-defined, for any value of k.

Theorem 2. *For any $k \geq 1$, there exists a tournament T such that for every set of k vertices B, there exists another vertex x such that $x \to y$ for all $y \in B$.*

Proof. We can assume k sufficiently large, because the theorem gets only stronger for larger k. Given k, we set $n = k + k^2 2^k$ and consider a uniformly random tournament on n vertices. This means, we select an arrow $x \to y$ or $y \to x$ randomly for each pair of vertices x, y.

First let's fix a set of vertices B, $|B| = k$, and analyze the event that no other vertex beats all the vertices in B. For each particular vertex x,

$$\Pr[\forall y \in B; x \to y] = \frac{1}{2^k}$$

and by taking the complement,

$$\Pr[\exists y \in B; y \to x] = 1 - \frac{1}{2^k}.$$

Since these events are independent for different vertices $x \in V \setminus B$, we can conclude that

$$\Pr[\forall x \in V \setminus B; \exists y \in B; y \to x] = (1 - 2^{-k})^{n-k} = (1 - 2^{-k})^{k^2 2^k} \leq e^{-k^2}.$$

By the union bound over all potential sets B,

$$\Pr[\exists B; |B| = k; \forall x \in V \setminus B; \exists y \in B; y \to x] \leq \binom{n}{k} e^{-k^2} \leq (k^2 2^k)^k e^{-k^2} = \left(\frac{k^2 2^k}{e^k}\right)^k.$$

For k sufficiently large, this is less than 1, and hence there exists a tournament where the respective event is *false*. In other words, $\forall B; |B| = k; \exists x \in V \setminus B; \forall y \in B; x \to y$. $\square$

It is known that $k^2 2^k$ is quite close to the optimal size of a tournament satisfying this property; more precisely, $ck2^k$ for some $c > 0$ is known to be insufficient.

4 Sum-free sets

Our third application is a statement about *sum-free sets*, that is sets of integers B such that if $x, y \in B$ then $x + y \notin B$. A question that we investigate here is, how many elements can be pick from any set A of n integers so that they form a sum-free set? As an example, consider $A = [2n]$. We can certainly pick $B = \{n+1, n+2, \ldots, 2n\}$ and this is a sum-free set of size $\frac{1}{2}|A|$. Perhaps this is not possible for any A, but we can prove the following.

Theorem 3. *For any set of nonzero integers A, there is a sum-free subset $B \subseteq A$ of size $|B| \geq \frac{1}{3}|A|$.*

Proof. We proceed by reducing the problem to a problem in the finite field Z_p. We choose p prime large enough so that $|a| < p$ for all $a \in A$. We observe that in Z_p (counting addition modulo p), there is a sum-free set $S = \{\lceil p/3 \rceil, \ldots, \lfloor 2p/3 \rfloor\}$, which has size $|S| \geq \frac{1}{3}(p-1)$.

We choose a subset of A as follows. Pick a random element $x \in Z_p^* = Z_p \setminus \{0\}$, and let

$$A_x = \{a \in A : (ax \bmod p) \in S\}.$$

Note that A_x is sum-free, because for any $a, b \in A_x$, we have $(ax \bmod p), (bx \bmod p) \in S$ and hence $(ax + bx \bmod p) \notin S$, $a + b \notin A_x$. It remains to show that A_x is large for some $x \in Z_p^*$. We have

$$\mathbf{E}[|A_x|] = \sum_{a \in A} \Pr[a \in A_x] = \sum_{a \in A} \Pr[(ax \bmod p) \in S] \geq \frac{1}{3}|A|$$

because $\Pr[(ax \bmod p) \in S]$ is equal to $|S|/(p-1) \geq \frac{1}{3}$ for any fixed $a \neq 0$. This implies that there is a value of x for which $|A_x| \geq \frac{1}{3}|A|$. $\square$