The Probabilistic Method

Instructor: Noga Alon
Notes by Nilava Metya

Spring 2024

Contents

Lecture 1

01/30/2024

1.1 Philosophy

Main philosophy of the probabilistic method: To prove existence of a structure (or a substructure of a given one), define a probability space of structures, and show that a random point in it satisfies the required properties with positive (often high) probability.

We will look at two examples today.

1.2 Example: Ramsey Theory

Definition 1 (Ramsey numbers)
For $k, \ell \geq 1$, let $r = r(k, \ell)$ be the smallest integer, if there exists any, satisfying the following property: for every coloring of edges of $G = K_r$ (the complete graph on r nodes) by red and blue, either $\exists$ a blue $K_k \subseteq G$ or a red $K_\ell \subseteq G$.

Example 1. $r(3, 3) = 6$.

A special case of Ramsey's theorem says that $\exists r(k, l) < \infty \forall k, l$. The proof, by induction (using Erdös-Szekeres theorem), gives $r(k, \ell) \leq \begin{pmatrix} k + \ell - 2 \\ k - 1 \end{pmatrix}$. In particular, $r(k, k) \leq \binom{2k-2}{k-1} < 4^k$.

Remark 1
The following are easy to observe: $r(k, \ell) = r(l, k), r(1, \ell) = 1, r(2, \ell) = \ell$.

All the exactly known Ramsey numbers for $\ell \geq k \geq 3$ are $r(3, 3) = 6, r(3, 4) = 9, r(3, 5) = 14, r(3, 6) = 18, r(3, 7) = 23, r(3, 8) = 28, r(3, 9) = 36, r(4, 4) = 18, r(4, 5) = 25$. It is only known that $41 \leq r(3, 10) \leq 42, 36 \leq r(4, 6) \leq 40, 43 \leq r(5, 5) \leq 48$, and some similar bounds for other Ramsey numbers.

Theorem 2 (Erdos '47)
If $\binom{n}{k}2^{1-\binom{k}{2}} < 1$ then $r(k,k) > n$. Therefore $r(k,k) \geq [1-o(1)]\,\frac{k}{e}2^{\frac{k-1}{2}}$.

Proof. Take the complete graph on n labelled vertices $[n] = \{1, \cdots, n\}$. Color each edge $\{i,j\}$ (for $1 \leq i < j \leq n$) randomly uniformly and independently either red or blue. For fixed $K \subseteq [n]$ with $k = |K|$, the probability that the graph induced by K is monochromatic is $2^{-\binom{k}{2}} + 2^{-\binom{k}{2}} = 2^{1-\binom{k}{2}}$. So

$$\begin{aligned}\mathbb{P}\left[\exists \text{ such monochromatic } K\right] &\leq \sum_{\substack{K\subseteq[n]\\|K|=k}} \mathbb{P}\left[K \text{ induces a monochromatic graph}\right]\\ &= \binom{n}{k}2^{1-\binom{k}{2}} \overset{\text{given}}{<} 1.\end{aligned}$$

Therefore, $\mathbb{P}\left[\nexists \text{ such monochromatic } K\right] > 0$. This means $r(k,k) > n$, which proves the first part.

Now,

$$\binom{n}{k}2^{1-\binom{k}{2}} \leq 2\left(\frac{en}{k}\right)^k \cdot 2^{-\binom{k}{2}} = 2\left(\frac{en}{2^{\frac{k-1}{2}}\cdot k}\right)^k$$

where the first inequality is due to $\binom{a}{b} \leq \left(\frac{ea}{b}\right)^b$. If $\frac{en}{2^{\frac{k-1}{2}}\cdot k} < 1-\varepsilon$ then for $k > k_0(\varepsilon)$ for some $k_0(\varepsilon)$, the RHS is < 1. This implies that $r(k,k) \geq [1-o(1)]\,\frac{k}{e}2^{\frac{k-1}{2}}$.[1] ∎

Remark 2
The lower bound was improved only by a factor of two since 1947.
The upper bound was improved several times, last time in 2023 by Campos, Griffiths, Morris, Sahasrabudhe to $(4-\varepsilon)^k$, for an absolute constant $\varepsilon > 0$.
Open: Does $\lim r(k,k)^{1/k}$ exist (for USD 100)? If exists, find it (for USD 250).

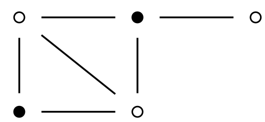
Remark 3
Open problem: Find an explicit coloring showing $r(k,k) > 1.0001^k$.

Remark 4
This proof provides a randomized algorithm for finding a coloring that shows $r(k,k) > \left\lfloor\sqrt{2^k}\right\rfloor$.
But given such a coloring, we don't know how to efficiently check that $\nexists$ a monochromatic K_k.

[1] Explanation for the last 'implies': We note that for every n satisfying the given condition, we have $r(k,k) > n$. Now for any $n < [1-\varepsilon]\,\frac{k}{e}2^{\frac{k-1}{2}}$, the condition is satisfied. Thus, $r(k,k)$ is more than all such n's, which is written as $[1-o(1)]\,\frac{k}{e}2^{\frac{k-1}{2}}$.

1.3 Example: Dominating Sets

Definition 3
If $G = (V, E)$ is a graph, we say $S \subseteq V$ is dominating if $\forall v \in V \setminus S \exists u \in S$ such that $\{u, v\} \in E$.

Example 2. The set of bold vertices in  form a dominating set.

Theorem 4
If $G = (V, E)$ is a graph with $|V| = n$ and minimum degree δ, then it has a dominating set of size at most $n \cdot \dfrac{1 + \ln(1+\delta)}{1+\delta}$.

Proof. Let $p = \frac{\ln(1+\delta)}{1+\delta}$. Clearly $p \in [0, 1]$. Let $X \subseteq V$ be a random subset of V obtained by choosing each $v \in V$ to randomly and independently lie in X with probability p. Since X is not necessarily a dominating set, we can *alter* it by

$$Y_X := \left\{ v \in V \setminus X \;\middle|\; \nexists u \in X \text{ with } \{u, v\} \in E \right\}.$$

By construction, $X \sqcup Y_X$ is a dominating set (note that they are disjoint).

Let's estimate the expected size of $X \cup Y_X$. First observe that $\mathbb{E}[|X \cup Y_X|] = \mathbb{E}[|X| + |Y_X|]$ due to disjointness, and this is further equal to $\mathbb{E}[|X|] + \mathbb{E}[|Y_X|]$ by linearity of expectation. $|X|$ is a sum of independent indicators, one for each vertex which takes 1 with probability p and 0 with probability $1 - p$. So $\mathbb{E}[|X|] = np$.
Note that $\mathbb{P}[v \in Y_X] = \mathbb{P}[v \notin X] \cdot \mathbb{P}[\text{no neighbor of } v \text{ is in } X] = (1-p)^{d_v} \leq (1-p)^{1+\delta} = \frac{1}{1+\delta}$ where d_v is the degree of v in G. Again $|Y_X| = \sum_{v \in V} \mathbf{1}_{v \in Y_X}$ whence $\mathbb{E}[|Y_X|] \leq \frac{n}{1+\delta}$.
This means $\mathbb{E}[|X \cup Y_X|] \leq n \left[\frac{1+\ln(1+\delta)}{1+\delta}\right]$. Since the 'average size' of a dominating set is less than or equal to the given quantity, $\exists$ a choice of X such that $X \cup Y_X$ is a dominating set of size at most $n \cdot \dfrac{1+\ln(1+\delta)}{1+\delta}$. ∎

Remark 5
We used *linearity of expectation*: $\mathbb{E}[X + Y] = \mathbb{E}[X] + \mathbb{E}[Y]$. We also used *alteration*: making a change after initial random choice, in this case we added Y_X to X. (To be discussed more)

Remark 6
Here $\exists$ an efficient algorith to find such a dominating set. Start with $\varnothing$ and keep adding vertices that dominate maximum of yet non-dominated vertices.

Remark 7
Estimate is essentially that for $n \gg \delta \gg 1$.

Lecture 2

02/01/2024

Examples continued from last lecture.

2.1 Example: Hypergraph $2-$coloring

Definition 5
A *hypergraph* is a pair $H = (V, E)$ of (finitely many) vertices V and edges $E \subseteq 2^V$.

We say a hypergraph is $n-$*uniform* if $|e| = n \forall e \in E$. In particular, graphs are $2-$uniform hypergraphs.

We say a hypergraph is said to be $2-$*colorable* if there exists a coloring of V with red and blue with no monochromatic edge.

We define the quantity

$$m(n) \coloneqq \min \{|E| \mid (V, E) \text{ is } n-\text{uniform hypergraph and not } 2-\text{colorable}\}$$

and interested in its asymptotics.

It is known that $m(1) = 1, m(2) = 3, m(3) = 17, m(4) = 23$ and for $n \geq 5$, $m(n)$ are unknown.

Proposition 6
$m(n) \geq 2^{n-1}$ for $n \geq 2$.

Proof. For the sake of contradiction, let $H = (V, E)$ be $n-$uniform with $|E| < 2^{n-1}$. We will show that H is $2-$colorable. Color randomly each vertex independently either red or blue with probability half for each color. For each edge $e \in E$, let A_e be the event that e is monochromatic. Then $\mathbb{P}[A_e] = 2 \cdot \left(\frac{1}{2}\right)^n = 2^{1-n}$. This means that $\mathbb{P}[\cup_{e \in E} A_e] \leq \sum_{e \in E} \mathbb{P}[A_e] = |E| \cdot 2^{1-n}$ which is less than 1 by assumption. This means that the event that no edge is monochromatic has positive probability, implying that there is a coloring for which there is no monochromatic edge. By definition, this is a $2-$coloring. ∎

Remark 8
The proof for lower bound of $r(k,k)$ is a special case. Take $n = \binom{k}{2}$. Vertices of the hypergraph are $E(K_n)$ and hyperedges are collections of $\binom{k}{2}$ edges of K_n that form a $k-$clique. So number of hyperedges is $\binom{n}{k}$.

Remark 9
It can be shown that $m(n) \leq O(n^2 2^{n-1})$, that is $\exists c > 0$ such that $m(n) \leq cn^2 2^{n-1}$ for all large n. Indeed if we take $2n^2$ vertices and $cn^2 2^{n-1}$ random subsets of size n, then with positive probability, every set of n^2 vertices contains an edge. So not 2−colorable.
Note that the interesting quantity here is $\frac{m(n)}{2^{n-1}}$ which is the expected number of monochromatic edges in a random coloring. Thus $1 \leq \dfrac{m(n)}{2^{n-1}} \leq O(n^2)$.

Lower bound for $\frac{m(n)}{2^{n-1}}$ has been improved by Beck, by Radhakrishnan + Srinivasan. Best (short) proof is by Cherkashin and Kozik which is the following.

Theorem 7
If $\exists k \geq 1, 0 \leq p \leq 1$ such that $k(1-p)^n + k^2 p < 1$ then $m(n) > k \cdot 2^{n-1}$.

Proof. Let n, k, p be as in the hypothesis of the theorem we're proving. Let $H = (V, E)$ be an $n-$uniform graph with $|E| = k \cdot 2^{n-1}$. For each $v \in V$ pick $x_v \in [0,1]$ uniformly randomly. (We can assume that these x_v's are unique because any two of them are equal with 0 probability). These x_v's define an ordering on the vertices, that is, we say $v < u$ iff $x_v < x_u$.

Now go over the vertices in increasing order and color each vertex blue unless forced to color it red (namely, the vertex appears as the last vertex in an otherwise blue edge). By construction, there is no blue edge. But there can be a red edge. Let's look at probability that such a thing happens.

Define $L = \left[0, \frac{1-p}{2}\right), M = \left[\frac{1-p}{2}, \frac{1+p}{2}\right), R = \left[\frac{1+p}{2}, 1\right]$. Let A_e be the event that edge $e \in E$ is fully contained in L or fully contained in R, and define $A := \bigcup_{e \in E} A_e$. Then $\mathbb{P}[A_e] = \mathbb{P}[x_v \in L \forall v \in e] + \mathbb{P}[x_v \in R \forall v \in e] = 2\mathbb{P}[x_v \in L \forall v \in e] = 2 \cdot \left(\frac{1-p}{2}\right)^n$. Thus

$$\begin{aligned}
\mathbb{P}[A] &\leq \sum_{e \in E} \mathbb{P}[A_e] \\
&\leq k \cdot 2^{n-1} \cdot 2 \cdot \left(\frac{1-p}{2}\right)^n \\
&= k(1-p)^n.
\end{aligned}$$

Suppose the event $\bigcup\limits_{e \in E} A_e$ does not happen and there is a red edge. The former means every edge has one vertex each in at least two of L, M, R. Consider the first red edge e_0, that is, the edge e with lowest value of $\min\limits_{v \in e} x_v$ among red edges. Let v_0 be the first vertex in e_0. Clearly $v_0 \notin R$, else e_0 would be completely in R. Also, $v_0 \notin L$ because otherwise v_0

is the last edge of some otherwise blue edge which would hence completely be in L. Thus $v_0 \in M$. Say v_0 is the last vertex of $f_0 \in E$. Altogether, we care that there are two edges e_0, f_0 with $e_0 \cap f_0 = \{v_0\}$ and $v_0 \in M$, also called a *conflicting* pair of edges. Also in this case, the probability that v_0 is the last vertex of f_0 is $\mathbb{P}\left[x_u \leq x_{v_0} \forall u \in f_0 \setminus \{v_0\}\right] = x_{v_0}^{n-1}$, and the probability that v_0 is the first vertex of e_0 is $\mathbb{P}\left[x_u \geq x_{v_0} \forall u \in e_0 \setminus \{v_0\}\right] = (1 - x_{v_0})^{n-1}$, because $|e_0| = |f_0| = n$ (by n−regularity of H). Thus

$$\begin{aligned}
\mathbb{P}\left[A^c \cap \{\exists \text{ red edge}\}\right] &\leq \mathbb{P}\left[\text{there is a conflicting pair of edges}\right] \\
&\leq \sum_{\substack{(e,f)\in E\times E \\ |e\cap f|=1}} \mathbb{P}\left[(e,f) \text{ is a conflicting pair}\right] \\
&= \sum_{\substack{(e,f)\in E\times E \\ |e\cap f|=1}} \mathbb{P}\left[(e\cap f \subseteq M) \cap (e \setminus (e\cap f) \subseteq L) \cap (f \setminus (e \cap f) \subseteq R)\right] \\
&= \sum_{\substack{(e,f)\in E\times E \\ |e\cap f|=1}} \mathbb{P}\left[e\cap f \subseteq M\right] \cdot \mathbb{P}\left[e \setminus (e\cap f) \subseteq L\right] \cdot \mathbb{P}\left[f \setminus (e \cap f) \subseteq R\right] \\
&= \sum_{\substack{(e,f)\in E\times E \\ |e\cap f|=1}} p \cdot x_{e\cap f}^{n-1} \cdot (1 - x_{e\cap f})^{n-1} \\
&\leq \sum_{\substack{(e,f)\in E\times E \\ |e\cap f|=1}} p \cdot \max_{x\in M} \left[x(1-x)\right]^{n-1} \\
&\leq (k \cdot 2^{n-1})^2 \cdot p \cdot \max_{x\in M} \left[x(1-x)\right]^{n-1} \\
&= k^2 \cdot 4^{n-1} \cdot p \cdot \frac{1}{4^{n-1}} = pk^2
\end{aligned}$$

So $\mathbb{P}\left[\exists \text{ red edge}\right] \leq \mathbb{P}\left[A\right] + \mathbb{P}\left[A^c \cap \{\exists \text{ red edge}\}\right] \leq k(1-p)^n + kp^2$. This quantity is < 1, whence $\mathbb{P}\left[\nexists \text{ red edge}\right] > 0$. This means that there is a coloring such that there is no red edge (there was no blue edge by construction). By definition, this is a 2−coloring. So $m(n)$ must be greater than the number of edges of this graph, namely $k \cdot 2^{n-1}$. ■

Corollary 8
$m(n) > 2^{n-2} \cdot \sqrt{\frac{n}{\ln n}}$.

Proof. If $k = \frac{1}{2}\sqrt{\frac{n}{\ln n}}$ and $p = \frac{\ln n}{n}$. Then $1 - p \leq e^{-p} \implies k(1-p)^n \leq ke^{-pn} = \frac{k}{n}$. Therefore $k^2 p + k(1-p^n) \leq \frac{n}{4 \ln n} \cdot \frac{\ln n}{n} + \frac{\sqrt{n}}{2n\sqrt{\ln n}} = \frac{1}{4} + \frac{1}{2\sqrt{n} \ln n} < 1$. By the above theorem, $m(n) > k \cdot 2^{n-1} = 2^{n-2} \cdot \sqrt{\frac{n}{\ln n}}$. ■

2.2 Example: Set Pairs

Theorem 9 (Bollobas)
Let (A_i, B_i) for $1 \leq i \leq h$ be pairs of subsets of $\mathbb{Z}$ satisfying that $A_i \cap B_i = \varnothing \forall i$, $A_i \cap B_j \neq \varnothing \forall i \neq j$ and $|A_i| = k, |B_i| = \ell \forall i$. Then $h \leq \binom{k+\ell}{k}$.
(This is tight: Take $|X| = k + \ell$ and (A_i, B_i) are partitions of X to disjoint sets of sizes k, ℓ.)

Proof. Order $\bigcup_{i=1}^{h} A_i \cup B_i$ randomly. Let E_i be the event that A_i precedes B_i, that is, $\max A_i < \min B_i$. Note that $\mathbb{P}[E_i] = \binom{k+\ell}{k}^{-1}$. Also, events are pairwise disjoint, since if both E_i, E_j occur together and (WLOG) $\max A_i \geq \max A_i$ then $\min B_i > \max A_i \geq \max A_j$ so $A_j \cap B_i = \varnothing$ which cannot happen. This means that $h \cdot \binom{k+\ell}{k}^{-1} = \sum_i \mathbb{P}[E_i] = \mathbb{P}[\bigcup_i E_i] \leq 1$. ∎