Math 155 (Lecture 31)

November 17, 2011

Let Ω be a finite probability space, and suppose we are given a collection of events $E_1, E_2, \ldots, E_m \subseteq \Omega$. In the last lecture, we proved the following result:

Theorem 1 (Lovász Local Lemma)**.** *Suppose there is a graph G with vertex set $\{1, 2, \ldots, m\}$ satisfying the following condition:*

$(*)$ *For each $1 \leq i \leq m$, if S is a set of vertices of G which are distinct from i and not adjacent to i, then E_i is independent of the set of events $\{E_j\}_{j \in S}$.*

Suppose further that we are given real numbers $0 \leq x_i < 1$ such that

$$P(E_i) \leq x_i \prod_{(i,j) \text{ adjacent}} (1 - x_j).$$

Then $P(E_1 \cup \cdots \cup E_m) \leq 1 - \prod_{1 \leq i \leq m}(1 - x_i)$. In particular, we have $E_1 \cup \cdots \cup E_m \neq \Omega$.

Corollary 2 (Lovász Local Lemma, Symmetric Version)**.** *In the situation of Theorem 1, suppose that the graph G has valence $\leq d$ at each vertex (that is, each vertex is adjacent to at most d other vertices). If each of the events E_i has probability $\leq \frac{1}{e(d+1)}$, then $P(E_1 \cup \cdots \cup E_m) < 1$. Here e denotes Euler's constant.*

Example 3. If G is the complete graph with vertex set $\{1, 2, \ldots, m\}$, then condition $(*)$ is vacuous. In this graph, every vertex has valence $m - 1$. Corollary 2 then reads as follows: if each of the events E_i has probability $\leq \frac{1}{em}$, then $P(E_1 \cup \cdots \cup E_m) < 1$.

In fact, we can do a little bit better. If each E_i has probability $< \frac{1}{m}$, then

$$P(E_1 \cup \cdots \cup E_m) \leq \sum_{1 \leq i \leq m} P(E_i) < \frac{m}{m} = 1.$$

However, this is only a slight improvement (a constant factor of $\frac{1}{e}$). In other words, when we have no information about the independence of our events, the local lemma reproduces roughly the same information obtained from the naive estimates $P(E \cup E') \leq P(E) + P(E')$.

To get a feeling for power of the local lemma, let's try it out in a simple example.

Question 4. Fix an integer $n \geq 0$. For what values of k does there exist an injective map $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, k\}$?

Of course, Question 4 is easy to answer directly: an injective map exists if and only if $k \geq n$. Nevertheless, it is instructive to try "reprove" this using the probabilistic method. Let Ω denote the collection of all maps from $\{1, \ldots, n\}$ to $\{1, \ldots, k\}$. We regard Ω as a finite probability space, where each outcome is assigned the same probability $\frac{1}{k^n}$.

For every pair of integers $1 \leq i < j \leq n$, let $E_{i,j} \subseteq \Omega$ be the collection of all maps $f : \{1, \ldots, n\} \to \{1, \ldots, k\}$ satisfying $f(i) = f(j)$. There are $\binom{n}{2}$ of these events, and each occurs with probability $P(E_{i,j}) = \frac{1}{k}$.

A map is injective if and only if it does not belong to any $E_{i,j}$. Consequently, to show that an injective map exists, it suffices to show that

$$P(\bigcup E_{i,j}) < 1.$$

The naive method gives

$$P(\bigcup E_{i,j}) \leq \sum_{i,j} P(E_{i,j}) = \binom{n}{2}\frac{1}{k}.$$

Consequently, an injective map will exist provided that $\binom{n}{2}\frac{1}{k} < 1$: that is, provided that $k > \binom{n}{2}$.

Now let's try a probabilistic analysis that takes into account the independence of the events $E_{i,j}$. Observe that the event $E_{i,j}$ is independent of the set of events $\{E_{i',j'}\}_{i',j' \in S}$, where $S = \{1, \ldots, n\} - \{i, j\}$. Put another way, let G be the graph whose vertices are two-element subsets of $\{1, \ldots, n\}$, where two such subsets are adjacent if they share an element. Then the graph G satisfies hypothesis $(*)$ of Theorem 1. Note that a fixed vertex $\{i, j\}$ is adjacent to exactly $2(n-2)$ other vertices in this graph. Consequently, Corollary 2 tells us that $P(\bigcup E_{i,j}) < 1$ provided that $P(E_{i,j}) = \frac{1}{k} < \frac{1}{e(2n-3)}$. That is, we learn that an injection exists provided that $k > e(2n-3)$ (in particular, any $k \geq 6n$ will do).

Remark 5. To get a feel for the difference between the two estimates, let's look at what the relevant probabilities actually are in our situation. The total number of injections from $\{1, \ldots, n\}$ to $\{1, \ldots, k\}$ is given by $\frac{k!}{(k-n)!} = k(k-1)\cdots(k-n+1)$, and the total number of maps is k^n. Consequently, the probability that a given map is an injection is given by the product

$$p = 1(1 - \frac{1}{k})(1 - \frac{2}{k})\cdots(1 - \frac{n-1}{k}).$$

Let's assume that $k \geq n$, so that p is positive. Then we have

$$\log p = \sum_{1 \leq i < n} \log(1 - \frac{i}{k}) = \sum_{0 \leq i < n} (-\frac{i}{k} + \frac{i^2}{2k^2} - \frac{i^3}{3k^3} + \cdots) > \sum_{1 \leq i < n} -\frac{i}{k} = \frac{-1}{k}\binom{n}{2}.$$

It follows that $p > e^{-\frac{\binom{n}{2}}{k}}$. In particular, if $k = \binom{n}{2}$, we have $p > \frac{1}{e}$. In other words, in the regime where the "naive" probabilistic proves the existence of an injective map, we actually get much more: a randomly chosen map from $\{1, \ldots, n\}$ to $\{1, \ldots, k\}$ has a reasonable chance of being injective.

Suppose instead that $k = 6n$, and (for simplicity) that n is even. If $i \geq \frac{n}{2}$, then $1 - \frac{i}{k} \leq 1 - \frac{1}{12}$. Consequently, the product

$$p = 1(1 - \frac{1}{k})(1 - \frac{2}{k})\cdots(1 - \frac{n-1}{k})$$

is bounded above by $(\frac{11}{12})^{n/2}$. Thus p decays exponentially in n: that is, the probability that a randomly chosen map $\{1, \ldots, n\} \to \{1, \ldots, 6n\}$ is very small.

This example is prototypical: naive probabilistic estimates generally give existence theorems only in the case where "most" of the objects under considerations have the desired property. But more sophisticated arguments using the Local Lemma can be used to prove the existence of objects which have "unlikely" properties.

Problem 6. Give a lower bound for the Ramsey numbers $R(3, n)$.

In Lecture 29, we saw that for each $\delta > 0$, we have $R(4, n) > n^{3/2-\delta}$ for $n \gg 0$. The same technique can be applied here to show that for $\delta > 0$, we have $R(3, n) > n^{1-\delta}$ for $n \gg 0$. But this isn't any better than the tautological bound $R(3, n) \geq n$: in particular, it is far from the upper bound

$$R(3, n) \leq \binom{n+3-2}{2} = \frac{n^2+n}{2}$$

coming from the proof of Ramsey's theorem. Let's see if we can do better using the Local Lemma.

Let Ω be the collection of all graphs with vertex set $\{1,\dots,k\}$. Fix $0 \le p \le 1$, and regard Ω as a probability space where each graph G occurs with probability $p^e(1-p)^{\binom{k}{2}-e}$, where e is the number of edges of G (that is, each edge occurs with probability p). For every 3-element subset $S \subseteq \{1,\dots,k\}$, let E_S denote the set of graphs containing S as a clique. For each n-element subset $T \subseteq \{1,\dots,k\}$, let F_T denote the set of graphs containing T as an anticlique. We would like to show that, if k is too small and p is appropriately chosen, the probability

$$P(\bigcup_S E_S \cup \bigcup_T F_T) < 1$$

(so there is a graph with neither a clique of size S nor an anticlique of size T).

If S is a 3-element subset of $\{1,\dots,k\}$, then the event E_S is independent of the events $\{E_{S'}, F_T\}$, where S' and T range over subsets of $\{1,\dots,k\}$ which do not share an edge with S (meaning they intersect S in at most one point). Let us therefore think of the collection of events $\{E_S, F_T\}$ as forming a graph, where two events are adjacent if the corresponding subsets of $\{1,\dots,k\}$ overlap in more than one point. This graph satisfies condition $(*)$ of Theorem 1. Let us set $p = \frac{1}{2}k^{-1/2}$, and define real numbers

$$x_{E_S} = \frac{1}{6}k^{-3/2} = y \qquad x_{F_T} = k^{-n} = z.$$

Let us study when these numbers satisfy the requirements of Theorem 1.

- Fix a set $S \subseteq \{1,\dots,k\}$ of size 3. Then the event E_S has probability $p^{-3} = \frac{1}{8}k^{-3/2}$. Note that S is adjacent to $3(k-3) < 3k$ other events of the type $E_{S'}$, and to $< \binom{k}{n}$ events of type F_T. Consequently, it will suffice to verify the inequality

  $$p^3 \le y(1-y)^{3k}(1-z)^{\binom{k}{n}}.$$

  We have

  $$(1-z)^{\binom{k}{n}} \ge 1 - \binom{k}{n}z = 1 - \frac{1}{k^n}\binom{k}{n} \ge 1 - \frac{1}{n!}$$

  $$(1-y)^{3k} \ge 1 - 3ky = 1 - \frac{1}{2}k^{-1/2}.$$

  The desired inequality will therefore follow if we can show

  $$\frac{1}{8}k^{-3/2} \le \frac{1}{6}k^{-3/2}(1 - \frac{1}{2}k^{-1/2})(1 - \frac{1}{n!})$$

  or

  $$\frac{3}{4} \le (1 - \frac{1}{2}k^{-1/2})(1 - \frac{1}{n!})$$

  which will be satisfied for all sufficiently large values of k and n.

- Fix a set $T \subseteq \{1,\dots,k\}$ of size n. Then the event F_T has probability $(1-p)^{\binom{n}{2}}$. Note that F_T is adjacent to $\le k\binom{n}{2}$ events of the form E_S, and $\le \binom{k}{n}$ events of the form $F_{T'}$. It will therefore suffice to verify the inequality

  $$(1-p)^{\binom{n}{2}} \le z(1-y)^{k\binom{n}{2}}(1-z)^{\binom{k}{n}}.$$

  Taking logarithms and multiplying by -1, we want

  $$\binom{n}{2}\log(\frac{1}{1-p}) \ge k\binom{n}{2}\log\frac{1}{1-y} + \binom{k}{n}\log\frac{1}{1-z} - \log z.$$

We have seen that the second term is bounded above by $\log \frac{1}{1-\frac{1}{n!}}$, and the third term is given by $n \log k$. Moreover, we have $\log \frac{1}{1-p} = p + p^2 + p^3 + \cdots > p$. It will therefore suffice to check that

$$p > k \log \frac{1}{1-y} + \frac{2}{n^2+n} \log(1 + \frac{1}{n!-1}) + \frac{1}{n+1} \log k.$$

Note that

$$\frac{1}{1-y} = y + \frac{y^2}{2} + \frac{y^3}{3} + \cdots = y + y(\frac{y}{2} + \frac{y^2}{3} + \cdots) \leq 2y$$

since $y \leq \frac{1}{6}$. It will therefore suffice to verify that

$$p > 2ky + \frac{2}{n^2+n} \log(1 + \frac{1}{n!-1}) + \frac{\log k}{n+1}.$$

Let's now assume that $k < (\frac{n}{13 \log n})^2$. The difference $p - 2ky$ is given by $\frac{1}{6}k^{-1/2} > \frac{13 \log n}{6n}$. It therefore suffices to verify the inequality

$$\frac{13 \log n}{6n} > \frac{2}{n^2+n} \log(1 + \frac{1}{n!-1}) + \frac{2 \log(\frac{n}{13 \log n})}{n} = \frac{2}{n^2+n} \log(1 + \frac{1}{n!+1}) + \frac{2 \log n}{n} - \frac{2 \log(13 \log n)}{n}$$

which follows as soon as

$$\frac{\log n}{6n} > \frac{2}{n^2+n} \log(1 + \frac{1}{n!+1}).$$

Any time these inequalities are satisfied, Theorem 1 implies the existence of a graph containing no clique of size 3 and no anticlique of size n, so that $k < R(3, n)$. We have proven:

Proposition 7. *For all sufficiently large values of n, we have $R(3, n) \geq (\frac{n}{13 \log n})^2$.*

In particular, the function $n \mapsto R(3, n)$ grows faster than $n^{2-\delta}$ for every positive real number δ. This is pretty close to optimal, since we know that $R(3, n) \leq \frac{n^2+n}{2}$.