Math 155 (Lecture 32)

November 20, 2011

In the last lecture, we described some applications of the Lovász local lemma which illustrate how it often gives more information than more naive probabilistic reasoning. We begin this lecture by revisiting one of these examples.

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

Recall that the naive probabilistic approach gives a weak upper bound: namely, such a map always exists when $k > \binom{n}{2}$. Using the local lemma, we gave a probabilistic existence proof which is valid for $k > e(2n-3)$ (in particular, for $k \geq 6n$), which is much closer to the optimal answer (namely, that we must have $k \geq n$).

To get a feel for the difference between the two estimates, let's look at what the relevant probabilities actually are. 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 with n: that is, the probability that a randomly chosen map $\{1, \ldots, n\} \to \{1, \ldots, 6n\}$ is injective is very small.

This example is prototypical: naive arguments 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.

Let's now describe another application.

Definition 2. Let G be a graph and $v \in G$ a vertex. The *degree* (or *valence*) of v is the number of vertices of G which are adjacent to v. If $d \geq 0$ is an integer, we say that a graph G is *d-regular* if every vertex has degree d. We say that G is *regular* if it is d-regular for some integer d.

Example 3. A graph G is 0-regular if and only if it has no edges.

Example 4. A graph G is 1-regular if and only if it is a disjoint union of copies of the complete graph on two vertices.

Example 5. A graph G is 2-regular if and only if it is a disjoint union of cycles of length ≥ 3.

We are going to prove the following result:

Proposition 6. *Let G be a finite d-regular graph, and let m be an integer such that $m \leq \frac{d}{1+\log(1+d^2)}$. Then G contains a cycle consisting of distinct vertices of G, whose length is divisible by m.*

Proof. Let V_G be the set of vertices of G, and let Ω be the set of all maps $V_G \to \mathbf{Z}/m\mathbf{Z}$: that is, the set of all vertex colorings of G using the set of colors $\mathbf{Z}/m\mathbf{Z} \simeq \{0, \ldots, m-1\}$. We will regard Ω as a finite probability space, where each coloring occurs with the same probability $\frac{1}{m^n}$, where n is the number of vertices of G.

For each vertex $v \in G$, let E_v be the set of all colorings with the following property: for every vertex w adjacent to v, we have $f(w) \neq f(v) + 1$ (modulo m). We will prove that $\Omega \neq \bigcup E_v$. Assuming that this is true, we can choose a vertex coloring $f : V_G \to \mathbf{Z}/m\mathbf{Z}$ with the following property: for every vertex $v \in V_G$, there exists an adjacent vertex $v^+ \in V_G$ with $f(v^+) = f(v) + 1$. Let v_0 be an arbitrary vertex of G. Then we can choose a vertex v_1 adjacent to G, such that $f(v_1) = f(v_0) + 1$. Similarly, we can choose a vertex v_2 adjacent to v_1, such that $f(v_2) = f(v_1) + 1 = f(v_0) + 2$. Continuing in this manner, we obtain a sequence of vertices

$$v_0, v_1, v_2, \ldots \in V_G.$$

Since V_G is finite, we must have $v_i = v_j$ for some $i < j$. Choose i and j as small as possible, so that the sequence of vertices $v_i, v_{i+1}, \ldots, v_j$ contains no repetitions (apart from the fact that $v_i = v_j$). Then

$$f(v_i) = f(v_j) = f(v_i) + (j - i)$$

in $\mathbf{Z}/m\mathbf{Z}$. It follows that $j - i$ is divisible by m, so that the vertices $v_i, v_{i+1}, \ldots, v_j$ form a cycle of length at least m (whose length is divisible by m).

It remains to prove that $\bigcup E_v \neq \Omega$: that is, that the probability $P(\bigcup E_v)$ is less than 1. Let's first estimate the probability of an event E_v. There are exactly d vertices w of G that are adjacent to v. For each of these vertices w, we have $f(w) \neq f(v)+1$ with probability $\frac{m-1}{m}$. Consequently we have $P(E_v) = (1 - \frac{1}{m})^d$.

We now note that E_v is independent of a set of events $\{E_w\}_{w \in S}$ provided that that the distance from v to S is greater than 2: that is, $v \notin S$, v is not adjacent to any vertex in S, and no vertex adjacent to v is adjacent to a vertex of S. Let us form a new graph G', whose vertices are the vertices of G, where two vertices v and w are adjacent in G' if they are either adjacent in G or have a common neighbor in G. If we fix $v \in G$, there are exactly d vertices of G which are adjacent to v, and each of these is adjacent to exactly $d - 1$ other vertices. It follows that the degree of v in G' is $\leq d^2$. Applying the Lovász local lemma (in its symmetric incarnation), we see that $P(\bigcup E_v) < 1$ provided that

$$P(E_v) < \frac{1}{e(1 + d^2)}$$

for each vertex $v \in V$. That is, we need

$$(1 - \frac{1}{m})^d \leq \frac{1}{e(d^2 + 1)}.$$

Taking logarithms and multiplying by -1, we need

$$d \log(\frac{1}{1 - \frac{1}{m}}) \geq 1 + \log(d^2 + 1)$$

Since $\log(\frac{1}{1-\frac{1}{m}}) = \frac{1}{m} + \frac{1}{2m^2} + \frac{1}{3m^3} + \cdots > \frac{1}{m}$, it will suffice to have $\frac{d}{m} \geq 1 + \log(d^2 + 1)$, which is equivalent to the inequality $m < \frac{d}{1+\log(d^2+1)}$. □