REU 2006 · Discrete Math · Lecture 8

Instructor: László Babai
Scribe: Megan Guichard
Editors: Sourav Chakraborty

July 12, 2006. Last updated July 13, 2006 at 1:00pm.
NOT PROOF-READ

8.1 Problem 1

One problem which was assigned a few days ago was

Problem 1. Let G be a graph with m edges. Show that one can remove $\leq \frac{m}{2}$ edges in such a way that what remains is bipartite (2-colorable).

A student gave a proof to the above problem using induction on the number of vertices. But we will give a proof that is using probabilistic methods.

Proof. Take G, and randomly color each vertex either red or blue. Then call an edge "bad" if its endpoints are the same color; the probability that a given edge will be bad is $\frac{1}{2}$.

Let the random variable X be the number of bad edges. Then the expected value $E(X)$ of X is $\frac{m}{2}$. (Reason: let X_i be the probability that edge i is bad; each X_i is an indicator variable which takes value 0 or 1 with equal probability. So $E(X) = \sum E(X_i) = \sum \frac{1}{2} = \frac{m}{2}$.)

Therefore, there exists an outcome (i.e., a coloring of the vertices) where the number of bad edges is $\leq \frac{m}{2}$. □

8.2 Problem 2 : Embarrassing tournaments

Another assigned exercise concerned "embarrassing" tournaments. Recall the definition of a tournament.

Definition 1. A tournament is an oriented complete graph, that is between any pair of vertices there exists exactly one directed edge. So it has $\binom{n}{2}$ edges. Hence on n vertices there are $2^{\binom{n}{2}}$ tournaments. If there is an edge from vertex i to vertex j we say that vertex i beats vertex j.

Definition 2. A tournament $G = (V, E)$ is called k-embarrassing if for all set $A \subset V$ of size k ($|A| = k$) there exists one vertex $v \in V$ such that v beats all the vertices in A.

Problem 2. Show that there exists a "2-embarrassing" tournament, one in which, for every pair of vertices, there exists a third vertex that beats both of them. More generally, show that for every k there exists a k-embarrassing tournament, where for every set of k vertices there exists a $k + 1^{\text{rm}}$ vertex that beats all of them.

The students gave two different kind of constructions of a graph on 7 vertices that is 2-embarrassing.

Proof 1. Figure 1 is a tournament that has 7 vertices and is 2-embarrassing.

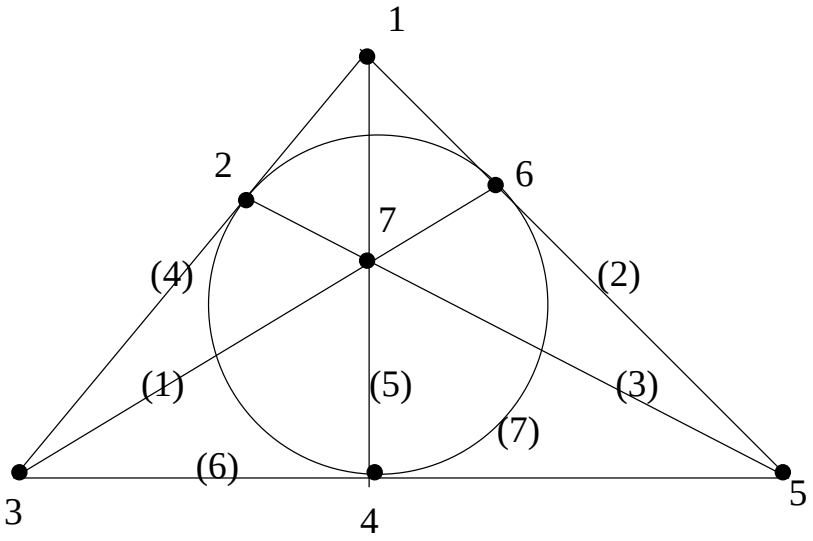

Figure 1: The vertices are labelled 1 to 7. The edges are labelled (1) to (7). A label (i) on an edge means that vertex i beats all the vertices on the edge.

This is a finite projective plane (Fano plane). It has the property that, through every two points, there is a unique line; and given any two lines, there is a unique point of intersection. (There are 7 lines in all, each having 3 points; each point is in 3 lines.) Once we check that the labelling is consistent, it is clear that the corresponding tournament has the desired property, because for any two points, there is a line connecting them, and the vertex named on that line betas both points. □

Exercise 3. Call a permutation on 7 elements a **collineation** if it preserves the lines in the Fano plane. Show that the number of collineations of the Fano plane is 168. This is in fact a group; it is the second smallest simple group (A_5 is the smallest).

Proof 2. We directly construct a 2-embarrassing tournament with 7 vertices. Label the

verices with the elements of the cyclic group of order 7. We want every two verices to be beaten by a third. In particular, given x and y, then one of $x - y$ and $y - x$ will be in $\{1, 2, 3\}$. Draw directed edges by saying that 0 beats 1, 2, and 4, and then cyclically rotate (so in general, x beats $x + 1$, $x + 2$, and $x + 4$). (See Figure 1). So, given x and $x + 1$, both are beaten by $x - 1$; x and $x + 2$ are beaten by $x - 2$; and x and $x + 3$ are beaten by $x - 1$.

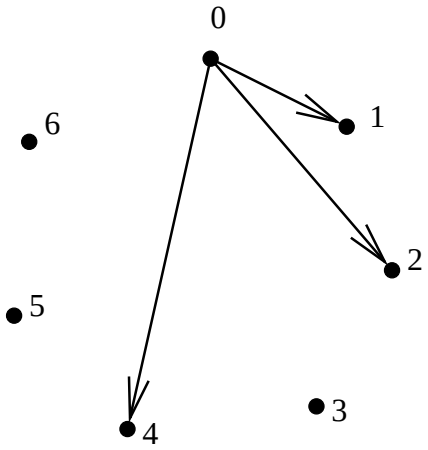

Figure 2: The vertices are labelled 0 to 6. The arrows indicate the vertices that vertex 0 beats

□

It will be interesting to see whether it is possible to extend the above proof to, say, 3-embarrassing tournaments.

8.3 Existential Proof of Problem 2

We will give a non-explicit proof that k-embarrassing tournaments exist.

Theorem 4 (Erdös). For every k, there exists a k-embarrassing tournament.

Proof. Let $P_n(k)$ be the probability that a random tournament with n vertices is k-embarrassing.

Claim 5. $\lim_{n\to\infty} P_n(k) = 1$.

Proof of Claim. Pick a random tournament on n vertices, by randomly orienting the edges on the graph. Let A be a subset with k vertices, and let $x \notin A$. Since the edges are oriented randomly so the probability that x beats everyone in A is $\frac{1}{2^k}$, and hence the probability that x does not beat everyone in A is $1 - \frac{1}{2^k}$.

Now let y be another vertex not in A. Then the probability that neither x nor y beats everyone in A is $(1-\frac{1}{2^k})^2$, because the events are independent. Similarly, the probability that no vertex outside A beats everyone in A is $(1-\frac{1}{2^k})^{n-k}$.

Now consider the probability that there exists a set A (of size k) which was not beaten by anyone. Call this $Q_n(k)$; it is equal to $1-P_n(k)$.

We can give an upper bound on $Q_n(k)$ using the **union bound**.

[Union bound says that if $X_1, \ldots, X_d$ are events then $\Pr(X_1 \cup \cdots \cup X_d) \leq \sum_{i=1}^{d} \Pr(X_i)$, regardless of independence.]

In our case, this means that

$$\Pr(\exists A \text{ which was not beaten by anyone}) < \binom{n}{k}\left(1-\frac{1}{2^k}\right)^{n-k}$$

But $\binom{n}{k}$ is a polynomial of degree k, and $\left(1-\frac{1}{2^k}\right)^{n-k}$ decays exponentially. So, as $n \to \infty$, this product goes to 0. That is $Q_n(k) \to 0$ and hence $P_n(k) \to 1$. □

Thus from the claim we have that as $n \to \infty$ a random tournament on n vertices is highly likely to be k-embarrassing. If for some n the probability that a random tournament is k-embarrassing is nonzero then there must be a k-embarrassing tournament for that n. □

Exercise 6. Show that $\forall c, 0 < c < 1, \forall k, \lim_{n\to\infty} n^k c^n = 0$.

But can we get an estimate on the n such that there is a k-embarrassing tournament on n vertices. In particular, we have shown

Lemma 7. If $\binom{n}{k}\left(1-\frac{1}{2^k}\right)^{n-k} < 1$, then there exists a k-embarrassing tournament with n vertices.

So we need so estimate the n for which the above inequality holds.

With some approximations, we see that $\binom{n}{k} < \frac{n^k}{k!}$, and $\left(1-\frac{1}{2^k}\right)^{-k} < 3$. Also, you can show that $1+x < e^x$ for all x, so

$$\left(1-\frac{1}{2^k}\right)^{n} < e^{-n/2^k}.$$

We would like to find the smallest n such that

$$\binom{n}{k}\left(1-\frac{1}{2^k}\right)^{n-k} < n^k\left(1-\frac{1}{2^k}\right)^{n} < n^k e^{-n/2^k} \leq 1$$

So

$$\begin{aligned} n^k &\leq e^{n/2^k} \\ k \ln n &\leq \frac{n}{2^k} \\ \frac{n}{\ln n} &\geq k \cdot 2^k \end{aligned}$$

Now if $\frac{n}{\ln n} = k \cdot 2^k$ then by taking log on both sides we see that asymptotically $\ln n = k \ln 2$. Now plugging it in the above inequality we get that the smallest n satisfying the inequality is

$$n \gtrsim k^2 2^k \cdot c$$

for some constant c.

Exercise* 8. Show that $n < 2^k$ is not enough.

8.4 Explicit construction of a k-embarrassing tournament

We will give a 2nd solution to Problem 2 by explicitly constructing one k-embarrassing tournament. The construction is due to Graham and Spencer.

Let p be a prime such that $p \equiv -1 \pmod 4$. Construct a tournament by saying i beats j if $i - j$ is a quadratic residue mod p. (Remember a is a quadratic residue mod p if p is not a divisor of a, and there exists x such that $x^2 \equiv a \pmod p$.)

We know that the number of quadratic residues mod p is $\frac{p-1}{2}$.

Define the **Legendre symbol**:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ 0 & \text{if } p|a \\ -1 & \text{otherwise} \end{cases}$$

For this to be a tournament, we need to check that there is only one edge connecting each pair of points; that is, we need

$$\left(\frac{i-j}{p}\right) = -\left(\frac{j-i}{p}\right).$$

Since $(j - i) = -1(i - j)$, it is sufficient to show that

$$\left(\frac{j-i}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{i-j}{p}\right).$$

Exercise 9. Prove these facts.

Question. When is -1 a quadratic residue?

The tournament constructed above is called a Paley tournament.

Theorem 10. For all k, there exists p_0 such that $p > p_0$ implies that the tournament constructed above is k-embarrassing.

The proof of this requires a theorem of André Weil, which we will not prove.

Theorem 11 (André Weil). Let f be a polynomial of degree d over $\mathbb{F}_p$, the field with p elements. Assume that $f \neq c \cdot g^2$, for all constants c and polynomials g. Then

$$\left| \sum_{j=0}^{p-1} \left(\frac{f(j)}{p} \right) \right| \leq (d-1)\sqrt{p}.$$

This theorem is known as Weil's character sum estimate.

Proof of Theorem 8.4. Fix a prime p, and define

$$\chi(a) = \left(\frac{a}{p} \right).$$

(χ is for "character.")

Consider the Paley tournament. Let A be a subset of k vertices, and let $b \notin A$. Then b beats A if

$$\chi(b - a_1) = \chi(b - a_2) = \cdots = \chi(b - a_k) = 1.$$

We expect this to happen $\approx \frac{p}{2^k}$ times. We will now prove that it is always close to this.

Let N be the number of times that this happens. Consider $(\chi(x - a_i) + 1)$. It is 0 if a_i beats x. So

$$\frac{1}{2^k} \prod_{i=1}^{k} (\chi(x - a_i) + 1)$$

will be 0 if at least one a_i beats x, and 1 if not. So then we have

$$\sum_{x \in \mathbb{F}_p} \frac{1}{2^k} \prod_{i=1}^{k} (\chi(x - a_i) + 1) \approx N$$

where the $\approx$ means here that the error is less than k.

We have

$$\begin{aligned} 2^k N &\approx \sum_{x \in \mathbb{F}_p} \prod_{i=1}^{k} (\chi(x - a_i) + 1) \\ &= \sum_{x \in \mathbb{F}_p} \sum_{I \subseteq \{1,\ldots,k\}} \prod_{i \in I} \chi(x - a_i) \\ &= \sum_{x \in \mathbb{F}_p} \sum_{I \subseteq \{1,\ldots,k\}} \chi(f_I(x)) \\ &= p + R \end{aligned}$$

for some remainder R. Here we define $f_I(x) = \prod_{i \in I} (x - a_i)$; recall that χ is multiplicative. On Friday, we will figure out what R is. The p comes from the case when $I = \emptyset$. $\square$