Discrete Math, Second Series, 11th Problem Set (August 11)

REU 2003

Instructor: László Babai
Scribes: Mridul Mehta and Tom Hayes

1 Multiply transitive groups

We use $\Omega^{(t)}$ to denote the set of ordered t-tuples of distinct elements of Ω. So if $|\Omega| = n$ then $|\Omega^{(t)}| = n(n-1) \cdot \dots \cdot (n-t+1)$.

Definition 1.1. A permutation group $G \leq \mathrm{Sym}(\Omega)$ is *t-transitive* if G acts transitively on $\Omega^{(t)}$. A 2-transitive group is also called *doubly transitive*; a 3-transitive group is *triply transitive*, etc.

Exercise 1.2. If G is t-transitive then $n(n-1) \cdot \dots \cdot (n-t+1) \mid |G|$.

Definition 1.3. The *degree of transitivity* of G is the largest t such that G is t-transitive.

Exercise 1.4. The degree of transitivity of S_n is n; the degree of transitivity of A_n is $n-2$.

Exercise 1.5. For $n \geq 4$, the degree of transitivity of D_n is 1.

Exercise 1.6. If $\mathrm{Aut}\, X$ is doubly transitive then $X = K_n$ or $\overline{K_n}$.

Definition 1.7. $\mathrm{AGL}(n,q)$ is the *affine general linear group*. This group acts on $\mathbb{F}_q^n$ by any composition of linear transformations and translations (exercise: one of each suffice). q is the order of the field, n is the dimension.

Exercise 1.8. $\mathrm{AGL}(n,q)$ acts doubly transitively on $\mathbb{F}_q^n$.

Exercise 1.9. If 3 points in $\mathbb{F}_q^n$ are not collinear then they are equivalent under AGL to every other such triple.

Exercise 1.10. $\mathrm{AGL}(n,2)$ is triply transitive. So is $\mathrm{AGL}(1,3)$. All others AGL's have degree of transitivity 2.

Exercise 1.11. For $n > 2$, $\mathrm{AGL}(n,2)$ is not 4-transitive.

Exercise 1.12. If G is t-transitive then G_x (stabilizer of a point) is $(t-1)$-transitive.

The following remarkable permutation groups were found by Mathieu around 1870. They are called "Mathieu groups;" they are defined as permutation groups of degree indicated in the subscript:

1. M_{24} is 5-transitive
2. M_{23} is 4-transitive
3. M_{12} is 5-transitive
4. M_{11} is 4-transitive

Theorem 1.13. *If $G \neq A_n, S_n$, then the degree of transitivity of G is ≤ 5; in fact the degree of transitivity is ≤ 3 unless $G = M_i$ for $i \in \{11, 12, 23, 24\}$.*

This is a consequence of the ENORMOUS Theorem.

ENORMOUS Theorem: Classification of finite simple groups. ($\approx$ 1980 or $\approx$ 1995). Proof is 15,000 pages long (human generated), by about 100 authors. There is a "revisionist project" to compress this proof to a more readable 5000 pages ...

This theorem has a large number of important, simply stated consequences. One of them:

Corollary 1.14. *Every finite simple group is generated by two elements.*

An earlier theorem is this:

Theorem 1.15 (Odd Order Theorem, Feit-Thompson, 1963). *Every (nonabelian) finite simple group has even order. Equivalently, every finite group of odd order is solvable.*

Exercise 1.16. Prove that these two statements are equivalent.

Remark 1.17. The Feit-Thompson theorem was originally 270 pages, and contributed to Thompson (a former University of Chicago graduate student) earning the Fields medal.

History: Burnside, circa 1900. Structure of doubly-transitive permutation groups via simple groups.

Combined with the Classification of Finite Simple Groups, Curtis, Kantor and Seitz obtained, in a 57-page paper, a **classification of doubly-transitive permutation groups** (except those with an abelian normal subgroup (called the "affine case")) (1976).

Theorem 1.13 (there are no 6-transitive permutation groups other than S_n and A_n) is a corollary to their work. Here is another consequence.

Corollary 1.18 (Schreier's Hypothesis). *If G is simple then $\mathrm{Out}(G)$ is solvable.*

Jordan proved (circa 1890) that $t < c \log^2 n / \log\log n$, where t is the degree of transitivity of any permutation group of degree n other than S_n and A_n.

Lemma 1.19. *$G \le S_n$, $p_1, \ldots, p_k$ distinct prime divisors of $|G|$, and $p_1 \cdots p_\ell \ge n^k$. Then*

$$(\exists \pi \in G)(2 \le \deg(\pi) \le n/k)$$

Claim 1.20. $(\exists \sigma \in G, \exists i \le \ell)(\#\{x \in \Omega \colon p_i \mid \textit{period of } x \textit{ under } \sigma\} \in [2, n/k])$

Proof of Lemma from Claim. Raise σ to power m which is the maximal divisor of $n!$ relatively prime to p_i. So all cycles in σ^m have length a power of p_i and $\sigma^m \ne 1$.

Proof of Claim. Set $Q(x) = \{p_i \colon p_i \mid \text{ period of } x\}$. Then

$$(\forall x)\left(\prod_{p_i \in Q(x)} p_i \le n\right)$$

But

$$\prod_{i=1}^{\ell} p_i \ge n^k.$$

Taking logarithms,

$$(\forall x)\left(\sum_{p_i \in Q(x)} \log p_i \le \log n\right)$$

But

$$\sum_{i=1}^{\ell} \log p_i \ge k \log n.$$

What we want to know is: does there exist i such that

$$f(i) := \sum_{x : p_i \in Q(x)} 1 \le n/k?$$

$$\begin{aligned}
\sum_{i=1}^{\ell} \log p_i f(i) &= \sum_{i=1}^{\ell} \log p_i \sum_{x : p_i \in Q(x)} 1 \\
&= \sum_{x} \sum_{i : p_i \in Q(x)} \log p_i \\
&\le n \log n.
\end{aligned}$$

The weighted average of $f(i)$ is thus

$$\frac{\sum_{i=1}^{\ell} \log p_i f(i)}{\sum_{i=1}^{\ell} \log p_i} \le \frac{n \log n}{k \log n} = \frac{n}{k}.$$

Thus in particular, there exists i such that $f(i) \le n/k$. □

Lemma 1.21. *Suppose G is t-transitive, where $t = p_1 + \cdots + p_\ell$. (Pretend we don't know the Enormous Theorem). Then there exists $\pi \in G$ such that π has cycles of length each p_i.*

Proof: Since G is t-transitive, we can require that π acts on the t elements by inducing orbits of lengths $p_1, \ldots, p_\ell$. □

Let x be such that $\sum_{p<x} p \approx n^4$, so that $x \approx 4 \ln n$. Let $t = \sum_{p<4 \ln n} p \approx c \ln^2 n / \ln \ln n$ (exercise!). $\prod_{p<x} p \approx \mathrm{e}^{x(1+o(1))}$.

(This ends a significant portion of the proof of Jordan's bound on the degree of transitivity. For the rest, see the B-Seress article handed out.)

2 Estimating Diameters of Cayley Graphs of S_n or A_n

Let $G = S_n$ or $G = A_n$. Let T be a generating set. Question: What is the distance (from the identity element, in the Cayley graph $\Gamma(G,T)$) of the element π from Lemma 1.21? I. e., what is the word length of π over T?

Build the directed graph of the effects of T on $\Omega^{(t)}$. Specifically, for every $\vec{x} \in \Omega^{(t)}$, for every $\sigma \in T$, put an edge from $\vec{x}$ to $\vec{x}^\sigma$.

Exercise 2.1. Since G acts t-transitively, this graph is strongly connected.

This implies a bound on the word length of $|\Omega^{(t)}| = n(n-1)\cdots(n-t+1) < n^t$.

This ends a significant portion of the proof that the diameter of all Cayley graphs of S_n and A_n is $< \mathrm{e}^{\sqrt{n \log n}(1+o(1))}$.

3 Possible Pathologies in Neighborhood Sequence of a Vertex-Transitive Graph X

$S_i(x) = \{y \mid \mathrm{dist}(x,y) = i\}$. Let $s_i = |S_i(x)|$. $s_0 = 1$, $s_1 =$ degree. s_i.

Claim: $s_4 \ge c s_3$, where $c = 2/13$, if $\mathrm{diam}(X) \ge 7$.

The increase s_{i+1}/s_i can be at most the degree minus 1. But how much can the value go down from one level to the next?

3.1 EXPANSION of vertex-transitive graphs

Let $S \subseteq V(X)$, and let $\partial S = \{x \in V \setminus S \mid (\exists y \in S)(x \sim y)\}$. The *isoperimetric ratio* is $\frac{|\partial S|}{|S|}$. In a continuous setting, this would be a ratio of surface area to volume.

For a network to be reliable, it should not be possible to disconnect a large part of the network by breaking a small number of edges. In other words, a large isoperimetric ratio is desirable for all subsets.

Theorem 3.1 (Global expansion, Aldous). *Let X be a finite connected vertex-transitive graph (undirected). If $|S| \leq |V|/2$ then*

$$\frac{|\partial S|}{|S|} \geq \frac{2}{2d+1},$$

where d is the diameter of X.

Proof: In B-Seress article (Corollary 2.3). □

Theorem 3.2 (local expansion). *Let X be a finite connected vertex-transitive graph (undirected). If $S \subseteq V$ and* $\operatorname{diam}(S) < \operatorname{diam}(V)$. *Then*

$$\frac{|\partial S|}{|S|} \geq \frac{2}{\operatorname{diam}(S)+2}.$$

Proof: This is Theorem 3.2 in the B-Seress article. □

Here is another version which does not assume the diameter of S is less than that of V:

Theorem 3.3 (local expansion). *Let X be a finite connected vertex-transitive graph (undirected), If $S \subseteq V$, and $|S| \leq |V|/2$, then*

$$\frac{|\partial S|}{|S|} \geq \frac{2}{2\operatorname{diam}(S)+1}.$$

Now we apply these results to neighborhood sequences. By definition, $s_3 = |\partial B(2,x)|$, where $B(2,x)$ is the *ball of radius* 2 around x. Now $|B(2,x)| = s_0 + s_1 + s_2$. So by the last result,

$$\frac{s_3}{s_0+s_1+s_2} \geq \frac{2}{9},$$

and more generally,

$$\frac{s_i}{s_0+\cdots+s_{i-1}} \geq \frac{2}{4i-3},$$

assuming either that $s_0 + s_1 + s_2 \leq n/2$ or $\operatorname{diam}(X) \geq 2i-1$.

Theorem 3.4. *Let G be an infinite, locally finite connected vertex-transitive graph. Then*

$$\frac{|\partial S|}{|S|} \geq \frac{1}{\operatorname{diam}(S)+1}.$$

Proof: Let $d = \operatorname{diam}(S)$. Let N denote the number of shortest paths of length $d+1$ passing through a given vertex. Count those among all such possible paths which intersect S. There are at least $|S|N/(d+2)$ of these. All of these intersect ∂S. But at most $|\partial S|N$ paths intersect the boundary. Hence

$$|\partial S|N \geq \frac{|S|N}{d+2}$$

and so $|\partial S|/|S| \geq 1/(d+2)$. □

Exercise 3.5. Improve the above proof to actually prove the theorem as stated (replace $d+2$ with $d+1$).

Wesley Pegden clarified that the neighborhood sequence of a locally infinite vertex-transitive graph cannot show any pathology: If X is a locally infinite, connected, vertex transitive graph, then $s_0 = 1, s_1 = \infty, \infty, \ldots$, possibly $s_{\text{diam}} = \textit{finite}$.

A further question: Are all the infinite cardinalities equal, except possibly for the last one? (Answer: yes – Wesley.)

Open question: what about directed vertex-transitive graphs with infinite out-degree?

Exercise 3.6. For all $d \geq 2$, construct an infinite vertex transitive, locally infinite graph of diam $= d$, such that $s_d =$ finite. (Probably possible)

4 Diameter of S_n

Recall the following result:

Lemma 4.1. *For $A, B \subseteq \Omega$, $|\Omega| = n$, and $G \leq \operatorname{Sym}(\Omega)$ transitive, then*

$$\mathrm{E}\left(|A \cap B^\sigma|\right) = \frac{|A||B|}{n}.$$

In other words, if $\mu(A) := |A|/n$, is the *normalized size*, then $\mathrm{E}\left(\mu(A \cap B^\sigma)\right) = \mu(A)\mu(B)$.

Proof: For each $x \in \Sigma$, define the indicator variables

$$\vartheta_x = \begin{cases} 1 & \text{if } x \in B^\sigma \\ 0 & \text{otherwise} \end{cases}$$

Then

$$|A \cap B^\sigma| = \sum_{x \in A} \vartheta_x.$$

By the linearity of expectation,

$$\mathrm{E}\left(|A \cap B^\sigma|\right) = \sum_{x \in A} \mathrm{E}(\vartheta_x) = \sum_{x \in A} \frac{|B|}{n} = \frac{|A||B|}{n}.$$

□

Recall that $\deg[\sigma, \tau] \leq 3|\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau)|$ (review!).

Claim 4.2. *For every $\epsilon > 0$, there exists c such that the following holds. If $G \leq S_n$, transitive, $G = \langle T \rangle$, $\sigma \in G$, $A := \operatorname{supp}(\sigma)$. Then $\exists \tau \in G$ such that $\operatorname{dist}_T(\tau) \leq n^c$ such that $|A \cap A^\tau| \leq \frac{|A|^2(1+\epsilon)}{n}$.*

Definition 4.3. Let ξ be the position of a particle in Ω, i. e., a random variable whose value is an element of Ω. We say ξ has an ϵ-nearly uniform distribution if

$$(\forall x \in \Omega)\Pr(\xi = x) = \frac{1 \pm \epsilon}{n}.$$

(We will use the shorthand $a = (1 \pm \epsilon)b$ in place of the more cumbersome $a \in [(1-\epsilon)b, (1+\epsilon)b]$.)

Definition 4.4 ("Lazy random walk"). Let $G = \langle T \rangle$, where $T = T^{-1}$ and $1 \in T$. Let $\xi_0 \in G$ be the starting point (arbitrary). Define $\xi_{t+1} = \xi_t^\sigma$, where $\sigma \in T$ is chosen uniformly at random.

Theorem 4.5. *Let $G = \langle T \rangle$, G transitive on Ω, $|\Omega| = n$. Let ξ_t be distributed according to a lazy random walk defined above. Then after $t \leq n^c$ steps, ξ_t is ϵ-nearly uniform.*

¿From this it follows that a random $\sigma \in G$ can be replaced with a short word in the generators in Lemma 4.1:

Corollary 4.6. *Let $G = \langle T \rangle$, G transitive on Ω, $|\Omega| = n$. Let σ be a lazy random word of length $t = n^c$ over T where c is as in the preceding theorem. Let $A, B \subset \Omega$. Then*

$$\mathrm{E}\left(|A \cap B^\sigma|\right) = \frac{|A||B|}{n}(1 \pm \epsilon).$$

Exercise 4.7. Prove this result by adapting the proof of Lemma 4.1.