REU 2006 · Discrete Math · Lecture 3

Instructor: László Babai
Scribe: Elizabeth Beazley
Editors: Eliana Zoque and Elizabeth Beazley
NOT PROOFREAD - CONTAINS ERRORS

June 26, 2006. Last updated June 27, 2006 at 12:41 p.m.

Check the website regarding the location for subsequent classes. The notes from last week are posted on Laci's website. Please email him comments, questions, or corrections regarding these notes.

3.1 Permutations and Permutation Groups

Definition 3.1.1. A **permutation** is a map $f : A \to A$ that is one-to-one and onto; *i.e.*, a bijection of the set A. We call A the *permutation domain*.

Definition 3.1.2. All permutations of A form the **Symmetric Group**, denoted $\mathrm{Sym}(A)$.

Denote the action of the permutation f on an element a by $a \mapsto a^f$. We can compose permutations $A \xrightarrow{f} A \xrightarrow{g} A$ by $a \mapsto a^f \mapsto (a^f)^g =: a^{fg}$. Similarly, $f^n := f \cdots f$ denotes f composed with itself n times. The identity permutation on the set A, denoted id_A, leaves every element fixed. The inverse of a permutation $a^{f^{-1}} = b$ is such that $b^f = a$. Note that since f is a bijection, then the inverse is well-defined.

Definition 3.1.3. The **degree of Sym(A)** is the order of the set A, denoted $|A|$.

Definition 3.1.4. Denote by $S_n = \mathrm{Sym}([n])$, the symmetric group of degree n, where $[n] = \{1, 2, \ldots, n\}$.

Definition 3.1.5. Let $\pi \in \mathrm{Sym}(A)$. We define the **support** of π to be $\mathrm{supp}(\pi) := \{a \in A : a^\pi \neq a\}$.

Example 3.1.6. Note that $\mathrm{supp}(\mathrm{id}) = \varnothing$. As another example, note that $|\mathrm{supp}((12)(34))| = 4$.

Definition 3.1.7. In general, we can define the **degree of a permutation** to be $\deg(\pi) := |\mathrm{supp}(\pi)|$.

Definition 3.1.8. A **k-cycle** is a permutation of degree k consisting of a single cycle; *e.g.*, $\pi = (a_1\ a_2\ \cdots\ a_k)$ and $|\text{supp}(\pi)| = k$. As a special case, the 2-cycles are called **transpositions**.

Here we use cycle notation $(a_1\ a_2\ \cdots\ a_k)$ to denote the function that maps $a_i \mapsto a_{i+1}$ and sends $a_k \mapsto a_1$. Note that the cycle notation is not unique, since $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$, for example.

Definition 3.1.9. The number of elements in the group is called the **order** of the group.

Example 3.1.10. The order of the symmetric group S_n is $n!$.

Permutations have parity, either even or odd.

Definition 3.1.11. We say that a permutation π is **even** if it can be expressed as a product of an even number of transpositions. Similarly, π is **odd** if it can be expressed as the product of an odd number of transpositions.

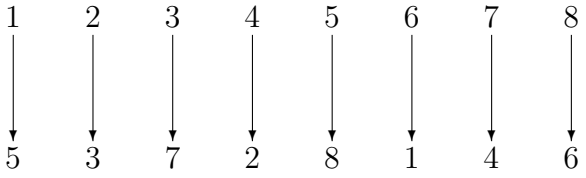
Definition 3.1.12. The **sign** of a permutation is defined as follows:

$$\text{sign}(\pi) = \begin{cases} 1, & \text{if } \pi \text{ is even} \\ -1, & \text{if } \pi \text{ is odd} \end{cases} \tag{3.1.1}$$

Definition 3.1.13. $m_n := \max_{\pi \in S_n} \{\min\{k : \exists \text{ transpositions } \tau_1, \dots \tau_k \text{ s.t. } \tau_1 \cdots \tau_k = \pi\}\}$.

Question 3.1.14. How many transpositions will we need in this product? What is an upper bound?

Let us consider the following permutation, in which we define the function using a diagram with arrows.



Let us begin by choosing $\tau_1 = (1\ 5)$. We can then consider where 5 is mapped, and write $\tau_2 = (5\ 8)$. Continuing in this manner, we use $n-1$ transpositions. An inductive argument would show in general that $m_n \leq n-1$. Can we improve on this bound?

We can provide an example of a permutation that requires less than $n-1$ transpositions. For example, the permutation that reverses the order of all of the elements in the set $[n]$ uses at most $\frac{n}{2}$ transpositions.

Exercise 3.1.15. If π is the n-cycle $(1\ 2\ \cdots\ n)$, then $k \geq n-1$, where k is such that $\exists$ transpositions $\tau_1, \dots \tau_k$ s.t. $\tau_1 \cdots \tau_k = \pi$.

3.2 Generators

Definition 3.2.1. We say that $\pi_1, \dots \pi_k$ **generate** S_n if $(\forall \sigma \in S_n)(\exists \rho_1, \dots \rho_l$ s.t. $\sigma = \rho_1 \cdots \rho_l$ and $(\forall j)(\exists i)(\rho_j = \pi_i$ or $\pi_i^{-1}))$.

We have proved that the $\binom{n}{2}$ transpositions generate S_n.

Claim 3.2.2. *The $n-1$ neighboring transpositions $(1\ 2), (2\ 3), \dots, (n-1\ \ n)$ generate S_n.*

To prove this Claim, we first note that all transpositions will generate S_n. Thus, we need only prove the following:

Lemma 3.2.3. *All transpositions are generated by neighbor transpositions.*

Proof. If $1 \leq i < j \leq n$, then

$$(i\ \ j) = (i\ \ i+1)(i+1\ \ i+2)\cdots(j-1\ \ j)(j-2\ \ j-1)(j-3\ \ j-2)(i\ \ i+1). \quad (3.2.1)$$

We have used $2(j-i)-1$ neighbor transpositions to form this product. Note that this is an odd number of transpositions. On the k^{th} step, this is $\leq 2(n-k)$, and $\sum_{k=1}^{n}(n-k) = \frac{n(n+1)}{2}$. □

Theorem 3.2.4. *Not all permutations are even. Equivalently, the identity permutation is not odd.*

If we write a permutation as a product of transpositions, then we use $\leq n-1$ transpositions. This observation yields the following:

Corollary 3.2.5. Every permutation is the product of $\leq 2n^2$ neighbor transpositions.

Definition 3.2.6. Let a_n and b_n be sequences. We say that $a_n = o(b_n)$, read a_n is **little-oh** of b_n, if $\lim_{n\to\infty} \frac{a_n}{b_n} = 0$.

If for the purposes of the definition of little-oh, we allow $\frac{0}{0} = 0$, then it will help us with computations. In general, such a convention will lead to a contradiction. Similarly, we can think of $\frac{0}{0} = 1$ in the definition of $a_n \sim b_n$. This idea will ONLY apply to these two definitions!

Exercise 3.2.7. Can every permutation be generated by a product of $o(n^2)$ neighbor transpositions?

Exercise 3.2.8. Prove that fewer than $n-1$ transpositions do not generate S_n

Note that one permutation is definitely not enough to generate S_n. Every permutation π has an **order**, the smallest power k such that $\pi^k = \mathrm{id}_{S_n}$. Thus, a single permutation can only generate a maximum of k permutations, where k is the order of the permutation. This number cannot be $n!$, the order of S_n. Further, note that S_n is not a commutative, or **abelian**, group: $(1\ 2)(2\ 3) = (1\ 3\ 2)$, but $(2\ 3)(1\ 2) = (1\ 2\ 3)$, which are not the same cycles. However, all cyclic groups, or groups generated by a single element, are necessarily abelian. In fact, if $\sigma := (1\ 3\ 2)$, then $\sigma^{-1} = (1\ 2\ 3)$. In general, $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$. Thus, if $\tau^{-1} = \tau$, where $\tau = \tau_1\tau_2$, then $(\tau_1\tau_2)^{-1} = \tau_2\tau_1$.

Definition 3.2.9. Let $A_n := \{\text{even permutations}\}$. Then A_n is a subgroup of S_n. That is, A_n is closed under multiplication, inverses, and contains the identity. We call A_n the **Alternating group**.

Exercise 3.2.10. Show that $|A_n| = \frac{n!}{2}$, for $n \geq 2$.

Exercise 3.2.11. Let ρ, π be cycles such that $|\mathrm{supp}(\rho) \cap \mathrm{supp}(\pi)| = 1$. Then ρ and π generate either A_{k+l-1} or S_{k+l-1}.

Exercise 3.2.12. Take the cycle $(1\ 2\ \cdots\ n-1)$ of length $n-1$ and one transposition involving the n^{th} element. Then these two elements generate S_n.

Exercise 3.2.13. The n-cycle $(1\ 2\ \cdots\ n)$ and the transposition $(1\ 2)$ generate S_n.

Exercise 3.2.14. A k-cycle is even $\iff$ k is odd.

Question 3.2.15. What is the **diameter** of S_n with respect to an n-cycle plus a transposition?

Provide an answer within a constant factor. That is, provide an upper and lower bound that differ by a constant.

3.3 Asymptotics

Definition 3.3.1. Let a_n, b_n be sequences. Then we say that $a_n = O(b_n)$, read **big-oh** of b_n, if $(\exists c)(\forall$ sufficiently large $n, |a_n| \leq C|b_n|)$.

In asymptotic notation, the idea is that a finite number of changes will have no effect. If any asymptotic statement on the board does not make sense, it is likely that we forgot to write "for sufficiently large n". Please insert it whenever necessary.

Definition 3.3.2. $a_n = \Omega(b_n)$ if $(\exists c > 0)(\forall$ sufficiently large $n, |a_n| \geq c|b_n|)$. Equivalently, we see that $a_n = \Omega(b_n) \iff b_n = O(a_n)$.

Definition 3.3.3. We say $a_n = \Theta(b_n)$ if $a_n = O(b_n)$ and $a_n = \Omega(b_n)$. That is, $(\exists c, C > 0)(\forall$ sufficiently large $n, c|b_n| \leq |a_n| \leq C|b_n|)$.

Exercise 3.3.4. If $a_n = \Theta(b_n)$ and $a_n, b_n \to \infty$, then $\ln(a_n) \sim \ln(b_n)$.

Exercise 3.3.5. The converse of the previous exercise is false.

3.4 Permutations and Probability

Recall the definitions of the finite probability space (Ω, P) from last time. (Refer to handouts or Lecture 2 notes online.)

Definition 3.4.1. If $A \subset \Omega$ is an event then $P(A) = \sum_{a \in A} P(a)$

Definition 3.4.2. Given a random variable $X : \Omega \to \mathbb{R}$, then the **expected value** is given by $E(X) := \sum_{a \in \Omega} X(a)P(a) = \sum_{y \in \mathbb{R}} yP(X = y)$.

Recall the exercise from last time:

Theorem 3.4.3. $E(X + Y) = E(X) + E(Y)$.

As a special case, we of course see that $E(X + X) = E(X) + E(X)$.

Exercise 3.4.4. $E(cX) = cE(X)$

Suppose that we have a club with 2000 adult members. There are 2000 cards numbered 1 to 2000. Every member of the club randomly chooses a card. We say that a member of the club is **lucky** if he draws a card containing the year of his birth.

Question 3.4.5. What is $E(\#$ lucky numbers$)$?

The claim is that you do not have to know the age distribution of the club members to answer this question. You just have to define the proper random variables. In fact:

Exercise 3.4.6. $E(\#$ lucky numbers$) = 1$.

Exercise 3.4.7. Every permutation is a *unique* product of disjoint cycles, where we say that two permutations are **disjoint** if their supports are disjoint. Here, we mean unique up to the order of terms in a cycle.

What can we say about the number of cycles that we require for such an expression?

Definition 3.4.8. $C(\pi) := \#$ cycles of π, when π is written as a product of disjoint cycles.

Example 3.4.9. Note that $C(\text{id}) = n$. Similarly, $C(n\text{-cycle}) = 1$ and $C(k\text{-cycle}) = n-k+1$.

Pick π at random, uniformly over S_n.

Theorem 3.4.10. $E(C(\pi)) \sim ln(n)$.

Proof. The power of the additivity of E is that we can define an event as a sum of random variables that we can compute easily and then apply Theorem 3.4.3. How can we write $C(\pi) = X_1 + X_2 + \cdots$, where we can deal easily with each individual random variable X_i?

Let $X_i = \#$ i-cycles. We can further break this up by writing $X_i = \frac{1}{i}\sum_{j=1}^{n} Z_{ij}$, where $Z_{ij} = \#$ i-cycles through point j. What event does Z_{ij} indicate? Z_{ij} is the **indicator** variable of the event that the cycle through j has length i. Z_{ij} is 1 if this event occurs and 0 if it does not.

Note 3.4.11. $E(\text{indicator variable}) = P(\text{the event indicated})$.

Thus, $E(Z_{ij}) = P(\text{cycle through } j \text{ has length } i) = \frac{1}{n}$. In particular, this does not depend on the length of the cycle. Using this fact, we write

$$E(X_i) = \frac{1}{i}\sum_{j=1}^{n} E(Z_{ij}) = \frac{1}{i}, \tag{3.4.1}$$

from which we can conclude

$$E(C(\pi)) = \sum_{j=1}^{n} E(X_i) = \sum_{i=1}^{n} \frac{1}{i} \sim \ln(n). \tag{3.4.2}$$

□

Recall the definition of $\nu(n)$ from Lecture 1. We proved that $\nu(j) \sim \ln\ln(n)$, for $1 \leq j \leq n$. Now, pick a j at random from $\{1, \ldots, n\}$, and consider $E(\nu(j))$. Use the additivity of expectation to show the following:

Exercise 3.4.12. $E(\nu(j)) \approx \sum_{p \leq n} \frac{1}{p}$