CMSC 27400-1/37200-1 Combinatorics and Probability **Spring 2005**

Lecture 13: April 27, 2005

Instructor: László Babai *Scribe: Raghav Kulkarni*

TA SCHEDULE: TA sessions are held in Ryerson-255, Monday, Tuesday and Thursday 5:30–6:30pm.
INSTRUCTOR'S EMAIL: laci@cs.uchicago.edu
TA's EMAIL: hari@cs.uchicago.edu, raghav@cs.uchicago.edu
IMPORTANT: Take-home test Friday, April 29, due Monday, May 2, **before** class.

Permutations

Definition: A *permutation* of a set A is a bijection $f : A \to A$.
Examples of permutation: Let $A = [6]$.

Let $f = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{matrix}$

Let $g = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{matrix}$

Definition: A digraph G is a *permutation graph* if $(\forall v \in V(G))(\deg^+(v) = \deg^-(v) = 1)$. ($\deg^+(v)$ is the outdegree of v and $\deg^-(v)$ is the indegree of v.)
Note that there is a bijection between the set of permutations of A and the set of permutation graphs on vertex set A. So, every permutation can be uniquely represented as a permutation graph.
Definition: A *k-cycle* is a permutation whose permutation graph consists of a directed k-cycle and directed self loops on rest of the vertices.
Let $x^f := f(x)$.
Multiplication (composition) of permutations: The *product* fg of the permutations f and g is a permutation defined as: $x^{fg} := (x^f)^g$ (first apply f, then apply g).
With f and g as in the examples of permutation:

$fg = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 2 & 3 & 4 \end{matrix}$

Exercise 13.1 *Show that any permutation graph is a union of disjoint directed cycles.*

Thus we have *the cycle notation of a permutation:* every permutation can be represented by a disjoint union of cycles.
Examples: The above examples of permutation can be represented in cycle notation as

follows: $f = (1,4)(2,3,5)(6)$ and $g = (1,2,3)(4,5,6)$. $((2,3,5) = (3,5,2) = (5,2,3))$.
Definition: The *support* of a permutation f: $\text{supp}(f) := \{x \in A \mid x^f \neq x\}$.
Definition: The permutations f and g are *disjoint* if $\text{supp}(f) \cap \text{supp}(g) = \emptyset$.

Exercise 13.2 *If f, g are disjoint then $fg = gf$. (f, g* commute*.)*

Exercise 13.3 *Find permutations f and g such that $fg = gf$ but f, g are* not *disjoint and $f \neq g$.*

Exercise 13.4 *True or False? : f and g commute iff ($\exists$ a permutation h, integers a, b)($f = h^a, g = h^b$).*

Definition: The *identity* permutation on A is the identity map $id_A : x \mapsto x$.
Observation: $(\forall f)(id_A f = f id_A = f)$. $\text{supp}(id_A) = \emptyset$.
Definition: The *inverse* of a permutation f is a permutation g such that $fg = gf = id_A$. The inverse of f is denoted by f^{-1}. $\text{supp}(f^{-1}) = \text{supp}(f)$.
Definition: A permutation f is *fixed point free* if $\text{supp}(f) = A$, i.e., $(\forall x)(x^f \neq x)$.
The set of all permutations form a *group* called the *Symmetric Group* S_A. If $|A| = n$ then the group is called the *symmetric group of degree n* and it is denoted by S_n. $|S_n| = n!$.
Definition: Let $B \subseteq S_n$. The *subgroup generated by B*, $\langle B \rangle :=$ set of all possible products of elements of B (and their inverses).
Definition: The *order* of a permutation f is the smallest $k > 0$ such that $f^k = id$.

Theorem 13.5 (Prime Number Theorem (PNT)) *$\pi(x) \sim \frac{x}{\ln x}$ where $\pi(x) :=$ the number of primes $\leq x$.*

Exercise 13.6 *Show that $\prod_{p \leq x} p = \mathrm{e}^{x(1+o(1))}$, i.e., show that $\ln(\prod_{p \leq x} p) \sim x$. (Hint: PNT.)*

Exercise 13.7 *If p_n is the n^{th} prime number then PNT (Theorem 13.5) is equivalent to $p_n \sim n \log n$.*

Exercise 13.8 $\sum_{p \leq x} p \sim \frac{x^2}{2 \ln x}$.

Exercise 13.9 *Combine Exercise 13.7 and 13.8 to show that the largest order of a permutation is at least $\mathrm{e}^{\sqrt{n \ln n}(1-\epsilon)}$ for every $\epsilon > 0$. (Hint: Cycle decomposition $2+3+5+7+11+\ldots$.)*

Theorem 13.10 (Landau) *The largest order of a permutation is $< \mathrm{e}^{\sqrt{n \ln n}(1+\epsilon)}$ for every $\epsilon > 0$.*

Consider a *random* permutation f. Let $\ell_1 :=$ length of the *first cycle* of f (*first cycle* is the cycle containing 1.) The probability that the legth of the first cycle of f is 1 is: $P(\ell_1 = 1) = \frac{1}{n}$. $P(\ell_1 = n) = \frac{1}{n}$. (Why?)

Exercise 13.11 *Show that for every i, $P(\ell_1 = i) = \frac{1}{n}$.*
(Give an AH-HA proof and also a tedious (calculating numerator) proof.)

Definition: A *transposition* is a permutation which is a 2-cycle.

Exercise 13.12 *(a) How many transpositions are there in S_n ?*
(b) Prove the transpositions generate S_n.

Exercise 13.13 *Prove that the minimum number of transpositions needed to generate S_n is $n - 1$.*

Let $T = \{(1, 2), (1, 2, \ldots, n)\}$.

Exercise 13.14 *Prove that T generates S_n.*

Definition: The *diameter* of a group G with respect to a set S of generators is the maximum over $g \in G$ of the lenght of the shortest word representing g in terms of members of S and their inverses.

Exercise 13.15 *Prove that the diameter of S_n with respect to T is $\Theta(n^2)$.*

OPEN PROBLEM: Does there exist a set of generators of S_n with respect to which the diameter of S_n is greater than $O(n^2)$?
CONJECTURE: For any set of generators of S_n, the diameter is polynomially bounded ($O(n^k)$ for some constant k).