CMSC 36500 / MATH 37500 Algorithms in Finite Groups

Instructor: László Babai
Scribe: Robert Green

Spring 2017

3 Lecture 3 April 4, 2017 Problems due April 6

3.1 Homework review

DO 3.1. Let T be a set of transpositions in S_n. View T as the edges of an undirected graph with n vertices. Prove that T generates S_n if and only if this graph is connected.

Notation 3.2. For a set A, $\binom{A}{k} := \{T \subseteq A \mid |T| = k\}$ denotes the set of k-subsets of A.

Review 3.3. $S_n^{(k)} \le S_{\binom{n}{k}}$ (induced action of S_n on k-subsets) is primitive for $1 \le k < n/2$ and imprimitive for $k = n/2$

Proof. Let $|A|$ be an n-set ($|A| = n$). Let $\Omega = \binom{A}{k}$, so we are looking at the induced action of $\mathrm{Sym}(A)$ on Ω. First we note that this action is transitive – any k-subset can be sent to any k-subset.

For $k = n/2$, pair up each k-subset with its complement. This pairing is an invariant partition of $\binom{A}{k}$, so the action is imprimitive.

For $k < n/2$, we need to show that the stabilizer of an element $X \in \Omega$ is a maximal subgroup of $\mathrm{Sym}(A)$. Let $Y = A \setminus X$ be the complement of X in A. Then the (setwise) stabilizer of X is $H := \mathrm{Sym}(X) \times \mathrm{Sym}(Y)$. We need to show that for any permutation $\pi \in \mathrm{Sym}(A) \setminus H$ we have $\langle H, \pi \rangle = \mathrm{Sym}(A)$. Let $G = \langle H, \pi \rangle$. It suffices to show that G contains a transposition (x, y) such that $x \in X$, $y \in Y$. (Why is this sufficient?)

Since $\pi \notin H$, there exist $u, v \in Y$ such that $x := u^\pi \in X$ and $y := v^\pi \in Y$ (why? – here we use that $|Y| > |X|$). So $\tau^\pi = (x, y)$, as desired. □

DO 3.4. For $k = n/2$, the only nontrivial system of imprimitivity is the system consisting of pairs of the form $\{S, S^c\}$.

Example 3.5. Consider the field $\mathbb{F}_p$ (p prime) and the set $AGL(1, p)$ of affine linear transformations of $\mathbb{F}_p$; these are the transformations of the form $x \mapsto ax + b$ ($x \in \mathbb{F}_p$) where $b \in \mathbb{F}_p$ and $a \in \mathbb{F}_p^\times$. This group has a normal subgroup T consisting of the translations $x \mapsto x + b$.

DO 3.6. T has order p, $T \overset{\min}{\triangleleft} AGL(1, p)$, and $AGL(1, p)/T = \mathbb{F}^\times$

Theorem 3.7 (CFSG)**.** *(Tiny maximal subgroups in symmetric groups) For all primes $p \notin \{7, 11, 17, 23\}$,*

$$AGL(1, \mathbb{F}_p) \overset{\max}{<} S_p$$

The label [CFSG] indicates that this result is only known to be derivable from the classification of finite simple groups.
(Source: Martin Liebeck, Cheryl Praeger, Jan Saxl: "A classification of the maximal subgroups of the finite alternating and symmetric groups," Journal of Algebra 111 (1987) 365-383.)

Definition 3.8. We say that a group (action) is *doubly transitive* if it is transitive on the $n(n-1)$ ordered pairs of elements of its permutation domain.

DO 3.9. $AGL(1,p)$ is doubly transitive

Definition 3.10. $AGL(d,\mathbb{F})$ is the set of d-dimensional affine linear transformations over a field $\mathbb{F}$:

$$AGL(d,\mathbb{F}) := \{\mathbf{x} \mapsto A\mathbf{x} + \mathbf{b} \mid A \in GL(d,\mathbb{F}), \mathbf{b} \in \mathbb{F}^d\}$$

where $\mathbf{x}$ ranges over $\mathbf{x} \in \mathbb{F}_p^d$. T again will denote the normal subgroup of translations $\mathbf{x} \mapsto \mathbf{x} + \mathbf{b}$.

DO 3.11.
1. T is doubly transitive
2. $T \triangleleft AGL(d,\mathbb{F})$
3. $AGL(d,\mathbb{F})/T \cong GL(d,\mathbb{F})$

Definition 3.12. We say that a group (action) is *t-transitive* if it is transitive on the $n(n-1)\dots(n-t+1)$ ordered t-tuples of elements of its permutation domain. The largest such t is the *degree of transitivity* of the group action; we denote this quantity by deg-tr(G).

Example 3.13. The degree of transitivity for S_n is n, and for A_n is $n-2$.

Definition 3.14. A subgroup of S_n is a "giant" if it is S_n or A_n. (This is not an established terminology.)

Theorem 3.15. *If $G \le S_n$ is not a giant, then*
1. *(Bochert, 1896)* deg-tr$(G) = O(\log^2 n/\log\log n)$
2. *(Wielandt, 1934)* deg-tr$(G) \le 3\ln n$
3. *[CFSG]* deg-tr$(G) \le 5$

3.2 A few more problems in group theory

HW 3.16. If G has a proper subgroup of index k then it has a proper normal subgroup of index $\le k!$

DO 3.17. For $n \ge 5$, if $H < S_n$ and $H \ne A_n$, then $|S_n : H| \ge n$

DO 3.18. The above is not true for S_4

Definition 3.19. If $G \curvearrowright \Omega$, then the homomorphism $h : G \to \mathrm{Sym}(\Omega)$ is called a *permutation representation* of G. Such a representation is called faithful if the kernel is trivial.

DO 3.20. Example of a non-faithful representation: Find an epimorphism $f : S_4 \twoheadrightarrow S_3$ and its kernel.

HW 3.21. If $G \le S_n$ is a transitive abelian subgroup then $|G| = n$

DO 3.22. If we drop the transitivity assumption above then $|G| \le 2^{n/2}$ and this is tight for n even. For n odd, find the tight bound.

DO 3.23.
1. Find the Sylow p-subgroups of S_n.
2. For $P \in \mathrm{Syl}_p(S_n)$ show that P is transitive if and only if $n = p^k$
3. Show that P is primitive if and only if $n = p$

DO 3.24. Infer from the above that if G is a p-group, then every maximal subgroup has index p and is normal.

DO 3.25. Suppose $G \curvearrowright \Omega$ and the corresponding homomorphism is $\varphi : G \to \mathrm{Sym}(\Omega)$. Consider $G^\varphi = Im(\varphi) \le \mathrm{Sym}(\Omega)$. Show that if G^φ is abelian then $G_x \triangleleft G$ and $\ker(\varphi) = G_x$.

DO 3.26. Suppose $G \curvearrowright \Omega$ and x, y are in the same orbit. Then G_x and G_y are conjugate.

3.3 Graph theory

Definition 3.27. A graph is an ordered pair $G = (V, E)$ where V is a set (the set of "vertices") and $E \subseteq \binom{V}{2}$ (the set of "edges"). The singular of "vertices" is "vertex."

Definition 3.28. A directed graph (digraph) is an ordered pair $G = (V, E)$ where V is a set and $E \subseteq V \times V$. Edges of the form (x, x) are called "loops" or "self-loops." We refer to E as the *adjacency relation.* Undirected graphs can be interpreted as digraphs where the adjacency relation is symmetric and irreflexive.

Definition 3.29. For a digraph (V, E), we define $E^- := \{(y, x) \mid (x, y) \in E\}$

Definition 3.30. A walk $x \to y$ of length k in a digraph is a sequence of vertices $x = v_0 \to v_1 \to \ldots \to v_k = y$ so that $(v_{i-1}, v_i) \in E$ for all i.

Definition 3.31. The *adjacency matrix* of a digraph G is a $|V| \times |V|$ matrix $A_G = (a_{ij})$ where $a_{ij} = 1$ if $(i, j) \in E$ and $a_{ij} = 0$ otherwise.

Example 3.32. Consider the matrix $(A_G)^2$. Observe that the (i, j) entry of this matrix counts the directed walks of length 2 from i to j.

DO 3.33. Consider the matrix $(A_G)^t$. Prove: the (i, j) entry of this matrix counts the directed walks of length t from i to j.

Definition 3.34. The (directed) distance from i to j, denoted $dist(i, j)$, is the length of the shortest (directed) walk from i to j. For undirected graphs this is a metric on V.

Definition 3.35. We say that vertex j is accessible from vertex i if $dist(i, j) < \infty$, or equivalently there exists a walk $i \dashrightarrow j$.

Definition 3.36. We say that i and j are mutually accessible if i is accessible from j and j is accessible from i.

DO 3.37. Mutual accessibility is an equivalence relation on V. The equivalence classes of this relation are called *strong components* of G. The digraph G is *strongly connected* if each vertex is accessible from each vertex (there is just one strong component).

Definition 3.38. The *symmetrization* of a digraph $G = (V, E)$, denoted $\widetilde{G} = (V, \widetilde{E})$, is an undirected graph defined so that $\{x, y\} \in \widetilde{E}$ if $x \neq y$ and also we have $x \to y$ or $y \to x$.

Definition 3.39. The *weak components* of a digraph G are the (strong) components of its symmetrization. For undirected graphs the two concepts coincide, so we just talk about "components."

Definition 3.40. We say y is an *out-neighbour* of x if $x \to y$ and an *in-neighbour* of x if $y \to x$. The number of out-neighbours of x is called the *out-degree* of x, denoted $\deg^+(x)$. The the number of in-neighbours of x is called the *in-degree* of x, denoted $\deg^-(x)$. For unidrected graphs, adjacent vertices are called *neighbors* and the number of neighbors of vertex x is its *degree*, $\deg(x)$.

Definition 3.41. A digraph G is *eulerian* if for all vertices v, we have $\deg^+(v) = \deg^-(v)$

HW 3.42. If G is an eulerian digraph then its weak components are strong.

DO 3.43. (Directed Handshake Theorem) For a digraph, prove:

$$\sum_{v \in V} \deg^+(v) = \sum_{v \in V} \deg^-(v) = |E|$$

DO 3.44. (Undirected Handshake Theorem) For a graph, prove:

$$\sum_{v \in V} \deg(v) = 2|E|$$

HW 3.45 (Due April 18)**.** Suppose an undirected graph G has no 4-cycles. Then $m = |E| = O(n^{3/2})$ and estimate the value of the constant implied by the big-Oh notation for large $n = |V|$.

Definition 3.46. The complete graph on n vertices, denote K_n, is the graph containing all the $\binom{n}{2}$ possible edges.

DO 3.47. If G has no triangle then $m \leq n^2/4$. This is called the Mantel-Turan theorem.

"Graph" without adjective will always refer to undirected graphs; we may add the adjective "undirected" for emphasis.

Definition 3.48. A graph is *d-regular* if every vertex has degree d. A graph is *strongly regular* with parameters (n, k, λ, μ) if it has n vertices, is k-regular, and the number of common neighbours of x and y is λ for $x \sim y$ and μ for $x \not\sim y$ (where $\sim$ denotes the adjacency relation).

Example 3.49. Two examples of strongly regular graphs are C_5 with parameters $(5, 2, 0, 1)$, and *Petersen's graph* with parameters $(10, 3, 0, 1)$. (Look up Petersen's graph.)

The following problem was misstated in class.

HW 3.50. Let G be a group of order r. Consider a graph with $n = r^2$ vertices so that $V = G \times G$ and two vertices (g_1, h_1) and (g_2, h_2) are adjacent if $g_1 = g_2$ or $h_1 = h_2$ or $g_1^{-1}h_1 = g_2^{-1}h_2$.

Prove that this graph is strongly regular and find its parameters.