CMSC 36500 / MATH 37500 Algorithms in Finite Groups

Instructor: László Babai
Scribe: Robert Green

Spring 2017

4 Lecture 4 April 6, 2017 Problems due April 11

4.1 Homework review - permutation groups

We will discuss a few of the homework problems from last time:

Review 4.1. If G has a proper subgroup H of index k then it has a proper normal subgroup of index at most $k!$

Proof. Let $S = G/H$ be the set of right cosets of H (of which there are k), and let $g \in G$ act on S by right multiplication $Hx \mapsto Hxg$. Let K denote the kernel of the associated homomorphism $\varphi : G \to S_k$. So K is a normal subgroup of G. Since $G/K \leq S_k$, we have $|G : K| \leq k!$. It remains to show that K is a proper subgroup of G. Indeed we show that $K \leq H$. Reason: if $g \in K$ then it fixes all right cosets; in particular it fixes H itself, so $Hg = H$, meaning $g \in H$. □

Definition 4.2 (Core of subgroup)**.** Let $H \leq G$. We define the core of H in G as the intersection of all conjugates of H:

$$\mathrm{Core}_G(H) = \bigcap_{g \in G} H^g \tag{3}$$

where $H^g = g^{-1}Hg$.

DO 4.4. Prove: $\mathrm{Core}_G(H)$ is the largest normal subgroup of G contained in H.

DO 4.5. Let $H \leq G$ and consider the action of G on G/H, the set of righ cosets of H, by right multiplication. This action is a homomorphism $\varphi : G \to \mathrm{Sym}(G/H)$. Prove:

$$\ker(\varphi) = \mathrm{Core}_G(H).$$

Review 4.6. Prove: if $G \leq S_n$ is a p-group then the length of each orbit is a power of p. (Hint: orbit-stabilizer lemma.)

Proof. It follows from the orbit-stabilizer lemma that $|x^G|$ always divides $|G|$. □

Review 4.7. Find the Sylow p-subgroups of the symmetric group S_n.

Solution. Let P be such a Sylow p-subgroup. The order of P is the highest power of p dividing $n!$, so

$$|P| = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \tag{8}$$

Let Ω be the permutation domain on which our symmetric group acts, so $|\Omega| = n$. First we solve the problem for $n = p^k$. Build a p-ary tree T of depth k of which the leaves are the elements of Ω. Assign to each

interior (non-leaf) node of T a cyclic permutation of its children. These cyclic permutations can be executed independently, so we get a permutation group of order p^N where N is the number of interior nodes, i.e.,

$$N = 1 + p + \cdots + p^{k-1} = \frac{n}{p} + \frac{n}{p^2} + \cdots + 1,$$

so this group has the right order and is therefore a Sylow p-subgroup. Note that this means that every Sylow p-subgroup acts on such a tree; in particular, for every $i \leq k$ they have blocks of imprimitivity of size p^i.

Now to general n. By the exercise above, each orbit of P has length p^i for some i. Write n in base p as $n = \sum_i a_i p^i$ where a_i is a p-ary digit, i.e., $0 \leq a_i \leq p-1$. So this is a sum of $\sum_i a_i$ powers of p. We claim that P has $\sum_i a_i$ orbits, out of which a_i have length p^i.

Divide up Ω into subsets of p-power sizes such that a_i subsets have size p^i for every i. Consider the direct product of the Sylow p-subgroups on these sets of size p^i. Verify that this group has the right order; therefore it is a Sylow p-subgroup of G. □

DO 4.9. Suppose $G \leq S_n$ is a primitive p-group. Then $n = p$.

Proof. We know that $n = p^k$ because G is transitive. Since G is a p-group, there exists $P \in \mathrm{Syl}_p(S_n)$ so that $G \leq P$. But G is imprimitive unless $k = 1$. The key observation here is that blocks of imprimitivity for a group are also blocks of imprimitivity for any subgroup. □

Definition 4.10 (Structure tree, structure forest)**.** Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group. We build a tree of which Ω is the set of leaves, such that the G-action on Ω extends to the tree. If G is primitive, we just add a root node and connect it to each element of Ω. If G is imprimitive, let $\{B_1, \ldots, B_k\}$ be a maximal system of imprimitivity, i.e., the blocks B_i are minimal blocks of imprimitivity. Let each B_i correspond to a node v_i in the tree; the set of children of v_i will be B_i. Let $\Omega_1 = \{v_1, \ldots, v_k\}$. It is clear that the G-action extends to the set Ω_1 so that the extension preserves the "parent" relation. Let $G_1 \leq \mathrm{Sym}(\Omega_1)$ be the image of the G-action on G_1. Now put a structure tree of G_1 on top of the set Ω_1. (End of inductive definition.)

If G is intransitive, build a structure tree separately for each orbit. The set of these structure trees is the structure forest.

DO 4.11. Let T be structure forest of $G \leq \mathrm{Sym}(\Omega)$ and let x be an interior node of (one of the trees in) T. Then the action of G_x on the set of children of x is primitive.

So, in a way, primitive groups are the "building blocks" of all permutation groups. (The "glue" that glues these building blocks together is very complicated, but by understanding the primitive groups in a structure forest of a permutation group G we gain a lot of information about G itself.)

DO 4.12. Structure trees are not unique. For instance, the dihedral group D_6 (of order 12) acting on the six vertices of a hexagon has two structure trees.

DO 4.13. Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group and $x \in \Omega$. Prove: the structure trees of G are in one-to-one correspondence with the maximal chains of subgroups connecting G_x to G. Such a chain has the form $G_x = H_0 < H_1 < \cdots < H_k = G$; maximality means H_{i-1} is a maximal subgroup of H_i for each i. The number k is the depth of the corresponding structure tree.

HW 4.14. (Due April 18) Find infinitely many transitive permutation groups G and two structure trees of G of different depths. (Ideally, the depths should have very different orders of magintude.)

HW 4.15. (Due April 18) Let $G \leq S_n$ be a transitive group. (a) Prove: there are at most $n-1$ maximal systems of imprimitivity (the blocks are minimal). (b) Prove that the bound $n-1$ is infinitely often tight.

4.2 Homework review - digraphs

Definition 4.16. Let $X = (V, E)$ be a digraph. A *cut* (A, B) is a partition of V into two non-empty parts A, B, so $A \cup B = V$ and $A \cap B = \emptyset$. $E(A, B) = E \cap (A \times B)$ is the set of edges from A to B.

DO 4.17. A digraph X is not strongly connected if and only if there exists a cut A, B so that $E(A, B) = \emptyset$.

DO 4.18. If X is a digraph and (A, B) a cut then

$$|E(A, B)| - |E(B, A)| = \sum_{v \in A} (\deg^+(v) - \deg^-(v)).$$

Review 4.19. If X is an eulerian digraph then all weak components of X are strong components.

Proof. We may assume without loss of generality (WLOG) that X is weakly connected. It follows that for every cut (A, B) we have $|E(A, B)| + |E(B, A)| > 0$. Now by DO 4.18 we have $|E(A, B)| = |E(B, A)|$ for every cut (A, B), and therefore $|E(A, B)| > 0$ for all cuts. But this means X is strongly connected by DO 4.17. □

4.3 Linear algebra review

Definition 4.20. The *transpose* of a $k \times n$ matrix $A = (a_{ij})$ is the $n \times k$ matrix $A^T = (a_{ji})$. A *row vector* is a $1 \times n$ matrix; the transpose of a row vector is a *column vector* ($n \times 1$ matrix). We shall think of $\mathbb{F}^n$ as the set of $n \times 1$ column vectors over the field $\mathbb{F}$.

Review 4.21. Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n$ be a polynomial over the field $\mathbb{F}$ with $a_n \neq 0$ (f has degree n). We say that "all roots of f belong to $\mathbb{F}$" if f can be factored as $f(t) = \prod_{i=1}^{n} (t - \lambda_i)$ where the λ_i are the roots and they occur in this expression with *multiplicity*. Note that the condition always holds of $\mathbb{F} = \mathbb{C}$.

Review 4.22. A column vector $\mathbf{x} \in \mathbb{F}^n$ is an eigenvector of the $n \times n$ matrix B over the field $\mathbb{F}$ if $\mathbf{x} \neq \mathbf{0}$ and there exists $\lambda \in \mathbb{F}$ such that $B\mathbf{x} = \lambda \mathbf{x}$.

Review 4.23. If A is an $n \times n$ matrix over a field $\mathbb{F}$ then its *characteristic polynomial* is $f_A(t) = \det(tI - A)$. The roots of the characteristic polynomial are the eigenvalues of A. We say that "all eigenvalues of A belong to $\mathbb{F}$" if all roots of f_A belong to $\mathbb{F}$.

Definition 4.24. If A is an $n \times n$ matrix then its *trace* is defined as the sum of the diagonal: $\text{Trace}(A) = \sum a_{ii}$.

DO 4.25. If A is an $n \times n$ matrix over the field $\mathbb{F}$ and all eigenvalues of A belong to $\mathbb{F}$ then

$$\text{Trace}(A) = \sum_{i=1}^{n} \lambda_i.$$

Definition 4.26. The *standard dot product* of two real vectors $\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$ and $\mathbf{y} = (y_1, \ldots, y_n)^T \in \mathbb{R}^n$ is $\mathbf{x} \cdot \mathbf{y} = \mathbf{x}^T \mathbf{y} = \sum x_i y_i$. The *norm* of $\mathbf{x}$ is defined as $\|\mathbf{x}\| = \sqrt{\mathbf{x} \cdot \mathbf{x}}$. The vectors $\mathbf{x}$ and $\mathbf{y}$ are *orthogonal* if $\mathbf{x} \cdot \mathbf{y} = 0$. A list $\mathbf{v}_1, \ldots, \mathbf{v}_k$ of vectors is an *orthonormal system* if $\mathbf{v}_i \cdot \mathbf{v}_j = \delta_{ij}$ where the Kronecker symbol δ_{ij} is the (i, j)-entry of the identity matrix. An orthonormal basis (ONB) of $\mathbb{R}^n$ is a basis that is orthonormal. A *unit vector* is a vector of norm 1.

Theorem 4.27. ***(Spectral Theorem)*** *Let B be an $n \times n$ symmetric real matrix. Then B has an orthonormal eigenbasis (i.e., a basis of $\mathbb{R}^n$ consisting of eigenvectors of B). In particular, all eigenvalues of B are real.*

It follows that the characteristic polynomial $f_B(t) = \det(tI - B)$ can be written as a product $\prod_i (t - \lambda_i)$ where the λ_i are the eigenvalues of B.

4.4 Spectral graph theory

Definition 4.28. Recall that a *walk* of length k is a sequence $v_0, v_1, \ldots, v_k$ of vertices such that $v_{i-1} \to v_i$ for all i (i.e., $(v_{i-1}, v_i) \in E$). A *path* is a walk with no repeated vertices. In an undirected graph a path does not have an inherent orientation, so when we count paths, the path $v_0, v_1, \ldots, v_k$ counts as the same path as $v_k, v_{k-1}, \ldots, v_0$. But when counting walks, we take their orientation into account, even if the graph is undirected.

(Some books and authors use the term "path" to mean what we call "walk." Please stick with our definition.)

Definition 4.29. A *closed walk* of length k is a walk of length k that starts and ends at the sme vertex ($v_0 = v_k$). A *cycle* is a closed walk without repeated vertices (besides the start and end). When counting closed walks, we take their start vertex into account; but when counting cycles, we don't, so a cycle of length k corresponds to k closed walks. Moreover, for undirected graphs, when counting cycles, we ignore their orientation; but when counting closed cycles, we don't.

Recall that by "graph" we mean "undirected graph."

Note that this means that the sum of the eigenvalues of a graph is zero, since all diagonal entries are zero.

Definition 4.30. The *distance* from vertex u to vertex v is

$$\operatorname{dist}(u, v) = \inf(\operatorname{length}(P))$$

where the infimum is taken over all walks P from u to v. This infimum is infinite if v is inaccessible from u.

DO 4.31. Show that in this definition we could have taken the infimum over all paths (as opposed to walks), the result would not change.

Definition 4.32. The *diameter* of the graph X is

$$\operatorname{diam}(X) = \sup_{x,y \in V} \operatorname{dist}(x, y)$$

Definition 4.33. By *eigenvalues of a graph* we mean the eigenvalues of its adjacency matrix.

HW 4.34. The number of distinct eigenvalues of a connected graph X is at least $1 + \operatorname{diam}(X)$

In the following sequence of exercises, X will always be a graph. We will assume that the eigenvalues of X are always given as $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$

DO 4.35. If X is regular of degree d then $\lambda_1 = d$ (that is, the greatest eigenvalue is d).

DO 4.36. If X is regular of degree d, then for all i, we have $|\lambda_i| \leq d$

DO 4.37. For a regular graph X of degree d we have $\lambda_2 = d$ if and only if X is disconnected.

Definition 4.38. A graph $X = (V, E)$ is *bipartite* if V can be legally coloured with two colours (adjacent vertices always receive different colors).

DO 4.39. If X is bipartite (not necessarily regular) then for all i we have

$$\lambda_i = \lambda_{n-i+1}$$

CH 4.40. If X is connected and $\lambda_n = -\lambda_1$ then X is bipartite.

HW 4.41. Find the eigenvalues (with multiplicity) and an eigenbasis for K_n (the complete graph with n vertices) and $K_{n,n}$ (the complete bipartite graph on (n, n) vertices (each part has n vertices)).