Graph Isomorphism course, Spring 2017
Instructor: László Babai
Notes by Angela Wu
Tuesday, April 18, 2017

7 Day 7, TWk4

7.1 Regular permutation groups

Definition 7.1 (Cayley)**.** A **right regular representation of** G is the representation $\rho : G \to \mathrm{Sym}(G)$, $\rho(g) : x \mapsto xg$, where $g \in G$ acts as right translation by g. This is a "permutation representation."

DO 7.2. ρ is faithful, or, $\mathrm{Ker}(\rho) = 1$.

We define $G_R = \mathrm{Img}(\rho) \le \mathrm{Sym}(G)$.

DO 7.3. G_R is transitive.

DO 7.4. $|G_x| = 1$.

A permutation group $H \le \mathrm{Sym}(\Omega)$ is **regular** if it is transitive and, $(\forall x \in \Omega)(|H_x| = 1$. Notice that the $\forall$ can be replaced by $\exists$ since H is transitive. A regular permutation group $H \le \mathrm{Sym}(\Omega)$ satisfies $|H| = |\Omega|$.

Definition 7.5. Let $f_i : G \to \mathrm{Sym}(\Omega_i)$ $(i = 1, 2)$ be two permutation representations of the group G. We say that f_1 and f_2 are *equivalent* if there is a bijection $\psi : \Omega_1 \to \Omega_2$ such that $(\forall g \in G)(f_1(g)\psi = \psi f_2(g))$. We say that the permutation groups $G_i \le \mathrm{Sym}(\Omega_i)$ $(i = 1, 2)$ are equivalent if there is a bijection $\psi : \Omega_1 \to \Omega_2$ such that $G_2 = \psi^{-1} G_1 \psi$.

DO 7.6. Prove: the groups $G_i \le \mathrm{Sym}(\Omega_i)$ $(i = 1, 2)$ are equivalent if and only if there exists a group G that has two equivalent pemutation representations $f_i : G \to \mathrm{Sym}(\Omega_i)$ $(i - 1, 2)$, such that $\mathrm{Img}(f_i) = G_i$.

DO 7.7. Prove: If G is a regular permutation group then G is equivalent to G_R (and therefore also to G_L).

Hint: Suppose $G \le \mathrm{Sym}(\Omega)$ is regular. Pick $x_0 \in \Omega$. Then the map $H \to \Omega$ given by $h \mapsto x_0^h$ is a bijection. (End Hint)

Definition 7.8. A permutation group $H \le \mathrm{Sym}(\Omega$ is **semiregular** if $(\forall x \in \Omega)(|H_x| = 1)$.

So, H is regular if and only if it is transitive and semiregular.

DO 7.9. Each orbit of a semiregular permutation group H has length $|H|$ (because $= |H : H_x|$).

Definition 7.10. The **left regular representation** $G \curvearrowright G$ given by $\lambda : G \to \mathrm{Sym}(G)$, $\lambda(g) : x \mapsto g^{-1}x$.

DO 7.11. $\lambda(gh) = \lambda(g)\lambda(h)$.

DO 7.12. $G_L := \mathrm{Img}(\lambda) \leq \mathrm{Sym}(G)$ is a regular permutation group isomorphic to G.

Definition 7.13. Let $S \subseteq G$. The **centralizer of S in G** is the subgroup $C_G(S) := \{g \in G : (\forall s \in S)(gs = sg)\}$ of G.

Claim 7.14. *$[G_L, G_R] = 1$, i.e., $G_L \leq C_{\mathrm{Sym}(G)}(G_R)$ and vice versa.*

HW 7.15. Show the following.

(a) If $G \leq \mathrm{Sym}(\Omega)$ is transitive, then $C_{\mathrm{Sym}(\Omega)}(G)$ is semiregular.

(b) If $G \leq \mathrm{Sym}(\Omega)$ is semiregular, then $C_{\mathrm{Sym}(\Omega)}(G)$ is transitive.

Corollary 7.16. *If $G \leq \mathrm{Sym}(\Omega)$ is regular, then $C_{\mathrm{Sym}(\Omega)}(G)$ is regular.*

Corollary 7.17. *$C_{\mathrm{Sym}(G)}(G_L) = G_R$.*

Proof. We know that the centralizer $C \geq G_R$, and a proper supergroup of G_R cannot be regular. □

HW 7.18. If $G \leq \mathrm{Sym}(\Omega)$ is primitive and $1 \neq N \triangleleft G$, then N is transitive.

Corollary 7.19. *If G is primitive and $1 \neq N \triangleleft G$ and N is abelian, then N is regular.*

Follows from below DO exercise.

DO 7.20. If $H \leq \mathrm{Sym}(\Omega)$ is transitive and abelian, then it is regular.

7.2 A bound on the order of primitive and solvable permutation groups

Corollary 7.21. *If $G \leq \mathrm{Sym}(\Omega)$ is primitive and solvable, then $|G| \leq n^{1+\log_2(n)}$, where $n = |\Omega|$.*

Proof. First, for $N \triangleleft G$, we consider the action $G \curvearrowright N$ by conjugation, given by $g : x \mapsto x^g = g^{-1}xg$ for $x \in n$. Notice that $\mathrm{Ker}(\phi) = \{g \in G : (\forall x \in N)(x^g = x)\} = C_G(N)$.

Let $N \triangleleft_{\min} G$ (N is a minimal normal subgroup in G). Then N is characteristically simple. Then, $N = T \times \cdots \times T$, where T is simple. If T is solvable, then $T \cong \mathbb{Z}_p$ and $N \cong \mathbb{Z}_p^k$.

Notice that N is transitive. Since N is abelian, N is regular and $n = p^k$. So $\phi : G \curvearrowright N$ by conjugation. Then, $\mathrm{Ker}(\phi) = C_G(N) = N$. From the lemma below, $\mathrm{Img}(\phi) \cong G/N$, so $G/N \leq \mathrm{Aut}(N) = \mathrm{Aut}(\mathbb{Z}_p^k) = \mathrm{GL}(k, p)$ (DO below).

We estimate $|\mathrm{GL}(k, p)| \leq |M^{k \times k}(\mathbb{F}_p)| = p^{k^2}$. So, we find that $|G| \leq |N||G/N| \leq p^{k^2} p^k = n^{k+1} = n^{1+\log_p n} \leq n^{1+\log_2 n}$. □

Corollary 7.22 (No longer HW, follows from above corollary)**.** *If $G \leq \mathrm{Sym}(\Omega)$ is primitive and solvable, then $|\Omega| = p^k$ (a prime power).*

Lemma 7.23. *If $H \leq \mathrm{Sym}(\Omega)$ is regular and abelian, then $C_{\mathrm{Sym}(\Omega)}(H) = H$.*

Proof. $C(H) \geq H$. But $C(H)$ is regular, so this cannot be a proper inclusion. □

DO 7.24. $\mathrm{Aut}(\mathbb{Z}_p^k) = GL(k, p)$.

HW 7.25. If $N \triangleleft G \leq \mathrm{Sym}(\Omega)$ is regular, then $|G| \leq n^{1+\log_2 n}$, where $n = |\Omega|$.

For two subsets $A, B \subseteq G$, we denote by $A \cdot B = AB = \{ab : a \in A, b \in B\}$.

DO 7.26. Suppose $K, L \leq G$. Then $KL \leq G$ if and only if $KL = LK$.

Notice that $G_R G_L = G_L G_R \leq \mathrm{Sym}(G)$.

HW 7.27. For what groups G is $G_L G_R$ primitive? Give a very simple characterization.

7.3 Graph isomorphism!

Definition 7.28. GRAPH ISOMORPHISM (GI) PROBLEM
Input: Graphs X, Y.
Question: Decide the question "Is $X \cong Y$?"

We denote by $\mathrm{ISO}(X,Y) : \{f : X \to Y \text{ isomorphisms}\}$ the set of graph isomorphisms from X to Y.

DO 7.29. $\mathrm{ISO}(X,Y) = \begin{cases} \phi & \text{if } X \ncong Y \\ \mathrm{Aut}(X)\sigma & \text{if } X \cong Y, \text{ for } \sigma \in \mathrm{ISO}(X,X) \end{cases}.$

If $G \leq S_n$, we know that the minimum number of generators is $\leq \log_2(n!) < n \log_2 n$.

Theorem 7.30 (Babai 1987)**.** *Every subgroup chain in S_n has length $\leq 2n-3$.*

Corollary 7.31. *Every non-redundant set of generators of a subgroup of S_n has $\leq 2n-3$ generators.*

Definition 7.32. MEMBERSHIP PROBLEM IN PERMUTATION GROUPS
Input: $\sigma_1, \dots, \sigma_k, \tau \in S_n$.
Question: $\tau \in \langle \sigma_1, \dots, \sigma_k \rangle$?

Theorem 7.33 (Furst-Hopcroft-Luks (1980))**.** MEMBERSHIP IN PERMUTATION GROUPS *can be solved in polynomial time.*

C. C. Sims (1960s) first gave a polynomial-time algorithm, without analysis. His algorithm was analyzed by Knuth, 1982-89.

DO* 7.34. GI decision problem is Cook-equivalent (polynomial time Turing-equivalent) to finding the set of isomorphisms. Also, GI is equivalent to finding an isomorphism (if it exists).
Note: the * is a "very little star."

DO 7.35. Isomorphism of digraphs is Karp-reducible (polynomial time many-one-reduction) to Isomorphism of graphs. In other words, there exists a polynomial-time algorithm that solves the following.
Input: digraphs X, Y
Output: graphs X', Y', such that $X \cong Y \iff X' \cong Y'$.

Definition 7.36. A vertex-colored graph is a triple $X = (V, E, f)$, where (V, E) is a graph and $f : V \to \{\text{colors}\}$ is a coloring a the vertices. Here $\{\text{colors}\}$ is an ordered set, usually of the form $[k]$ where k is the number of colors used. Isomorphisms of vertex-colored graphs preserve the vertex colors by definition.

DO 7.37. Isomorphism of vertex-colored graphs is Karp reducible to isomorphism of graphs.

Definition 7.38. A coloring $g : V \to \{\text{colors}\}$ is a refinement of the coloring $f : V \to \{\text{colors}\}$ if the associated partition of V is a refinement, i.e., $(\forall x, y \in V)(g(x) = g(y) \implies f(x) = f(y))$.

7.4 Naive vertex refinement — a heuristic idea

NAIVE REFINEMENT STEP

Input: a vertex-colored graph $X = (V, E, f)$

Output: a refined coloring g defined as follows.

For $x \in V$ let $h(x) = (f(x); \deg_i(x) \mid i \in \{\text{colors}\})$ where $\deg_i(x)$ denotes the number of neighbors of x of color i.

Now sort the strings $h(x)$ $(x \in V)$ lexicographically and let $g(x) = j$ if $h(x)$ is the j-th string in the lexicographic order.

Naive refinement is the following algorithm:

NAIVE REFINEMENT

repeat call NAIVE REFINEMENT STEP

until partition stable

Definition 7.39 (Equitable partition)**.** Let $X = (V, E)$ be a graph and $V = C_1 \sqcup \cdots \sqcup C_k$ be a partition of its vertex set. We say that this partition is *equitable* if

1. For all i, $X[C_i]$ (the induced subgraph on vertices in C_i) is regular.
2. For all i, j, the graph given by $X[C_i, C_j]$ (the induced bipartite graph on $C_i \times C_j$) is semiregular.

A coloring f splits V into color classes: $V = C_1 \sqcup \cdots \sqcup C_k$ where $C_i = f^{-1}(i)$.

DO 7.40. The coloring f is stable under naive refinement if and only if the corresponding partition is equitable.

Theorem 7.41 (Babai-Erdős-Selkow (1979))**.** *For almost all graphs, naive refinement completely splits the graph in* 2 *rounds.*

Challenge 7.42 (Abe Mowshowitz, 1970)**.** If the characteristic polynomial of A_X is irreducible over $\mathbb{Q}$, then naive refinement completely splits the graph.