Algorithms in Finite Groups

MATH 37500: László Babai
Scribe: Tim Black

10/16/14

6 Large primitive permutation groups, coherent configurations

Exercise 6.1 (from previous homeworks)**.** $N \lhd G \leq S_n$, N regular $\implies$ $|G| \leq n^{1+\log_2 n}$.

Proof. $G \to \mathrm{Aut}(N)$ by conjugation, with kernel $C_G(N)$.

N is regular $\implies$ $C_G(N) \leq C_{S_n}(N)$, which is regular $\implies$ $|C_G(N)| \leq n$. Therefore, $|G| \leq n|\mathrm{Aut}(N)|$.

Say N is generated by d elements, $\langle S\rangle = N$, $|S| = d$. Then for $f \in \mathrm{Aut}(N)$, f is determined by $f|_S$, so $|\mathrm{Aut}(N)| \leq \#\{S \to N\} = n^d$. The proof is completed by the following exercise. □

Exercise 6.2. If $|G| = n$, every minimal set of generators has at most $\log_2 n$ elements.

6.1 Large primitive permutation groups

Cameron's classification of large primitive groups (1981) heavily depends on Classification of Finite Simple Groups (CFSG).

Definition 6.3. Socle of a group = product of the minimal normal subgroups.

- The "giants": S_n, A_n.
- Next largest: $\approx n^{\sqrt{n}}$ $\qquad S_k \wr S_2$, $n = k^2$
- $\approx n^{\sqrt{n/2}}$ $\qquad S_k^{(2)}$, $n = \binom{k}{2}$.
- $\exp(\tilde{O}(n^{1/3}))$
- $\ldots \exp(\tilde{O}(n^{1/k}))$: a finite number of groups for each k; the socle is a product of alternating groups.

Elementary result:

Theorem 6.4 (Bochert 1892)**.** *If $G < S_n$, not giant, primitive, then $|S_n : G| \geq (\frac{n+1}{2})!$, then $|G| < \exp(\frac{n}{2} \ln n)$.*

Theorem 6.5 (Praeger-Saxl 1980)**.** *$|G| \leq 4^n$ for all n (not just sufficiently large n) (Uses elementary group theory building on Wielandt 1934)*

Theorem 6.6 (Babai 1981)**.** *If G is uniprimitive (that is, primitive and not doubly-transitive), then $|G| < \exp(4\sqrt{n} \log^2 n)$ (pure graph theory, no groups involved)*

Theorem 6.7 (Xiaorai Sun, John Wilmes 2014)**.** *If G is uniprimitive, $|G| < \exp(\tilde{O}(n^{1/3}))$ with the known exceptions (again pure graph theory)*

Theorem 6.8. *(follows from CFSG) If G is not giant, is doubly transitive: $|G| < n^{1+\log_2 n}$. This is tight: consider $AGL(d, 2)$.*

Theorem 6.9 (Burnside)**.** *If G doubly-transitive, $N min \lhd G$, then either N is abelian ("affine case") or N is simple. $G \leq \mathrm{Aut}(N)$.*

All nonaffine doubly-transitive groups are known (Cartis-Kantor-Seitz 1970s). Elementary results:

Theorem 6.10 (Babai 1982)**.** *Doubly-transitive, not giant $\implies |G| < \exp(\exp(\sqrt{\log n})) \ll \exp n^\epsilon$ (by elementary combinatorics, using basic concepts of permutation groups plus Wielandt)*

Theorem 6.11 (Pyber 1989)**.** *$|G| < n^{\log^2 n}$ (elementary combinatorics, uses a little bit of group theory, uses Wielandt). By even more elementary means, $|G| < n^{\log^3 n}$.*

6.2 Coherent configurations

Definition 6.12. A *configuration* $\mathfrak{X} = (\Omega; R_0, \ldots, R_{r-1})$ of rank r consists of a partition $\Omega \times \Omega = R_0 \cup R_1 \cup \cdots \cup R_{r-1}$ such that

(i) $\mathrm{diag}(\Omega) = R_0 \cup \cdots \cup R_{r_0-1}$ a subpartition, and

(ii) $(\forall i)(\exists j)(R_i^{-1} = R_j)$, where the superscript -1 indicates switching the order of the pairs.

Write the *color* $c(x, y) = i$ if $(x, y) \in R_i$. The *rank* is $\mathrm{rank}(\mathfrak{X}) = r$. A configuration is a *coherent configuration* if furthermore

(iii) there exist parameters p_{ij}^k, $0 \leq i, j, k, \leq r - 1$, such that

$$(\forall (x, y) \in R_k)(|\{z \mid c(x, z) = i, c(z, y) = j\}| = p_{ij}^k).$$

Definition 6.13. "Group case": Let $G \leq \mathrm{Sym}(\Omega)$.
Define $\mathfrak{X}(G) = (\Omega; \text{orbits of } G \text{ on } \Omega \times \Omega)$.

Exercise 6.14. This is a coherent configuration.

Exercise 6.15. $G \leq \mathrm{Aut}(\mathfrak{X}(G))$.

Definition 6.16. $X = (V, E)$ is a *strongly regular graph* (*SRG*) with parameters (n, k, λ, μ) if

- $n = |V|$,
- $k = \deg x$ for all $x \in V$,
- every pair of adjacent vertices has λ common neighbors, and
- every pair of nonadjacent vertices has μ common neighbors.

Exercise 6.17. If X is SRG, disconnected, then $G = r \cdot K_s = K_s \cup \cdots \cup K_s$. It has parameters $(rs, s-1, s-2, 0)$.

Exercise 6.18. If X is SRG, then $\overline{X}$ is SRG.

Definition 6.19. A graph $X = (V, E)$ gives rise to a configuration $\mathfrak{X}(X) = (V; \mathrm{diag}(V), E, \overline{E})$.

Exercise 6.20. $\mathfrak{X}(X)$ is coherent $\iff$ X SRG.

Definition 6.21. A *Latin square* is an $n \times n$ matrix in which every row is a permutation of $\{1, \ldots, n\}$, and every column is also a permutation of $\{1, \ldots, n\}$.

Definition 6.22. Let $L = (\ell_{ij})$ be a Latin square. The *point graph of* L is a graph with n^2 vertices (i, j), $1 \leq i, j \leq n$, with $(i, j) \sim (i', j')$ if $i = i'$ or $j = j'$ or $\ell_{ij} = \ell_{i'j'}$.

Exercise 6.23. These graphs are SRG (find the parameters).

Definition 6.24. An *isomorphism* of Latin squares is allowed to permute the rows amongst themselves, permute columns amongst themselves, permute the symbols that are used as labels, swap rows with columns (that is, take the transpose), swap rows with symbols, or swap columns with symbols. There are $(n!)^3 3!$ isomorphisms from a given Latin square, corresponding to elements of the group $S_n \wr S_3$.

Exercise 6.25. (a) If $k \geq 4$ then (a) all automorphisms of $\mathrm{Point}(L)$ are induced by $\mathrm{Aut}(L)$; (b) all isomorphisms between point graphs of Latin squares are induced by isomorphisms of the corresponding Laton squares. In particular, one can canonically reconstruct a Latin square from its point graph.

Theorem 6.26 (Cameron, Babai 1981)**.** *Almost all Latin squares have no automorphisms.*

Definition 6.27. A configuration is a *homogeneous configuration* if $R_0 = \mathrm{diag}(\Omega)$.

Exercise 6.28. $\mathfrak{X}(G)$ homogeneous $\iff$ G transitive.

Notation 6.29. $c(x) = c(x, x)$. $\deg_i^+(x)$ denotes the out-degree of vertex x in color i, and $\deg_i^-(x)$ the in-degree.

Exercise 6.30. $c(x,y)$ determines $c(x)$ and $c(y)$.

Exercise 6.31. Let $\mathfrak{X}$ be a coherent configuration. If $c(x) = c(y)$ then $(\forall i)(\deg_i^+(x) = \deg_i^+(y))$ and $(\forall i)(\deg_i^-(x) = \deg_i^-(y))$,

Exercise 6.32. If $c(x) \neq c(y)$, then $\forall i\ \deg_i^+(x)\deg_i^+(y) = 0$.

Definition 6.33. The digraph (V,E) is *Eulerian* if $(\forall x \in V)(\deg^+(x) = \deg^-(x)$, where $\deg^+$ denotes out-degree and $\deg^-$ denotes in-degree.

Exercise 6.34. If $\mathfrak{X}$ is a homogeneous coherent configuration, then $(\forall i)(\deg_i^+ = \deg_i^-)$, i.e. $(\forall i)((\Omega, R_i)$ is Eulerian).

Definition 6.35. Let (V,E) be a digraph. *Weakly connected*: $(V, E \cup E^{-1})$ is connected (that is, the underlying undirected graph is connected). *Strongly connected*: $(\forall x,y)(\exists x \to \cdots \to y$ a walk).

Exercise 6.36. If an Eulerian digraph is weakly connected then it is strongly connected.

Definition 6.37. A *primitive coherent configuration* is a configuration that is

(1) homogeneous,

(2) $(\forall i \geq 1)((\Omega, R_i)$ is connected as a directed graph).

Theorem 6.38. *The permutation group G is primitive $\iff$ the coherent configuration $\mathfrak{X}(G)$ is primitive.*

$G \leq \mathrm{Aut}(\mathfrak{X}(G))$.

(i) If G is primitive, then $\mathfrak{X}(G)$ is primitive (connected components of (V, R_i) form a system of imprimitivity).

(ii) If $\mathfrak{X}(G)$ is primitive, then G is primitive (an edge within a block cannot be sent to a cross-block edge).

Exercise 6.39. If $\mathfrak{X}$ is coherent, $x, y \in \Omega$, then the number of $x \to y$ walks (note: walks are not required to be self-avoiding) of a given length k and color composition $i_1, \ldots, i_k$ depends only on $c(x,y)$ and the list $(i_1, \ldots, i_k)$ of colors.

Exercise 6.40. If $\mathfrak{X}$ is coherent, then (a) all weak components (components of the underlying undirected graph) of color i have the same number of vertices and same diameter. (b) However, they don't need to be isomorphic. Construct a homogeneous coherent configuration in which one of the color classes has nonisomorphic components.

Exercise 6.41. Let $\mathfrak{X}$ primitive coherent configuration, $\tilde{R}_i = R_i \cup R_i^{-1}$. If $(\Omega, \tilde{R}_i) = \tilde{X}_i$ is not complete, then $\mathrm{diam}\left(\overline{\tilde{X}_i}\right) = 2$.

Exercise 6.42. $|\mathrm{Aut}(\text{Latin Square})| \leq n^{1+\log_2 n}$ (or something similar).