Algorithms in Finite Groups

MATH 37500: László Babai
Scribe: Angela Wu

10/21/14

7 Exercise Regarding Coherent Configurations

Consider the action of $G \leq \mathrm{Sym}(\Omega)$ on $\Omega \times \Omega$.

Definition 7.1. A *configuration* $\mathfrak{X}(\Omega, R_0, \ldots, R_{r-1})$ is given by a partition $\Omega \times \Omega = R_0 \sqcup \ldots \sqcup R_{r-1}$ satisfying (1) $\mathrm{diag}(\Omega) = R_0 \sqcup \ldots \sqcup R_{r_0}$, and (2) $(\forall i)(\exists j)(R_i^{-1} = R_j)$. We call $\mathrm{rank}(\mathfrak{X}) := r$ the *rank* of $\mathfrak{X}$. We say the color $c(x,y)$ of the pair (x,y) is $c(x,y) = i$ if $(x,y) \in R_i$.

Definition 7.2. A configuration is *coherent* if in addition, for any $0 \leq i,j,k \leq r-1$, there exists p_{ij}^k such that for all pairs $(x,y) \in R_k$ we have $\#\{z : c(x,z) = i, c(z,y) = j\} = p_{ij}^k$.

Definition 7.3. A digraph (V,E) is *weakly connected* if $(V, E \cup E^{-1})$ is connected. A digraph (V,E) is *strongly connected* if, for any $u, v \in V$, there is a directed path from u to v. The *indegree* $\deg^-(v)$ of a vertex $v \in V$ is the number of incoming edges, and the *outdegree* $\deg^+(v)$ of a vertex $v \in V$ is the number of outgoing edges.

Exercise 7.4. Suppose that $\mathfrak{X}$ is a coherent configuration. We write $c(x) = c(x,x)$. We prove the following series of exercises:

1. If $c(x) = c(y)$, then for any i, $\deg_i^{+/-}(x) = \deg_i^{+/-}(y)$.

2. Given a string of colors $\vec{C} \in [r]^\ell$ of length ℓ and vertices $u, v \in V$, define $\#u \xrightarrow{C} v$ to be the number of (possibly repeating) walks from u to v via ℓ steps of colors in the order prescribed by $\vec{w}$. Show that $\#u \xrightarrow{C} v = f(c(u,v), \vec{C})$ is a function depending only on $\vec{C}$ and the color of $c(u,v)$.

3. Show that for any i, all the weak components of (Ω, R_i) have the same size and diameter.

4. Find a coherent configuration $\mathfrak{X}$ such that, for some i, (Ω, R_i) has two non-isomorphic weak components.

Proof. 1. Consider $x, y \in \Omega$ such that $c(x) = c(y) = k$. For any i, $\deg_i^+(x) = p^k_{i,i^{-1}} = \deg_i^+(y)$ and $\deg_i^-(x) = p^k_{i^{-1},i} = \deg_i^-(y)$.

2. We define $f(c_0, \vec{C})$ to be the number of walks from u to v, vertices satisfying $c(u,v) = c_0$, via colors in the order prescribed by $\vec{C}$. We show that $f(c_0, \vec{C})$ is well defined, by induction on $\ell = |\vec{C}|$.

   The claim is true for $\ell = 1$ and $\ell = 2$ by the definition of coherent configuration. Let $u, v \in \Omega$, let $c_0 = c(u,v)$, and let $\vec{C} = (c_1, \ldots, c_\ell) \in [r]^\ell$. We count:
   $$\#u \xrightarrow{C} v = \sum_{j \in [r]} f(j, c_1, \ldots c_{\ell-1}) \cdot p^{c_0}_{j,c_\ell}, \tag{1}$$
   which is independent of the choice of vertices u, v.

3. Diameter: Suppose that C_1 and C_2 are two distinct weak components of (Ω, R_i) with diameter diam_1 and diam_2 respectively. Suppose that $u, v \in C_1$ satisfy $\mathrm{dist}_i(u,v) = \mathrm{diam}_1$. Let $k = c(u,v)$. Then, $f(k, i^{\pm 1} \ldots i^{\pm 1}) = 0$ (with $\mathrm{diam}_1 - 1$ i's) for any choice of signs. But, $f(k, \pm 1 \ldots i^{\pm 1}) \geq 1$ (diam_1 i's) for some choice of signs. Thus, the shortest i-colored path from u to v has length exactly diam_1. By exercise 1., we find that there is $u' \in C_2$ such that $c(u') = c(u)$. Since $\deg_k^+(u') = \deg_k^+(u)$, we find that there also exists v' such that $d(u', v') = k$. By exercise 2. and the discussion above, we find that the minimum length of an i-colored path from u' to v' is exactly diam_1. So, $u', v' \in C_2$, and $\mathrm{diam}_2 \geq \mathrm{diam}_1$. The same argument shows that $\mathrm{diam}_1 \geq \mathrm{diam}_2$, so they are equal.

   Size: Let C_1 and C_2 be two nonempty connected components of (Ω, R_i). Pick some $x \in C_1$ and some $y \in C_2$ such that $c(y) = c(x)$ (possible by exercise 1). Define $B_i(x,n)$ to be the ball centered at x of radius n on (Ω, R_i). Notice that $|B_i(x,n)|$ is determined entirely by $f(c(x), \vec{C})$ for $\vec{C} \in [c]^*$. Since $c(y) = c(x)$, $|B_i(y,n)| = |B_i(x,n)|$ for all i. Thus, the size of the i-component containing x, $|\bigcup_n B_i(x,n)|$, and the size of the i-component containing y, $|\bigcup_n B_i(x,n)|$, must be equal.

4. Consider a Latin square $\mathcal{L}$, with corresponding graph $X(\mathcal{L}) = (V, E)$ defined by $V = [k]^2$ and $(i,j) \sim (i', j')$ if $i = i'$, $j = j'$ or $\ell(i,j) = \ell(i',j')$. We note that $X(\mathcal{L})$ must be strongly regular with parameters $(k^2, 3(k-1), k, 6)$.

   Let $X_1 = (V_1, E_1)$ and $X_2 = (V_2, E_2)$ be the graphs for two nonisomorphic Latin squares. Define $\mathcal{X} = (\Omega, R_1, R_2, R_3, R_4)$ be the homogeneous coherent configuration given by $\Omega = V_1 \sqcup V_2$, $R_1 = E_1 \sqcup E_2$, $R_2 = \overline{E_1} \sqcup \overline{E_2}$, and $R_3 = V_1 \times V_2 \sqcup V_2 \times V_1$. Then, the components of the graph (Ω, R_1) correspond exactly to X_1 and X_2, which are non-isomorphic.

□

Other examples of strongly regular graphs include:

- $L(K_v)$, with parameters $\left(\binom{v}{2}, 2(v-1), v-2, 4\right)$ and $\mathrm{Aut} \cong S_v$.
- $L_(K_{v,v})$, with parameters $(v^2, 2v-2, v-2, 2)$ and $\mathrm{Aut} \cong S_v \wr S_2$.

In particular, the above graphs give examples of strongly regular graphs with large automorphism groups.

Do 7.5. Show that if a strongly regular graph X is disconnected, then $X = r \cdot K_s$, with automorphism group $S_s \wr S_r$.

Exercise 7.6. Prove: If the line graph $L(X)$ of some graph X is strongly regular then either $L(X)$ is disconnected (so $L(X)$ is the union of complete graphs of equal size, so X is the union of star graphs and possibly triangles) or X is a complete graph, or a complete bipartite graph with equal parts, or the pentagon.

Theorem (Babai 1981). If $\mathfrak{X}$ is a coherent configuration of rank ≥ 3 with n vertices then $|\,\mathrm{Aut}(\mathfrak{X})| \leq \exp(4\sqrt{n}\ln^2 n)$.

See the proof in a separate document.