Graph Isomorphism course, Spring 2017
Instructor: László Babai
Notes by Angela Wu and the instructor
Tuesday, May 16, 2017

15 Day 15, TuWk8

15.1 "Large" permutation groups

Recall that $\mathrm{Soc}(G)$ is defined to be the product of minimal normal subgroups.
Recall [Cameron & CFSG, as refined by Maróti]: If $G \leq S_n$, G is primitive, $|G| > n^{1+\log_2 n}$, and $n \geq 25$, then $n = \binom{m}{t}^\ell$ for some m, t, ℓ and

- If $\ell = 1$, then G is a Johnson group, $G = S_m^{(t)}$ or $A_m^{(t)}$.
- In general, $\mathrm{Soc}(G) = (A_m^{(t)})^\ell = A_m^{(t)} \times \cdots \times A_m^{(t)}$, and $(A_m^{(t)})^\ell \leq G \leq S_m^{(t)} \wr S_\ell$. So, G acts on ordered ℓ-tuples of t-subsets of $[m]$.

We discuss how the GI algorithm addresses the two cases separately below.

15.1.1 $\ell \geq 2$: Luks-reduction works

We consider the case $\ell \geq 2$, where the conclusion will be that Luks-reduction accomplishes what we want.

DO 15.1. If $\ell \geq 2$, then $\mathrm{Soc}(G)$ acts imprimitively on $\binom{[m]}{t}^\ell$.

Consider $\varphi : G \to S_\ell$, with transitive image. Note that $\mathrm{Soc}(G) \leq \mathrm{Ker}\,\varphi$.

Lemma 15.2. *If $m > (\log_2 n)^2$, then $|G : \mathrm{Ker}\,\varphi| \leq n$.*

15.1.2 $\ell = 1$: difficult case

In this case, a large primitive group G is $G = S_m^{(t)}$ or $G = A_m^{(t)}$. This is the case where Luks's algorithm gets stuck.

If G is imprimitive and $\widetilde{G}$ the image of its action on a minimal system of imprimitivity (so $\widetilde{G}$ permutes the blocks), then the number of blocks is $\binom{m}{t}$ and $\widetilde{G} = S_m^{(t)}$ or $A_m^{(t)}$ (a Johnson group) acting on the blocks. Since $S_m^{(t)} \cong S_m$ and $A_m^{(t)} \cong A_m$, we infer a G-action on a set Γ, with $|\Gamma| = m$, as a giant. We refer to Γ as the "ideal set" while Ω (the set of positions) is the "real world." We have $|\Gamma| \leq |\Omega|$.

Let x be the input string. Consider $\mathrm{Aut}_G(x) \leq G \xrightarrow{\varphi} \mathrm{giant}(\Gamma)$. Our goal is to (1) decide whether $\varphi(\mathrm{Aut}(G))$ is *almost* giant (testable by efficient Luks reduction) or (2) encase $\varphi(\mathrm{Aut}_G(x)) \leq M < \mathrm{Sym}(\Gamma) = S_m$. Denote $n = |\Omega|$ and $m = |\Gamma|$.

We want $|M|$ to be much smaller than $\mathrm{Sym}(\Gamma)$, specifically, we want $|S_m : M| > c^m$ for some constant $c > 1$. So, this can only repeat $O(\log m)$ times.

Let $H := \mathrm{Aut}_G(x)$. Consider $\varphi : H \twoheadrightarrow \bar{H} \leq S_m$. An intermediate goal is to find an $\bar{H}$-invariant structure on Γ. Then, use this to find a good canonical partition of Γ with no dominant color

($\geq 90\%$) or to find an equipartition of the dominant color. This is an unattainable goal – there exist counterexamples: the Johnson graphs (see below).

However, it is possible to either find a canonical coloring of Γ with no dominant color, or find a canonical equipartition of the dominant color, or find a canonical Johnson graph on a dominant color.

Definition 15.3 (Johnson graphs)**.** We define the **Johnson graph** $J(k,t)$, for $k \geq 2t+1$. The graph has $\binom{k}{t}$ vertices which we label as $\{v_T : T \subseteq [k], |T| = t\}$. Two vertices are adjacent, $v_T \sim v_S$, exactly if $|T \setminus S| = 1$.

15.2 Post-quiz homework assignment

DO 15.4. The quiz has been posted. Work out the quiz problems without time pressure.

HW 15.5 (Last bonus question on quiz)**.** If $G \leq S_n$ is primitive, then G has ≤ 2 minimal normal subgroups.

HW 15.6. $\operatorname{Aut}(J(m,t)) = S_m^{(t)}$. Note: $\geq$ is trivial.

In your solution to problem 15.6 you may use the following results.

Theorem 15.7 (Erdős-Ko-Rado Theorem)**.** *If $\mathcal{F} \subseteq \binom{[k]}{t}$ for $k \geq 2t+1$ is an intersecting family, i.e., $(\forall A, B \in \mathcal{F})(|A \cap B| \geq 1)$, then $|\mathcal{F}| \leq \binom{k-1}{t-1}$.*

Remark 15.8. Note that this bound is tight, as demonstrated by picking an element $x \in [k]$ and taking all t-subsets of $[k]$ containing x.

Theorem 15.9 (Hilton-Milner Theorem)**.** *The only extremal systems in the EKR Theorem are the systems described in Remark 15.8.*