CMSC 36500 / MATH 37500 Algorithms in Finite Groups

Instructor: László Babai
Scribe: Robert Green
This lecture was given by Bohdan Kivva

Spring 2017

5 Lecture 5 April 11, 2017 Problems due April 13

5.1 Homework review - spectral graph theory

Review 5.1. If X is a connected graph of diameter d then A_X, the adjacency matrix of X, has at least $d+1$ distinct eigenvalues

Proof. Assume $A = A_X$ has k distinct eigenvalues and let m_A be the minimal polynomial of A. The matrix A is symmetric and therefore diagonalizable; it follows that $k = \deg m_A$. Let $m_A(t) = \sum_{i=0}^{k} \alpha_i t^i$ where $\alpha_k = 1$, so $A^k = -\sum_{i=0}^{k-1} \alpha_i A^i$. Let $d = \operatorname{diam} X$. Assume for a contradiction that $k \leq d$. Then there is a pair (i, j) of vertices at distance exactly k. But then the (i, j) entry of A^k is not zero while the (i, j) entry of A^ℓ is zero for all $\ell < k$, a contradiction, proving the claim. □

Review 5.2. If X is d-regular then all eigenvalues are bounded by d in absolute value.

Proof. First observe that d-regularity means $\sum_j a_{ij} = d$ for every i. Suppose $Ax = \lambda x$ where $x \neq 0$. Choose x_i to be the coordinate of x of maximum absolute value. Then

$$d|x_i| \geq \sum_j a_{ij}|x_j| \geq |\sum_j a_{ij}x_j| = |\lambda||x_i|$$

which gives us $|\lambda| \leq d$. □

5.2 On the Automorphism Groups of Strongly Regular Graphs

Definition 5.3. Let G, H be groups. We say that H is involved in G if there exists $K \triangleleft L \leq G$ so that $H \cong L/K$

Definition 5.4. We say that t is the thickness of G if t is the maximal degree of an alternating group A_t involved in G. That is, A_t is involved in G but A_{t+1} is not involved in G. We denote the thickness of G by $\theta(G)$.

Definition 5.5. For any graph X we can construct $L(X)$, the line graph of X, so that vertices of $L(X)$ are edges of X, and two vertices in $L(X)$ are adjacent if their corresponding edges are incident on a common vertex in X.

Definition 5.6. The complement of a graph X, denoted $\bar{X}$, is a graph on the same vertex set as X with $(u, v) \in \bar{E} \iff (u, v) \notin E$

Theorem 5.7. ***(Babai, Cameron, Pálfy 1982)*** *If G is a primitive permutation group of degree n and thickness t, then $|G| \leq n^{O(t)}$*

Example 5.8. (Thickness of automorphism groups)

1. Consider $X = K_n$. Its automorphism group has thickness n, as $\mathrm{Aut}(X) = S_n$
2. Consider $L(K_n)$ which has vertex set of size $\binom{n}{2}$ and is strongly regular with parameters $(\binom{n}{2}, 2(n-2), n-2, 4)$. We want to understand $\mathrm{Aut}(L(K_n))$, and we immediately observe that S_n is a subgroup by its induced action on pairs of vertices. If $n \geq 5$ then all cliques of size ≥ 4 in $L(K_n)$ correspond to "stars" (i.e., lots of edges incident on a single vertex) in K_n. We then have exactly n maximal cliques of size $n-1$ in $L(K_n)$. We observe that an automorphism of $L(K_n)$ is entirely determined by how it permutes these maximal cliques. Thus we have $n!$ automorphisms of $L(K_n)$

DO 5.9. Find $\mathrm{Aut}(L(K_{n,n}))$ and deduce that $\theta(\mathrm{Aut}(L(K_{n,n}))) = n$

Definition 5.10. We say that a strongly regular graph X is trivial if it or its complement is disconnected

Definition 5.11. The neighborhood of a vertex v is the set of all verteces adjacent to v. It is denoted $N(v)$

Definition 5.12. We say that a strongly regular graph X is graphic if it or its complement is a line graph

HW 5.13. Find all trivial strongly regular graphs

HW 5.14. If X is strongly regular then its complement is strongly regular

HW 5.15. Find all graphic strongly regular graphs

Our target is the following result.

Theorem 5.16 (Babai 2014)**.** *Let X be a strongly regular graph that is not trivial or graphic. Then*

$$\theta(\mathrm{Aut}(X)) = O\left(\frac{\ln^2(n)}{\ln(\ln(n))}\right)$$

Reference:
László Babai: On the Automorphism Groups of Strongly Regular Graphs I. In: Proc. 5th Innovations in Theoretical Comp. Sci. conf. (ITCS'14), ACM Press, January 2014, pp 359-368. Click here for the PDF: http://people.cs.uchicago.edu/∼laci/papers/14itcs.pdf

Lemma 5.17. *Let $G \leq S_n$ be a permutation group on $[n]$ and suppose that any element of G has order $\leq n^c$. Then*

$$\theta(G) \leq \frac{\ln^2(n)}{2\ln(\ln(n))} c^2 (1 + o(1))$$

Proof. Suppose A_t is involved in G. Let $z(t)$ be an element of maximum order in A_t. How do we get elements of largest possible order? We find elements g_i of prime order p_i and then the order of their product is the product of the p_i. The only condition we must obey is that $\sum_i p_i \leq n$. We have $z \leq n^c$ immediately and using the prime number theorem we can get $z^t = \exp(\sqrt{t \log t (1 + o(1))})$. Solving for t gives the desired result. □

Lemma 5.18. ***(Babai, Seress 1987)*** *Let $\sigma \in S_n$ and $|\sigma| = n^\alpha$. Then there exist m so that $\sigma^m \neq 1$ and σ^m fixes at least $n(1 - 1/\alpha)$ elements. (Here α is a real number > 1.)*

Proof. Let $G = \langle\sigma\rangle$. Consider the prime factorization of $|\sigma| = n^\alpha = \prod_{i=1}^r q_i$ where $\{q_1, \ldots, q_k\}$ are powrs of distinct primes. Then

$$\alpha \log(n) = \sum_i \log(q_i). \tag{19}$$

For $x \in [n]$, define $P(x) = \{i \mid q_i \big| |x^G|\}$. Note that for all $x \in [n]$ we have

$$\prod_{i \in P(x)} q_i \leq n \text{ and therefore } \sum_{i \in P(x)} \log q_i \leq \log n. \tag{20}$$

Let $n_i = |\{x \mid i \in P(x)\}|$. Let us estimate the weighted average W of the n_i with weights $\log q_i$. Then

$$W = \frac{\sum_i n_i \log(q_i)}{\sum_i \log(q_i)} = \frac{1}{\alpha \log(n)} \sum_{x \in [n]} \sum_{i \in P(x)} \log(q_i) \leq \frac{n \log(n)}{\alpha \log(n)} = \frac{n}{\alpha}.$$

So $W \leq n/\alpha$ and therefore there exists i such that $n_i \leq n/\alpha$. Now let $m = |\sigma|/p_i$ be the corresponding maximal divisor of $|\sigma|$. So $\sigma^m \neq 1$ and it fixes all but n_i points. □

From now we assume without loss of generality that the degree k of X is at most $(n-1)/2$, since the automorphisms of a graph are precisely the automorphisms of its complement.

Lemming 5.21. *Let X be a nontrivial strongly regular graph. Then*

$$k - \min(\lambda, \mu) \leq 2(k - \max(\lambda, \mu))$$

and

$$k^2 > n \cdot \min(\lambda, \mu)$$

Corollary 5.22.

$$\frac{1}{2} > \frac{k}{n} \frac{\min(\lambda, \mu)}{k}$$

and

$$\max(\lambda, \mu) < \frac{3k}{4}$$

Definition 5.23. We say that a vertex z distinguishes x and y if it is adjacent to exactly one of x and y

Corollary 5.24. *Any pair of vertices in X is distinguished by at least $k = \min(\lambda, \mu)$ other vertices.*

Proof. x and y are distinguished by $N(x) \Delta N(y)$ which has size $2(|N(x)| - |N(x) \cap N(y)|) \geq 2(k - \max(\lambda, \mu))$ □

Lemma 5.25. *Any automorphism of a nontrivial strongly regular graph X fixes at most $n - k/2$ vertices.*

Proof. Suppose F is the set of fixed vertices of some automorphism σ. Let $x \in V \setminus F$, so that $\sigma(x) \neq x$. Let $D(x)$ be the set of vertices that distinguish x and $\sigma(x)$. Note that $D(x) \cap F \neq 0$, implying that

$$|F| \leq n - |D(x)| \leq n - k + \min(\lambda, \mu) < n - k/2$$

□

Proposition 5.26. *If X is a nontrivial strongly regular graph and $k \geq n/4$ then the order of any element in* $\mathrm{Aut}(X)$ *is* $\leq n^8$

Proof of Theorem 5.16 to be continued.