CO 444/644 Algebraic Graph Theory

Keven Qiu
Instructor: Jane Gao

Contents

Chapter 1

Introduction

We will focus on simple, undirected graphs without loops unless explicitly stated. We use $X = (V, E)$ to denote graphs and G for groups. $V(X)$ and $E(X)$ are the sets of vertices and edges of graph X respectively and $\deg(v)$ to denote the degree of a vertex $v \in V(X)$.

Definition: Isomorphism

An isomorphism between graphs X, Y is a function $f : V(X) \to V(Y)$ such that $uv \in E(X)$ if and only if $f(u)f(v) \in E(Y)$.

1.1 Automorphisms

Definition: Automorphism

An automorphism of the graph X is an isomorphism $f : X \to X$.

$\mathrm{Aut}(X)$ is the set of all automorphisms of X.

$\mathrm{Sym}(V)$ is used to denote the symmetric group of permutations on V. In group theory, we may have used $V = [n]$. We may use this notation alongside $\mathrm{Sym}(n)$ when explicitly enumerating the vertices of a graph from 1 to n.

Proposition

$\mathrm{Aut}(X) \leq \mathrm{Sym}(V(X))$ with the group operation for $\sigma, \tau \in \mathrm{Aut}(X)$ defined $\sigma\tau := \tau \circ \sigma$.

For $g \in \mathrm{Sym}(V(X))$ and $v \in V(X)$, let v^g denote $g(v)$. Let S^g denote $\{g(v) : v \in S\}$ for set S.

Suppose $Y \subseteq X$ is a subgraph and $g \in \mathrm{Aut}(X)$. Y^g is the graph defined $V(Y^g) = V(Y)^g$ and $E(Y^g) = \{u^g v^g : uv \in E(Y)\}$.

E.g. The following is an example of graphs X and Y along with functions that are and are not automorphisms.

Let $X = (\{1,2,3,4\}, \{12,13,14,23,34\}), Y = (\{1,2,3\}, \{12,13,23\}), Y^g = (\{1,3,4\}, \{13,14,34\})$ where $g(1) = 3, g(2) = 4, g(3) = 1, g(4) = 2$. $f(1) = 1, f(2) = 4, f(3) = 3, f(4) = 2$ is an automorphism while Y^g where $f(1) = 3, f(2) = 3, f(3) = 4, f(4) = 1$ is not an automorphism.

Lemma

For $v \in V(X)$ and $g \in \mathrm{Aut}(X)$, $\deg(v) = \deg(v^g)$.

Proof. Let $Y(v)$ be the subgraph of X induced by v and the neighbors $N_X(v)$. Then

$$Y(v) \cong Y(v)^g = Y(v^g)$$

so $\deg(v) = \deg(v^g)$.

Lemma

Let $u, v \in V(X)$ and $g \in \mathrm{Aut}(X)$, then the length of the shortest paths are preserved, i.e. $d(u,v) = d(u^g, v^g)$.

Proof. Show that a shortest uv-path in X is mapped to a shortest $u^g v^g$-path by g.

1.2 Homomorphisms

Definition: Homomorphism

Let X and Y be graphs. We say $f : V(X) \to V(Y)$ is a homomorphism if $x \sim y$ implies $f(x) \sim f(y)$ in Y.

$\sim$ is for adjacency and $f : X \to Y$ instead of $f : V(X) \to V(Y)$ for simplicity.

Let $\chi(X)$ denote the chromatic number of X, the minimum number of colors needed to color the vertices of a graph such that no two adjacent vertices have the same color.

Let K_r denote the complete graph on r vertices where every pair of distinct vertices is connected by an edge. We say that K_r is a clique, where it generally is a subset of vertices of a graph such that every two distinct vertices in the clique are adjacent.

Lemma

$$\chi(X) = \min\{r \in \mathbb{N} : \exists \text{ homomorphism } X \to K_r\}$$

Proof. Let $k = \chi(X)$. We first show $k \geq \min\{r \in \mathbb{N} : \exists \text{ homomorphism } X \to K_r\}$. Let f be a k-coloring of X. Then f is a homomorphism from X to K_k.

Next, we show that $k \leq \min\{r \in \mathbb{N} : \exists \text{ homomorphism } X \to K_r\}$. Let $\overline{r} = \min\{r \in \mathbb{N} : \exists \text{ homomorphism } X \to K_r\}$. Let $h : X \to K_{\overline{r}}$ be a homomorphism. Then $h^{-1}(v)$ is an independent set. So, giving $h^{-1}(v)$ distinct colors yields an $\overline{r}$-coloring.

Definition: Retraction

A homomorphism $f : X \to Y$ such that

1. $Y \subseteq X$.

2. $f|_Y = id$, the identity map.

If a retraction from X to Y exists, we call Y a retract of X.

We use the notation $f|_Y$ to mean the function f when restricted to the domain of Y.

E.g. Suppose $K_r \cong Y \subseteq X$ and $\chi(X) = r$. We will prove that Y is a retract of X. The proof is as follows: let $f : V(X) \to [r]$ where $r = \chi(X)$ be an r-coloring of X. Then, Y receives distinct colors since $Y \cong K_r$. Without loss of generality, assume $V(Y) = [r]$. Then f is a homomorphism from X to K_r and $f|_Y = id$. Therefore, f is a retraction.

E.g. Recall that a cycle graph C_n is defined $V(C_n) = \{0, \dots, n-1\}$ where $n \geq 3$ and $E(C_n) = \{ij : i - j \equiv \pm 1 \pmod n\}$. Let $g = (1, 2, \dots, n-1, 0) \in \mathrm{Aut}(C_n)$. This can be viewed as a rotation. We can define the subgroup

$$R = \{g^m : 0 \leq m \leq n-1\} \leq \mathrm{Aut}(C_n)$$

to capture all possible rotations.

We can define reflections. Let h be defined $h(i) = -i \pmod n \in \mathrm{Aut}(C_n)$. We can see that R and Rh are disjoint cosets of $\mathrm{Aut}(C_n)$ and $Rh \leq \mathrm{Aut}(C_n)$. It follows that $|\mathrm{Aut}(C_n)| \geq 2n$.

Definition: Circulant Graph

Let $\mathbb{Z}_n = \{0, \dots, n-1\}$ and $C \subseteq \mathbb{Z}_n \setminus \{0\}$ be closed under inverse, that is, $x \in C \implies -x \in C$. We define the circulant graph $X = X(\mathbb{Z}_n, C)$ where $V(X) = \mathbb{Z}_n, E(X) = \{ij : i - j \in C\}$.

One can show that the arguments from the previous example for C_n also hold for $X = X(\mathbb{Z}_n, C)$. That is, $|\mathrm{Aut}(X(\mathbb{Z}_n, C))| \geq 2n$. We can generalize this result for arbitrary groups using Cayley graphs.

Definition: Johnson Graph

Given $v \geq k \geq i$ as integers where $[v] = \{1, \dots, v\}$, the Johnson graph $J = J(v, k, i)$ is defined $V(J) = \{S \subseteq [v] : |S| = k\}, E(J) = \{ST : |S \cap T| = i\}$.

$J(5, 2, 0)$ is the Peterson graph. $J(v, k, 0)$ is the Kneser graph.

Proposition

There exists a subgroup of $\mathrm{Aut}(J(v, k, i))$ that is isomorphic to $\mathrm{Sym}(v)$.

Proof. For $g \in \mathrm{Sym}(v)$, define $\tau_g : \binom{[v]}{k} \to \binom{[v]}{k}$ as $\tau(S) = S^g$. Note that $|S \cap T| = |S^g \cap T^g|$ for vertices $S, T \in J(v, k, i)$ since we are essentially just relabeling elements of S and T, so

$\tau_g \in \mathrm{Aut}(J(v,k,i))$. We can conclude that

$$\{\tau_g : g \in \mathrm{Sym}(v)\} \cong \mathrm{Sym}(v)$$

Chapter 2

Groups

Definition: Homomorphism

Given groups G and H, $f : G \to H$ is a homomorphism if for all $g, h \in G$,

$$f(gh) = f(g)f(h)$$

Definition: Kernel

The kernel of a homomorphism f is defined

$$\ker(f) = f^{-1}(1)$$

Definition: Group Action

Suppose G is a group and V is a set. A homomorphism $f : G \to \mathrm{Sym}(V)$ is a permutation representation of G and we call it an action of G on V.

E.g. Let X be a graph and take $V = V(X)$. Let $G = \mathrm{Aut}(X)$. Then $f : G \to \mathrm{Sym}(V)$ defined $f(g) = g$ for $g \in G$ is an action.

E.g. Let G be a group. Let $f : G \to \mathrm{Sym}(V)$ where V is arbitrary be defined $f(g) = id$ where id is the identity permutation. f is an action.

Definition: Faithful Action

The action f is faithful if $\ker(f) = \{1\}$.

We can see that the first action example above is faithful, but not the second.

Let group G act on V, via $f : G \to \mathrm{Sym}(V)$. Let $g \in G$, we use the notation

$$x^g := g^{f(g)} \text{ and } S^G := S^{f(g)}$$

where S is an arbitrary set.

Definition: G-Invariant

Let group G act on V and $g \in G$. S is G-invariant if $S = S^g$ for all $g \in G$.

Definition: Orbit

Let group G act on V. The orbit of $x \in V$ is

$$x^G := \{x^g : g \in G\}$$

One may show that V is partitioned into disjoint orbits and each orbit is G-invariant and transitive (for every x, y in the same orbit, there exists $g \in G$ where $x^g = y$).

Definition: Stabilizer

Let $G \leq \mathrm{Sym}(V)$ and $x \in V$. The stabilizer of x is

$$G_x := \{g \in G : x^g = x\}$$

Lemma

Let $G \leq \mathrm{Sym}(V)$ and $x \in V$, then $G_x \leq G$.

Lemma

Let $G \leq \mathrm{Sym}(V)$ and let S be an orbit of G. Let $x, y \in S$, then

$$H := \{h \in G : x^h = y\}$$

is a right coset of G_x. Conversely, if H is a right coset of G_x, then for all $h, h' \in H$, $x^h = x^{h'}$.

Proof. ($\implies$) G is transitive on S, so there exists $g \in G$ where $x^g = y$. For any $h \in H$, $x^h = y$ by the definition of H. So, $x^h = x^g$. Then,

$$x^{hg^{-1}} = x \implies hg^{-1} \in G_x \implies h \in G_x g$$

($\impliedby$) Assume $H = G_x g$ for some $g \in G$. Let $h, h' \in H$ where $h = \sigma g$ and $h' = \sigma' g$ for some $\sigma, \sigma' \in G_x$. We have

$$x^h = x^{\sigma g} = x^g = x^{\sigma' g} = x^{h'}$$

Lemma (Orbit-Stabilizer)

Let G be a permutation group acting on V with $x \in V$. Then

$$|G_x| \left|x^G\right| = |G|$$

Proof. Let $\mathcal{H}$ be the set of right cosets of G_x and define $f : x^G \to \mathcal{H}$ as

$$f(y) = \{g \in G : x^g = y\}$$

The previous lemma shows that f is a bijection. Therefore, $|\mathcal{H}| = \left|x^G\right|$. Since the right cosets of G_x partition G, we have

$$|G| = |G_x|\,|\mathcal{H}| = |G_x|\left|x^G\right|$$

Definition: Conjugate

Let G be a permutation group and let $g, h \in G$. g is conjugate to h if there is some $\sigma \in G$ such that

$$g = \sigma h \sigma^{-1}$$

Proposition

If H is a subgroup of G and $g \in G$, then $gHg^{-1} \leq G$ and $gHg^{-1} \cong H$.

Lemma

If $y \in x^G$, then G_x and G_y are conjugate.

Proof. Suppose $y = x^g$ where $g \in G$. We will prove that $g^{-1}G_x g = G_y$.

($\subseteq$) Note that $y^{g^{-1}} = x$. For every $h \in G_x$, $y^{g^{-1}hg} = x^{hg} = g^g = y$.

($\supseteq$) For $h \in G_y$, $x^{ghg^{-1}} = y^{hg^{-1}} = y^{g^{-1}} = x$. Then $ghg^{-1} \in G_x$, rearranging gives $h \in g^{-1}G_x g$.

Definition: Fix

Let $G \leq \mathrm{Sym}(V)$ and $g \in G$. Then

$$\mathrm{fix}(g) = \{v \in V : v^g = v\}$$

Lemma (Burnside)

Let $G \leq \mathrm{Sym}(V)$. Then

$$\#\text{ of orbits of } G = \frac{1}{|G|}\sum_{g \in G} |\mathrm{fix}(g)|$$

Proof. Let $\Lambda = \{(g, x) : g \in G, x \in V, x \in \mathrm{fix}(g)\}$. We will apply a double-counting argument. Observe that

$$|\Lambda| = \sum_{g \in G} |\mathrm{fix}(g)| = \sum_{x \in V} |G_x|$$

Equating these gives

$$\begin{aligned}
\sum_{g\in G}|\mathrm{fix}(g)| &= \sum_{x\in V}|G_x| \\
&= \sum_{x\in V}\frac{|G|}{|x^G|} && \text{(Orbit-Stabilizer)} \\
&= |G|\sum_{x\in V}\frac{1}{|x^G|} \\
&= |G|\,(\#\text{ of orbits of } G)
\end{aligned}$$

Definition: Asymmetric Graph

A graph X is asymmetric if $\mathrm{Aut}(X) = \{id\}$.

Theorem

Let $\mathcal{G}_n = \{X \text{ on } [n]\}$ and $X \in \mathcal{G}_n$ be chosen uniformly random, then

$$\lim_{n\to\infty} \Pr(X \text{ is asymmetric}) = 1$$

Proof. Let $X \in \mathcal{G}_n$, $\mathrm{Iso}(X) = \{Y \in \mathcal{G}_n : X \cong Y\}$.

Lemma: $|\mathrm{Iso}(X)| = \frac{n!}{|\mathrm{Aut}(X)|}$.

Proof. (Lemma) Let $G = \mathrm{Sym}([n])$. For $g \in G$, let $\tau_g : \mathcal{G}_n \to \mathcal{G}_n$ where $X \mapsto X^g$. Let $H := \{\tau_g : g \in G\}$ acts on $\mathcal{G}_n$ and $H \cong G$.

$$n! = |G| = |H| = |H_X| \cdot \left|X^H\right| = |\mathrm{Aut}(X)|\,|\mathrm{Iso}(X)|$$

Let $\mathcal{H}$ be the set of isomorphism classes of graph on $[n]$. Let $\mathcal{H} \in \mathcal{H}$. If $X \in \mathcal{C}$ is asymmetric, then $|\mathcal{C}| = n!$. If X is symmetric, then $|\mathcal{C}| \le \frac{n!}{2}$.

Let ρ be the proportion of $\mathcal{C} \in \mathcal{H}$ such that $|\mathcal{C}| = n!$. Now,

$$2^{\binom{n}{2}} = |\mathcal{G}_n| = \sum_{\mathcal{C}\in\mathcal{H}} |\mathcal{C}| \le \rho\,|\mathcal{H}|\,n! + (1-\rho)\,|\mathcal{H}|\,\frac{n!}{2}$$

Claim: $|\mathcal{H}| = (1+o(1))\frac{2^{\binom{n}{2}}}{n!}$, where $o(1)$ denotes some $x_n \in \mathbb{R}$ such that $\lim_{n\to\infty} x_n = 0$.

By claim, $2^{\binom{n}{2}} \le (1+o(1))\frac{2^{\binom{n}{2}}}{n!}\cdot n!\left(\rho + \frac{1-\rho}{2}\right) = (1+o(1))2^{\binom{n}{2}}\cdot\frac{1+\rho}{2}$.

Thus, $\rho = 1 + o(1)$. Then the proportion of asymmetric graphs in $\mathcal{G}_n$ is $\rho\,|\mathcal{H}|\,n!/2^{\binom{n}{2}} = 1 + o(1)$.

Proof. (Claim) Consider $\mathcal{P} = \{\tau_g : g \in \mathrm{Sym}([n])\}$ acting on $\mathcal{G}_n$ where $\tau_g(x) = x^g$. The set of orbits is $\mathcal{H}$. Burnside's Lemma tells us $|\mathcal{H}| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{fix}(\tau_g)|$.

Observation: Every g induces a permutation G_g on $E(K_{[n]})$. Let C be an orbit under σ_g. Then, if X is fixed by τ_g, then X either contains all edges in C or no edges in C.

Let $\text{orb}_2(\sigma_g)$ be the number of orbits under σ_g. Thus, $|\text{fix}(\tau_g)| = 2^{\text{orb}_2(\sigma_g)}$. If $g = id$, then $\text{orb}_2(\sigma_g) = \binom{n}{2}$. If $g = (i, j)$ for some $i, j \in [n]$, $\text{orb}_2(g) = (n-2) + \binom{n}{2} - 2(n-2)$.

The contribution to Burnside's Lemma from a simple transposition is $\binom{n}{2}2^{\binom{n}{2}-(n-2)} = 2^{\binom{n}{2}} \cdot \binom{n}{2}2^{-(n-2)}$. With some technical work we skip, we can show that $\sum_{\substack{g\in G\\ g\neq id}} |\text{fix}(\tau_g)| = o(1) \cdot |\text{fix}(\tau_{id})|$

$$\frac{1}{n!}\,|\text{fix}(\tau_{id})| \leq |\mathcal{H}| = \frac{1}{n!}(1+o(1))\,|\text{fix}(\tau_{id})| \implies |\mathcal{H}| = (1+o(1))\frac{2^{\binom{n}{2}}}{n!}$$

Definition: Block of Imprimitivity

Let G be a transitive permutation group on V and $S \subseteq V$. S is a block of imprimitivity for G if $S \neq \emptyset$ and $\forall g \in G$, $S^g = S$ or $S^g \cap S = \emptyset$.

$S = \{u\}$ for all $u \in V$ and $S = V$ are trivial blocks of imprimitivity.

Definition: Primitive

G is primitive if there does not exist non-trivial blocks of imprimitivity. Otherwise, G is imprimitive.

Remark: We assume transitivity since if G has an orbit $S = x^G$ such that $|S| \geq 2, S \neq V$, then S is a block of imprimitivity.

E.g. If $G = \text{Aut}(K_n)$, G is primitive.

E.g. Let $G = \text{Aut}(C_4)$, G is not primitive.

E.g. Let $G = \text{Aut}(C_{2n})$

Lemma

Let G be a transitive permutation group on V. Let $x \in V$. Then, G is primitive if and only if G_x is a maximal subgroup of G (no K such that $G_x < K < G$).

Proof. We prove G is imprimitive if and only if there exists K such that $G_x < K < G$.

($\implies$) Let S be a block of imprimitivity with $2 \leq |S| < |V|$. With loss of generality, we may assume that $x \in S$ since G is transitive. Let $G_S = \{g \in G : S^g = S\}$ which is a subgroup of G. We prove that $G_x < G_S$.

Let $g \in G_x$. Then $x \in S \cap S^g$, so $S^g = S$ (by definition of block of imprimitivity. Since $|S| \geq 2$, $\exists y \in S, y \neq x$. Let $h \in G$ such that $x^h = y$, this implies $h \notin G_x$. Then, $y \in S \cap S^h \implies S = S^h \implies h \in G_S$. These two points give us $G_x < G_S$. $G_S < G$ since $S = S^g$ for all $g \in G_S$ but G is transitive.

($\impliedby$) Suppose there exists K with $G_x < K < G$. Let $S = x^K$. $2 \leq |S| < |V|$ (assignment).

Claim: For all $g \in G$, if $S \cap S^g \neq \emptyset$, then $g \in K$ and $S = S^g$.

Proof. (Claim) Assume $y \in S \cap S^g$. $y \in S \implies \exists h \in K : y = x^h$. $y \in S^g \implies \exists h' \in K : y = x^{h'g}$. Combining, we get $x = x^{h'gh^{-1}} \implies h'gh^{-1} \in G_x < K \implies g \in (h')^{-1}Kh \in K$.

E.g. Consider K_3 and the vertex 1. $G_1 = \{id, (1)(23)\}, G = \text{Aut}(K_3)$. There is no bigger subgroup, so G_1 is maximal.

E.g. Consider C_4 and 1. $G_1 = \{id, (1)(3)(24)\}, K = \{id, (1)(3)(24), (13)(24), (13)(2)(4)\}$. Here $G_1 < K < \text{Aut}(C_4)$. We constructed $K = \{g \in \text{Aut}(C_4) : \{1, 3\}^g = \{1, 3\}\}$.

Chapter 3

Transitive Graphs

3.1 Vertex-Transitive Graphs

Definition: Vertex-Transitive Graphs

X is vertex-transitive if $\text{Aut}(X)$ acts transitively on $V(X)$.

Definition: k-Cube Q_k

$V(Q_k) = 2^{[k]}, E(Q_k) = \{ij : H(i,j) = 1\}$ where H is the Hamming distance (positions where the binary string is different).

Lemma

Q_k is vertex-transitive.

Proof. For all $v \in 2^{[k]}$, define $\rho_v : 2^{[k]} \to 2^{[k]}$ such that $x \mapsto x + v$. Since $H(x,y) = H(x+v, y+v)$, $\rho_v \in \text{Aut}(Q_k)$. So $\{\rho_v : v \in 2^{[k]}\} \leq \text{Aut}(Q_k)$, which acts transitively on $V(Q_k)$.

Proof. For all $v \in \text{Sym}([k])$, define $\tau_v : 2^{[k]} \to 2^{[k]}$, $S \mapsto S^v$. Since $H(x,y) = H(\tau_v(x), \tau_v(y))$, $\{\tau_v : v \in \text{Sym}([k])\} \leq \text{Aut}(Q_k)$.

Note $\{\rho_v : v \in 2^{[k]}\} \cap \{\tau_v : v \in \text{Sym}([k])\} = \{id\}$. $\{\rho_v : v \in 2^{[k]}\}\{\tau_v : v \in \text{Sym}([k])\} \subseteq \text{Aut}(Q_k)$ and $\left|\{\rho_v : v \in 2^{[k]}\}\{\tau_v : v \in \text{Sym}([k])\}\right| = \frac{\left|\{\rho_v : v \in 2^{[k]}\}\right|\left|\{\tau_v : v \in \text{Sym}([k])\}\right|}{\left|\{\rho_v : v \in 2^{[k]}\} \cap \{\tau_v : v \in \text{Sym}([k])\}\right|} = 2^k k!$.

Remark: Cycles and Circulant graphs are vertex-transitive.

Definition: Cayley Graph

Given group G and $C \subseteq G$ satisfying

- $1 \notin C$
- $x \in C \implies x^{-1} \in C$

Then $X = X(G, C)$ such that $V(X) = G$ and $E(X) = \{gh : hg^{-1} \in C\} = \{gh : gh^{-1} \in C\}$.

Lemma

Cayley graphs are vertex-transitive.

Proof. For any $v \in G$, define $\rho_v : G \to G, x \mapsto xv$. $xy \in E(X(G,C)) \Leftrightarrow xy^{-1} \in C \Leftrightarrow (xv)(yv)^{-1} \in C \Leftrightarrow \{\rho_v(x), \rho_v(y)\} \in E(X(G,C))$.

Lemma

Johnson graphs are vertex-transitive.

3.2 Edge-Transitive Graphs

A group acting on V naturally induces an action on

$$\binom{V}{2} \& (V)_2 = \{ij \in V^2 : i \neq j\}$$

by $\{u, v\}^g := \{u^g, v^g\}$ and $(u, v)^g = (u^g, v^g)$.

Definition: Edge-Transitive Graph

X is edge-transitive if $\mathrm{Aut}(X)$ acts transitively on $E(X)$.

Definition: Arc-Transitive Graph

X is arc-transitive if $\mathrm{Aut}(X)$ acts transitively on $\{ij : ij \in E(X)\}$

Proposition

Arc-transitive $\implies$ vertex-transitive and edge-transitive.

Proposition

There exist graphs that are edge-transitive, but not vertex-transitive.

Proposition

There exist graphs vertex-transitive, but not edge-transitive.

Theorem

Edge-transitive graphs that are not vertex-transitive are bipartite.

Proof. Without loss of generality, we may assume that X has no isolated vertices.

2-orbits: Let $xy \in E(X)$. For $w \in V(X)$, $wz \in E(X)$ for some $z \in V(X)$. There exists $\sigma \in \mathrm{Aut}(X)$, $\{x^\sigma, y^\sigma\} = \{w, z\}$. This implies every vertex in X is either in x^G or y^G. However, X is not vertex-transitive, $x^G \neq y^G$, this gives the bipartition.

If $wz \in E(X)$ and $wz \in x^G$ (or $wz \in y^G$), this implies no $\sigma \in \mathrm{Aut}(X)$ would map xy to wz since $x^G \cap y^G = \emptyset$.