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 $f : G \to \text{Sym}(V)$ 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 $G = \text{Aut}(X)$. Then $f : G \to \text{Sym}(V)$ defined $f(g) = g$ for $g \in G$ is an action.

E.g. Let G be a group. Let $f : G \to \text{Sym}(V)$ 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 $f : G \to \text{Sym}(V)$. 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. ($\Longrightarrow$) 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,

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

($\Longleftarrow$) 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

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

Definition: Asymmetric Graph

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

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

Lemma: $|\text{Iso}(X)| = \frac{n!}{|\text{Aut}(X)|}$.
Proof. (Lemma) Let $G = \text{Sym}([n])$. 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 $H \cong G$.

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

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 $|\mathcal{C}| \leq \frac{n!}{2}$.

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

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

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

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

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 $\mathrm{Aut}(X)$ 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 $H(x,y) = H(x+v, y+v)$, $\rho_v \in \mathrm{Aut}(Q_k)$. So $\{\rho_v : v \in 2^{[k]}\} \leq \mathrm{Aut}(Q_k)$, which acts transitively on $V(Q_k)$.

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

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

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 with no isolated vertices 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 $\sigma \in \text{Aut}(X)$, $\{x^\sigma, y^\sigma\} = \{w, z\}$. 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 $\sigma \in \text{Aut}(X)$ would map xy to wz since $x^G \cap y^G = \emptyset$.

Theorem

If X is vertex, edge-transitive, k-regular, k-odd, then X is arc-transitive.

Lemma

If X is a vertex, edge-transitive, k-regular, not arc-transitive, then k is even.

Proof. Define $D(X)$ with $V(D(X)) = V(X)$ and $E(D(X)) = \{(x, y) : xy \in E(X)\}$. Let $xy \in E(X), \Omega_1 = (x, y)^G, \Omega_2 = (y, x)^G, G = \text{Aut}(X)$. X is edge-transitive implies $\Omega_1 \cup \Omega_2 = E(D(X))$. X is not arc-transitive implies $\Omega_1 \cap \Omega_2 = \emptyset$.

Thus, $\forall uv \in E(X)$, $(u, v) \in \Omega_1 \implies (v, u) \in \Omega_2$. $\text{Aut}(X) = \text{Aut}(\Omega_1)$ which acts transitively on $V(D(X)) = V(\Omega_1)$, so $d^+_{\Omega_1} = d^-_{\Omega_1} = d^+_{\Omega_2} = d^+_{\Omega_2}$ where $+$ means in-degree and $-$ means out-degree. Therefore, $k = d^+_{\Omega_1} + d^-_{\Omega_1} \equiv 0 \pmod 2$.

3.3 Edge-Connectivity

Definition: Edge Atom

An edge atom of X is a minimum $S \subseteq V(X)$ such that $|\delta(S)| = \kappa_1(X)$.

In this course $\partial(S) = \delta(S)$.

Lemma

Any two distinct edge atoms are disjoint.

Proof. Let $\kappa = \kappa_1(X)$. Let A, B be distinct edge atoms. By minimality, $|A|, |B| \leq \frac{|V(X)|}{2}$. Suppose $A \cap B \neq \emptyset$:

Case 1: $A \cup B = V(X)$, then $|A| = |B| = \frac{|V(X)|}{2}$ implies $A \cap B = \emptyset$, a contradiction.

Case 2: $A \cup B \subsetneq V(X)$, then $|\partial(A \cup B)| \geq \kappa, |\partial(A \cap B)| \geq \kappa + 1$.

$$\kappa + \kappa + 1 \leq |\partial(A \cup B)| + |\partial(A \cap B)| \leq |\partial(A)| + |\partial(B)| = 2\kappa$$

This is a contradiction.

Lemma

Suppose S is a block of imprimitivity under $\mathrm{Aut}(X)$, then $X[S]$ is regular.

Proof. Let $u, v \in S, u \neq v$. Let $Y = X[S]$. X is vertex-transitive by assumption, this implies $\exists g \in \mathrm{Aut}(X)$, $u^g = v \implies S = S^g$. Hence, $\{g|_S : g \in \mathrm{Aut}(X)\} \subseteq \mathrm{Aut}(Y)$. $\deg_Y(u) = \deg_Y(u^g) = \deg_Y(v)$ since automorphism preserves degree.

Theorem

If X is connected, k-regular, and vertex-transitive, then $\kappa_1(X) = k$.

Proof. Obviously, $\kappa_1(X) \leq k$. For $\kappa_1(X) \geq k$, let S be an edge atom. Let $g \in \mathrm{Aut}(X)$ and $B = S^g$. Then by the first lemma, either $S = B$ or $S \cap B = \emptyset$. So, S is a block of imprimitivity.

The second lemma implies $X[S]$ is ℓ-regular for some $0 \leq \ell \leq k-1$ because X is connected. Thus, $|\partial(S)| = |S|(k - \ell)$ such that $|S| \geq \ell + 1$. $|\partial(S)| \geq k$ (proof omitted).

This is $|\partial(S)| = k$ when $|S| = 1, \ell = 0$ or $|S| = k, \ell = k-1$.

Theorem

If X is connected and vertex-transitive, then

(a) X has a matching missing ≤ 1 vertex.

(b) Every edge in X is contained in a maximum matching.

Proof. **(a)** A vertex is critical if it is saturated by every maximum matching.

Case 1: There exists a critical vertex.
Every vertex is critical by vertex-transitivity, so X has a perfect matching.

Case 2: No critical vertex.
We prove $\forall u, v$, a maximum matching misses at most one of them by induction on $\ell = d(u, v)$.

Base case: $\ell = 1$, this is trivially true.

Assume $\ell \geq 2$. Inductive hypothesis applies to (x, y) where $d(x, y) \leq \ell - 1$. Take uv-path P with $|P| = \ell \geq 2$. There exists $x \notin \{u, v\}$ on P. x is not critical means there exists a maximum matching M_x missing x. The inductive hypothesis applies (u, x) and (v, x) implies M_x saturates u and v.

Suppose on the contrary, there exists a maximum matching M that misses both u and v. There exists an alternating ux-path and vx-path in $M \Delta M_x$ by claim (below). $u = v$, a contradiction.

Claim: Suppose (z, w) is a pair of vertices such that a maximum matching cannot miss both of them. Then $M_z \Delta M_w$ must contain an alternating zw-path.
Proof. (Claim) Suppose on the contrary that z and w lies in distinct components of $M_z \Delta M_w$. $M := M_w \Delta P$ is a maximum matching missing both z, w, a contradiction.

(b) By strong induction on number of vertices and number of edges.

Base case: Empty graph, this is trivial.

Inductive hypothesis: Suppose on the contrary that $\exists e \in E(X)$ that e is not in any maximum matching of X. This implies X is not edge-transitive.

Let Y be the subgraph of X induced by $e^{\mathrm{Aut}(X)}$. Y is vertex, edge-transitive, so $Y \neq X$. Inductive hypothesis applies to every component of Y.

Case 1: Y is connected.
By part (a) and that Y is vertex, edge-transitive, e is contained in a maximum matching of Y (which is a maximum matching of X).

Case 2: Y contains multiple components C_i.
Claim: $V(C_i)$ is a block of imprimitivity under $\mathrm{Aut}(X)$. $C_i \cong C_j$ for all $i, j \in [m]$.

Inductive hypothesis applies to each C_i. Case 2(a): each C_i has a perfect matching, this contradicts case 1. Case 2(b): each C_i has a matching missing 1 vertex.

Define Z where $V(Z) = \{C_1, \ldots, C_m\}, E(Z) = \{C_i C_j : \exists exy \in E(X), x \in C_i, y \in C_j\}$. It is easy to show that Z is connected and vertex-transitive. Part (a) implies Z has a matching missing ≤ 1 vertex. We have found a maximum matching of X containing e. A contradiction.

3.4 Cayley Graphs

Definition: Regular Group

A permutation group acting on V is regular if

- $G_x = \{1\}$ for all $x \in V$ (semi-regular)
- G is transitive.

Proposition

If G acts on V is regular, then $|G| = |V|$.

Proof. $|G| = |G_x| \left|x^G\right| = 1 \cdot \left|x^G\right| = |V|$.

Theorem

Let G be a group and $C \subseteq G \setminus \{1\}$ inverse-closed. Then, $\text{Aut}(X(G,C))$ contains a regular subgroup isomorphic to G.

Proof. **(a)** Let $X = X(G,C)$. Define $\tau_g : V(X) \to V(X), \sigma \to \sigma g$ for all $\sigma \in V(X) = G$.

- $\{\tau_g : g \in G\} \leq \text{Aut}(X)$.
- $\{\tau_g : g \in G\}$ acts transitively on G.
- $\{\tau_g : g \in G\} \cong G$.
- $\{\tau_g : g \in G\}$ is semi-regular.

Theorem

Suppose X is a graph. If $G \leq \text{Aut}(X)$ acts regularly on $V(X)$, then $X \cong X(G,C)$ for some inverse-closed $C \subseteq G \setminus \{1\}$.

Proof. G is regular, so $|G| = |V(X)|$. Fix $u \in V(X)$. $\exists$ a unique $g \in G$ such that $u^g = v$ for all $v \in V(X)$. Call this g as g_v. Let $C = \{g_v : v \sim u\}$.

First $1 \notin C$, $u \nsim u$. Next, we prove $X \cong X(G,C)$ by isomorphism $f(x) = g_x, \forall x \in V(X)$. $xy \in E(X)$ if and only if $\{x^{g_x^{-1}}, y^{g_x^{-1}}\} \in E(X)$ if and only if $\{u, u^{g_y g_x^{-1}}\} \in E(X)$ if and only if $g_y g_x^{-1} \in C$ since $u^{g_x} = x, u^{g_y} = y, g_x, y_y \in G \leq \text{Aut}(X)$.

By symmetric proof using g_y^{-1}, we obtain $xy \in E(X)$ if and only if $\{u, u^{g_x g_y^{-1}}\} \in E(X)$ if and only if $g_x g_y^{-1} \in C$, so C is inverse-closed.

Theorem

(a) If $\theta : G \to G$ is an automorphism, then $X(G,C) \cong X(G,\theta(C))$ and $C \subseteq G \setminus \{1\}$ is inverse-closed.

(b) $\exists (G, C_1, C_2)$ such that $X(G,C_1) \cong X(G,C_2)$, but there is no automorphism θ on G such that $C_2 = \theta(C_1)$.

Proof. **(a)** We prove that $\theta : V(X) \to V(X)$, $X = X(G,C)$ is an isomorphism.

$$\begin{aligned} hg^{-1} \in C &\Leftrightarrow \theta(hg^{-1}) \in \theta(C) \\ &\Leftrightarrow \theta(h)\theta(g)^{-1} \in \theta(C) \\ &\Leftrightarrow \theta(h)\theta(g^{-1}) \in \theta(C) \end{aligned}$$

Definition: Generating Set

Let G be a group. We say a subset $C \subseteq G$ be generating for G if every element in G can be expressed as a product of elements in C.

Proposition

$X(G, C)$ if connected if and only if C is generating for G.

Theorem

Every connected vertex-transitive graph is isomorphic to a retract of a Cayley graph.

Proof. Let $x \in V(X)$, $C = \{g \in \mathrm{Aut}(X) : x^g \sim x\}$, and G be the subgroup of $\mathrm{Aut}(X)$ that is generated by C. G acts transitively on $V(X)$. Let $Y = X(G, C)$. For every $y \in V(X)$, let $C_y := \{g \in G : x^g = y\}$. C_y is a right coset of G_x. $C = \bigcup_{y \sim x} C_y, C \cap G_x = \emptyset$ since $x \nsim x$.

Moreover, for any $a, b \in G$, $x^a \sim x^b \Leftrightarrow x \sim x^{ba^{-1}} \Leftrightarrow ba^{-1} \in C$.

Claim 1: $C = GxCG_x$.

Let $A_1, \ldots, A_k$ be the set of right cosets of G_x. Let $a_1 \in A_1, \ldots, a_k \in A_k$.
Claim 2: In $Y = X(G, C)$, $\forall 1 \leq i < j \leq k$, $e(A_i, A_j) = 0$ or $e(A_i, A_j) = |A_i|\,|A_j|$. Moreover, $\forall 1 \leq i \leq k$, $e(A_i) = 0$.

Claim 3: $Y[a_1, \ldots, a_k] \cong X$.

Claim 4: $Y[a_1, \ldots, a_k]$ is a retract of Y.

Proof. (Claim 1) $\subseteq$ is obvious. ($\supseteq$) Let $h, h' \in G_x$ and $g \in C$. Then $x \sim x^g$. Since $x^h = x = x^{h'} \implies x = x^h \sim x^{gh} = x^{h'gh}$. So we know that $h'gh \in C \implies G_xCG_x \subseteq C$.

Proof. (Claim 2) For any $g' \in G$, $g' \in A_j$ for some j. $G' = ga_j$ for some $g \in G_x$. Suppose $g, h \in G_x$, then $ga_i \sim ha_j \Leftrightarrow ga_i(ha_j)^{-1} \in C \Leftrightarrow ga_ia_j^{-1}h^{-1} \in C \Leftrightarrow a_ia_j^{-1} \in g^{-1}Ch \in G_xCG_x = C$ by claim 1.

Statement 2: Is implied immediately by $1 \notin C$ since $a_i = a_j$ in this case and $a_ia_i^{-1} = 1 \notin C$.

Proof. (Claim 3) As shown in claim 2, $\forall 1 \leq i < j \leq k$, $a_i \sim a_j$ in $Y[a_1, \ldots, a_j]$ if and only if $a_ia_j^{-1} \in C$.

Let $\rho : V(X) \to \{a_1, \ldots, a_k\}, y \mapsto a_j$ where $a_j \in C_y$. Verify that ρ is an isomorphism.

Proof. (Claim 4) Let $\tau : V(Y) \to \{a_1, \ldots, a_k\}, g \mapsto a_j$ if $g \in A_j$. Claim 2 implies τ is a homomorphism, $\tau|_{\{a_1,\ldots,a_k\}} = id$.

Chapter 4

Generalized Polygons

Definition: Incidence Structure

Given a set $\mathcal{P}$ of points and a set $\mathcal{L}$ of lines, and incidence relation $I \subseteq \mathcal{P} \times \mathcal{L}$. If $(p, L) \in I$, then the point p is in line L. The triple $\mathcal{I} = (\mathcal{P}, \mathcal{L}, I)$ defines an incidence structure.

Definition: Dual Incidence Structure

The triple $\mathcal{I}^* = (\mathcal{L}, \mathcal{P}, I^*)$ where

$$I^* = \{(L, p) \in \mathcal{L} \times \mathcal{P} : (p, L) \in I\}$$

is called the dual of $\mathcal{I}$.

Definition: Incidence Graph $X(\mathcal{I})$

Given $\mathcal{I} = (\mathcal{P}, \mathcal{L}, I)$, $X(\mathcal{I})$ is the incidence graph defined by the bipartite graph on $\mathcal{P} \cup \mathcal{L}$ such that $\{(p, L) \in E(X) : (p, L) \in I\}$.

$X(\mathcal{I}^*) \cong X(\mathcal{I})$.

Definition: Automorphism of $\mathcal{I}$

An automorphism of $(\mathcal{P}, \mathcal{L}, I)$ is a permutation σ on $\mathcal{P} \cup \mathcal{L}$ such that $\mathcal{P}^\sigma = \mathcal{P}, \mathcal{L}^\sigma = \mathcal{L}$ and $(p^\sigma, L^\sigma) \in I \Leftrightarrow (p, L) \in I$.

Definition: Partial Linear Space

$\mathcal{I} = (\mathcal{P}, \mathcal{L}, I)$ is a partial linear space if for any $x, y \in \mathcal{P}, x \neq y$, there is at most one line $L \in \mathcal{L}$ such that $(x, L) \in I$ and $(y, L \in I)$.

We say x, y are joined by L and x, y are collinear.

Lemma

If $\mathcal{I}$ is a partial linear space, then any two lines are incident with at most one point.

Lemma

If $\mathcal{I}$ is a partial linear space, then $X(\mathcal{I})$ has girth ≥ 6.

Proof. If X contains a 4-cycle p, L, q, M, then p and q are incident to 2 lines, which is forbidden by partial linear space. Since the girth of X is even (bipartite) and it cannot be 4, then the girth is at least 6.

Definition: Projective Planes

A partial linear space satisfying

(1) Any two lines meet at a unique point.

(2) Any two points are joined by a unique line.

(3) There exists three non-collinear points (a triangle).

Theorem

A partial linear space $\mathcal{I}$ is a projective plane if and only if $X(\mathcal{I})$ has diameter 3 and girth 6.

Proof. ($\implies$) Let $\mathcal{I} = (\mathcal{P}, \mathcal{L}, I)$ be a projective plane.

Definition:

Let $\mathbb{F}_q$ be a finite field of order q. Let $V = \mathbb{F}_q^3$.

$$PG(2, q) = (\mathcal{P}, \mathcal{L}, I)$$

where $\mathcal{P} = \{\langle u \rangle : u \in V \setminus \{0\}\}$, $\mathcal{L} = \{\langle u, v \rangle : u, v \in V \text{ linearly independent}\}$, $I = \{(p, L) \in \mathcal{P} \times \mathcal{L} : p \subseteq L\}$.

We can also write $\mathcal{L} = \{\langle u \rangle^\perp : u \in V \setminus \{0\}\}$. V contains $q^3 - 1$ non-zero vectors. This implies $|P| = \frac{q^3-1}{q-1} = 1 + q + q^2$ and $|\mathcal{L}| = 1 + q + q^2$

Every line contains $q^2 - 1$ non-zero vectors, and each line is incident with $\frac{q^2-1}{q-1} = 1 + q$ points. Similarly, every point is incident with $1 + q$ lines.

The Fano plane is $PG(2, 2)$.

Lemma

$PG(2, 9)$ is a projective plane.

Proof. Let $L_1 = \langle u, v \rangle \in \mathcal{L}$ and $L_2 = \langle u', v' \rangle \in \mathcal{L}$ such that $L_1 \neq L_2$. $\dim(L_1 + L_2) =$

$\dim(L_1) + \dim(L_2) - \dim(L_1 + L_2) \geq 2 + 2 + 3 = 1$, but $\dim(L_1 \cap L_2) \leq 1$ because $L_1 \neq L_2$, so $\dim(L_1 \cap L_2) = 1$.

Let $P_1 = \langle u \rangle \in P$ where $v \notin \langle u \rangle$. Suppose L is a line incident with both u and v. $\langle u, v \rangle \subseteq L$. Since $\dim(L) = 2$, $L = \langle u, v \rangle$.

Let u, v, w be linearly independent. Obviously $P_1 = \langle u \rangle, P_2 = \langle v \rangle, P_3 = \langle w \rangle$ form a triangle.

Definition: $GL(3, q)$

$$GL(3, q) = \{3 \times 3 \text{ invertible matrices over } \mathbb{F}_q\}$$

$GL(3, q)$ is a group and acts on P and $\mathcal{L}$.

Lemma

$GL(3, q) \leq \mathrm{Aut}(PG(2, q))$.

Proof. Take $A \in GL(3, q)$ and $p \sim L$ in $PG(2, q)$. Show that $p^A \sim L^A$.

Theorem

$X(PG(2, q))$ is arc-transitive.

Proof. For any (p_1, L_1) such that $p_1 \sim L_1$, (p_2, L_2) such that $p_2 \sim L_2$, write $p_1 = \langle u_1 \rangle, L_1 = \langle u_1, v_1 \rangle$ and $p_2 = \langle u_2 \rangle, L_2 = \langle u_2, v_2 \rangle$. There exists $A \in GL(3, q)$ where $Au_1 = u_2$ and $Av_1 = v_2$. This implies $(p_1, L_1)^A = (p_2, L_2)$. Define $\pi : P \times \mathcal{L} \to P \times \mathcal{L}$ where $\langle u \rangle \mapsto \langle u \rangle^\perp$ for all $u \in V \setminus \{0\}$ and $\langle v \rangle^\perp \mapsto \langle v \rangle$ for all $v \in V \setminus \{0\}$. Then prove $\pi : \mathrm{Aut}(X(PG(2, q)))$ and $P^\pi = \mathcal{L}$ and $\mathcal{L}^\pi = P$.

Chapter 5

Homomorphisms

We write $X \to Y$ to mean there exists a homomorphism from X to Y. Transitive means $X \to Y, Y \to Z$ implies $X \to Z$. Reflexive means $X \to X$.

Are homomorphisms symmetric, i.e. for all $X \neq Y$, $X \to Y \implies Y \to X$? No, take $X = K_2$ and $Y = K_3$.

Are homomorphisms anti-symmetric, i.e. for all $X \neq Y$, $X \to Y \implies Y \not\to X$? No, take $X =$ square graph and $Y = K_2$.

Definition: Core

A graph X is a core if every homomorphism from X to its subgraph is an automorphism.

Definition: Core of a Graph

A graph Y is a core of graph X if Y is a core and $X \to Y, Y \subseteq X$.

Lemma

If Y is a core of X, then Y is a retract of X.

Proof. Let $f : X \to Y$ be a homomorphism. Then $g := f|_Y$ is an automorphism. So $g^{-1} \circ f$ is a retraction.

E.g. K_n is a core. C_n is a core if n is odd.

Definition: Odd Girth

The odd girth of X is the length of a shortest odd cycle.

A bipartite graph's odd girth is ∞.

Lemma

Suppose $X \to Y$, then

(a) $\chi(X) \leq \chi(Y)$.

(b) Odd girth of $X \geq$ odd girth of Y.

Corollary

(a) $C_{2n+1} \not\to K_2$ and C_{2n+1} is a core.

(b) Petersen graph $\not\to C_4$.

(c) A graph is critical if its χ-number is strictly greater than the χ-number of its proper subgraphs.

Critical graphs are cores.

Lemma

Let X be connected. If every path of length 2 of X lies in a shortest odd cycle, then X is a core.

From this lemma, we see the Petersen graph is a core.

Proof. Suppose on the contrary X is not a core. This means there exists $Y \subseteq X, Y \neq X$, $f : X \to Y$ retraction. So $\exists u \sim v$, $v \in V(Y), u \notin V(Y)$. Let $w = f(u) \implies u \nsim w$ and $w \sim v$. w, v, w is a 2-path, so there exists a shortest cycle C using the path u, v, w. $f(C)$ is a walk of length $|C|$, but has repeated vertices. There exists a shorter odd cycle than C, a contradiction.

Lemma

Suppose Y_1, Y_2 are cores. Then, Y_1, Y_2 are homomorphically equivalent if and only if $Y_1 \cong Y_2$.

Proof. Let $f_1 : Y_1 \to Y_2, f_2 : Y_2 \to Y_1$ homomorphisms. Then, $f_1 \circ f_2$ and $f_2 \circ f_1$ are homomorphisms $Y_1 \to Y_1, Y_2 \to Y_2$. Y_1, Y_2 are cores implies $f_1 \circ f_2$ and $f_2 \circ f_1$ are surjective. Both have to be bijective homomorphisms, implying isomorphisms.

Definition: Homomorphically Equivalent

Two graphs X, Y are homomorphically equivalent if $X \to Y$ and $Y \to X$.

Theorem

Every graph has a unique core $X^\bullet$, up to isomorphism.

Proof. The existence is trivial. For uniqueness, let Y_1, Y_2 be two cores. $Y_1 \to X \to Y_2$ and $Y_2 \to X \to Y_1$. So Y_1 and Y_2 are homomorphically equivalent. The lemma implies $Y_1 \cong Y_2$.

Theorem

Two graphs are homomorphically equivalent if and only if their cores are isomorphic.

Proof. ($\implies$) Suppose $X \to Y, Y \to X$. Then, $X^\bullet \to X \to Y \to Y^\bullet$ and $Y^\bullet \to Y \to X \to X^\bullet$. So $X^\bullet \cong Y^\bullet$.

Theorem

$\to$ defines a partial order on the family of cores.

Proof. $\to$ is reflective and transitive. Lemma implies $\to$ is anti-symmetric.

Definition: Lattice

For all $x \neq y$, $x \wedge y$ and $x \vee y$ exist where $\wedge$ is greatest lower bound and $\vee$ is the least upper bound.

Definition: Product

Let Y, Z be graphs. $Y \times Z$ is defined by $V(Y \times Z) = V(Y) \times V(Z)$ and $(y, z) \sim (y', z')$ if $y \sim y'$ and $z \sim z'$.

Lemma

(a) Suppose Y and Z are connected, then $Y \times Z$ disconnected if and only if Y, Z are both bipartite.

(b) $(Y_1 + Y_2) \times Z \cong Y_1 \times Z + Y_2 \times Z$.

(c) $Y \times Z \cong Z \times Y$.

(d) $P_x : V(X \times Y) \to V(X), (x, y) \mapsto x$ and $P_y : V(X \times Y) \to V(Y), (x, y) \mapsto y$ are homomorphisms from $X \times Y$ to X and to Y.

Theorem

Let X, Y, Z be graphs. If $f : Z \to X$ and $g : Z \to Y$ are homomorphisms, then there exists a unique homomorphism $\phi : Z \to X \times Y$ such that $f = P_x \circ \phi$ and $g = P_y \circ \phi$.

Proof. Let $\phi(z) = (f(z), g(z))$ for all $z \in Z$. If $u \sim v$ in Z, then $f(u) \sim f(v), g(u) \sim g(v)$. Then $\phi(u) \sim \phi(v)$ implies ϕ is a homomorphism.

Since $f = P_x \circ \phi, g = P_y \circ \phi$, (f, g) determines ϕ.

We will denote ϕ by $\phi_{f,g}$ since it is uniquely determined by f and g.

Proposition

(a) $X \times Y \to X, X \times Y \to Y$.

(b) If $Z \to X, Z \to Y$, then $Z \to X \times Y$.

(c) $|\text{Hom}(Z, X \times Y)| = |\text{Hom}(Z, X)| \cdot |\text{Hom}(Z, Y)|$.

Proof. (a) comes from Lemma (d).

(b) by previous theorem.

(c) $\varphi : \text{Hom}(Z, X) \times \text{Hom}(Z, Y) \to \text{Hom}(Z, X \times Y)$. We take $(f, g) \to \phi_{f,g}$ unique is a bijection by previous theorem.

Theorem

$\to$ defines a lattice on the family of cores.

Proof. Least upper bound: $X \to X+Y \to (X+Y)^{\bullet}, Y \to X+Y \to (X+Y)^{\bullet}$, so $(X+Y)^{\bullet}$ is an upper bound.

To prove it is the least, suppose Z is a core such that $X \to Z, Y \to Z$. Then $X + Y \to Z$ implies $(X + Y)^{\bullet} \to Z \implies X \vee Y = (X + Y)^{\bullet}$.

Greatest lower bound: $X \times Y \to X$ and $X \times Y \to Y$ by proposition (a). This implies $(X \times Y)^{\bullet}$ is a lower bound for X and Y.

To prove it is the greatest, suppose Z is a core such that $Z \to X, Z \to Y$. By proposition (b), $Z \to (X \times Y) \to (X \times Y)^{\bullet} \implies X \wedge Y = (X \times Y)^{\bullet}$.