CO 444 Algebraic Graph Theory

Ilia Chtcherbakov

Winter 2015

0 Preamble

CO 444, Algebraic Graph Theory. Offered by Professor Chris Godsil at the University of Waterloo in the Winter 2015 term. Composed and mlbaked by Ilia Chtcherbakov (`ischtche@uwaterloo.ca`).

Textbook: C. Godsil, G. Royle. *Algebraic Graph Theory.* New York: Springer-Verlag, 2001. ISBN 0-387-95220-9.

0.1 Introduction

Algebraic graph theory is the study of the relationship between graph theoretic problems and algebraic ones. This course coalesces together techniques, tools, and ideas from graph theory, group theory, linear algebra, and enumeration, among others, and uses them to answer a wide class of questions and pose interesting new ones.

The topics covered include Cayley graphs, graph homomorphisms, graph spectra, and equitable partitions, all of which can be found in the book. Then the final third of the course covers some current research topics in algebraic graph theory—in our case, quantum walks, expanders, Ramanujan graphs, and the matching polynomial. Some additional material treated in the book but left out of the course is presented in the final section.

Exercises litter the notes, mostly for enrichment. Questions, on the other hand, are merely interesting and worth investigating—some are open problems. Easier proofs tend to be elided without notice; more difficult proofs are at least sketched, but rarely treated in full rigour.

0.2 Conventions

Recall that a **graph** $G = (V, E)$ consists of a (finite) set V of 'vertices' and a set $E \subseteq \binom{V}{2}$ of 2-subsets called 'edges' of G. Abbreviate $\{u, v\} \in E$ as $uv \in E$ or $u \sim v$. A **subgraph** $H = (V', E')$ of G is a graph such that $V' \subseteq V$ and $E' \subseteq E$. H is **spanning** if $V' = V$ and **induced** if $E' = E \cap \binom{V'}{2}$.

A **multigraph** has E a multiset with elements from $\binom{V}{1} \cup \binom{V}{2}$. A **directed graph** has E a set with elements from $V \times V$, with adjacencies denoted $(u, v) \in E$ or $u \to v$.

Recall also that a **homomorphism** is a structure-preserving map between two objects. For instance, a homomorphism of groups preserves the group operation—$\phi(gh) = \phi(g)\phi(h)$—while a homomorphism of graphs preserves adjacency—$u \sim v \implies \phi(u) \sim \phi(v)$. An **isomorphism** is a bijective homomorphism *whose inverse is also a homomorphism*—while bijective group homomorphisms are isomorphisms, this is not the case for all objects. An **endomorphism** (**automorphism**) is a homomorphism (isomorphism) from an object to itself—denote the monoid (under composition) of endomorphisms of X by $\mathrm{End}(X)$ and the group of automorphisms by $\mathrm{Aut}(X)$.

1 Cayley Graphs

Let G be a (finite) group and $C \subseteq G$. The **Cayley graph** $X(G, C) = (V, E)$ on G is the graph with $V = G$ and for $x, y \in V$, $x \sim y$ iff $yx^{-1} \in C$. Generally this is a digraph; to avoid loops we must have that $1 \notin C$, and to make edges undirected, C must be closed under taking inverses.[1] For $g \in G$ and $c \in C$, we have $g \sim cg$.

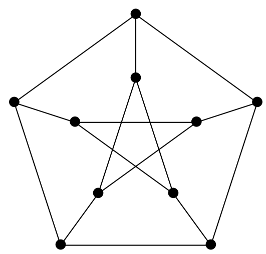
[1] In these notes, a Cayley graph will always be a graph—we will refer to the general case as a Cayley digraph if necessary.

A Cayley graph on $\mathbb{Z}_n$, the cyclic group of order n, is called a **circulant**. A Cayley graph on $\mathbb{Z}_2^d$ is called a **cubelike**. A graph is **Cayley** if it is isomorphic to $X(G, C)$ for some G and C, and likewise it is a circulant or cubelike if G is $\mathbb{Z}_n$ or $\mathbb{Z}_2^d$, respectively. For example, the n-cycle $C_n \cong X(\mathbb{Z}_n, \{\pm 1\})$ is a circulant and the d-cube $Q_d \cong X(\mathbb{Z}_2^d, B)$, where B is the standard basis $\{ e_i \mid 1 \leq i \leq n \}$, is a cubelike.

Exercise. Show that a cubelike $X(\mathbb{Z}_2^d, C)$ is connected if C spans $\mathbb{Z}_2^d$ as a $\mathbb{Z}_2$-vector space.

Exercise. Show that the diameter of a connected cubelike is bounded above by its valency. When are they equal?

A graph X is **vertex-transitive** if for every pair of vertices $u, v \in V(X)$, there exists an automorphism mapping u to v. Cayley graphs are vertex-transitive, but the converse does not hold: an important example is the **Petersen graph**, pictured below.



It suffices to check all the groups of order 10 to see that Petersen is not Cayley—there happen to be two, $\mathbb{Z}_{10}$ and $D_5 = \langle r, s \mid r^2 = s^5 = (rs)^2 = 1 \rangle$. The valency of Petersen is 3, so $|C| = 3$. C has at least one pair of elements which are not each other's inverse, so if G is abelian, then $X(G, C)$ must contain a square. Petersen has girth 5, so G is not abelian, i.e. it cannot be $\mathbb{Z}_{10}$.

Suppose there exists a connection set C so that Petersen $\cong X(D_5, C)$. Then $C = C^{-1}$, so either one or all three elements of C must have order two. $C = \{ r, s, s^{-1} \}$ doesn't work, as there would be a 4-cycle, and WLOG this exhausts the cases where only one element of C has order two. If every element of C is self-inverse, it still fails (*Exercise.*) so Petersen is vertex-transitive but not Cayley.

1.1 Permutation Groups

The automorphisms $\mathrm{Aut}(X)$ of a graph X form a group, which has an interesting action on the vertex set $V(X)$. We now recall some theory of group actions. Let G be a finite group.

Given a set Ω, denote the symmetric group $\mathrm{Sym}(\Omega) = \{ f : \Omega \to \Omega \text{ bijective} \}$. A **permutation group** of Ω is a subgroup of $\mathrm{Sym}(\Omega)$. A **permutation representation**, more commonly known as a **group action**, is a group homomorphism $\phi : G \to \mathrm{Sym}(\Omega)$. More conveniently, a group action can be thought of as a map $(.) : G \times \Omega \to \Omega$ such that for all $x \in \Omega$ and $g, h \in G$, $1.x = x$ and $g.h.x = gh.x$.

If G acts on a set Ω, define an equivalence relation $\approx$ on Ω by $x \approx y$ if $g.x = y$ for some $g \in G$. The equivalence classes $G.x := \{ g.x \mid g \in G \}$ in $\Omega/\approx$ are called the **orbits** of G in Ω (with respect to the action). Write Ω/G for $\Omega/\approx$. By definition, two ordits are either equal or disjoint.

G acts **transitively** on Ω if $|\Omega/G| = 1$; equivalently, if for all $x, y \in \Omega$, there exists $g \in G$ such that $g.x = y$. For example, a graph X is vertex-transitive if $\mathrm{Aut}(X)$ acts transitively on $V(X)$. An action is **free** if for any $x \in \Omega$ and $g, h \in G$, $g.x = h.x$ implies $g = h$. An action that is both free and transitive is **regular**. When G acts regularly on Ω, for any $x, y \in G$ there exists exactly one $g \in G$ such that $g.x = y$.

If G acts on Ω, this naturally induces actions on a number of other sets. G acts on the Cartesian power Ω^k pointwise, by $g.(x_1, ..., x_k) = (g.x_1, ..., g.x_k)$. Of particular interest in some applications are the orbits of G in Ω^2, called **orbitals**. G also acts on k-subsets $\binom{\Omega}{k}$ elementwise (*Exercise.*) and hence on the power set $2^\Omega = \bigcup_k \binom{\Omega}{k}$.

Let V be a set and $\phi : G \to \mathrm{Sym}(V)$ be an action. If E is a union of orbits in $\binom{V}{2}/G$, then G can be said to act on the graph $X = (V, E)$. This occurs iff the action factors $\phi : G \to \mathrm{Aut}(X) \hookrightarrow \mathrm{Sym}(X)$. G also acts on the graph objects like paths, walks, and also **s-arcs** of X, that is, walks on X of length $s + 1$ with no backtracking.

Let G act on Ω and $x \in \Omega$. The stabilizer $G_x := \{ g \in G \mid g.x = x \}$ of x is the subgroup of G fixing x. The orbits and stabilizers of an action are intimately related.

Theorem (Orbit–Stabilizer). *Let G act on Ω. Then for all $x \in \Omega$, $|G| = |G_x|\,|G.x|$.*

Proof. Let $g, h \in G$ and suppose $g.x = h.x$. Then $g^{-1}h.x = g^{-1}.h.x = g^{-1}.g.x = 1.x = x$, so $g^{-1}h \in G_x$ and $h = gg^{-1}h \in gG_x$. Conversely, if $h \in gG_x$, then $g^{-1}h \in G_x$, so $h.x = g.g^{-1}h.x = g.x$. Hence, for each $g.x \in G.x$, there are $|gG_x| = |G_x|$ elements of G that send x to $g.x$. Thus $|G| = |G_x|\,|G.x|$. □

Orbit–Stabilizer is a useful result for counting things. Another result with this property is Burnside's Lemma, which states that the number of orbits of an action is equal to the average number of fixed points of each group element. Let $\Omega^g := \{ x \in \Omega \mid g.x = x \}$ be the set of fixed points of $g \in G$.

Theorem (Burnside's Lemma). *Let G act on Ω. Then $|\Omega/G| = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} |\Omega^g|$.*

Proof. By double-counting the set $\{ (g, x) \in G \times \Omega \mid g.x = x \}$, we see that

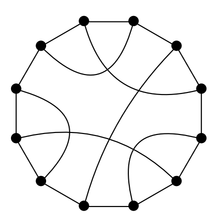
$$\sum_{g \in G} |\Omega^g| = \sum_{x \in \Omega} |G_x| = \sum_{G.x \in \Omega/G} |G.x|\,|G_x| = \sum_{G.x \in \Omega/G} |G| = |\Omega/G|\,|G|. \quad \square$$

A powerful application of Burnside's Lemma is determining the number of isomorphism classes of graphs on n vertices. $\mathrm{Sym}(n)$ acts naturally on the vertices of the complete graph K_n, so it also acts on $2^{E(K_n)}$, the set of all graphs on n vertices. The orbits of this action are exactly the isomorphism classes of graphs on n vertices.

Exercise. Determine the number of isomorphism classes of graphs with 5 vertices.

1.2 Graphical Regular Representations

For a graph X, $\mathrm{Aut}(X) \leq \mathrm{Sym}(V(X))$. It is reasonable to ask which finite groups arise as the automorphism group of some graph—due to a theorem of Frucht, the answer is all of them. In fact, there is a lot of freedom in this result: you can take the graph to be cubic (also due to Frucht). Below is the Frucht graph, a cubic graph whose automorphisms realize the trivial group.



If $X = X(G, C)$ is Cayley, $G \leq \mathrm{Aut}(X)$ because X is vertex-transitive. A more refined question than the previous would be to ask which groups G admit Cayley graphs X such that $G \cong \mathrm{Aut}(X)$. Such an X is said to be a **graphical regular representation** (GRR) for G.

Let $X = X(G, C)$ and $\Gamma = \mathrm{Aut}(X)$. Supposing $\gamma \in \Gamma$, $\gamma.1 = g \in G \leq \Gamma$, so $g^{-1}\gamma.1 = 1$ and $\gamma \in g\Gamma_1$. $G \cap \Gamma_1 = 1$, so we can use Orbit–Stabilizer to find $|\Gamma| = |\Gamma_1||G|$. So X is a GRR iff the vertex stabilizers are trivial.

Lemma. *Let $X = X(G, C)$ where C generates G. If the subgraph induced by C is asymmetric, X is a GRR.*

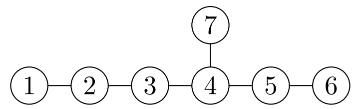
Proof. C generates G, so X is connected. Let $\phi \in \mathrm{Aut}(X)_1$. The subgraph induced by C is asymmetric, so ϕ must fix every element of C. Inducting on the distance from 1, ϕ is the identity map, so $\mathrm{Aut}(X)_1$ is trivial. □

If G admits an automorphism ϕ that fixes C—that is, $\phi(C) := \{ \phi(c) \mid c \in C \} = C$—then $\phi \in \mathrm{Aut}(X(G, C))_1$. If ϕ is not the identity, X is not a GRR. If G was an abelian group, for instance, the inversion map $g \mapsto g^{-1}$ is an automorphism that fixes C, and it is not the identity unless every element of C has order two. Thus, abelian G do not admit GRRs unless $G = \mathbb{Z}_2^d$ for some d. (*Exercise.* Does $\mathbb{Z}_2^d$ admit a GRR?)

Let G be an abelian group and suppose $x \in G$ has order 2. The **generalized dicyclic group** $\mathrm{Dic}(G, x)$ is a group generated by G and a new element y such that $y^2 = x$ and $gy = yg^{-1}$ for all $g \in G$. For instance, $\mathrm{Dic}(\mathbb{Z}_4, 2)$

is isomorphic to the quaternion group $Q = \{ \pm 1, \pm i, \pm j, \pm k \}$. Besides abelian groups, generalized dicyclic groups also do not admit GRRs. (*Exercise.*)

Other than that, groups tend to have GRRs. As an example of the positive, note that edges of K_n correspond to transpositions of $\mathrm{Sym}(n)$, so the edges of a spanning subgraph Y will generate $\mathrm{Sym}(n)$. If Y has no triangles, then we can recover it from $X = X(\mathrm{Sym}(n), E(Y))$. Then if Y is asymmetric, the vertex stabilizers of X must be trivial and hence X is a GRR. Consider the case $n = 7$ and $Y = E_7$, depicted below.



1.3 Linear Cayley Graphs

Let $\mathbb{F}_q$ be the finite field of order $q = p^k$, p prime. Recall $\mathbb{F}_q \cong \mathbb{Z}_p[x]/(P(x))$ for some irreducible polynomial $P(x)$ of degree k. Consider the vector space $\mathbb{F}_q^d$, and let $M \in \mathbb{F}_q^{d\times m}$ be a $d\times m$ matrix with entries in $\mathbb{F}_q$. Then the **linear Cayley graph** of M is

$$X(M) := X\big(\mathbb{F}_q^d, \{ \lambda c \mid \lambda \in \mathbb{F}_q \text{ nonzero, } c \text{ is a column of } M \}\big).$$

$X(M)$ is vertex-transitive, has size q^d and, if no two columns of M are linearly dependent, is $m(q-1)$-regular.

If I is the $d\times d$ identity matrix over $\mathbb{F}_q$, define the **Hamming graph** $H(d, q) := X(I)$. This is the graph of strings of length d in a q-element alphabet, where two strings are adjacent if they differ in exactly one position.[2] $H(d, 2)$ is the d-cube. In fact, when $q = 2$, $X(M)$ is a cubelike, and all cubelike graphs arise in this manner.

Exercise. Show that $X(M)$ is connected iff $\mathrm{rank}(M) = d$.

Exercise. If $Q \in \mathbb{F}_q^{d\times d}$ is invertible, show that $X(M) \cong X(QM)$.

Remark. Observe for general Cayley graphs as well, if $\phi \in \mathrm{Aut}(G)$, then $X(G, C) \cong X(G, \phi(C))$.

Exercise. Characterize the relation between M and N if $X(M) \cong X(N)$.

As the exercises suggest, given a linear Cayley graph $X(M)$ we may assume M is in reduced row-echelon form.

For each column c of M, there is a clique $\{ \lambda c \mid \lambda \in \mathbb{F}_q \}$ of size q, though it is not necessarily a maximal clique.

Proposition. *Let $M \in \mathbb{F}_q^{d\times m}$. If there exists $a \in \mathbb{F}_q^d$ such that $a^\mathsf{T} M$ has no zero entries, $X(M)$ is q-colourable.*

Proof. We confirm that assigning the colour $a^\mathsf{T} v$ to the vertex v is a proper q-colouring. Take any edge $uv \in E(X(M))$. Then by definition, $v - u = \lambda M e_i$ for some $i \le m$ and $\lambda \in \mathbb{F}_q \backslash 0$, where e_i is the i-th basis vector.

$$a^\mathsf{T} v - a^\mathsf{T} u = a^\mathsf{T}(v - u) = \lambda a^\mathsf{T} M e_i = \lambda (a^\mathsf{T} M)_i \neq 0$$

by hypothesis, so $a^\mathsf{T} u \neq a^\mathsf{T} v$ and the colouring is proper. Finally, $a^\mathsf{T} v \in \mathbb{F}_q$, so it can take at most q values. □

1.4 Coset Graphs

Consider $X = X(G, C)$ with $H \le G$. Notice that H naturally partitions G and hence $V(X)$ into left or right cosets.

The right cosets $Hg = \{ hg \mid h \in H \}$ are the orbits of H under the action of left multiplication. Each subgraph induced by a right coset is a Cayley subgraph of X, isomorphic to $X(H, C')$ for C' the restriction of C to H.

The left cosets $gH = \{ gh \mid h \in H \}$ are obtuse and weird, but in some sense capture transversal **(TODO)**

[2] Under this intepretation, there is nothing special about q being a prime power, which is why **Hamming distance** is the name for the more general phenomenon of two strings being at some distance in $H(\text{length}, \text{alphabet})$.

2 Graph Homomorphisms

A **homomorphism of graphs** f is a function $f : V(X) \to V(Y)$ such that if $uv \in E(X)$, then $f(u)f(v) \in E(Y)$. That is, f maps vertices to vertices and edges to edges. If there exists a graph homomorphism from X to Y, write $X \to Y$. If X is a subgraph of Y, the inclusion map is a homomorphism.

Lemma. *Let $f : X \to Y$ be an embedding—an injective homomorphism. Then $|E(X)| \leq |E(Y)|$.* □

An **isomorphism** is a bijective homomorphism whose inverse is also a homomorphism. Unlike with groups, rings, and other nice objects, bijective homomorphisms are not automatically isomorphisms: consider $\bar{K}_2 \to K_2$.

Theorem. *Let $f : X \to Y$ be a bijective homomorphism. Then f is an isomorphism iff $|E(X)| = |E(Y)|$.* □

Corollary. *If $f : X \to Y$ and $g : Y \to X$ are embeddings, then $X \cong Y$.* □

If two vertices are adjacent in X, a homomorphism $X \to Y$ cannot map them to the same vertex in Y unless Y contains loops. So if $f : X \to Y$ is a graph homomorphism, the preimage $f^{-1}(y)$ of any $y \in V(Y)$ is a coclique. $f^{-1}(y)$ is the **fibre** of f at y, and if f is surjective, these fibres induce a partition of X called the **kernel** of f.[3]

Many graph theoretic questions can be reformulated as questions about homomorphisms. For instance,

— A graph X is n-colourable iff $X \to K_n$, so $\chi(X) = \min\{\, n \mid X \to K_n \,\}$.

— $K_n \to X$ iff X contains an n-clique, so $\omega(X) = \max\{\, n \mid K_n \to X \,\}$.

— Questions about cocliques of X may be addressed by either considering $K_n \to \bar{X}$ or examining the fibres of homomorphisms to X allows.

— X has odd girth n iff n is minimal such that $C_n \to X$.

As a convention, if $f : X \to Y$ is a homomorphism and Z is a subgraph of X, then $f(Z)$ is the image of Z in Y, tracking both vertices and edges. However, if U is a subset of $V(X)$, then $f(U)$ is the subgraph of Y *induced* by $\{\, f(u) \mid u \in U \,\}$.

2.1 The Lattice of Homomorphism-Equivalence Classes

The relation $\to$ (hom-existence) is reflexive and transitive. However, it is neither symmetric—$K_2 \to X$ iff X is nonempty, but $X \to K_2$ iff X is bipartite—nor antisymmetric—trees on two or more vertices are both nonempty and bipartite. So the most we may say is that $\to$ is a preorder.

Remark. $\to$ is also not total. There exists a graph X such that $K_3 \not\to X$ (X is triangle-free) and $X \not\to K_3$ (X is not 3-colourable). Due to a theorem of Grötzsch, such an X must be nonplanar. The smallest example, the Grötzsch graph, has 11 vertices.

Say that X and Y are **homomorphically equivalent** (hom-equivalent) if $X \to Y$ and $Y \to X$, and write $X \leftrightarrow Y$. $\leftrightarrow$ is an equivalence relation, and $\to$ is a partial order on the equivalence classes of this relation. Armed with a poset on the finite graphs, it behooves us to ask if it might be a lattice. Recall that a poset $(P, \leq)$ is a lattice if for all $X, Y \in P$ there is a unique least upper bound (the "join") $X \vee Y$ and a unique greatest lower bound (the "meet") $X \wedge Y$.

Given two graphs X, Y, consider their disjoint union $X + Y$. Trivially $X, Y \to X + Y$ by inclusion. To show this is a join, it remains to show that whenever $X, Y \to Z$, $X + Y \to Z$ as well. Suppose $f : X \to Z$ and $g : Y \to Z$ are homomorphisms. Then the map $h : X + Y \to Z$ given by

$$h(u) = \begin{cases} f(u) & u \in V(X) \\ g(u) & u \in V(Y) \end{cases}$$

is a homomorphism as well, so $+$ is a join for the lattice of graphs.

[3] The use of surjectivity is twofold. First, our partitions will have no empty cells, by convention. Second, if $f : X \to Y$ is not surjective, it might be more prudent to restrict the codomain Y to the image $f(X)$.

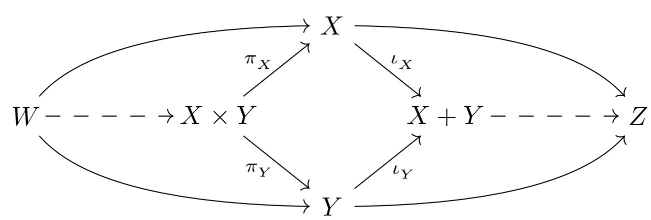
Given two graphs X and Y, define their **direct product** (also categorical, tensor, or Kronecker product) $X \times Y$ to be the graph with on the vertex set $V(X) \times V(Y)$ where $(x, y)(x', y')$ is an edge iff $xx' \in E(X)$ and $yy' \in E(Y)$.

Up to isomorphism, the direct product is commutative, associative, and distributes over disjoint union. However, it is not cancellative—consider for instance $K_2 \times 2K_3 \cong 2C_6 \cong K_2 \times C_6$. Also, the identity for this operation would be a vertex with a loop, so there is no identity in the graphs.

Obervse that $X \times Y$ has obvious projections to each of its factors—$\pi : X \times Y \to X$ given by $\pi(x, y) = x$ is a homomorphism, because $xx' \in E(X)$ is a prerequisite to $(x, y)(x', y') \in E(X \times Y)$, and the same occurs for Y—so $X \times Y \to X, Y$. Now, let W be a graph with homomorphisms $f : W \to X$ and $g : W \to Y$. Then we can define $h : W \to X \times Y$ by $h(w) = (f(w), g(w))$, and this is a homomorphism. Hence $\times$ is a meet.

Theorem. *The poset of hom-equivalence classes of graphs forms a lattice.* □

This is called the **hom-lattice** of graphs.



Proposition. *If* $\mathrm{Hom}(X, Y)$ *denotes the set of homomorphisms from* X *to* Y*, then*

$$\left|\mathrm{Hom}(W, X \times Y)\right| = \left|\mathrm{Hom}(W, X)\right| \left|\mathrm{Hom}(W, Y)\right| \quad \textit{and} \quad \left|\mathrm{Hom}(X + Y, Z)\right| = \left|\mathrm{Hom}(X, Z)\right| \left|\mathrm{Hom}(Y, Z)\right|.$$

Proof. Given $f : X \to Z$ and $g : Y \to Z$, the homomorphism $h : X + Y \to Z$ constructed above has the property that, if $\iota_X : X \to X + Y$ and $\iota_Y : Y \to X + Y$ are the analogous inclusion maps to $X + Y$, then $f = \iota_X \circ h$ and $g = \iota_Y \circ h$. Thus, h determines f and g and vice versa, so we have a bijection between $\mathrm{Hom}(W, X \times Y)$ and $\mathrm{Hom}(W, X) \times \mathrm{Hom}(W, Y)$.

The direct product has a similar relationship to the projections $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$. □

2.2 Cores

In analogy with the integers modulo n, it is reasonable to ask if there is a canonical representative of each hom-equivalence class in the hom-lattice.

-1 The End

Thus ends the offering. The text contains a treatment of algebraic graph theory both broader and deeper than these notes, but I couldn't resist writing a little more about some topics extending what was covered in the course.

-1.1 Map Graphs

-1.2 Fractional Colourings

-1.3 Welzl's Theorem