Spring 2018

Cayley Graphs of PSL(2) over Finite Commutative Rings

Kathleen Bell
Western Kentucky University, kathleen.bell085@topper.wku.edu

CAYLEY GRAPHS OF $PSL(2)$ OVER FINITE COMMUTATIVE RINGS

A Thesis
Presented to
The Faculty of the Department of Mathematics
Western Kentucky University
Bowling Green, Kentucky

In Partial Fulfillment
Of the Requirements for the Degree
Master of Science

By
Kathleen Bell

May 2018

CAYLEY GRAPHS OF $PSL(2)$ OVER FINITE COMMUTATIVE RINGS

Date Recommended 4/26/18

Dominic Lanphier, Director of Thesis

Tom Richmond

John Spraker

Jason Rosenhouse

Dean, Graduate Studies and Research   Date 5/1/18

ACKNOWLEDGMENTS

I have been blessed with the support of many people during my time in graduate school; without them, this thesis would not have been completed.

To my parents: thank you for prioritizing my education from the beginning. It is because of you that I love learning.

To my fiancé, who has spent several “dates” making tea and dinner for me while I typed math: thank you for encouraging me and believing in me.

To Matthew, who made grad school fun: thank you for truly being a best friend. I cannot imagine the past two years without you.

To the math faculty at WKU: thank you for investing your time in me. I know that as I begin my career teaching mathematics, I carry with me the things I have learned from you - not only mathematics and teaching techniques, but a general love for students.

And to Dr. Lanphier: thank you for your time, your advice, and your patience. If I set as my goal to be as helpful, encouraging, and knowledgeable a teacher as you are, I will be aiming for the best.

CONTENTS

LIST OF FIGURES

CAYLEY GRAPHS OF $PSL(2)$ OVER FINITE COMMUTATIVE RINGS

Kathleen Bell May 2018 Pages 40

Directed by: Dominic Lanphier, Tom Richmond, John Spraker, and Jason Rosenhouse

Department of Mathematics Western Kentucky University

Hadwiger's conjecture is one of the deepest open questions in graph theory, and Cayley graphs are an applicable and useful subtopic of algebra.

Chapter 1 will introduce Hadwiger's conjecture and Cayley graphs, providing a summary of background information on those topics, and continuing by introducing our problem. Chapter 2 will provide necessary definitions. Chapter 3 will give a brief survey of background information and of the existing literature on Hadwiger's conjecture, Hamiltonicity, and the isoperimetric number; in this chapter we will explore what cases are already shown and what the most recent results are. Chapter 4 will give our decomposition theorem about $PSL_2(R)$. Chapter 5 will continue with corollaries of the decomposition theorem, including showing that Hadwiger's conjecture holds for our Cayley graphs. Chapter 6 will finish with some interesting examples.

CHAPTER 1

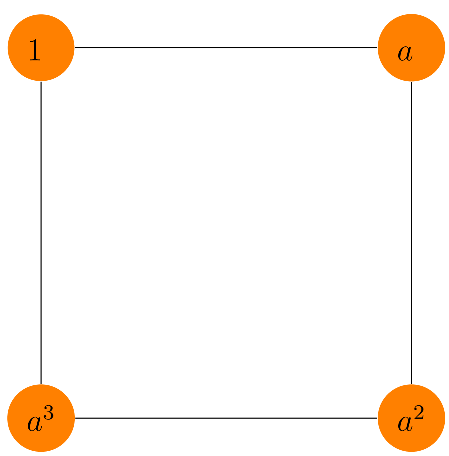
INTRODUCTION

A longstanding conjecture in graph theory is Hadwiger's conjecture, which states that for every integer $n \geq 0$, if a graph has no K_{n+1} minor then the graph is n-colorable. This is perhaps the most difficult and celebrated open problem (it has only been proven for $n < 6$) in graph theory.

We investigate a special class of Cayley graphs and establish several interesting properties of these graphs. We chose to examine Cayley graphs because Cayley graphs form nice models for networks; they are highly symmetric, sparse, and yet well-connected. Examining this class of graphs also helps us to break down important conjectures like Hadwiger's.

A Cayley graph is one constructed from a group and a symmetric generating subset. A Cayley graph illustrates the group to which it is attached. Because they are highly symmetrical graphs, it is believed that this structure extends to certain graphical properties such as Hamiltonicity. Consequently, it has been conjectured that all Cayley graphs are Hamiltonian.

Example 1.1: The Cayley graph $G(C_4, \{a, a^{-1} \mid a^4 = 1\})$



For R a finite commutative ring let

$$SL_2(R) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \;\middle|\; a, b, c, d \in R,\ ad - bc = 1 \right\}$$

and let $PSL_2(R) = SL_2(R)/\langle \pm I \rangle$, where $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We study Cayley graphs of $PSL_2(R)$ with respect to certain generating sets.

By studying the structure of such graphs, we hope to establish various properties for them. For example, we want to find an appropriate K_n minor of these graphs and establish Hadwiger's conjecture for these graphs. Further, we will study other properties of these graphs such as their connectedness. In particular, we will investigate the isoperimetric number of these graphs [18], following the methods of [14] and [15].

A Hamilton path in a graph is a path that contains every vertex of the graph exactly once. A Hamilton cycle is a cycle that contains every vertex only once in the cycle. The Hamiltonicity of various classes of graphs is a long standing problem and it was conjectured in [16] that every Cayley graph has a Hamilton cycle [6], [8], [11], [19], [21], [24]. Such graphs are called *Hamiltonian.* We will also investigate the Hamiltonicity of these classes of Cayley graphs.

CHAPTER 2

COLORINGS, MINORS, AND CAYLEY GRAPHS

In this chapter we will define relevant terms such as a $k-$coloring of a graph, a Cayley graph, a graph minor, etc., primarily using the definitions from [23].

2.1 - Definitions from Graph Theory

Definition 2.1.1. *A graph* G is a set of elements $V(G)$, called the *vertices* and a set of unordered pairs of those elements, referred to as *edges.*

We typically represent the elements as nodes, and we typically represent the edges by putting line segments between the nodes. If there is at most one edge between any two vertices, we call the graph a *simple graph.* If we allow multiple edges between any two vertices, the graph is called a *multigraph.*

We begin by discussing graph colorings. We notice that the vertices of a graph G can be partitioned into independent sets, that is, sets of vertices where no two vertices in the same set are adjacent. If the vertices of a graph can be partitioned into k independent sets, we say that the graph is *k-colorable.* If all the vertices in any given set were assigned the same color, then no two vertices of the same color would be adjacent.

Definition 2.1.2. A *proper* $k-$*coloring* of a graph G is a partition of $V(G)$ into k independent sets.

A proper vertex coloring of a graph G is a labeling of the vertices of G with colors such that no two vertices sharing the same edge have the same color.

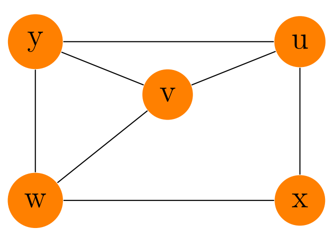
Definition 2.1.3. A graph is $k-$*colorable* if it has a proper coloring with at most k colors.

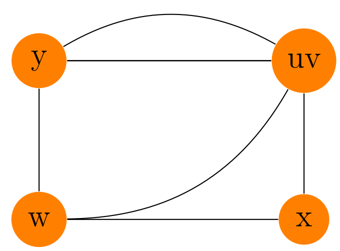
Definition 2.1.4. The *chromatic number* $\chi(G)$ of a graph G is the smallest number of colors needed to color the vertices of G so that no two adjacent vertices share the same color.

We now consider some useful operations on graphs. In order to study Hadwiger's conjecture, we must manipulate graphs by deleting and contracting edges. To *contract* an edge is to bring its two endpoints together and make them one point, and then remove the edge that connected the two vertices. Doing so creates a graph $G \cdot e$ with one fewer edge and one fewer vertex than the original graph G.

Definition 2.1.5. In a graph G, a *contraction* of an edge e with endpoints u, v is the replacement of u and v with a single vertex whose incident edges are the edges other than e that were incident to u or to v.

Example 2.1: Contraction of edge uv



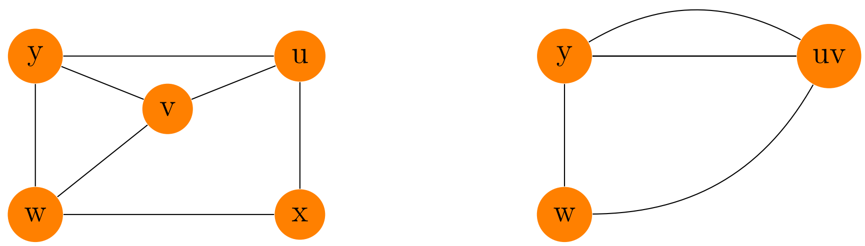


By contracting and deleting edges and/or deleting vertices, we can create what is known as a graph minor. We define a graph minor following [22].

Definition 2.1.6. A graph H is a *minor* of a graph G if a copy of H can be obtained from G by a series of operations of either deleting vertices, deleting or contracting edges, or both.

In a sense, we think of G as "containing" a copy of H when H is a graph minor of G.

Example 2.2: Making a graph minor by contracting edge uv and deleting vertex x



Hadwiger's conjecture requires there to be no minor of an n-colorable graph G that is a complete graph on $n+1$ vertices. The complete graph is formed by making every pair of vertices adjacent. It is therefore the most connected that a graph can be.

Definition 2.1.7. The *complete graph,* denoted K_n, is the graph on n vertices where every pair of vertices is adjacent.

We now have all the necessary terminology to present Hadwiger's conjecture.

2.1.1 Hadwiger's conjecture (Hadwiger)**.** *For every integer n, if a graph G has no K_{n+1} minor, then G is n-colorable.*

Note that K_{n+1} is not n-colorable, but it is $n+1$ colorable.

Let G be a graph.

Definition 2.1.8. The *Hadwiger number* $\eta(G)$ is the largest natural number n for which the complete graph K_n is a minor of G.

The second property which we will show for our Cayley graphs is Hamiltonicity.

Definition 2.1.9. A *Hamilton path* in a graph G is a path that contains every vertex of G exactly once.

Definition 2.1.10. A *Hamilton cycle* in a graph G is a cycle containing every vertex of G exactly once.

Definition 2.1.11. A graph G is *Hamilton connected* if for any pair of vertices $u, v \in G$, there exists a Hamilton path from u to v.

The third property which we will try to find for our Cayley graphs is their isoperimetric number. The isoperimetric number of a graph is a measure of its connectedness. For all the small subsets A of vertices of a graph G, consider the minimum ratio between the size of the edge boundary of A (the set of edges going from a vertex of A to a vertex not in A) and the number of vertices in A — this gives the isoperimetric number of G.

Definition 2.1.12. The *isoperimetric number,* or *Cheeger constant,* denoted $h(G)$, is defined by

$$h(G) = \min \left\{ \frac{|\partial A|}{|A|} : A \subset V(G), 0 < |A| \leq \frac{1}{2}|V(G)| \right\},$$

where ∂A denotes the edge boundary of A, that is, the set of edges between A and $V(G) - A$.

The isoperimetric number measures the ease with which a graph can be disconnected. Also, if we interpret the graph as a network, the isoperimetric number measures the size of bottlenecks in the network. A small isoperimetric number means that there are bottlenecks, making the network less reliable.

Definition 2.1.13. A graph G is a *wheel graph* if it can be created by connecting a vertex w to each of the vertices $c_1, ..., c_n$ of a cycle.

Definition 2.1.14. An $m \times n$ *grid graph* has vertex set (x, y) for $x, y \in \mathbb{N}$ with $1 \leq x \leq m$ and $1 \leq y \leq n$. We say (x_1, y_1) is adjacent to (x_2, y_2) when $x_1 = x_2$ and

$|y_1 - y_2| = 1$, or when $y_1 = y_2$ and $|x_1 - x_2| = 1$. The graph looks like a rectangular grid.

The grid graphs we will study will be square $n \times n$ grids with integers modulo n, so that the ends are adjacent to each other, which is essentially a grid on a torus.

2.2 - Definitions from Algebra

Definition 2.2.1. A *group* $(\Gamma, \cdot)$ is a set Γ together with an operation $\cdot$ such that the operation combines any two elements a and b of Γ to form a third element of Γ. A group also has associativity, a unique identity, and inverses [9]. If for all $a, b \in \Gamma$, $a \cdot b = b \cdot a$, we call Γ *Abelian.*

Definition 2.2.2. A subset $S \subset \Gamma$ is a *generating set* for the group Γ if every element of Γ can be expressed as the combination (under the group operation) of finitely many elements $s \in S$ and their inverses. If for all $s \in S$, we have $s^{-1} \in S$, then S is a *symmetric generating set* for Γ.

Definition 2.2.3. A *ring* R is a set with two binary operations, addition and multiplication, such that for all $a,\ b,\ c \in R,$ we have: $a+b = b+a, a+(b+c) = (a+b)+c$, there is an additive identity 0 such that $a + 0 = a$ for all $a \in R$, there is an element $-a \in R$ such that $a + (-a) = 0$, $(ab)c = a(bc)$, and $a(b + c) = ab + ac$, and $(b + c)a = ba + ca$. [9]

We will primarily be studying finite commutative rings – that is, finite Abelian groups under addition, with associative and commutative multiplication that is left and right distributive over addition. Even more specifically, we will be studying a certain type of finite commutative ring called a local ring – a ring of the form R/n where n is an ideal of the ring R. Finite commutative rings are always direct sums of local rings.

Definition 2.2.4. An *ideal* I of a ring R is a subset of R that forms an additive group and has the property that, whenever $r \in R$ and $n \in I$, then $rn \in I$ and $nr \in I$.

Definition 2.2.5. An element $r \in R$ is a *unit* if r has a multiplicative inverse in R. The set of units is called $R^{\times}$.

Definition 2.2.6. A non-zero element r is a *zero divisor* of a ring R if there exists a non-zero element $x \in R$ such that $rx = 0$ or $xr = 0$. We denote the set of zero divisors of a ring R as $Z(R)$.

Lemma 2.2.7. *In a finite commutative ring with unity, every non-zero element is either a unit or a zero divisor.*

Proof. Let $r \in R, r \neq 0, r \notin Z(R)$. Let $a, b \in R$ so that $ra = rb$. Then $r(a-b) = 0$. Since $r \notin Z(R)$ and $r \neq 0$, we must have $a - b = 0$. This implies $a = b$. Consider the set $\{r^n | n \in \mathbb{Z}\}$. As R is finite, $r^i = r^j$ for some $i \neq j$, and without loss of generality we may assume that $i > j$. Thus, since $r^i = r^j$ it follows that $r^j r^{i-j} = r^j$. Since we can cancel the r's from the argument above, we have $r^{i-j} = 1$. Now, $i - j > 0$, so if $i - j = 1$, then $1 = r^{i-j} = r$ and so $r = 1$ and r is a unit. If $i - j > 1$, then $1 = r^{i-j} = rr^{i-j-1}$ and r has a multiplicative inverse, so r is a unit. □

Note that this is not necessarily true for infinite rings; for example, consider $R = \mathbb{Z}$, an infinite ring. Then $R^{\times} = \{-1, 1\}$ and $Z(R) = \emptyset$, leaving all other elements of $\mathbb{Z}$ as neither units nor zero divisors. In this paper we will call the subset of a ring that is the collection of non-zero elements which are neither zero divisors nor units $\widetilde{R}$.

Note that a group has closure if performing the group operation on elements of the group yields an element of the group.

Lemma 2.2.8. *Let R be a ring and Z(R) be the semigroup (has closures but might not have inverses or identity) of zero divisors. We assume that $R = R^{\times} \cup Z(R)$. Let*

$\alpha, \beta \in R$ such that $\nexists z \in Z(R)$ with $z\alpha = z\beta = 0$. (ie, α and β can not have the same zero divisor). Then $\exists x, y \in R$ such that $x\alpha - y\beta = 1$.

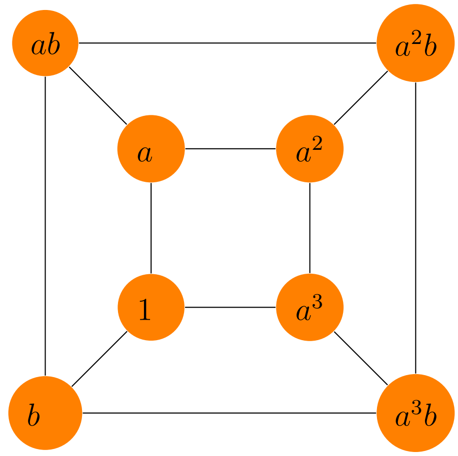
Proof. If $\beta - \alpha \in R^\times$, then take $x = y = (\beta - \alpha)^{-1}$. Then $x\alpha - y\beta = (\beta - \alpha)^{-1}\beta - (\beta - \alpha)^{-1}\alpha = (\beta - \alpha)^{-1}(\beta - \alpha) = 1$. If $\beta - \alpha \notin R^\times$, then by Lemma 2.2.7, $(\beta - \alpha) \in Z(R)$. Then $\exists z_1 \in Z(R)$ such that $z_1(\beta - \alpha) = 0$ and so $z_1\alpha = z_1\beta$. As $z_1 \in Z(R), \exists z_2 \in Z(R)$ such that $z_2 z_1 = 0$. Then $z_2 z_1 \beta = z_2 z_1 \alpha = 0$, and as $z_2 z_1 \in Z(R)$, the assumption is contradicted. Thus, $\beta - \alpha \in R^\times$ and the result follows. □

One example of a finite ring is $\mathbb{Z}$ mod n, the integers modulo an ideal (n). $\mathbb{Z}_n^\times$ is the set of congruence classes (mod n) represented by integers coprime to n. $Z(\mathbb{Z}_n)$ is the set of congruence classes (mod n) of elements which are not coprime to n. For a specific example, consider $\mathbb{Z}_4$: $\mathbb{Z}_4^\times = \{[1], [3]\}$ and $Z(\mathbb{Z}_4) = \{[2]\}$ since $1 \times 1 \equiv 1 \pmod 4, 3 \times 3 = 9 \equiv 1 \pmod 4$ and $2 \times 2 = 4 \equiv 0 \pmod 4$. The projective special linear group for this example is $PSL_2(\mathbb{Z}_n) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \;\middle|\; a, b, c, d \in \mathbb{Z}_n,\ ad - bc = 1 \right\} / \pm \langle I \rangle$.

Cayley graphs are constructed from groups. Let $\Gamma = \{g_1, \ldots, g_n\}$ be a finite group and let $S \subset \Gamma$ be a symmetric generating set for Γ. The Cayley graph $G = G(\Gamma, S)$ is defined by $V(G) = \{g_1, \ldots, g_n\}$ and $g_i, g_j \in V(G)$ are adjacent if there exists $s \in S$ so that $sg_i = g_j$. Cayley graphs are amenable to study using group theory.

As an example, we give the Cayley graph for D_4, the dihedral group of the square.

Example 2.3: The Cayley graph $G(D_4, \{a, b, a^{-1} \mid a^4 = b^2 = 1, ab = ba^3\})$



A generating set for $PSL_2(\mathbb{Z} \bmod n)$ is $\{\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)\}$. This is a nice generating set because the Cayley graph it generates is Hamiltonian if n is prime [11]; usually Hamiltonian graphs are highly connected, but this graph is only cubic (every vertex has degree 3). This leads us to ask: what do such graphs look like for other generating sets?

2.3 - Quotients of Cayley Graphs and Platonic Graphs

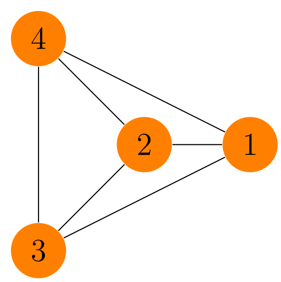
A quotient graph Q_G of a graph G is a graph whose vertices are blocks of a partition of $V(G)$, where blocks B_1 and B_2 are adjacent vertices in Q_G if some vertex in B_1 is adjacent to some vertex in B_2 in G. These blocks are the cosets of a subgroup N.

Lemma 2.3.1. *A quotient of a Cayley graph is a minor of a Cayley graph.*

Proof. Let $G = G(\Gamma, S)$ be a Cayley graph of a group Γ. The quotient graph G/N has vertices associated to the cosets gN of Γ/N. Two vertices of G, g_1, g_2, are in the same coset if and only if $g_1 = g_2 n$ for some $n \in N$. Thus the vertices of G/N are obtained by contracting the edges between g and gn for $n \in N$. Since minors are obtained by contracting edges and deleting vertices and/or edges, G/N is a minor of G. $\square$

A *Platonic graph* is a graph corresponding to the skeleton of a regular, convex polyhedron (the skeleton of a polyhedron is the graph created when the faces of a polyhedron are removed, leaving only its edges and vertices.) There are five Platonic solids and hence five Platonic graphs (the tetrahedral graph, cubic graph, octahedral graph, dodecahedral graph, and icosahedral graph). All of these are regular (every vertex has the same degree), planar, Hamiltonian graphs. Example 2.4 shows the tetrahedral graph.

Example 2.4: The tetrahedral graph



Platonic graphs, like quotient graphs of Cayley graphs, are minors of Cayley graphs.

In [14], it was found that for a prime p, the Platonic graph π_p can be partitioned into $\frac{p-1}{2}$ isomorphic copies of W_{p+1}, the wheel on $p+1$ vertices, with $2p$ edges joining every pair of wheels. That is, π_p is the complete multigraph $K^{2p}_{\frac{p-1}{2}}$, in which each vertex should be viewed as a wheel.

CHAPTER 3

A BRIEF SURVEY OF THE EXISTING LITERATURE

In this chapter we will survey the existing literature on Hadwiger's conjecture, Hamiltonicity, and the isoperimetric number.

3.1 - Hadwiger's conjecture

In 1943, Hadwiger presented his conjecture, "For every $n \in \mathbb{Z}_{\geq 0}$, every graph with no K_{n+1} minor is n-colorable" along with the proof for $n \leq 3$ [12]. It had already been shown by Klaus Wagner that when $n = 4$, the conjecture is equivalent to the famous Four Color Theorem. Before it was proved in 1976 by Appel and Haken (with substantial and nontrivial use of computer calculations) in [2] and [3], the Four Color Conjecture, as it was then known, was the most celebrated conjecture in graph theory. Hadwiger's conjecture has since been shown for the case $n = 5$ by Robertson, Seymour, and Thomas in [20], using the Four Color Theorem in their proof.

The cases for $n \geq 6$ are all open, although some specific results have been found when restrictions are put upon the graphs. Some weaker results have also been found. For example, Albar and Gonçalves proved in 2013 that every K_7-minor free graph is 8-colorable and every K_8-minor free graph is 10-colorable, improving the previously known bounds by one [1]. This is still slightly weaker than Hadwiger's conjecture, which says that every K_7-minor free graph is 6-colorable and every K_8-minor free graph is 7-colorable. It can also be shown (by applying a theorem in [4] and a theorem in [10]) that almost every graph G either has a K_{n+1}-minor or is n-colorable. This is a weakening of Hadwiger's conjecture, which says that every graph G either has a K_{n+1}-minor or is n-colorable. By "almost every", we mean that the proportion of graphs that satisfy Hadwiger's conjecture tends to 1 as the number of vertices increases.

3.2 - Hamiltonicity

The question of whether or not all Cayley graphs are Hamiltonian was first raised as a weaker version of the 1969 Lovász conjecture [16], which says that every finite, connected, vertex-transitive graph is Hamiltonian (a graph is vertex-transitive if no vertex can be distinguished from any other vertex by the edges and vertices surrounding it.) The advantage of studying the weaker version of the Lovász conjecture is that Cayley graphs are connected to a finite group and a generating set, so it is possible to show that the conjecture holds for particular kinds of groups and generating sets, rather than attempting to prove the conjecture in full generality.

Many particular Cayley graphs have been shown to be Hamiltonian, but the arguments are ad hoc and not easily genearlized. It was shown in 1983 by Marusic that Cayley graphs of finite Abelian groups are guarunteed to have a Hamilton cycle [17] . In 1986, D. Witte proved that the Cayley graphs of p-groups (a group Γ such that all the elements of Γ have a power of p as their order, for some prime p) are Hamiltonian [24].

3.3 - Isoperimetric number

The isoperimetric number has many applications in combinatorics, such as finding bounds on graph eigenvalues (the eigenvalues of the adjacency matrix of a graph), or on measuring the connectedness of a graph to find good expanders. However, though useful, $h(G)$ is difficult to calculate exactly. An oft-used alternative is to find bounds for $h(G)$ based on other properties of the particular graph in question. We present some of the bounds that have been found recently.

In 1993, Brooks, Perry, and Petersen [5] found the following bounds for the isoperimetric number of certain Platonic graphs: for p a prime such that $p \equiv 1 \pmod 4$, $\frac{p^2-2p+5}{4(p-1)} \leq h(\pi_p) \leq \frac{p(p-1)}{2(p+1)}$.

In 2009, Huang, Jin, and Liang found the following bound for the isoperimetric number of a k-degree Cayley graph (an undirected graph with $n(k-1)^n$ vertices for any $n \geq 2, k \geq 3$): $h(G_n) \leq \frac{2}{n-1}$ [13].

One of the more recent results for $\mathbb{Z}_n$ was found two years later; Lanphier and Rosenhouse [15] used combinatorics to find upper and lower bounds for the isoperimetric number of regular graphs with high degree, and they gave the specific application of the Platonic graphs over the rings $\mathbb{Z}_n$. For $\pi_{\mathbb{Z}_n}$, the isoperimetric number is bounded above and below as follows, where $\prod_{p|n}$ represents the product over those primes p which divide n: $\frac{n}{2}(1 - \sqrt{1 - 2\prod_{p|n}\left(1 - \frac{1}{p}\right) + \prod_{p|n}\left(1 - \frac{1}{p^2}\right)}) \leq h(\pi_{\mathbb{Z}_n}) \leq \frac{n}{2} - \frac{1}{\prod_{p|n}\left(1+\frac{1}{p}\right)}$.

CHAPTER 4

THE DECOMPOSITION THEOREM

In this chapter, we seek to find a decomposition for the quotient graphs of the Cayley graphs of $PSL(2)$ over finite commutative rings. By discovering the structure of the quotient graphs, we are able to study the structure and properties of the Cayley graphs.

First we will define the Cayley graphs we study, as well as their quotient graphs. We will show that the quotient group is isomorphic to 2-tuples, which are easier to study than the original matrices, and then we will examine the adjacencies that exist in the quotient graph. In particular, we will show that for finite rings without zero divisors, the quotient graph looks like a complete multigraph of wheels. Each vertex in a wheel sends two edges to every other wheel.

We now define our Cayley graphs. Let R be a finite commutative ring, with $n = |R|$. Then

$$SL_2(R) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in R, ad - bc = 1\}$$

and

$$\Gamma_R = PSL_2(R) = SL_2(R)/\{\pm I\}.$$

For $a \in R^\times$, let $I_a \in \Gamma_R$ be $I_a = \left(\begin{smallmatrix} 0 & a \\ -a^{-1} & 0 \end{smallmatrix}\right)$. Let t_R be a symmetric generating set for R^+, where R^+ is the ring as a group under addition. This means that R^+ has generators as a group under addition. Some examples are: $\mathbb{Z}^+$ has generators $\{1, -1\}$, $\mathbb{Z}_n^+$ has generator $\{1\}$, and $\mathbb{Z}_i^+$ has generators $\{1, -1, i, -i\}$. Let

$$T_R^+ = \{\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) | t \in t_R\},$$

$$T_R^- = \{\left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right) | t \in t_R\},$$

and let $T_R = T_R^+$ or T_R^-. Let S_R be a symmetric generating set for Γ_R so that $I_a \cup T_R \subset S_R$ for some $a \in R^\times$. Let $G_R = G(\Gamma_R, S_R)$ be the Cayley graph of Γ_R with respect to S_R. Note that G_R is $|S_R|$-regular. For example, for $R = \mathbb{Z}_n$, the ring of integers modulo n, then $1 \in \mathbb{Z}_n^\times$ and $\{-1, 1\}$ is a symmetric generating set for $\mathbb{Z}_n$. Thus we can take $S_R = \{\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & \pm 1 \\ 0 & 1 \end{smallmatrix}\right)\}$. In this case, G_R is a cubic graph.

Our first major mathematical step will be to examine quotient graphs of Cayley graphs of $PSL_2(R)$. If we let N_R be the subgroup of $PSL_2(R)$ that is the set of matrices

$$N_R = \{\left(\begin{smallmatrix} a & r \\ 0 & a^{-1} \end{smallmatrix}\right) \mid r \in R, a \in R^\times - \{0\}\},$$

then the quotient $PSL_2(R)/N_R \approx \{\left(\begin{smallmatrix} c & d \end{smallmatrix}\right) \mid c, d \in R, cd \neq 0\}$.

We will study graphs related to these objects as a prelude to generalizing our findings to Cayley graphs.

Let G'_R denote the quotient graph G_R/N_R, which is to say $G'_R = G'_{R,a}$. That is, G'_R is the multigraph whose vertices are given by the cosets of Γ'_R, where $\Gamma'_R = G/N$. Then distinct cosets of $N_R\gamma_1$ and $N_R\gamma_2$ are joined by as many edges as there are in G_R of the form (v_1, v_2) where $v_1 \in N_R\gamma_1$ and $v_2 \in N_R\gamma_2$. Note that Γ'_R is not a group, so G'_R is not a Cayley graph. However, G'_R is induced from the Cayley graph G_R, and is therefore useful to study in order to glean information about the G_R.

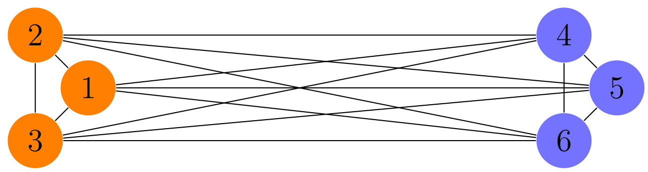
Lemma 4.1.1. *G'_R is a minor of G_R.*

Proof. Recall that by Lemma 2.3.1, quotient graphs are minors. G'_R is a quotient graph of G_R, hence G'_R is a minor of G_R. □

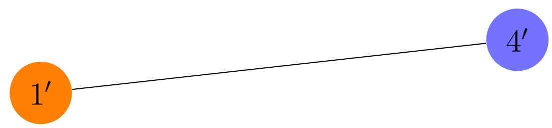
Note that the Cayley graph of N_R is a grid. G'_R is obtained by taking a copy of G_R and contracting each little copy of N_R within G_R to a single point. Then G'_R

contains $K_{|R^\times|}$ as a minor. As G'_R is a minor of G_R, it follows that G_R also contains $K_{|R^\times|}$ as a minor.

Example 4.1: G_R



Example 4.2: G'_R: the two copies of N_R contracted to single points



This allows us to prove the following proposition, where the isomorphism is an isomorphism of sets.

Proposition 4.1.2. $\Gamma'_R \cong \{\pm 1\}\backslash\{(\begin{smallmatrix}\alpha & \beta\end{smallmatrix})|\alpha, \beta \in R, (z\alpha, z\beta) \neq (0,0) \text{ for } z \in Z(R)\}$.

Proof. Let

$$S = \{\pm 1\}\backslash\{(\begin{smallmatrix}\alpha & \beta\end{smallmatrix})|\alpha, \beta \in R, (z\alpha, z\beta) \neq (0,0), z \in Z(R)\}.$$

Let $[(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix})]$ denote an element in Γ'_R where $[(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix})]$ denotes the equivalence class in Γ'_R of $(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}) \in \Gamma_R$. Let $[(\begin{smallmatrix}\gamma & \delta\end{smallmatrix})]$ denote an element in S. Define $\phi : \Gamma'_R \to S$ as the mapping given by $\phi([(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix})]) = [(\begin{smallmatrix}\gamma & \delta\end{smallmatrix})]$. Suppose that A $= (\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}) \in PSL_2(R), A' = (\begin{smallmatrix}\alpha' & \beta' \\ \gamma' & \delta'\end{smallmatrix}) \in PSL_2(R)$, are such that $\phi(A) = \phi(A')$. Then $[(\begin{smallmatrix}\gamma & \delta\end{smallmatrix})] = [(\begin{smallmatrix}\gamma' & \delta'\end{smallmatrix})]$, so $(\begin{smallmatrix}\gamma & \delta\end{smallmatrix}) = \pm(\begin{smallmatrix}\gamma' & \delta'\end{smallmatrix})$. Recall that $PSL_2(R) = SL_2(R)(\mathrm{mod} \pm 1)$. Therefore $(\begin{smallmatrix}\alpha' & \beta' \\ \gamma' & \delta'\end{smallmatrix}) = (\begin{smallmatrix}\alpha' & \beta' \\ \pm\gamma' & \pm\delta'\end{smallmatrix})$. Now if we mod both sides of the equality by ± 1, we see that $(\begin{smallmatrix}\alpha' & \beta' \\ \gamma' & \delta'\end{smallmatrix}) = (\begin{smallmatrix}\pm\alpha' & \pm\beta' \\ \gamma' & \delta'\end{smallmatrix})$. Since $(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}) = (\begin{smallmatrix}\alpha' & \beta' \\ \gamma & \delta\end{smallmatrix}) \in PSL_2(R)$, both have determinant 1. So, $\alpha\delta - \gamma\beta = 1$ and $\alpha'\delta - \gamma\beta' = 1$, and thus $\alpha'\alpha\delta - \alpha'\gamma\beta = \alpha'$ and $\alpha\alpha'\delta - \alpha\gamma\beta' = \alpha$, and so $\gamma(\beta'\alpha - \alpha'\beta) = \alpha' - \alpha$.

Similarly, we get $\alpha\beta'\delta - \beta\beta'\gamma = \beta'$ and $\alpha'\beta\delta - \beta\beta'\gamma = \beta$, so $\delta(\alpha\beta' - \alpha'\beta) = \beta' - \beta$. Setting $a = \alpha\beta' - \alpha'\beta \in R$, we get $\gamma a = \alpha' - \alpha$ and $\delta a = \beta' - \beta$, so $\alpha' = \alpha + \gamma a$ and $\beta' = \beta + \delta a$. Therefore

$$\left(\begin{smallmatrix} \alpha' & \beta' \\ \gamma & \delta \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha+\gamma a & \beta+\delta a \\ \gamma & \delta \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right),$$

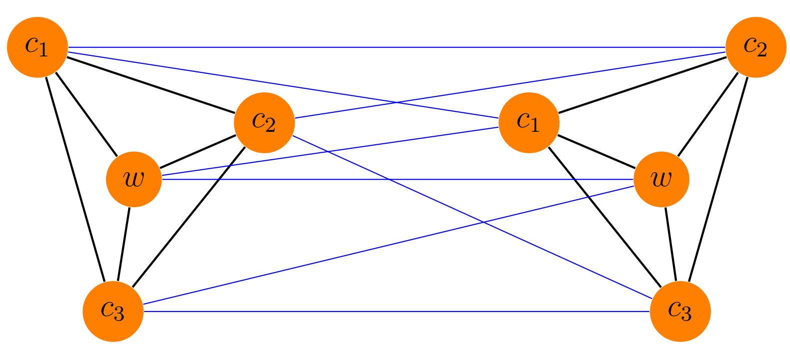
and so

$$[\left(\begin{smallmatrix} \alpha' & \beta' \\ \gamma & \delta \end{smallmatrix}\right)] = [\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)] = [\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)],$$

making ϕ one-to-one. Now to show ϕ is onto, let $[(\,\gamma\ \delta\,)] \in S$. By Lemma 2.2.8, there exists $x, y \in R$ such that $x\delta - y\gamma = 1$. Then $\det\left(\begin{smallmatrix} x & y \\ \gamma & \delta \end{smallmatrix}\right) = 1$ and so $\left(\begin{smallmatrix} x & y \\ \gamma & \delta \end{smallmatrix}\right) \in PSL_2(R)$. Therefore $\phi[\left(\begin{smallmatrix} x & y \\ \gamma & \delta \end{smallmatrix}\right)] = [(\,\gamma\ \delta\,)]$, making ϕ onto. □

We now loosely define the three main subgraphs that partition a Cayley graph. The subgraph induced by the units we will call C_R; the subgraph induced by the zero divisors we will call O_R, and the subgraph induced by the elements that are neither units nor zero divisors we will call T_R. Note that T_R does not exist if R is finite, by Lemma 2.2.7. C_R looks like a complete multigraph of wheels (see Example 4.3), and O_R seems to orbit it. These subgraphs are defined more rigorously in section 4.2.

Example 4.3: A complete multigraph on two copies of W_4



Note that if our ring $R = \mathbb{Z}_p$ for a prime p, then $O_{\mathbb{Z}_p} = \emptyset$ and so $\frac{|O_{\mathbb{Z}_p}|}{|C_{\mathbb{Z}_p}|} = 0$. When n is not prime we have that $O_{\mathbb{Z}_n}$ is nonempty. In that case, we have the following result, which shows that $O_{\mathbb{Z}_n}$ can be arbitrarily large or small in comparison to $C_{\mathbb{Z}_n}$.

Proposition 4.1.3. *Let $\epsilon > 0$ be arbitrarily small and $M > 0$ be arbitrarily large. There exists an $n \in \mathbb{N}$ such that $0 < \frac{|O_{\mathbb{Z}_n}|}{|C_{\mathbb{Z}_n}|} < \epsilon$ and there exists another $n \in \mathbb{N}$ such that $\frac{|O_{\mathbb{Z}_n}|}{|C_{\mathbb{Z}_n}|} > M$.*

Proof. From [14], we have

$$|PSL_2(\mathbb{Z}_n)| = \frac{n^3}{2} \prod_{p|n} \left(1 - \frac{1}{p^2}\right)$$

and so

$$|G'_{\mathbb{Z}_n}| = \frac{n^2}{2} \prod_{p|n} \left(1 - \frac{1}{p^2}\right).$$

From the decomposition of $C_{\mathbb{Z}_n}$ we have

$$|C_{\mathbb{Z}_n}| = \frac{n(n+1)}{2} \prod_{p|n} \left(1 - \frac{1}{p}\right) \text{[14]}.$$

Thus

$$\begin{aligned} |O_{\mathbb{Z}_n}| &= |G'_{\mathbb{Z}_n}| - |C_{\mathbb{Z}_n}| \\ &= \frac{n^2}{2} \prod_{p|n} \left(1 - \frac{1}{p^2}\right) - \frac{n(n+1)}{2} \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ &= \frac{n}{2} \prod_{p|n} \left(1 - \frac{1}{p}\right) \left(n \prod_{p|n} \left(1 + \frac{1}{p}\right) - n - 1\right). \end{aligned}$$

Thus

$$\begin{aligned}\frac{|O_{\mathbb{Z}_n}|}{|C_{\mathbb{Z}_n}|} &= \frac{\frac{n}{2}\prod_{p|n}\left(1-\frac{1}{p}\right)\left(n\prod_{p|n}\left(1+\frac{1}{p}\right)-n-1\right)}{\frac{n+1}{2}n\prod_{p|n}\left(1-\frac{1}{p}\right)} \\ &= \frac{n}{n+1}\prod_{p|n}\left(1+\frac{1}{p}\right)-1.\end{aligned}$$

The Riemann zeta function $\zeta(s)=\sum_{n=1}^{\infty} n^{-s}$, for $s \in \mathbb{C}$ and $Re(s)>1$, has the Euler product expansion $\zeta(s)=\prod_{p\ prime}\frac{1}{1-\frac{1}{p^s}}$, and it is well known that $|\zeta(s)| \to \infty$ as $s \to 1$. Then let $P_k=\prod_{j=1}^{k}(1-\frac{1}{p_j})$ be the product over the first k primes. Since $\zeta(s)\to\infty$ as $s\to 1$, we have that as k increases $\prod_{j=1}^{k}(1-\frac{1}{p_j^s})^{-1}\to\infty$. It follows that $P_k \to 0$ as k increases. Let $Q_k=\prod_{j=1}^{k}\left(1+\frac{1}{p_j}\right)$ be the product over the first k primes. Then

$$\begin{aligned}P_kQ_k &= \left(\prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right)\right)\left(\prod_{j=1}^{k}\left(1+\frac{1}{p_j}\right)\right) \\ &= \prod_{j=1}^{k}\left(1-\frac{1}{p_j^2}\right).\end{aligned}$$

As

$$\begin{aligned}\zeta(2) &= \frac{\pi^2}{6} \\ &= \prod_{p\ prime}\left(1-\frac{1}{p_j}\right)^{-1},\end{aligned}$$

then $P_kQ_k \to \frac{6}{\pi^2}$ as k increases. Thus if we take $n_k = p_1 \dots p_k$, a product of the first

k primes, then as k increases, we see that

$$\frac{|O_{\mathbb{Z}_n}|}{|C_{\mathbb{Z}_n}|} = \frac{n_k}{n_k+1}\prod_{p|n}\left(1+\frac{1}{p}\right) - 1$$

grows arbitrarily large.

Now take $n = p^r$. Then

$$\begin{aligned}\frac{|O_{\mathbb{Z}_n}|}{|C_{\mathbb{Z}_n}|} &= \frac{n}{n+1}\prod_{p|n}\left(1+\frac{1}{p}\right) - 1\\ &= \frac{p^r}{p^r+1}\left(1+\frac{1}{p}\right) - 1\\ &= \frac{p^{r-1}-1}{p^r+1}.\end{aligned}$$

If $p > \frac{1}{\epsilon}$, then $\epsilon > \frac{1}{p}$ and $p^r \cdot \frac{1}{p} < \epsilon p^r + \epsilon + 1$. Thus, $p^{r-1} - 1 < \epsilon(p^r + 1)$ and $\frac{|O_{\mathbb{Z}_n}|}{|C_{\mathbb{Z}_n}|} = \frac{p^{r-1}-1}{p^r+1} < \epsilon$. □

4.2 - The structure of quotient graphs

The following lemma helps us start to understand the structure of the quotient graphs. The brackets around $[(\alpha, \beta)]$ and $[(\gamma, \delta)]$ indicate that (α, β) and (γ, δ) are up to $\pm$ equivalence classes.

Lemma 4.2.1. *Let $[(\alpha, \beta)]$ and $[(\gamma, \delta)]$ be vertices in G'_R. Then $[(\alpha, \beta)]$ and $[(\gamma, \delta)]$ are adjacent in G'_R if and only if det$\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) = \pm a^{-1}$.*

Proof. Let $\Psi_\Gamma : \Gamma_R \to \Gamma'_R$ denote the quotient map, which is $\Psi_\Gamma(g) = N_R g$, and let $\phi : \Gamma'_R \to S$ denote the isomorphism of sets from Proposition 4.1.3. For $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in G_R$, let $\Psi_G\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) = \Phi(\Psi_\Gamma\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)) = [(\,\gamma\ \delta\,)]$, and so $\Psi_G : G_R \to G'_R$ is a graph homomorphism. Note that if $g_1 \in \Psi_G^{-1}(g'_1)$ and $g_2 \in \Psi_G^{-1}(g_2^{-1})$ so that $g_1 = \left(\begin{smallmatrix}0 & a\\ -a^{-1} & 0\end{smallmatrix}\right)g_2$, then g_1 and g_2 are adjacent in G_R. It follows that g'_1 and g'_2 are adjacent in G'_R. Let $[(\,\alpha\ \beta\,)]$

and $[(\begin{smallmatrix}\gamma & \delta\end{smallmatrix})]$ be vertices in G'_R so that $\det(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}) = \pm a^{-1}$. Then $(\begin{smallmatrix}a\alpha & a\beta \\ \gamma & \delta\end{smallmatrix})$ and $(\begin{smallmatrix}a\gamma & a\delta \\ \alpha & \beta\end{smallmatrix})$ are in Γ_R, and $(\begin{smallmatrix}0 & a \\ -a^{-1} & 0\end{smallmatrix})(\begin{smallmatrix}a\alpha & a\beta \\ \gamma & \delta\end{smallmatrix}) = (\begin{smallmatrix}a\gamma & a\delta \\ \alpha & \beta\end{smallmatrix})$. Since Γ_R is defined modulo $\{\pm I\}$, we have $[(\begin{smallmatrix}-a\gamma & -a\delta \\ \alpha & \beta\end{smallmatrix})] = [(\begin{smallmatrix}a\gamma & a\delta \\ -\alpha & -\beta\end{smallmatrix})]$ in Γ_R. Thus $(\begin{smallmatrix}a\alpha & a\beta \\ \gamma & \delta\end{smallmatrix})$ and $(\begin{smallmatrix}-a\gamma & -a\delta \\ \alpha & \beta\end{smallmatrix})$ are adjacent in G_R, joined by an edge that corresponds to the involution $(\begin{smallmatrix}-a\gamma & -a\delta \\ \alpha & \beta\end{smallmatrix})$ in S_R. From the first paragraph of the proof, we have that $[(\begin{smallmatrix}\alpha & \beta\end{smallmatrix})]$ and $[(\begin{smallmatrix}\gamma & \delta\end{smallmatrix})]$ are adjacent in G'_R.

Now let $\Psi : G_R \to G'_R$ be the graph homomorphism induced by the quotient map. Let $g'_1 \in [(\alpha, \beta)] \in V(G'_R)$ and $g'_2 \in [(\gamma, \delta)] \in V(G'_R)$ be adjacent in G'_R. It follows that there exist $g_1 \in \Psi^{-1}(g'_1)$ and $g_2 \in \Psi^{-1}(g'_2)$ so that g_1 is adjacent to g_2 in G_R. The quotient map Ψ takes $(\begin{smallmatrix}x & y \\ z & w\end{smallmatrix}) \in G_R$ to $[(\begin{smallmatrix}z & w\end{smallmatrix})] \in G'_R$ so $g_1 = (\begin{smallmatrix}x & y \\ \alpha & \beta\end{smallmatrix})$ and $g_2 = (\begin{smallmatrix}w & z \\ \gamma & \delta\end{smallmatrix})$ where $\det(g_2) = \pm 1$. Since g_1 and g_2 are adjacent in G_R, it follows that $g_2 = (\begin{smallmatrix}1 & \pm t \\ 0 & 1\end{smallmatrix})g_1$ or $g_2 = (\begin{smallmatrix}0 & a \\ -a^{-1} & 0\end{smallmatrix})g_1$. In the former case, we would have $g'_2 = \Psi(g_2) = \Psi(g_1) = g'_1$, which contradicts G'_R being a simple graph. So we must have the latter case. Thus, $(\begin{smallmatrix}w & z \\ \gamma & \delta\end{smallmatrix}) = g_2 = (\begin{smallmatrix}0 & a \\ -a^{-1} & 0\end{smallmatrix})g_1 = (\begin{smallmatrix}0 & a \\ -a^{-1} & 0\end{smallmatrix})(\begin{smallmatrix}x & y \\ \alpha & \beta\end{smallmatrix}) = (\begin{smallmatrix}a\alpha & a\beta \\ -a^{-1}x & -a^{-1}y\end{smallmatrix})$ and so $w = a\alpha$ and $z = a\beta$. Thus

$$\begin{aligned}\det(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}) &= a^{-1}\det(\begin{smallmatrix}a\alpha & a\beta \\ \gamma & \delta\end{smallmatrix}) \\ &= a^{-1}\det(\begin{smallmatrix}w & z \\ \gamma & \delta\end{smallmatrix}) \\ &= \pm a^{-1}.\end{aligned}$$

□

This leads us to

$$V(G'_R) = V(C_R) \cup V(O_R)$$

where C_R has a distinct structure. Let $\alpha \in R^\times$, and define $V(\alpha) \subset V(G'_R)$ by

$$V(\alpha) = \{(0, \alpha), (a^{-1}\alpha, \beta) | \beta \in R\}.$$

Let $H(\alpha) = G[V(\alpha)]$ be the subgraph of G'_R induced by $V(\alpha)$. Note that $|H(\alpha)| = n+1$. Further note that $|N_R| = n$, implying that $|V(G'_R)| = \frac{|V(G_R)|}{n}$. We also have that G_R is $|S_R|-$regular.

Let $H(\alpha) \neq H(\alpha')$ with $\alpha, \alpha' \in R^\times$.

Lemma 4.2.2. *$(\begin{smallmatrix} \alpha & \beta \end{smallmatrix}) \in H(\alpha)$ is adjacent to two elements in $H(\alpha')$.*

Proof. Let $(\begin{smallmatrix} \alpha & \beta \end{smallmatrix}) \in H(\alpha)$ and $(\begin{smallmatrix} \alpha' & \beta' \end{smallmatrix}) \in H(\alpha')$. Then by Lemma 4.2.1, $(\begin{smallmatrix} \alpha & \beta \end{smallmatrix})$ is adjacent to $(\begin{smallmatrix} \alpha' & \beta' \end{smallmatrix})$ if and only if $\det(\begin{smallmatrix} \alpha & \beta \\ \alpha' & \beta' \end{smallmatrix}) = \pm a^{-1}$, that is, if and only if $\alpha\beta' - \alpha'\beta = \pm a^{-1}$. So $(\begin{smallmatrix} \alpha & \beta \end{smallmatrix})$ is adjacent to $(\begin{smallmatrix} \alpha' & \beta' \end{smallmatrix})$ if and only if $\beta' = \alpha^{-1}(\alpha'\beta \pm a^{-1})$. There are two elements β'_1 and $\beta'_2 \in R$ that satisfy this, which means there are two elements $(\begin{smallmatrix} \alpha' & \beta'_1 \end{smallmatrix})$ and $(\begin{smallmatrix} \alpha' & \beta'_2 \end{smallmatrix}) \in H(\alpha')$ adjacent to $(\begin{smallmatrix} \alpha & \beta \end{smallmatrix})$. □

This means that each vertex in a wheel is adjacent to two vertices within any other wheel. We now examine the structure of $H(\alpha)$. Recall that $H(\alpha) = \{(\begin{smallmatrix} 0 & \alpha \end{smallmatrix}), (\begin{smallmatrix} \alpha^{-1}a^{-1} & \beta \end{smallmatrix}) \mid \beta \in R\}$. Note that if $(\begin{smallmatrix} \alpha^{-1}a^{-1} & \beta \end{smallmatrix})$ is adjacent to $(\begin{smallmatrix} \alpha^{-1}a^{-1} & \beta' \end{smallmatrix})$ then

$$\begin{aligned} \pm a^{-1} &= \det(\begin{smallmatrix} \alpha^{-1}a^{-1} & \beta \\ \alpha^{-1}a^{-1} & \beta' \end{smallmatrix}) \\ &= \alpha^{-1}a^{-1}(\beta' - \beta) \end{aligned}$$

and so $(\beta' - \beta) = \pm\alpha$, making $\beta' = \beta \pm \alpha$. Thus, if there is some $n \in \mathbb{N}$ so that $n = 0$ in R, then $H(\alpha)$ contains a cycle

$$(\begin{smallmatrix} a^{-1}\alpha^{-1} & \beta \end{smallmatrix}), (\begin{smallmatrix} a^{-1}\alpha^{-1} & \beta+\alpha \end{smallmatrix}), (\begin{smallmatrix} a^{-1}\alpha^{-1} & \beta+2\alpha \end{smallmatrix}), \ldots, (\begin{smallmatrix} a^{-1}\alpha^{-1} & \beta+(n-1)\alpha \end{smallmatrix}).$$

Depending on the structure of R, there can be several such cycles in $H(\alpha)$.

Lemma 4.2.3. *Let $\alpha, \delta \in R^\times$. If $\delta \neq \pm\alpha$, then $H(\delta) \cap H(\alpha) = \emptyset$.*

Proof. As G_R is modulo ± 1, then so is G'_R and therefore $H(\pm\alpha) = H(\alpha)$. Suppose $\delta \neq \pm\alpha$, then $(0, \delta) \neq (0, \alpha)$, and if $(a^{-1}\delta, \beta) = (a^{-1}\alpha, \beta')$ for some $\beta, \beta' \in R$, then

$a^{-1}\delta = a^{-1}\alpha$. Thus $\alpha = \delta$, which gives a contradiction. Therefore, we must have $H(\alpha) \cap H(\delta) = \emptyset$. $\square$

Let C_R be the subgraph of G'_R induced by the $H(\alpha)$'s. That is, $V(C_R) = \bigcup_{\alpha} V(H(\alpha))$ where the union is over the distinct $H(\alpha)$'s (by Lemma 4.2.3, the wheels do not overlap.)

Now let

$$O_R = \{(\gamma, \delta) \in G'_R | (\gamma, \delta) \notin C_R\}.$$

Lemma 4.2.4. $O_R = \{(\gamma, \delta) \in G'_R | \gamma \in Z(R)\}$.

Proof. Let

$$S_R = \{(\gamma, \delta) \in G'_R | \gamma \in Z(R)\}.$$

For $(\gamma, \delta) \in S_R, (\gamma, \delta) \in G'_R$ and $\gamma \in Z(R)$, so $\gamma \neq 0$. Since $\gamma \in Z(R)$, by Lemma 2.3.7 $\gamma \notin R^\times$. Thus $\gamma \neq a^{-1}\alpha$ for any $\alpha \in R^\times$, implying that $(\gamma, \delta) \notin C_R$. Therefore, $(\gamma, \delta) \in O_R$, and $S_R \subseteq O_R$. Now let $(\gamma, \delta) \in O_R$. If $\gamma = 0$, then $(0, \delta) \in G'_R$, and since G'_R is connected, there must be some $(\alpha, \beta) \in G'_R$ such that $\det\left(\begin{smallmatrix} \alpha & \beta \\ 0 & \delta \end{smallmatrix}\right) \in R^\times$. This implies that $\delta \in R^\times$. Then $(0, \delta) \in H(\delta)$ and so $(0, \delta) \notin O_R$, and it follows that $\gamma \neq 0$. If $\gamma \in R^\times$, then $\gamma = a^{-1}\alpha$ for some $\alpha \in R^\times$, and so $(\gamma, \delta) = (a^{-1}\alpha, \delta) \in H(\alpha)$. Therefore $\gamma \notin R^\times$. By the previous lemma, this implies that $\gamma \in Z(R)$ and so $(\gamma, \delta) \in S_R$. Thus $O_R \subseteq S_R$ and the result follows. $\square$

Note that above we are looking only at the subset of zero divisors and units in R, because we are concerned only with the finite case.

This gives us $G'_R = C_R + O_R$, where $C_R \cap O_R = \emptyset$. Note that if $\gamma \in Z(R), \delta \notin Z(R)$, then $(\gamma, \delta) \in O_R$.

Corollary 4.2.5. *If* $|R| < \infty$ *and* $Z(R) = \emptyset$*, then* $G'_R = C_R$.

This guides us to examine the structure of O_R more closely, as having zero divisors adds complications to the structure of G'_R.

4.3 - The Decomposition

As we have already discussed, a ring R can be partitioned into three disjoint subsets (the units, the zero divisors, and for infinite rings, a third subset of elements which are neither units nor zero divisors); in general, $R = R^\times \cup Z(R) \cup \widetilde{R}$.

For $\alpha \in \widetilde{R}$, let

$$J(\alpha) = \{\left(\begin{smallmatrix} \alpha & \beta \end{smallmatrix}\right) \mid \beta \in R\}.$$

Note that if $\alpha \neq \pm\alpha'$ with $\alpha, \alpha' \in \widetilde{R}$, then $J(\alpha) \cap J(\alpha') = \emptyset$. Further, it is clear that $J(\alpha) \cap O_R = \emptyset$ and $J(\alpha) \cap C_R = \emptyset$.

Lemma 4.3.1. *For any $\alpha \notin R^\times \cup Z(R), J(\alpha)$ is an independent set of G'_R indexed by R.*

Proof. Let $v, v' \in J(\alpha)$. Then $v = \left(\begin{smallmatrix} \alpha & \beta \end{smallmatrix}\right)$ and $v' = \left(\begin{smallmatrix} \alpha' & \beta' \end{smallmatrix}\right)$ for some $\beta, \beta' \in R$. We have

$$\begin{aligned} \det\left(\begin{smallmatrix} \alpha & \beta \\ \alpha' & \beta' \end{smallmatrix}\right) &= \alpha\beta' - \alpha\beta \\ &= \alpha(\beta' - \beta). \end{aligned}$$

Since $\alpha \notin R^\times$, we see that $\alpha(\beta' - \beta)$ cannot be a unit in R. Thus $\left(\begin{smallmatrix} \alpha & \beta \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \alpha' & \beta' \end{smallmatrix}\right)$ cannot be adjacent in G'_R, so the vertices in $J(\alpha)$ are independent. Clearly the vertices in $J(\alpha)$ are indexed by R. □

Therefore, if there exists some $\alpha \in R - (R^\times \cup Z(R))$, then G'_R contains an independent set of size $|R|$. Furthermore, the edges in T_R are those that connect different $J(\alpha)s$.

Let $T_R = \bigcup_{\alpha \in \widetilde{R}} J(\alpha)$. This leads us to the general decomposition of the associated Cayley graph, G'_R.

We have now proved the main result of this paper: the decomposition of the graph G'_R and the corresponding decomposition of G_R. The point is that the subgraph C_R has an organized, connected, and studiable structure, whereas O_R and T_R have much less structure. However, $T_R = \emptyset$ for finite rings, and O_R depends upon the zero divisors of R. In particular, $O_R = \emptyset$ if R has no zero divisors.

Theorem 4.3.2. *The graph G'_R has the following decomposition:*

$$V(G'_R) = V(C_R) \;\cup\; V(O_R) \;\cup\; V(T_R)$$

where

$$V(C_R) = \bigcup_{\alpha \in R^\times/\{\pm 1\}} V(H(\alpha)),$$
$$H(\alpha) = \{\left(\begin{smallmatrix} \alpha & \beta \end{smallmatrix}\right) \mid \beta \in R\}.$$

If $H(\alpha) \neq H(\alpha')$ then the number of edges between $H(\alpha)$ and $H(\alpha')$ is

$$e(H(\alpha), H(\alpha')) = 2|R|,$$

$$V(O_R) = \{(\gamma, \delta) \in G'_R \mid \gamma \in Z(R)\},$$

and

$$T_R = \bigcup_{\alpha \in \widetilde{R}} J(\alpha),$$
$$\text{where } J(\alpha) = \{\left(\begin{smallmatrix} \alpha & \beta \end{smallmatrix}\right) \in G'_R \mid \beta \in R\}.$$

If R is finite and C'_R denotes the multigraph obtained from C_R by contracting each $H(\alpha)$ to a single vertex, then C'_R contains a spanning subgraph isomorphic to $K^{2|R|}_{\frac{|R^\times|}{2}}$, the complete multigraph on $\frac{|R^\times|}{2}$ vertices with $2|R|$ edges joining each pair of vertices.

Note that if $|R| < \infty$ then $T_R = \emptyset$, and if $Z(R) = \emptyset$ then $O_R = \emptyset$.

CHAPTER 5

CONSEQUENCES OF THE DECOMPOSITION THEOREM

In this chapter, we wish to prove Hadwiger's conjecture and Hamiltonicity for the graphs we have been studying, and to find a bound on their isoperimetric number.

5.1 - Hadwiger's conjecture

Let R be finite and $G_R = G(\Gamma_R, S_R)$. Recall that Hadwiger's conjecture would imply that $\eta(G) \geq \chi(G)$.

Corollary 5.1.1. *For R and G_R as above, we have $\eta(G_R) \geq \frac{|R^\times|}{2}$.*

Proof. G_R contains C_R, which contains $K^{2|R|}_{\frac{|R^\times|}{2}}$ as a minor. □

The proof that Hadwiger's conjecture holds for the Cayley graphs requires the use of Brooks' theorem.

5.1.1 Brooks' theorem (Brooks)**.** *For any connected undirected graph G with maximum degree $\Delta(G)$,*

$$\chi(G) \leq \Delta(G),$$

unless G is a complete graph or an odd cycle, in which case $\chi(G) = \Delta(G) + 1$.

We are now able to show that Hadwiger's conjecture holds for our Cayley graphs.

Theorem 5.1.2. *For R finite, if $\frac{|R^\times|}{2} \geq |S_R|$ then Hadwiger's conjecture holds for $G_R = G(\Gamma_R, S_R)$.*

Proof. From Corollary 5.1.1 and the hypothesis, we have

$$\eta(G_R) \geq \frac{|R^\times|}{2} \geq |S_R|.$$

Now, G_R is $|S_R|-$regular so we have $\Delta(G_R) = |S_R|$ and $\eta(G_R) \geq \Delta(G_R)$. By Brooks' theorem, since G_R is connected, non-complete, and non-cyclic, $\eta(G_R) \geq \Delta(G_R) \geq \chi(G_R)$. □

Note that G_R is non-cyclic because $|S| \geq 3$. In a cyclic Cayley graph, for example the Cayley graph of a cyclic group, we are only able to have one generator a and also its inverse a^{-1}. But the graph G_R has the involution as a generator $\left(\begin{smallmatrix} 0 & a \\ -a^{-1} & 0 \end{smallmatrix}\right)$ and also $\left(\begin{smallmatrix} 1 & t_R \\ 0 & 1 \end{smallmatrix}\right)$ where t_R generates the additive group R^+. Thus, there are at least 2 elements that we need for t_R, so G_R has at least 3 generators and so is at least a cubic graph. Therefore it is not cyclic.

We have established that $\eta(G_R) \geq \frac{|R^\times|}{2}$ for all G_R with generating sets S_R that satisfy $I_a \cup T_R \subseteq S_R$. By Brooks' Theorem, $\Delta(G_R) \geq \chi(G_R)$ as G_R is non-complete and is not an odd cycle. Since G_R is regular of degree $|S_R|$, it follows that $|S_R| \geq \chi(G_R)$. Therefore, if $\frac{|R^\times|}{2} \geq |S_R|$, then Hadwiger's conjecture holds for G_R.

5.2 - Hamiltonicity

Recall that a wheel graph is a graph created by connecting a vertex w to each of the vertices $c_1, \ldots, c_n$ of a cycle.

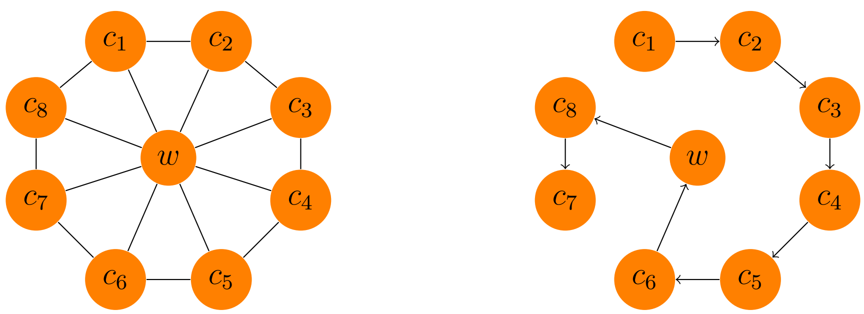
Lemma 5.2.1. *Wheel graphs are Hamilton connected.*

Proof. We can prove this by construction. Let W be a wheel graph, and call its vertex that is adjacent to every other vertex w. For any two vertices $c_i, c_k \in W$, we can create a Hamilton path from c_i to c_k. We begin at c_i and go clockwise around the cycle until we reach the vertex c_{k-1}, the vertex in the cycle adjacent to c_k on its left.

From the definition of a wheel graph, c_{k-1} is also adjacent to w, the center vertex, so we go from c_{k-1} to w, which is also adjacent to c_{i-1}. We then go from w to c_{i-1} and from there go counterclockwise until we get to c_k. This gives a Hamilton path. If either of our desired endpoints is the center vertex, the construction is even simpler; in this case we begin with the center vertex and go to c_{k+1}, the vertex adjacent to the other endpoint. Then we go around the cycle until we get back to c_k. □

Below is an example illustrating how we would construct a Hamilton path from c_1 to c_7 in a wheel with nine vertices. On the left we illustrate what that wheel looks like, on the right we show the construction.

Example 5.1: Constructing a Hamilton path from c_1 to c_7



Proposition 5.2.2. *Let R be a finite commutative ring so that $Z(R) = \emptyset$. Then G'_R is Hamiltonian.*

Proof. From the Decomposition Theorem, G'_R has the structure of a complete multigraph $K^{2|R|}_{\frac{|R^\times|}{2}}$ with $\frac{|R^\times|}{2}$ vertices, and so that there is a wheel graph at each vertex. Let $w_1, w_2, \ldots w_{\frac{|R^\times|}{2}}$ denote the distinct wheels so that

$$V(G'_R) = \bigcup_{j=1}^{\frac{|R^\times|}{2}} V(w_j).$$

Then there is a set of edges $\{e_j\}_{j=1}^{\frac{|R^\times|}{2}}$ so that

$$w_1 \overset{e_1}{-} w_2 \overset{e_2}{-} w_3 ... w_{\frac{|R^\times|}{2}} \overset{e_{\frac{|R^\times|}{2}}}{-} w_1.$$

Further, as there are $2|R|$ edges in G'_R between any pair of wheels, we can find distinct vertices $u_{1,j}, u_{2,j} \in V(w_j)$ so that e_j has endpoints $u_{2,j}$ and $u_{1,j+1}$. If $j = \frac{|R^\times|}{2}$ then $e_{\frac{|R^\times|}{2}}$ has endpoints $u_{2,\frac{|R^\times|}{2}}$ and $u_{1,1}$. From Lemma 5.2.1, there is a Hamilton path P_j in W_j from $u_{1,j}$ to $u_{2,j}$, for any j. Thus we have

$$u_{1,1}P_1u_{2,1} \overset{e_1}{-} u_{1,2}P_2u_{2,2} \overset{e_2}{-} ... \overset{e_{\frac{|R^\times|}{2}-1}}{-} u_{1,\frac{|R^\times|}{2}} P_{\frac{|R^\times|}{2}} u_{2,\frac{|R^\times|}{2}} \overset{e_{\frac{|R^\times|}{2}}}{-} u_{1,1},$$

which gives a Hamilton cycle in G'_R. □

Lemma 5.2.3. *If $\left(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}\right)$ is adjacent to $\left(\begin{smallmatrix} w & z \\ \gamma & \delta \end{smallmatrix}\right)$ in G_R, and $\left(\begin{smallmatrix} x' & y' \\ \alpha & \beta \end{smallmatrix}\right)$ is adjacent to $\left(\begin{smallmatrix} w' & z' \\ \gamma' & \delta' \end{smallmatrix}\right)$ with $\gamma \neq \gamma'$, then $\left(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} x' & y' \\ \alpha & \beta \end{smallmatrix}\right)$ in G_R.*

Proof. If $\left(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}\right)$ is adjacent to $\left(\begin{smallmatrix} w & z \\ \gamma & \delta \end{smallmatrix}\right)$, then

$$\begin{aligned} \left(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 0 & a \\ -a^{-1} & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} w & z \\ \gamma & \delta \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} a\gamma & a\delta \\ \alpha & \beta \end{smallmatrix}\right), \end{aligned}$$

so $\left(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}\right) = \left(\begin{smallmatrix} a\gamma & a\delta \\ \alpha & \beta \end{smallmatrix}\right)$. Similarly, if $\left(\begin{smallmatrix} x' & y' \\ \alpha & \beta \end{smallmatrix}\right)$ is adjacent to $\left(\begin{smallmatrix} w' & z' \\ \gamma' & \delta' \end{smallmatrix}\right)$, then $\left(\begin{smallmatrix} x' & y' \\ \alpha & \beta \end{smallmatrix}\right) = \left(\begin{smallmatrix} a\gamma' & a\delta' \\ \alpha & \beta \end{smallmatrix}\right)$, and as $\gamma \neq \gamma'$, then $a\gamma \neq a\gamma'$, the result follows. □

Let $v \in V(G'_R)$ and let $G(v)$ denote the $|R|$ vertices in $V(G'_R)$ equivalent to v under the action of N_R. For convenience, we also refer to the subgraph induced by these N_R vertices as $G(v)$.

Lemma 5.2.4. *Let R be a finite commutative ring with $|R|$ odd. If $|t_R| \geq 4$ then the graphs $G(v)$ are Hamilton connected.*

Proof. Let $\phi : R^+ \to N_R$ be the mapping $\phi(x) = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$. Then

$$\begin{aligned} \phi(x+y) &= \left(\begin{smallmatrix} 1 & x+y \\ 0 & 1 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) \\ &= \phi(x)\phi(y), \end{aligned}$$

so ϕ is a homomorphism. It is clear that ϕ is onto, and if $\phi(x) = \phi(y)$ then $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)$, so $x = y$. Thus ϕ is also an isomorphism.

For $t \in t_R$, the symmetric generating set for R^+, then $\phi(t) = \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) \in T_R$, the symmetric generating set for N_R. It follows that ϕ induces an isomorphism between the Cayley graphs $G(R^+, t_R)$ and $G(N_R, T_R)$.

Because $T_R \subseteq S$, where S is the generating set for G_R, then by construction $G(v)$ is isomorphic to $G(N_R, T_R)$. Therefore $G(v)$ is isomorphic to $G(R^+, t_R)$.

Since $|t_R| \geq 4$, $G(R^+, t_R)$ is a Cayley graph of an Abelian group with at least 4 generators, so it contains a spanning subgraph isomorphic to a grid. Thus $G(v)$ contains a spanning subgraph isomorphic to a grid. By Theorem 4 of [6], grid graphs are Hamilton connected if and only if they are neither cyclic nor bipartite. Because the grid graph in $G(v)$ is $|t_R|$-regular, and $|t_R| \geq 4$, the graph is not cyclic. Since $|R|$ is odd, the cycle generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in G(v)$ has odd length. It is well-known (see [23]) that bipartite graphs do not contain cycles of odd length. Thus the grid graph in $G(v)$ is not bipartite and so it is Hamilton connected. It follows that $G(v)$ is Hamilton connected. □

Lemma 5.2.5. *Let $[(\begin{smallmatrix} \alpha & \beta \end{smallmatrix})] \in V(G'_R)$ be adjacent to distinct vertices $[(\begin{smallmatrix} \alpha & \beta_0 \end{smallmatrix})]$ and $[(\begin{smallmatrix} \alpha & \beta_1 \end{smallmatrix})]$ in G'_R. Then there exist distinct vertices $\left(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} x' & y' \\ \alpha & \beta \end{smallmatrix}\right)$ such that $\left(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}\right)$ is adjacent to a vertex $\left(\begin{smallmatrix} x_0 & y_0 \\ \alpha & \beta_0 \end{smallmatrix}\right)$ in G_R and $\left(\begin{smallmatrix} x' & y' \\ \alpha & \beta \end{smallmatrix}\right)$ is adjacent to a vertex $\left(\begin{smallmatrix} x_1 & y_1 \\ \alpha & \beta_1 \end{smallmatrix}\right)$ in G_R.*

Proof. Let $\phi : G_R \to G'_R$ be the mapping on the graphs induced by the quotient map on the respective groups. Then $\phi(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}) = [(\alpha\ \beta)]$. As $[(\alpha\ \beta)]$ is adjacent to $[(\alpha\ \beta_0)]$ in G'_R then there are vertices in the respective preimages of ϕ, $(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix})$ and $(\begin{smallmatrix} x_0 & y_0 \\ \alpha & \beta_0 \end{smallmatrix})$, that are adjacent in G_R. Therefore, there is some $s \in S$, the symmetric generating set of Γ_R, so that $s(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}) = (\begin{smallmatrix} x_0 & y_0 \\ \alpha & \beta_0 \end{smallmatrix})$. If $s \in T_R$, then $s = (\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix})$ and

$$\begin{aligned} s(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}) &= (\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix})(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}) \\ &= (\begin{smallmatrix} x+t\alpha & y+t\beta \\ \alpha & \beta \end{smallmatrix}). \end{aligned}$$

But since $\beta \neq \beta_0$, this cannot be equal to $(\begin{smallmatrix} x_0 & y_0 \\ \alpha & \beta_0 \end{smallmatrix})$.

Thus

$$\begin{aligned} s(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}) &= (\begin{smallmatrix} 0 & -a \\ -a^{-1} & 0 \end{smallmatrix})(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}) \\ &= (\begin{smallmatrix} -a\alpha & y+-a\beta_0 \\ -a^{-1}x & -a^{-1}y \end{smallmatrix}), \end{aligned}$$

which gives $(\begin{smallmatrix} x_0 & y_0 \\ \alpha & \beta_0 \end{smallmatrix}) = (\begin{smallmatrix} -a\alpha & -a\beta \\ -a^{-1}x & -a^{-1}y \end{smallmatrix})$. Thus $(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}) = (\begin{smallmatrix} -a\alpha & -a\beta_0 \\ \alpha & \beta \end{smallmatrix})$. Similarly, if $(\begin{smallmatrix} x' & y' \\ \alpha & \beta \end{smallmatrix})$ is adjacent to $(\begin{smallmatrix} x_1 & y_1 \\ \alpha & \beta_1 \end{smallmatrix})$ then $(\begin{smallmatrix} x' & y' \\ \alpha & \beta \end{smallmatrix}) = (\begin{smallmatrix} -a\alpha & -a\beta_1 \\ \alpha & \beta \end{smallmatrix})$. $\beta_0 \neq \beta$, so $(\begin{smallmatrix} x & y \\ \alpha & \beta \end{smallmatrix}) \neq (\begin{smallmatrix} x' & y' \\ \alpha & \beta \end{smallmatrix})$ and these vertices are adjacent to the appropriate vertices in the statement of the lemma. Note that the same argument deals with the center vertex so it does not need to be addressed separately. □

As a direct result of the decomposition and the lemmas above, we have the following corollary. Note that G_R is $1 + |t_R|$-regular (and G'_R is $|R|$-regular).

Corollary 5.2.6. *For R a finite commutative ring such that $|R|$ is odd, $Z(R) = \emptyset$, and $|t_{R^+}| \geq 4$, G_R is Hamiltonian.*

Proof. Let $k = |G_R|$. Since G'_R is Hamiltonian, there is a Hamilton cycle $v_1, ..., v_k$ in G'_R. Let e_i be the edge joining v_i to v_{i+1} for $1 \leq i \leq k-1$ and let e_k be the edge joining v_k to v_1. Let $\{G(v_i)\}_{i=1}^k$ denote the $|R|$ vertices in G_R that give rise to the vertex $v_i \in V(G'_R)$. In other words, for $\phi : G_R \to G'_R$ the usual mapping induced by the quotient map, we have $\phi(v) = v_i$ for any $v \in G(v)_i$.

For every e_i as above, there is a pair of vertices $w_{2,i}, w_{1,i+1} \in V(G_R)$ that are the endpoints of e_i, where $w_{2,i} \in G(v)_i$ and $w_{1,i+1} \in G(v)_{i+1}$. Note that it is understood that if $i = k$ then $w_{1,k+1}$ is $w_{1,1}$ and $G(v)_{i+1}$ is $G(v)_1$. Therefore, for each i there are vertices $w_{1,i}$, $w_{2,i} \in G(v)_i$ so that $w_{1,i}$ is adjacent to $w_{2,i-1}$ and $w_{2,i}$ is adjacent to $w_{1,i+1}$.

Now $\phi(w_{1,i}) = \phi(w_{2,i}) = v_i$, and v_i is adjacent to v_{i-1} and v_{i+1}. By the previous lemmas, there exist distinct vertices, which we label $w_{1,i}, w_{2,i}$, in the preimage of v_i so that $w_{1,i}$ is adjacent to some $w_{2,i-1}$ in the preimage of v_{i-1}, and $w_{2,i}$ is adjacent to some $w_{1,i+1}$ in the preimage of v_{i+1}. Therefore we can assume that $w_{1,i}$ and $w_{2,i}$ are distinct.

Since $G(v)_i$ is Hamilton connected, there is a Hamilton path P_i from $w_{1,i}$ to $w_{2,i}$ in $G(v)_i$. Thus we have a Hamilton cycle

$$w_{1,1}P_1w_{2,1} \overset{e_1}{-} w_{1,2}P_2w_{2,2} \overset{e_2}{-} \ldots \overset{e_{k-1}}{-} w_{1,k}P_kw_{2,k} \overset{e_k}{-} w_{1,1}$$

in G_R. □

5.3 - Isoperimetric number

Note that if $|R| < \infty$ and $Z(R) = \emptyset$, then $V(G'_R) = V(C_R)$.

If $|R^\times| \equiv 0 \bmod 4$, then C_R can be decomposed into two sets S and S', each with $\frac{|R^\times|}{4}$ copies of $H(\alpha)$.

As there are $2|R|$ edges between any two distinct $H(\alpha)$s, then there are $\frac{2|R||R^\times|}{4}$ edges from one $H(\alpha)$ in S and all the other $H(\alpha)$s in S'. Thus there are $2|R|(\frac{|R^\times|}{4})^2$ edges between S and S'. There are $|R| + 1$ vertices in each $H(\alpha)$, so there are

$\frac{|R^\times|}{4}(|R|+1)$ vertices in S. So we have

$$
\begin{aligned}
h(G'_R) &\leq \frac{|\partial S|}{|S|} \\
&= \frac{2|R|(\frac{|R^\times|}{4})^2}{\frac{|R^\times|}{4}(|R|+1)} \\
&= \frac{|R|(|R^\times|}{2(|R|+1)}.
\end{aligned}
$$

As $|N_R| = |R|$, there are $|R|$ vertices in G_R for each vertex in G'_R, so we get

$$h(G_R) \leq \frac{|R^\times|}{2(|R|+1)}.$$

If $|R^\times| \equiv 2 \pmod 4$, then C_R can be decomposed into two sets S and S', where S has $\frac{\frac{|R^\times|}{2}-1}{2} = \frac{|R^\times|}{4} - \frac{1}{2}$ copies of $H(\alpha)$ and S' has

$$\frac{\frac{|R^\times|}{2}+1}{2} = \frac{|R^\times|}{4} + \frac{1}{2}$$

copies of $H(\alpha)$. Thus S has

$$(|R|+1)(\frac{|R^\times|}{4} - \frac{1}{2})$$

vertices. As argued above, there are

$$2|R|(\frac{|R^\times|}{4} - \frac{1}{2})(\frac{|R^\times|}{4} + \frac{1}{2}) = 2|R|((\frac{|R^\times|}{4})^2 - \frac{1}{4})$$

edges between S and S'. Thus

$$h(G_R) \leq \frac{|\partial S|}{|S|}$$

$$= \frac{2|R|((\frac{|R^\times|}{4})^2 - \frac{1}{4})}{(|R|+1)(\frac{|R^\times|}{4} - \frac{1}{2})}$$

$$= \frac{|R|(|R^\times|+2)}{2(|R|+1)}$$

and so $h(G_R) \leq \frac{|R^\times|+2}{2(|R|+1)}$.

Corollary 5.3.1. *Let* $|R| < \infty$ *and* $Z(R) = \emptyset$. *Then*

$$h(G_R) \leq \begin{cases} \frac{|R^\times|}{2(|R|+1)} & |R^\times| \equiv 0 \pmod 4 \\ \frac{|R^\times|+2}{2(|R|+1)} & |R^\times| \equiv 2 \pmod 4. \end{cases}$$

Note that this only holds in general for rings without zero divisors; rings where $Z(R) \neq \emptyset$ have to be examined on a case-by-case basis.

CHAPTER 6

INTERESTING EXAMPLES

One ring we might want to study is the ring of integers modulo an odd prime p - a ring without zero divisors. Let $R = \mathbb{Z}_p$, for odd prime p. By Corollary 5.3.1, the isoperimetric number is bounded as follows:

$$h(G_R) \leq \begin{cases} \frac{p-1}{2(p+1)} & p \equiv 1 \pmod 4 \\ \frac{p+1}{2(p+1)} & p \equiv 3 \pmod 4. \end{cases}$$

In either case, $h(G_R) \leq \frac{1}{2}$.

We are also able to show Hamiltonicity for this ring. Let $S_R = \{\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & \pm 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & \pm 2 \\ 0 & 1 \end{smallmatrix}\right)\}$, a generating set for $PSL(2, \mathbb{Z}_p)$. We have the Cayley graph $G(PSL_2(\mathbb{Z}_p), S_R)$ is Hamiltonian by Corollary 5.2.6.

As an example of a ring for which we can show Hadwiger's conjecture, let $R = \mathbb{Z}_n$ and let $S_R = \{\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & \pm 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & \pm 2 \\ 0 & 1 \end{smallmatrix}\right)\}$, a generating set for $PSL(2, \mathbb{Z}_n)$. When

$$\begin{aligned} |\mathbb{Z}_n^\times| &\geq 2|S_R| \\ &= 10, \end{aligned}$$

so $n \prod_{p|n} \left(1 - \frac{1}{p}\right) \geq 10$, then Hadwiger's conjecture holds for $G(PSL(2, \mathbb{Z}_n), S_R)$ by Theorem 5.1.2.

Bibliography

[1] B. Albar and D. Gonçalves, On triangles in K_r-minor free graphs, J. Graph Theory (2013), 429-490.

[2] K. Appel and A. Haken, Every planar map is four colorable, Part I. Discharging, Illinois J. Math. 21 (1977), 429-490.

[3] K. Appel, A. Haken, and J. Koch, Every planar map is four colorable, Part II. Reducibility, Illinois J. Math. 21 (1977), 491-567.

[4] B. Bollobás, P.A. Catlin, and P. Erdős, Hadwiger's conjecture is true for almost every graph, Europ. J. Combinatorics, 1 (1980)195-199.

[5] R. Brooks, P. Perry, and P. Petersen, On Cheeger's inequality, Comment. Math Helvetici 68 (1993) 599-621.

[6] C.C. Chen and N.F. Quimpo, On strongly Hamiltonian Abelian group graphs, Combinatorial Mathematics VIII, Proceedings, Geelong, Australia 1980, Lect. Notes in Math., 884, Springer-Verlag, New York, 1981, 23-34.

[7] P.M. Cohn, Rings of zero divisors, Proc. Amer. Math. Soc., 9 (1958), 909-914.

[8] S. Curran and J. Gallian, Hamiltonian cycles and paths in Cayley graphs and digraphs – a survey, Discrete Math., 156 (1996), 1-18.

[9] J.A. Gallian, Contemporary Abstract Algebra, 9^{th} ed., Brooks Cole, 2016.

[10] G. R. Grimmitt and C.J.H. McDiarmid, On colouring random graphs, Math. Proc. Cambridge Phil Soc., 77 (1975), 313-324.

[11] H.H. Glover and Y.Y. Yang, A Hamilton cycle in the Cayley graph of the $\langle 2, p, 3\rangle$ presentation of $PSL_2(p)$, Discrete Math., 160 (1996), 149-163.

[12] H. Hadwiger, Über eine Klassifikation der Streckenkomplexe, Vierteljahress chr. Naturforsch. Ges. Zurich, 88, (1943), 133-142.

[13] Z. Huang, Y. Jin, and K. Liang, On the isoperimetric number of a k-degree Cayley graph, Applied Mathematics Letters, 22 (2009), 1451-1457.

[14] D. Lanphier and J. Rosenhouse, Cheeger constants of Platonic graphs, Discrete Math., 277, (2004), 101-113.

[15] D. Lanphier and J. Rosenhouse, Isoperimetric numbers of regular graphs of high degree with applications to arithmetic Riemann surfaces, Electron. J. Combin. 18 no. 1 (2011), Paper 164, 16 pp.

[16] L. Lovász, Problem 11 in Combinatorial Structures and their Applications, Gordon and Branch, New York, 1970.

[17] D. Marusic, Hamiltonian Circuits in Cayley Graphs, Discrete Math., 46, (1983), 49-54.

[18] B. Mohar, Isoperimetric numbers of graphs, J. Combin. Theory Series B, 47, (1989), 274-291.

[19] I. Pak and R. Radoicic, Hamiltonian paths in Cayley graphs, Discrete Math., 309, (2009), 5501-5508.

[20] N. Robertson, P. Seymour, and R. Thomas, Hadwiger's conjecture for K_6-free graphs, Combinatorica 13 (1993), 279-361.

[21] P. Schupp, On the structure of Hamiltonian cycles in Cayley graphs of finite quotients of the modular group, Theor. Comput. Sci., 204, (1998), 233-248.

[22] A. Thomason, The extremal function for complete minors, J. Combin. Theory Series B, 81, (2001), 318-338.

[23] D.B. West, Introduction to Graph Theory, 2nd ed., Prentice-Hall, Inc., Upper Saddle River, NJ, 2001.

[24] D. Witte and J. Gallian, A survey: Hamiltonian cycles in Cayley graphs, Discrete Math., 51, (1984), 293-304.