Honors Thesis: Investigating the Algebraic Properties of Cayley Digraphs

Alexis Byers, Wittenberg University
Mathematics Department

April 30, 2014

This paper utilizes Graph Theory to gain insight into the algebraic structure of a group using a Cayley digraph that depicts the group. Using the properties of Cayley digraphs, we investigate how to tell if a given digraph is a Cayley digraph, and we attempt to build Cayley digraphs. We then use the Cayley digraph to find information about the structure of the corresponding group. Finally, we examine the results of removing generators from a Cayley digraph and what it means if the digraph remains connected or is disconnected by the process.

Contents

1 Introduction

1.1 Graph Theory

Leonhard Euler is largely referred to as the father of Graph Theory for his solution to a famous problem involving the seven bridges of Königsberg. In his 1736 publication entitled, *Solutio Problematis ad Geometriam Situs Pertinentis* (Translated, *The solution to a problem relating to the geometry of position*), Euler considered the seven bridges that connected the city of Königsberg, in Prussia, across the Pregel River.[1]

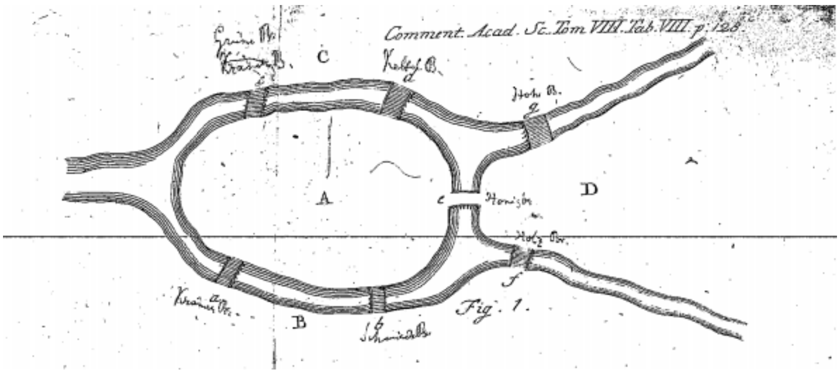

Figure 1: Euler's map of the seven bridges of Königsberg included in his publication.[2]

Euler faced the question: Is it possible to cross every bridge in Königsberg exactly once, and then return to the starting point? Arguing that this was impossible, Euler used a *graph* for the first time in history.[4] His *graph*, a set of *vertices*, together with a set of *edges* connecting pairs of vertices, looked similar to the following graph, $\mathcal{G}$:

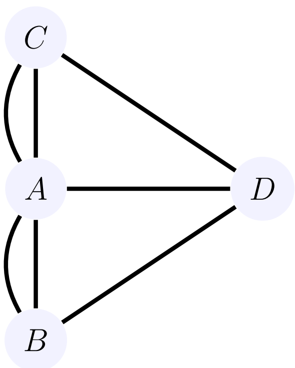

Figure 2: A graph $\mathcal{G}$, modeling the Königsberg bridges.

Each vertex in the graph represents a land mass in Königsberg, and each edge represents a bridge connecting two land masses. Notice that this graph is *connected*, meaning that there exists a sequence of edges between any two vertices in the graph. Thus, if we are at any land mass, we can get to any other land mass by crossing one or more bridges.

Euler observed that every time you step onto a land mass from a bridge, you must also leave the land mass by a bridge. Then, it follows that, to cross each bridge exactly once, you must have an even number of bridges so that having entered a land mass, one can also exit it. Since each land mass in Königsberg has an odd number of bridges connecting it to other land masses, at some point, one will enter a land mass but not be able to exit the land mass by an untraversed bridge. In Graph Theory, this parallels the idea that, for connected graphs, whenever you enter a vertex from one edge, you must then leave that vertex by another edge. Consequently, in order to traverse each edge exactly once, the graph needs to have an even number of edges adjacent to each vertex; in other words, the *degree* of every vertex needs to be even.

This kind of traversal problem, where one must traverse every edge exactly once and return to start, is described in modern Graph Theory as finding an *Eulerian Tour*, due to Euler's contribution to this problem.[6] Although we briefly consider Eulerian Tours in this paper, we find more connections in our research with *walks* in graphs, which are similar to Eulerian Tours except that we allow edges and vertices to be repeated. In particular, we utilize *closed walks*, which are simply walks in which the endpoints are the same.[6]

We could also look at a *subgraph*, of the graph of Königsberg, such as the graph $\mathcal{H}$ given below. We define a *subgraph* $\mathcal{H}$ of a graph $\mathcal{G}$ as a graph such that the vertex set of $\mathcal{H}$ is a subset of the vertex set of $\mathcal{G}$, and the edge set of $\mathcal{H}$ is a subset of the edge set of $\mathcal{G}$.[6]

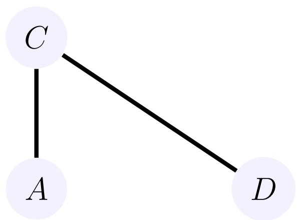

Figure 3: Subgraph $\mathcal{H}$ of the graph $\mathcal{G}$ of the Königsberg bridges.

A concept that we will use extensively in this paper is that of a *directed graph*, or *digraph*, which is a graph in which the edges have associated directions from one vertex to the other.[6] A digraph analog of the Königsberg graph may look like this:

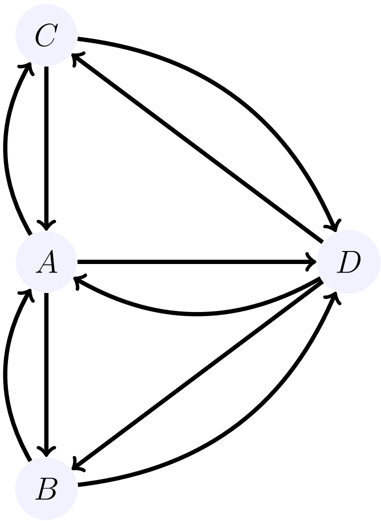

Figure 4: Digraph analog of the Königsberg bridge graph.

Note that in a digraph, I may have undirected edges; we can think of each undirected edge as two directed edges, one directed toward one end vertex, and one directed toward the other end vertex.

1.2 Group Theory

The beauty of Graph Theory is that it can be considered in isolation, but it also has many applications to other fields. In particular, this paper considers the ways that Graph Theory can aid in the study of the mathematical field of Group Theory. To begin, we will give the basic definitions that one without any knowledge of Group Theory should know before reading this paper.

First, a *binary operation* * on a set S is a function mapping S x S into S.[3] A binary operation can be addition, multiplication, modular arithmitic, etc. In this paper, without loss of generality, we resort to using multiplicative notation for the binary operation of arbitrary groups unless otherwise stated.

The most important definition for this field is obviously that of a *group*: a set G, together with a binary operation * is a *group* $< G, * >$, if G is closed[1] under *, if * is associative[2], if there exists an identity element[3], and if there exists an inverse[4] for every element of G.[3]

[1] A set S is closed under * if for all elements a, b in S, $a * b$ is also in S.[3]
[2] A binary operation * is associative in a set S if for all elements a, b, c in S, $(a * b) * c = a * (b * c)$.[3]
[3] The identity element of a set S is an element e of S such that $e * x = x * e = x$ for all x in S.[3]
[4] The inverse of an element a in a set S is an element a' such that $a' * a = a * a' = e$.[3]

Example 1.1. *If you look at the set $\mathbb{Z}$ of all integers, then you might notice that $\mathbb{Z}$ is a group under addition, but not under multiplication since not every element of $\mathbb{Z}$ has an inverse under multiplication. For example, 3 is an element of $\mathbb{Z}$, but 3 does not have an inverse in $< \mathbb{Z}, \cdot >$; there is no integer that you can multiply by 3 and get 1, the identity in $< \mathbb{Z}, \cdot >$.*

Example 1.2. *A type of group that is used often in this paper is the* group of integers modulo n, *$\mathbb{Z}_n$, where $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$, and the operation used is* modular arithmetic, *which can be described in the following way: for an integer z, and natural numbers n and r, then $(z \mod n) = r$ if r is the remainder when z is divided by n. For elements a, b in $\mathbb{Z}_n$, we define $a + b = (a + b) \mod n$.*

We describe the *order* of a group G as the number of elements in G.[3]

Example 1.3. *The group of integers, $\mathbb{Z}$, with addition, has infinite order, while $\mathbb{Z}_6$, with modular arithmetic, has order 6 (in general, $\mathbb{Z}_n$ has order n).*

We call a group G *abelian* if its binary operation is commutative[5].[3]

Example 1.4. *Both the groups $< \mathbb{Z}, + >$ and $< \mathbb{Z}_n, + >$ are abelian.*

If H, a subset of a group G, is closed under the binary operation of G, and if H is a group under the binary operation of G, then H is a *subgroup* of G. A *proper subgroup* of a group G is any subgroup of order strictly less than the order of G.[3] And the *index* of a subgroup H of G is the order of G divided by the order of H.

Example 1.5. *The group $< 2\mathbb{Z}, + >$, with elements of only the even integers, is a subgroup of $< \mathbb{Z}, + >$. But $< \mathbb{Z}^+, + >$, with elements of only the positive integers, is not a subgroup of $< \mathbb{Z}, + >$. Even though $\mathbb{Z}^+$ is a subset of $\mathbb{Z}$ that is closed under the operation, $< \mathbb{Z}^+, + >$ is not a group under the binary operation (since there are no inverses).*

A group G is *generated* by a set of elements S if S is a subset of G and every element of G can be written as a combination of the elements in S.

For a group G, let $x \in G$. Then the set $\{x^n | n \in \mathbb{Z}\} = < x >$, [6] a subgroup of G, is the *cyclic subgroup* of G generated by x. We say that the *order of an element* x is the order of the cyclic subgroup generated by x.[3] We denote the order of an element x by $o(x)$.

And a group is *cyclic* if there exists an element g in G such that $G = < g >$ (i.e there exists an element that generates all of G). We call g a *generator* of G.[3]

[5]An operation * is commutative in a set S if for all elements g and g' in S, $g * g' = g' * g$.[3]

[6]The symbol "$\in$" means "an element of", and we be used often to denote an element's membership in a set.

Example 1.6. *The easiest example of a cyclic group is* $<\mathbb{Z}_n, +>$. *Consider* $<\mathbb{Z}_6, +>$ *and* $1 \in \mathbb{Z}_6$. *The cyclic subgroup generated by* 1 *would be*

$$\begin{aligned} <1> &= \{1, 1^2, 1^3, 1^4, 1^5, 1^6\} && (1) \\ &= \{1, 2, 3, 4, 5, 0\} && (2) \end{aligned}$$

which is found by repeatedly adding 1 *to itself. Since* $<1>= \{1, 2, 3, 4, 5, 0\} = \mathbb{Z}_6$, *then we would say that* 1 *generates* $\mathbb{Z}_6$, *or that* 1 *is a generator of* $\mathbb{Z}_6$. *And since there exists a single element that generates the whole group,* $\mathbb{Z}_6$ *is cyclic.*

For a subgroup H of a group $<G, *>$, the *left cosets* of H in G are sets gH such that g is an element of G and $gH = \{g * h | h \in H\}$. Similarly, the *right cosets* of H in G are sets Hg such that for an element g of G, $Hg = \{h * g | h \in H\}$. And a subgroup H is a *normal subgroup* in G if the left and right cosets agree, i.e. $gH = Hg$ for all elements g in G.[3]

Example 1.7. *Consider the group* $G = \mathbb{Z}_2 \times \mathbb{Z}_5$[7], *which is a* direct product[8] *of groups* $\mathbb{Z}_2$ *and* $\mathbb{Z}_5$. *Let's look at the cosets of subgroup* $H = \{(0, 1), (0, 2), (0, 3), (0, 4), (0, 0)\}$. *Suppose we choose* $(1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_5$. *Then,*

$$\begin{aligned} (1,1)H &= \{(1,1)*(0,1), (1,1)*(0,2), (1,1)*(0,3), (1,1)*(0,4), (1,1)*(0,0)\} && (3) \\ &= \{(1,2), (1,3), (1,4), (1,5), (1,1)\} && (4) \end{aligned}$$

And $(1, 1)H$ *is a left coset of* H *in* G. *Similarly,*

$$\begin{aligned} H(1,1) &= \{(0,1)*(1,1), (0,2)*(1,1), (0,3)*(1,1), (0,4)*(1,1), (0,0)*(1,1)\} && (5) \\ &= \{(1,2), (1,3), (1,4), (1,5), (1,1)\} && (6) \end{aligned}$$

So $H(1, 1)$ *is a right coset of* H *in* G.

Notice that $(1, 1)H = H(1, 1)$. *If we show* $gH = Hg$ *is true for all elements* g *in* G, *not just* $(1, 1)$, *then* H *is normal in* G.

Next is the most important definition for the understanding of this paper.

Definition 1.8. *A* Cayley digraph *is a visual representation of a group. It is a directed graph in which each element of a group* G *is represented by a vertex, and each edge represents multiplication on the right*[9] *by an element of a generating set of* G. *[3]*

[7] Notice that $\mathbb{Z}_2 \times \mathbb{Z}_5$ is actually $\mathbb{Z}_{10}$.

[8] A direct product between two groups $<G, *>$ and $<G', *'>$ is the group $<G \times G', *>$ where we define (g, g') as an element of $G \times G'$ if $g \in G$ and $g' \in G'$. Then, for elements (g_1, g_1') and (g_2, g_2') of $G \times G'$, we define $(g_1, g_1') * (g_2, g_2') = (g_1 * g_2, g_1' *' g_2')$.[3]

[9] By convention, we always multiply on the right. We will break this convention briefly later in the paper, but it is assumed that we are using right multiplication in all Cayley digraphs unless explicitly stated otherwise.

For example, if we say that the generator g is represented in a Cayley Digraph of a group G by a solid arrow, then we would interpret the following as $x * g = y$.

We want to point out two conventions that we use when dealing with Cayley digraphs.

First, the manner in which we denote inverse of a generator: In the above figure, the solid edge is represented by right multiplication by a generator g. If we travel in the opposite direction of this arrow, we can think of that as multiplication on the right by the inverse of g, or g^{-1}. So the figure tells us that $x * g = y$, but also that $yg^{-1} = x$.

Second, note that in a Cayley digraph, we can still have undirected edges, as in Example 1.10, that we would interpret again just as two directed edges, one directed toward one end vertex, and one directed toward the other end vertex. And a generator represented by any undirected edge will have order two in the corresponding group.

Example 1.9. *The Cayley digraph of* $< \mathbb{Z}_6, + >$*, where we represent each solid arrow as multiplication on the right by the element* 1*, is shown in Figure 5:*

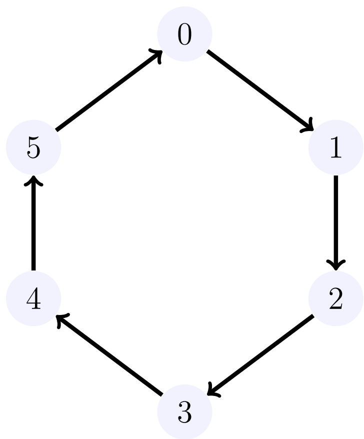

Figure 5: Cayley digraph of $< \mathbb{Z}_6, + >$ with generating set $\{1\}$.

Example 1.10. *Note that, by using different sets of generators, we can construct a different Cayley digraph of* $< \mathbb{Z}_6, + >$*. Suppose instead, we consider the generating set* $\{2, 3\}$*. Each element does not generate* $< \mathbb{Z}_6, + >$ *by itself, but together they do. Let a solid arrow represent "multiplication" on the right by* 2 *and a dashed arrow represent multiplication on the right by* 3*. Then the Cayley digraph of* $< \mathbb{Z}_6, + >$ *would look like:*

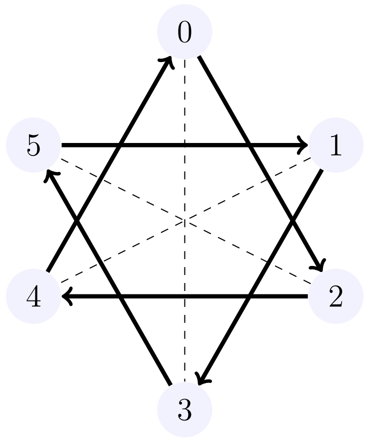

Figure 6: Cayley digraph of $< \mathbb{Z}_6, + >$ with generating set $\{2, 3\}$.

By our convention, the name of each vertex in a Cayley digraph is not unique. We can name each vertex independently, or we can name each vertex by the sequence of edges between the identity and that vertex.

For example, we can refer the vertex represented by 3 in Figure 5 equivalently as $\{1, 1, 1\}$ since we can travel from 0 to 3 by a sequence of three edges represented by multiplication on the right by 1.

In Figure 6, we can refer to the vertex represented by 3 equivalently as the sequence $\{2, 2, 3, 2\}$ since if you begin at 0 and follow two 2 edges, a 3 edge, and then another 2 edge, you will be at vertex 3. Furthermore, the vertex 3 could be represented by $\{2, 3, 2, 2\}$, or $\{2, 3, 2, 3, 2, 3\}$, or many other different sequences. Each of these representations are acceptable in this paper.

2 Properties of Cayley Digraphs

Since this paper focuses on Cayley digraphs, let's discuss their construction. In order to preserve the algebraic properties of the group, we construct Cayley digraphs in a specific way. We care about four properties in particular.

Theorem 2.1. *There are four properties that every digraph, $\mathcal{G}$, must satisfy in order to be a Cayley digraph*[10]*:*

1. *$\mathcal{G}$ must be connected.*
2. *Given vertices x and y, there exists at most one edge going from x to y.*

[10]These properties will be referred to later in the paper by the numbers as listed here.

3. *Every vertex x in $\mathcal{G}$ has exactly one edge of each type starting at x and one of each type ending at x.*

4. *If two different sequences of edges starting at some vertex x go to the same vertex y, then whenever those sequences begin at the same vertex in $\mathcal{G}$, they should always lead to the same vertex. [3]*

Proof. The first property applies since for elements g, x, h in a group G, every equation $gx = h$ has a solution. In a group, we know that every element has in inverse; thus, if $gx = h$, then we know $x = g^{-1}h$. So g is connected to h by a path in $\mathcal{G}$.

Since the solution to $gx = h$ is unique in a group, the second property applies.

The third property applies because, for any element $x \in G$ and for each generator g, we can compute xg and $(xg^{-1})g = x$. We know we can compute xg since the G is closed, and we know that $(xg^{-1})g = x$ because we have associativity of our operation and an identity in G: $(xg^{-1})g = x(g^{-1}g) = x(e) = x$.

And the fourth property applies since, for elements x, h, q, r, u in G, if $xq = h$ and $xr = h$, then $uq = ux^{-1}h = ur$. Thus, we have that the operation is well defined.
[3] □

On the other hand, we can also show that, given a digraph that satisfies the four properties, it must be a Cayley digraph for a group.

Theorem 2.2. *Every digraph that satisfies the above four properties is a Cayley digraph for a group. [3]*

Proof. Let $\mathcal{G}$ be a directed graph with n different types of edges, and suppose that $\mathcal{G}$ satisfies the four properties in Theorem 2.1.

Choose any vertex from $\mathcal{G}$ and label it e, as we will aim to prove that this is the identity element in the corresponding group G. Since $\mathcal{G}$ is vertex-symmetric, by the third property, then our choice of e does not matter. Now label each different type of edge $g_1, g_2, \ldots, g_n$. For each g_i edge leading away from e, label the vertex at the end of that edge g_i.

Let any edge g_i starting at $x \in V(\mathcal{G})$ and ending at $y \in V(\mathcal{G})$ represent the right multiplication of x by g_i equal to y (i.e., $xg_i = y$). By property 1 we know we can denote any other vertex, y in G by a sequence of edges from e to y, or, equivalently, as a product of $g_1, g_2, \ldots, g_n$.

Thus, we can define any vertex $x \in \mathcal{G}$ as a sequence of edges, S_1. Suppose there is another sequence of edges, S_2, that can define x. So, starting at vertex e, two different sequences of edge types lead to the same vertex x. By property 4, we know then that those same sequences starting from any vertex u will lead to the same v. Thus, we have that the operation we have defined on the vertices of $\mathcal{G}$ is well defined: given any sequence of edges from e to x, that sequence can be used to represent multiplication on the right by x.

And as a consequence of property 1 and the construction of $\mathcal{G}$, we know that the operation we have defined is closed.

Now, let x, y, $z \in V(\mathcal{G})$. Consider $(xy)z$. We would represent the vertex arrived at if we began at x and followed a sequence of edges that defines y as (xy). We know (xy) exists in $\mathcal{G}$ by the third property. Then $(xy)z$ would be the vertex arrived at from vertex (xy) after following the sequence of edges defined by z. Now $x(yz)$ would represent the vertex arrived at after starting at x and following the sequence of edges defined by yz. Since we concatenate the sequences of edges defined by two elements of $V(\mathcal{G})$ when we multiply them, $(xy)z$ and $x(yz)$ will be a sequence of edges that go from the same vertex x to the same vertex xyz. Thus, $(xy)z = x(yz)$, and the operation of $\mathcal{G}$ is associative.

By how we have defined e, we have that e will be the identity since $e(g_i) = (g_i)e = g_i$ for any vertex labeled g_1, g_2, $\ldots$, g_n in the way described earlier. And since each element of G can be defined as the product of g_i's, then using associativity, we know e times any element of $V(\mathcal{G})$ will be that element because for any vertex $v \in V(\mathcal{G})$, $v = (g_a)(g_b)\ldots(g_\alpha)$, and

$$\begin{aligned} e(v) &= e(g_a)(g_b)\ldots(g_\alpha) && (7)\\ &= (e(g_a))(g_b)\ldots(g_\alpha) && (8)\\ &= (g_a)(g_b)\ldots(g_\alpha) && (9)\\ &= v. && (10) \end{aligned}$$

We can define the inverse of any edge g as going in the opposite direction of how g is directed in $\mathcal{G}$.[11] Thus, we would interpret (gg^{-1}) as starting at e, traveling to g, and then traveling in the opposite direction on the edge g, back to e. Therefore, $(gg^{-1}) = e$ as desired. So, we would define the *inverse* of any element x of $V(\mathcal{G})$, as the sequence of edges to get from x to e. This sequence can easily be found by traveling backwards through the sequence of edges used to describe x in the first place. (i.e., if $x = (g_1)(g_2)(g_3)$, then $x^{-1} = (g_3^{-1})(g_2^{-1})(g_3^{-1})$). Then xx^{-1} will be interpreted as starting at e, traveling to x, and then traveling back to e. Thus, $xx^{-1} = e$. Hence, all elements of $V(\mathcal{G})$ have inverses.

Therefore, we have defined a set of elements, $V(\mathcal{G})$, and an operation such that $V(\mathcal{G})$ is closed, has an identity, has inverses for all elements, and the operation is associative. Thus, $< V(\mathcal{G}), * >$ is a group.

$\square$

[11] If g has order two, and therefore is represented by an undirected edge, then $g = g^{-1}$, and that undirected edge will represent both g and g^{-1}.

From this theorem, we know that if we can draw any graph that has these four properties, then the graph will be a Cayley digraph for a group. A question, however, is how hard is it to actually draw a graph, without a preconceived notion of the group you intend it to represent, that satisfies the four properties. In particular, we found the last property is especially hard to predict.

In his text, *A First Course in Abstract Algebra*, Fraleigh claims that the four properties that characterize every Cayley digraph have been used in discovering groups.[3] Thus, we attempt to "discover" a group from a digraph that satisfies the four properties. Our process is as follows: we choose an arbitrary number of vertices, choose one to two types of edges that are intended to be generators, and then attempt to draw a digraph that encompasses all four properties. Constructing a digraph the satisfies the first three is easy enough, but it takes us several attempts to find a digraph that satisfies the last condition. The following is one of the first attempts that proves to fail the fourth property. The "generators" g_1 and g_2 are represented by solid arrows and dashed arrows, respectively.

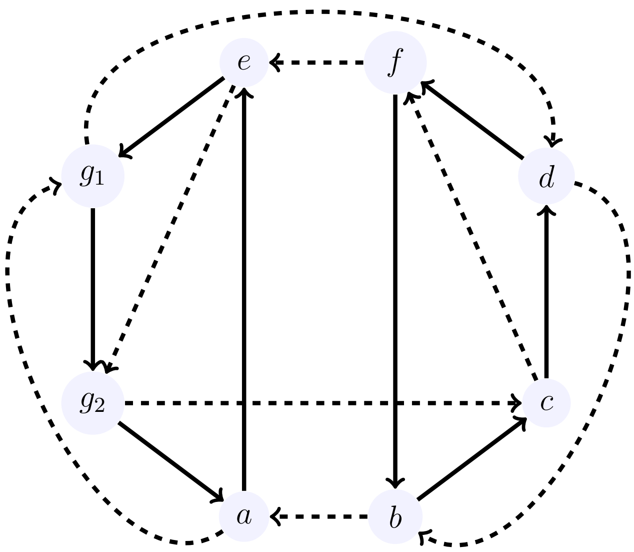

Figure 7: Failed attempt at drawing a digraph that satisfied all four properties.

As you can see, in Figure 7, the sequence of edges $S_1 = \{g_2\}$ is the same as sequence $S_2 = \{g_2, g_1, g_2, g_1\}$ if you start at e. If the fourth property is satisfied, then no matter what vertex at which we start, we should end up at the same vertex by following S_1 or S_2. However, if we start at vertex g_1 and follow S_1, we are at vertex d; and if we start at vertex g_1 and follow S_2, we are at vertex g_1. Since we do not end at the same vertex, the fourth property is not satisfied, and this digraph is not a Cayley digraph of a group.

Using the same process, we finally managed to discover a digraph that turned out to be the Cayley digraph for the Dihedral group on 10 elements, DiH_5, which is the group of symmetries of a regular pentagon. In the following digraph, let the solid edges represent multiplication on the right by the generator g_1 and the dashed edges represent multiplication on the right by the generator g_2.[12]

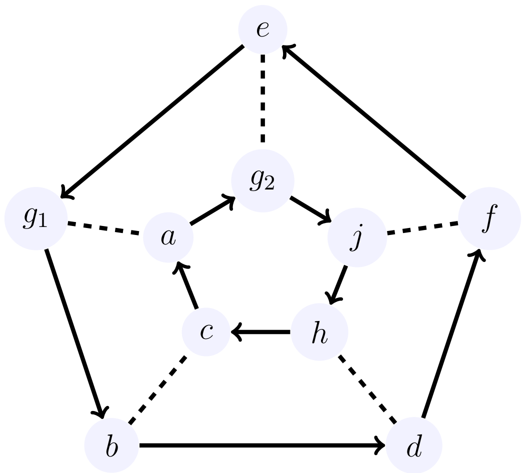

Figure 8: Cayley Digraph of DiH_5

	e	g_1	g_2	a	b	c	d	f	h	j
e	e	g_1	g_2	a	b	c	d	f	h	j
g_1	g_1	b	a	c	d	h	f	e	j	g_2
g_2	g_2	j	e	f	h	d	c	a	b	g_1
a	a	g_2	g_1	e	j	f	h	c	d	b
b	b	d	c	h	f	j	e	g_1	g_2	a
c	c	a	b	g_1	g_2	e	j	h	f	d
d	d	f	h	j	e	g_2	g_1	b	a	c
f	f	e	j	g_2	g_1	a	b	d	c	h
h	h	c	d	b	a	g_1	g_2	j	e	f
j	j	h	f	d	c	b	a	g_2	g_1	e

Table 1: Cayley Table for DiH_5

We can confirm that the digraph we discovered is a Cayley digraph for a group by com-

[12]Note that the dashed edges have no arrow tips; this is because each undirected edge represent two directed edges, one in each direction, between the two vertices.

pleting the Cayley Table[13] for the set of vertices in our digraph, as seen above, and then matching this table with the Cayley table for DiH_5.[5]

However, even though we successfully "discovered" a Cayley digraph, the question remains as to whether or not, given a digraph, we can visually detect if the fourth property is satisfied. We come to the conclusion that there is no simple way to check the satisfaction of the fourth property without checking every sequence of edges in the graph, which is often more time consuming than just naming the elements and investigating the multiplication table.

This question sparked an interest in finding properties of a group that *could* be visually determined by its Cayley digraph, as the next section reveals.

3 Information given by the Structure of a Cayley Digraph

3.1 Abelian

Wondering what properties of a group we can determine from the structure of a Cayley digraph, we begin with the following question: Can you tell from a Cayley digraph whether the corresponding group is abelian?

Fraliegh claims that the answer is yes.[3] Thus, we come up with a method for analyzing a Cayley digraph to ascertain if a group is abelian.

Proposition 3.1. *Given a Cayley digraph $\mathcal{G}$ of some group G with generating set $\{g_1, g_2, \ldots, g_n\}$, represented by n different edge types in $\mathcal{G}$, one can determine if G is abelian by the following method:*

1. *Choose any two types of edges $\mathcal{G}$, say g_1 and g_2.*
2. *Select a vertex in $\mathcal{G}$, say x.*
3. *Starting at x, follow a g_1 edge, then a g_2 edge. Note the vertex at which you finish.*
4. *Now, starting at x, follow a g_2 edge, then a g_1 edge. Note the vertex at which you finish.*

[13] A Cayley Table is a table that lists the elements of the group on the top row and left-most column, and each box in ith row and jth column is the element that represents the ith element times the jth element.[3]

5. *If the vertex at which you finish after the sequence of edges $\{g_2, g_1\}$ is the same vertex at which you finished when you followed the sequence of edges $\{g_1, g_2\}$, then repeat this process for every pair of generators. If you finish at the same vertex each time, then G is abelian.*
6. *If you finish at different vertices for any of the pairs of generators, then G is not abelian.*

If we follow the above process, it is obvious that each pair of generators will commute. But why does this mean that G is abelian?

Proof. Suppose we have a Cayley digraph $\mathcal{G}$ of some group G with generating set $\{g_1, g_2, \ldots, g_n\}$.

If we find that there exist generators g_i and g_j such that $g_i g_j \neq g_j g_i$ by the above process, then we know that G cannot be abelian, since every element of G must commute.

However, if we find that each pair of generators $\{g_1, g_2, \ldots, g_n\}$ in G commute with each other by the above process, then for any two elements $x, y \in G$, we can write x and y as some product of generators, $x = g_a g_b \ldots g_k$ and $y = g_{a'} g_{b'} \ldots g_{k'}$. Then, we know that:

$$\begin{aligned}
xy &= (g_a g_b \ldots g_k)(g_{a'} g_{b'} \ldots g_{k'}) && (11)\\
&= g_a g_b \ldots (g_{a'} g_k) g_{b'} \ldots {g_k}' && (12)\\
&= g_a g_b \ldots g_{a'} (g_{b'} g_k) \ldots g_{k'} && (13)\\
&\vdots && (14)\\
&= (g_{a'} g_{b'} \ldots g_{k'})(g_a g_b \ldots g_k) && (15)\\
&= yx && (16)
\end{aligned}$$

Thus, we know that for any two elements $x, y \in G$, we have $xy = yx$. Hence, by definition, G must be abelian.

□

Example 3.2. *To illustrate this method, consider the following Cayley digraph $\mathcal{G}$, representing some group G.*

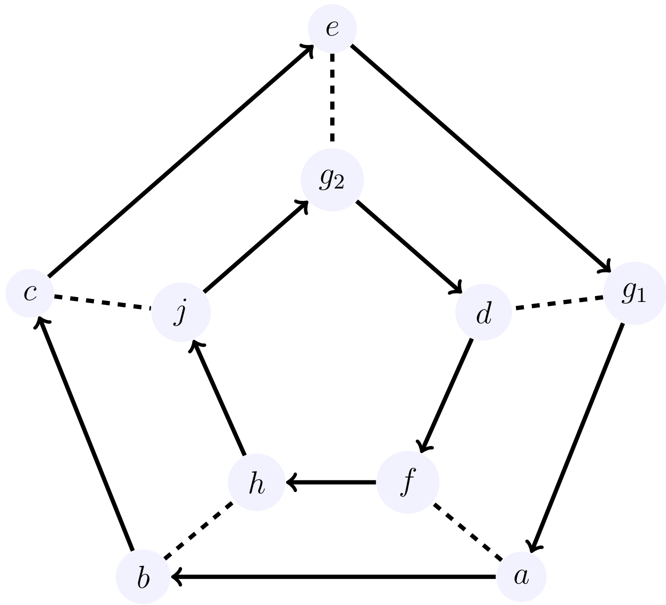

Figure 9: Given a Cayley Digraph $\mathcal{G}$.

Since we only have two generators, we call them g_1 and g_2. Now, let's select vertex e. If we begin at e and follow the sequence of edges $\{g_1, g_2\}$ we will end at vertex d. Similarly, if we start at vertex e and follow the sequence of edges $\{g_2, g_1\}$, we will end at vertex d again. Thus, $eg_1g_2 = g_1g_2 = d$ and $eg_2g_1 = g_2g_1 = d$ so $g_1g_2 = g_2g_1 = d$. And, by Proposition 3.1, G is abelian.

After close inspection, you may notice that $\mathcal{G}$ is actually a Cayley digraph of $\mathbb{Z}_2 \times \mathbb{Z}_5$, with generators $(0, 1)$ and $(1, 0)$ as g_1 and g_2 respectively.

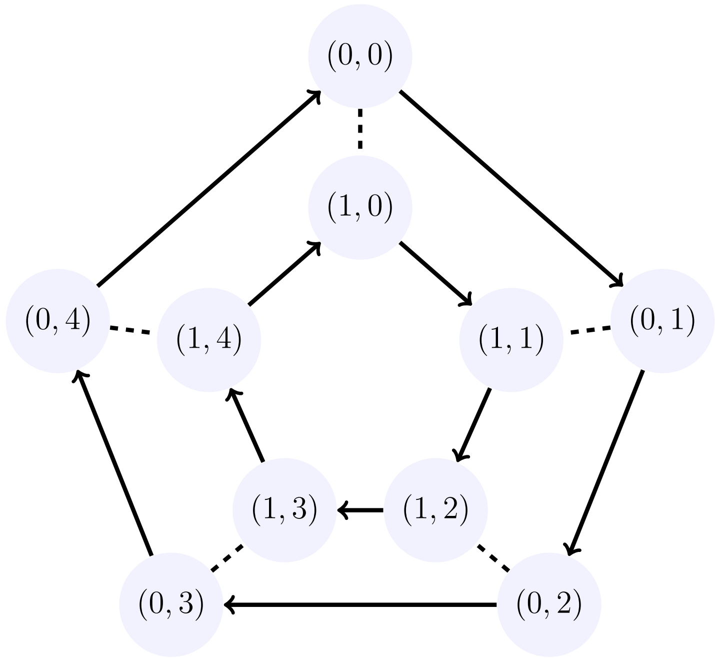

Figure 10: Cayley Digraph of $\mathbb{Z}_2 \times \mathbb{Z}_5$

Since we know that $\mathbb{Z}_2 \times \mathbb{Z}_5$ is actually $\mathbb{Z}_{10}$, which we know to be abelian, we get the result that we would expect from Proposition 3.1.

Example 3.3. *On the other hand, suppose you are given the following digraph $\mathcal{G}'$ of some group G'.*

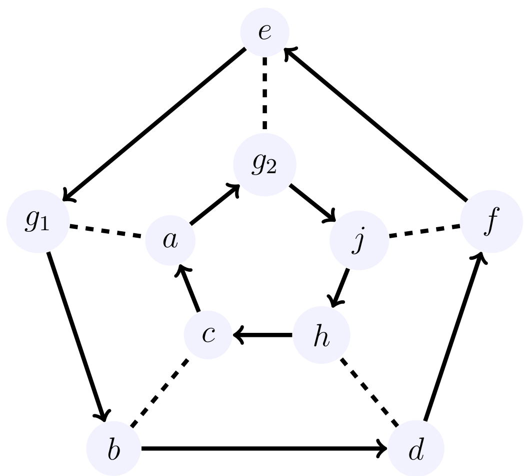

Figure 11: Given a Cayley Digraph $\mathcal{G}'$.

Again, we only have two types of edges in our Cayley digraph, so we must use generators g_1 and g_2 again. Let's choose the vertex e again. Then, beginning at vertex e, if we follow *the sequence of edges* $\{g_1, g_2\}$*, we will finish at vertex* a*. And, starting at vertex* e*, if we follow the sequence of edges* $\{g_2, g_1\}$*, we will finish at vertex* j*. Since* $a = g_1 g_2 \neq g_2 g_1 = j$*, then Proposition 3.1 tells us that* G' *is not abelian.*

You may notice that Figure 11 is isomorphic to a Cayley digraph of DiH_5*, which we know to be nonabelian.*

3.2 Cyclic

A similar question we consider is: Can you tell from a Cayley digraph whether the corresponding group is cyclic?

We have no immediate answer to this question from any reference we could find, as we did with the previous question, and we find no elegant answer as we had hoped, but we do manage to describe a method for investigating if a group is cyclic from a Cayley digraph.

Proposition 3.4. *Given a Cayley digraph* $\mathcal{G}$ *of some group* G*, it can be determined if* G *is cyclic if you can construct a closed walk in* $\mathcal{G}$*, starting at the identity, consisting of a sequence of one single path and that closed walk includes all of* $\mathcal{G}$*.*

Example 3.5. *Suppose we consider the following Cayley digraph of* $\mathcal{G}^*$ *of some group* G^**.*

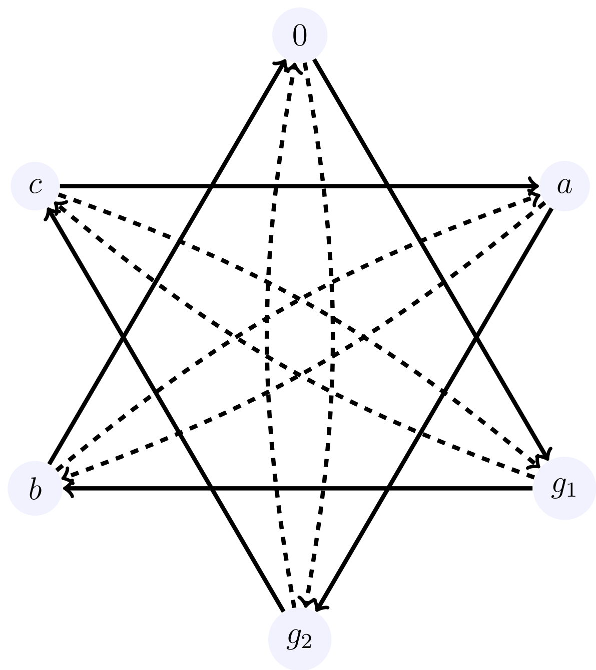

Figure 12: Given Cayley digraph $\mathcal{G}^*$ of group G^*.

By Proposition 3.4, if we can find a closed walk in $\mathcal{G}^*$ by repeating a sequence of one single path that consists of every vertex and edge of $\mathcal{G}^*$, then G^* is cyclic.

Consider the following path: $\{g_1, g_2\}$. We claim that if you repeat this sequence, then you will have a closed walk of $\mathcal{G}^*$ that is all of $\mathcal{G}^*$, and thus prove that G^* is cyclic.

Let's check: Start at e. If we follow this sequence once, we have traversed the following red edges, and we included the following red vertices in our walk:

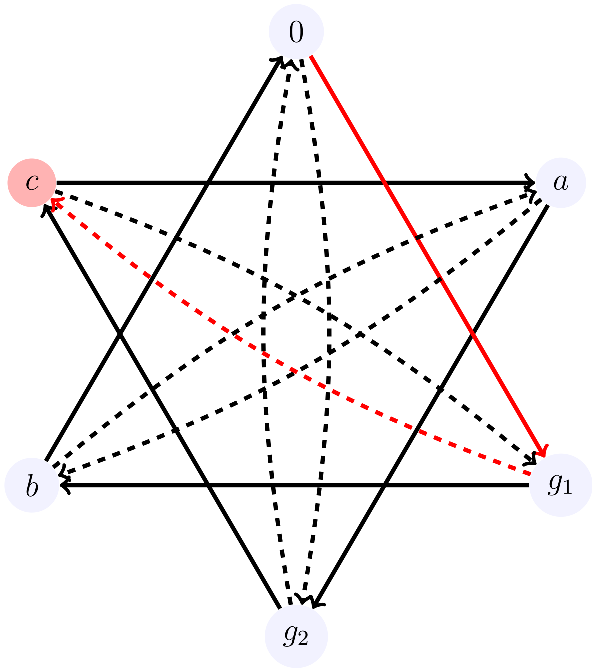

Figure 13: Given Cayley digraph $\mathcal{G}^*$ of group G^* after we have traversed the edges in the sequence $\{g_1, g_2\}$.

If we repeat this sequence of edges over and over again, we get the following graphs, with the traversed edges in red, and included vertices in red:

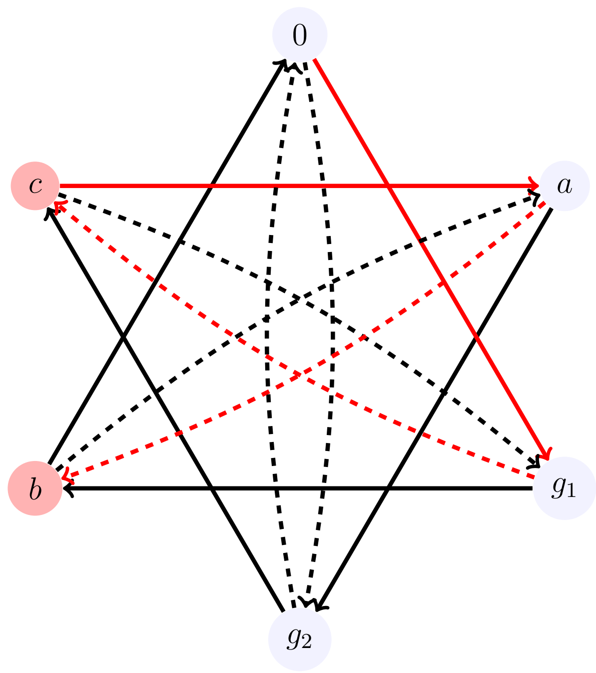

Figure 14: Given Cayley digraph $\mathcal{G}^*$ of group G^* after we have traversed the edges in the sequence $\{g_1, g_2\}$ twice.

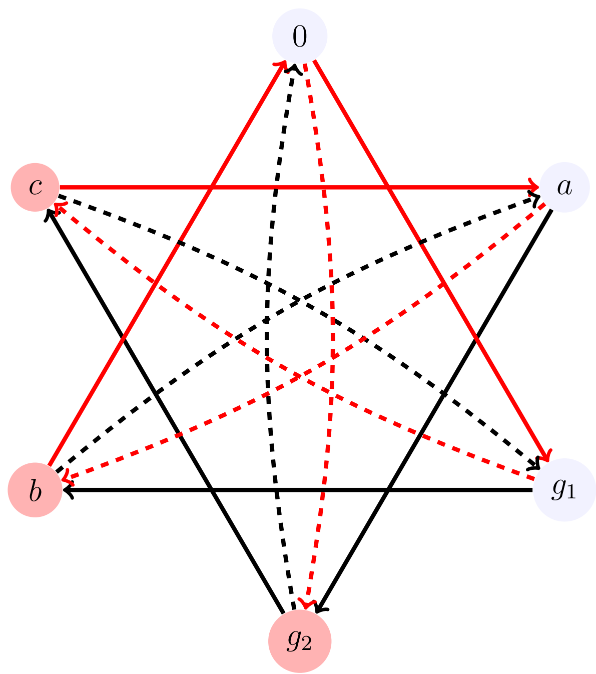

Figure 15: Given Cayley digraph $\mathcal{G}^*$ of group G^* after we have traversed the edges in the sequence $\{g_1, g_2\}$ three times.

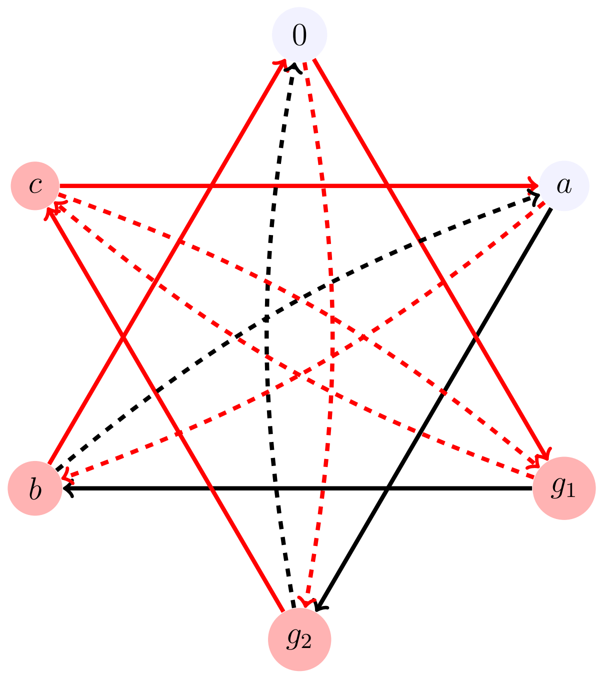

Figure 16: Given Cayley digraph $\mathcal{G}^*$ of group G^* after we have traversed the edges in the sequence $\{g_1, g_2\}$ four times.

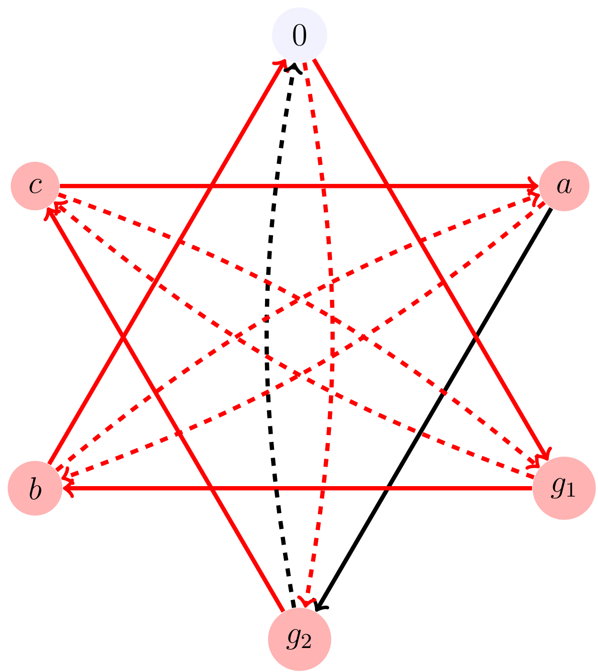

Figure 17: Given Cayley digraph $\mathcal{G}^*$ of group G^* after we have traversed the edges in the sequence $\{g_1, g_2\}$ five times.

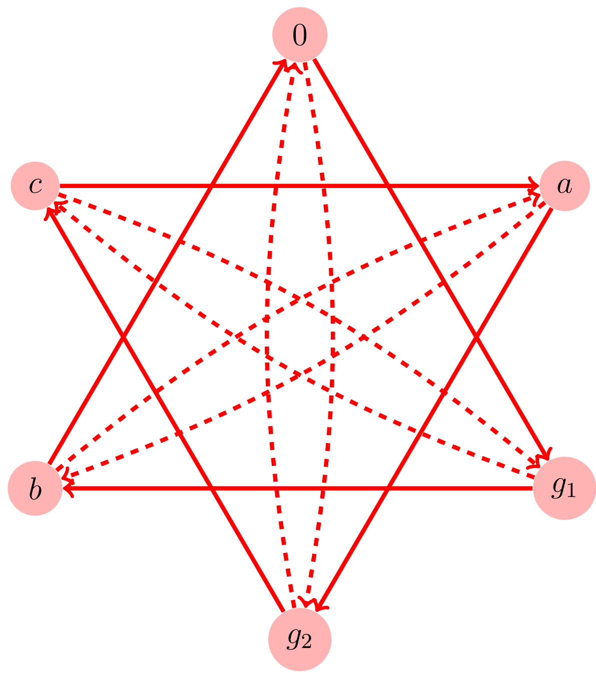

Figure 18: Given Cayley digraph $\mathcal{G}^*$ of group G^* after we have traversed the edges in the sequence $\{g_1, g_2\}$ six times.

Thus, by repeating that sequence of edges $\{g_1, g_2\}$ six times, we have included every vertex and every edge of $\mathcal{G}^*$ in our walk and returned to where we began, at vertex e. By Proposition 3.4, we have that G^* is cyclic. In fact, $\mathcal{G}^*$ is isomorphic to the Cayley digraph of $< \mathbb{Z}_6, + >$ with generating set $\{2, 3\}$, where generator g_1 corresponds to 2 and g_2 corresponds to 3. And we know all groups $< \mathbb{Z}_n, + >$ to be cyclic.

3.3 Cyclic Subgroups

Now that we know how to determine if a group is cyclic based its representation in a Cayley digraph, we consider how to determine, from a Cayley digraph, the cyclic subgroups of the group being represented.

Proposition 3.6. *Given a Cayley digraph $\mathcal{G}$ of some group G, you can find all of the cyclic subgroups of G by the following method:*

1. *Choose a vertex of $\mathcal{G}$. Say x.*
2. *Since each vertex of $\mathcal{G}$ can be represented by a sequence of edges of $\mathcal{G}$, use this representation for x.*
3. *Let $\mathcal{S}$ be the set of vertices reached by starting at the identity and repeatedly applying the sequence of edges that represent x until you arrive back at the identity.*

4. Then the set $\mathcal{S}$ will contain the elements of G in the cyclic subgroup of G generated by x.

Note: To find all cyclic subgroups of G, you can repeat this process for every element of G.

Proof. Let $\mathcal{G}$ be a Cayley digraph for some group G and let y be an element of G. Suppose you used the above procedure of repeatedly applying the sequence of edges that represent y in $\mathcal{G}$ to get the set $\mathcal{S}$ of vertices reached by this process. Then, we can think of each vertex in $\mathcal{S}$ as a "power" of y since you have arrived at that vertex from the identity just by following "y". And $\mathcal{S} = \{y, y^2, \ldots, y^{o(y)} = e\}$ is the cyclic subgroup generated by y.

□

Example 3.7. *Let's find a cyclic subgroup of the following Cayley digraph $\hat{\mathcal{G}}$ of some group $\hat{G}$.*

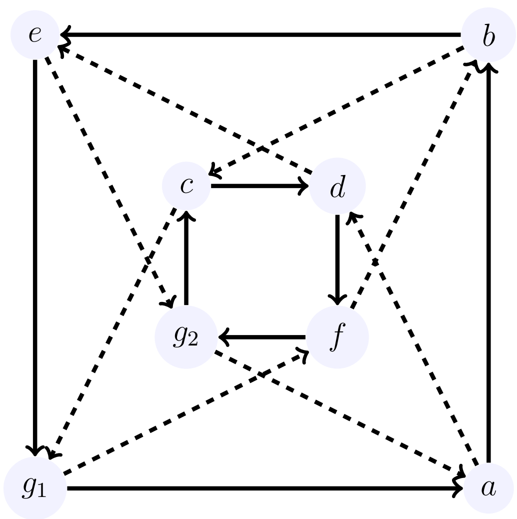

Figure 19: Given Cayley digraph $\hat{\mathcal{G}}$ of some group $\hat{G}$.

14

We can choose any vertex in $\hat{\mathcal{G}}$, so let's choose vertex c. Our first step is to write c as a sequence of g_1 and g_2 edges, starting at the identity. Thus, $c = g_2 g_1$. We will let $\mathcal{S}$ represent the set of vertices reached by repeatedly applying the sequence of edges $\{g_2, g_1\}$.

Now, we will begin at the identity and follow $\{g_2, g_1\}$ to our vertex c. Our path will be highlighted in red, as well as the elements being added to $\mathcal{S}$.

[14] $a = g_1^2 = g_2^2$, $b = g_1^3$, $c = g_2 g_1$, $d = g_2^3$, $f = g_1 g_2$

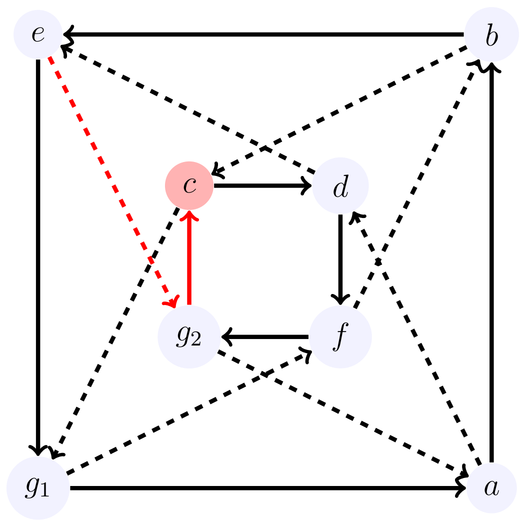

Figure 20: Given Cayley digraph $\hat{\mathcal{G}}$ of some group $\hat{G}$, following the sequence of edges $\{g_2, g_1\}$.

At this point, $\mathcal{S}$ contains c.

We will now repeatedly follow the sequence of edges $\{g_2, g_1\}$ until we arrive back at e, keeping track of our set $\mathcal{S}$ along the way.

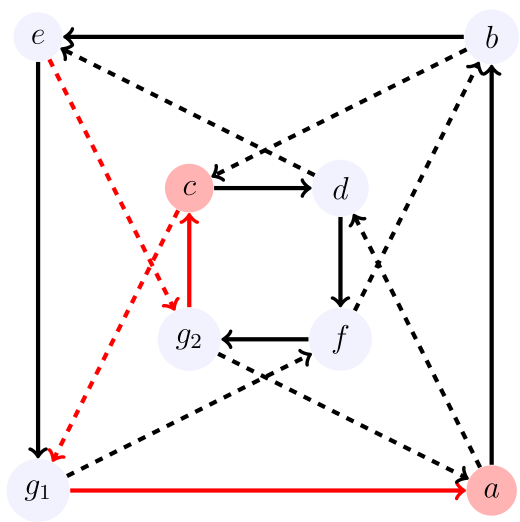

Figure 21: Given Cayley digraph $\hat{\mathcal{G}}$ of some group $\hat{G}$, following the sequence of edges $\{g_2, g_1\}$.

Now, $\mathcal{S}$ contains c and a.

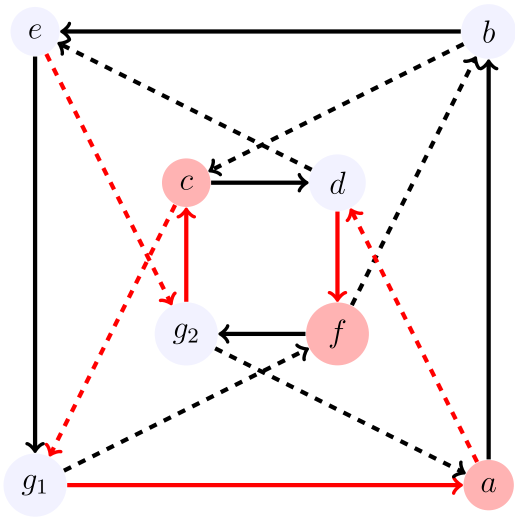

Figure 22: Given Cayley digraph $\hat{\mathcal{G}}$ of some group $\hat{G}$, following the sequence of edges $\{g_2, g_1\}$.

Now, $\mathcal{S}$ contains c, a, and f.

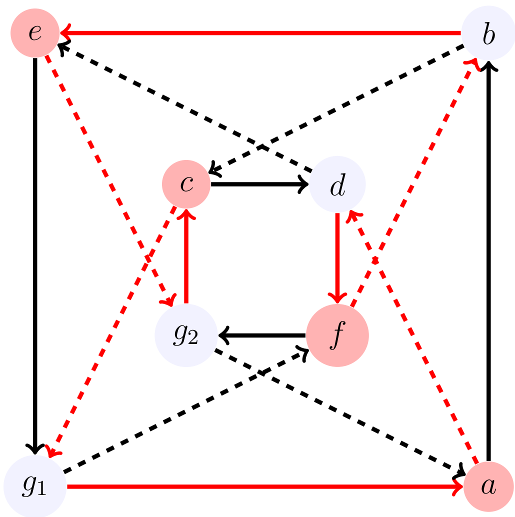

Figure 23: Given Cayley digraph $\hat{\mathcal{G}}$ of some group $\hat{G}$, following the sequence of edges $\{g_2, g_1\}$.

Thus, we are back at e, and $\mathcal{S} = \{c, a, f, e\}$. Therefore, by Proposition 3.6, the set $\mathcal{S}$ represents the cyclic subgroup generated by c, i.e.,

$$< c > = \{c, a, f, e\} \tag{17}$$
$$= \{c = g_2 g_1, a = (g_2 g_1)^2, f = (g_2 g_1)^3, e = (g_2 g_1)^4\}. \tag{18}$$

We also consider whether, given a Cayley digraph, if we can get information about the normal subgroups of a group. We found a partial answer to this question after we discovered the process presented in the next section, where we remove edge types from the digraph and possibly disconnect the Cayley digraph. We will discuss how to look at a Cayley digraph to find certain normal subgroups of a group later in this next section.

4 Disconnecting Cayley Digraphs

We find that removing one type of edge from a given Cayley digraph may give us valuable information about the group. Does the graph stay connected? Does it become disconnected? If so, what do the connected components look like? The answers to these questions lead to interesting results about the underlying group structure.

4.1 Connected

First, let's investigate what happens when we remove all edges of one type from a Cayley digraph, but the digraph remains connected.

Example 4.1. *Consider the following Cayley digraph of* $<\mathbb{Z}_6, +>$*, with generating set* $\{1, 2\}$*, where the solid edges represent* 1 *and the dashed edges represent* 2*:*

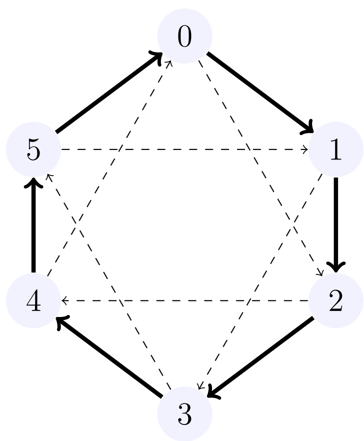

Figure 24: Cayley digraph of $<\mathbb{Z}_6, +>$ with generating set $\{1, 2\}$.

If we take away the dashed edges, then we have the following connected digraph:

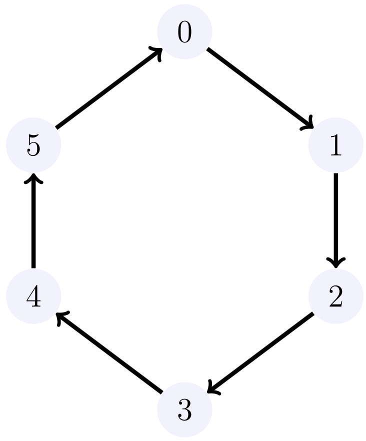

Figure 25: Resulting digraph when generator 2 is removed.

This is still a Cayley digraph of $< \mathbb{Z}_6, + >$*, as you can see.*

Examples similar to the one above lead us to the following theorem.

Theorem 4.2. *Let* $\mathcal{G}$ *be a Cayley digraph of a group* G*. Suppose all edges of one type are removed from* $\mathcal{G}$*, and the resulting graph* $\mathcal{G}'$ *remains connected. Then* $\mathcal{G}'$ *remains a Cayley digraph of* G*.*

Proof. Let $\mathcal{G}$ represent a Cayley digraph of a group G. Then $\mathcal{G}$ satisfies the four properties.

If we remove one type of edge from $\mathcal{G}$, and the resulting graph $\mathcal{G}'$ is connected, then we know that $\mathcal{G}'$ satisfies the first condition.

Since $\mathcal{G}' \subset \mathcal{G}$, then it is easy to see how properties 2, 3, and 4 hold in $\mathcal{G}'$. Since the only change made between graphs $\mathcal{G}$ and $\mathcal{G}'$ is the removal of edges, and $\mathcal{G}$ satisfied properties 2, 3, and 4, then the following is true: $\mathcal{G}'$ will not have more than one edge from some vertex x to some vertex y, else $\mathcal{G}$ would have failed property two. Every vertex in $\mathcal{G}'$ will still have exactly one edge of each type starting and ending at that vertex since all edges of just one type have been removed. And, finally, we know that there are no sequences in $\mathcal{G}'$ that fail the fourth property else those sequences would have failed the fourth property in $\mathcal{G}$ as well.

Thus, $\mathcal{G}'$ satisfies all four properties and must be a Cayley digraph of G by Theorem 2.1. $\square$

Theorem 4.2 makes intuitive sense if we think about the interpretation of the Cayley digraph in algebraic terms. If one generator is removed from the original generating set, but that set still generates the entire group, then we still have a generating set for the group. Thus, there should be a Cayley digraph to represent it relative to the new generating set. In the previous example, it is obvious that the second digraph is still a Cayley digraph of $< \mathbb{Z}_6, + >$ because the new generating set, $\{1\}$, still generates $< \mathbb{Z}_6, + >$.

4.2 Disconnected

More interesting results come from studying what happens when a Cayley digraph becomes disconnected when one edge type is removed.

Theorem 4.3. *Let $\mathcal{G}$ be the Cayley digraph of a group G. Suppose all edges of one type are removed from $\mathcal{G}$ and the resulting graph $\mathcal{G}'$ is disconnected. Then:*

1. *The connected component containing the identity of G is the Cayley digraph of a proper subgroup H of G.*
2. *The other connected components correspond to the distinct left cosets of H in G.*

Proof. (1) Each connected component in $\mathcal{G}$ is a proper subgraph of $\mathcal{G}$ and represents a proper subset of G. Consider the connected component H containing the identity. Even though one type of edge has been removed, the properties 2, 3, and 4 were satisfied in $\mathcal{G}$, and these properties will still hold if we remove one edge type, as seen in the proof of Theorem 4.2. Thus, the connected component containing the identity satisfies all four properties and has the identity element of G. And, by Theorem 2.2, this component represents a Cayley digraph of a proper subgroup, H, of G.

(2) We will prove the second part of this theorem with a double inclusion; we will show that for some element x of G, the left coset xH is a subset of the connected component containing x in $\mathcal{G}'$, and then we will show that the connected component containing x is a subset of xH.

Consider a connected component in $\mathcal{G}'$, and let x be an element of that component. Let $h_1 \in H$. Then there exists a path from the identity to h_1 in H.

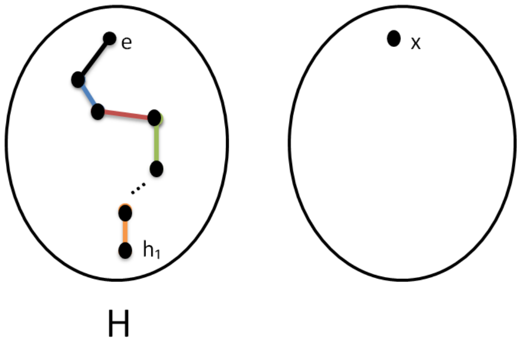

Figure 26: There is some path in H between e and h_1.

Since this path exists in $\mathcal{G}$, and $\mathcal{G}$ is a Cayley digraph, then, by the third property, we know we can construct the same path from x to xh_1 in the connected component containing x in $\mathcal{G}'$. We can do this in the following way: we know that the first edge in the path from e to h_1 will be adjacent to x because there existed exactly one edge of each type starting at x in $\mathcal{G}$.

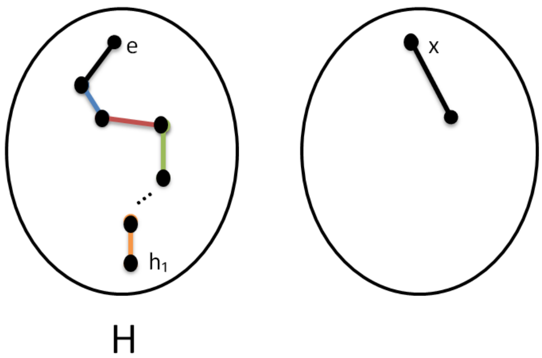

Figure 27: We know that this first edge is adjacent to x because the third property of Cayley digraphs is satisfied in $\mathcal{G}$.

Similarly, we know that the next edge in the path from e to h_1 will be adjacent to the vertex that is adjacent to x by the first edge for the same reason.

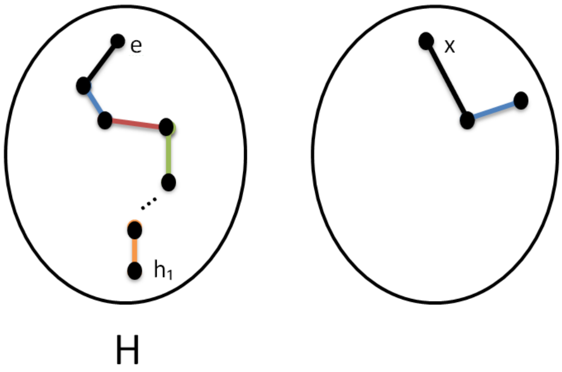

Figure 28: We know that this second edge is incident to the first edge because of the same reason.

In this way, we can construct the same path from x to the vertex xh_1 that existed between e and h_1. We can call this vertex xh_1 by the convention of our Cayley digraph and right multiplication.

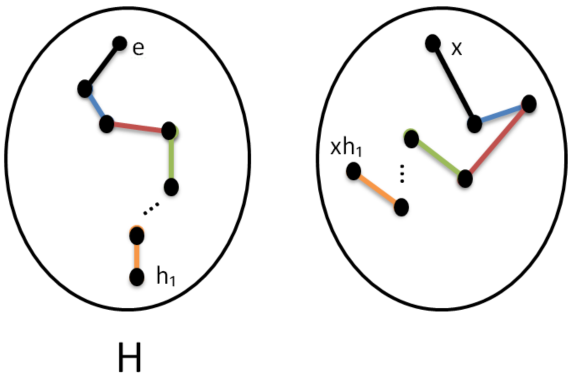

Figure 29: We can construct the path represented by h_1, and we know have xh_1 in the connected component containing x.

Thus, for any element $h \in H$, we know xh is in the connected component containing x. Since the set $\{xh|h \in H\}$ is the left coset xH, we have xH is a subset of the connected component containing x. We have proven the forward inclusion.

Now, consider an element y of the connected component containing x. We know x and y must be connected by a sequence of edges in $\mathcal{G}'$. Let's call this sequence $\mathcal{S}$.

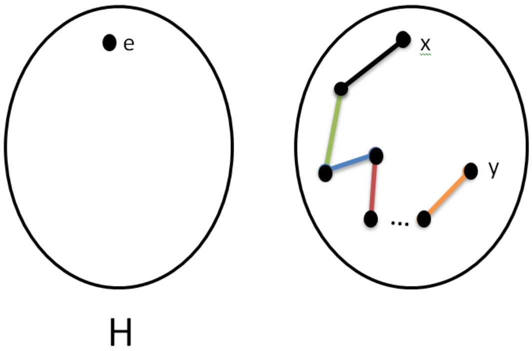

Figure 30: Since x and y are in the same connected component, we know that they are connected by some sequence of edges $\mathcal{S}$ in $\mathcal{G}'$.

Using the same logic as before, we can construct that same sequence of edges $\mathcal{S}$ in H, starting at the identity. The vertex at which the sequence $\mathcal{S}$, starting from the identity, ends is an element of H, say h^*.

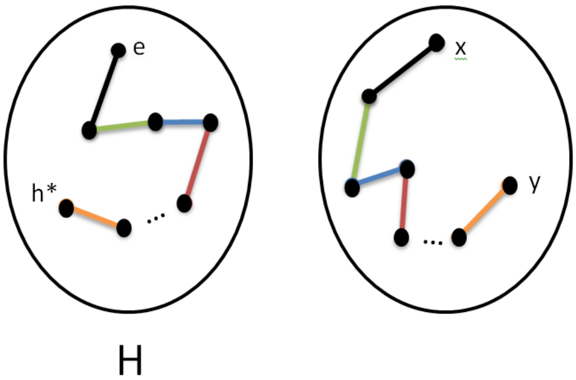

Figure 31: This sequence of edges $\mathcal{S}$ exists in H.

By property four of Cayley digraphs, we know that wherever this sequence $\mathcal{S}$ exists, it is equivalent to multiplication on the right by h^*. Thus, in the connected component containing x, we can interpret y as xh^*, since if we follow the sequence $\mathcal{S}$ (equivalent to h^*) starting at x, we get to y. Thus, every element of the connected component containing x can be written as xh where $h \in H$. Therefore the connected component containing x is a subset of the left coset xH. And, we have the reverse inclusion.

So we have the connected component containing x as a subset of xH, and xH as a subset of the connected component containing x. Hence, the connected component containing x is the same as the left coset xH.

In general, we have that each of the connected components of $\mathcal{G}'$ represent a left coset of H in G. □

By this result, it follows that:

Corollary 4.4. *The number of connected components in $\mathcal{G}'$ will be equal to the index of H in G.*

To illustrate the concept of Theorem 4.3, let's reconsider the Cayley digraph that represents the group DiH_5, with generating set $\{g_1, g_2\}$, where each solid edge is represented by multiplication on the right by g_1 and each dashed edge is represented by multiplication on the right by g_2:

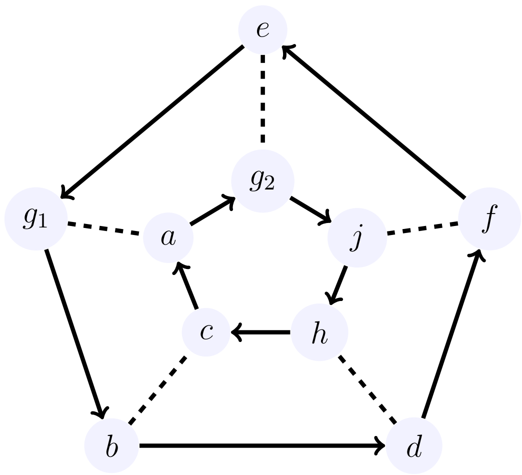

Figure 32: Cayley Digraph of DiH_5 with generating set $\{g_1, g_2\}$ and right multiplication.

If we take away generator g_1, represented by the solid, directed edges, then the corresponding digraph looks like the following:

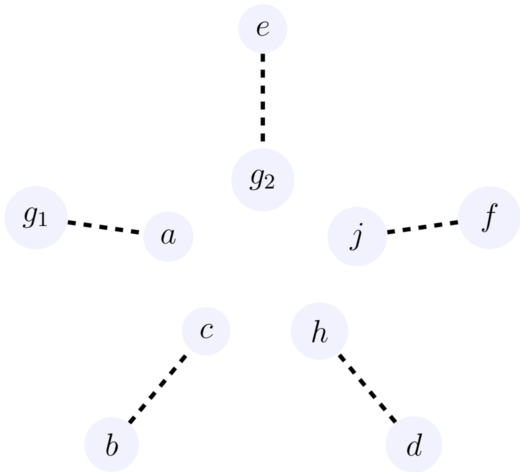

Figure 33: Resulting digraph when g_1 edges are removed.

Thus, by our theorem, $H = \{e, g_2\}$ is a subgroup of DiH_5 and the left cosets are:

$$g_1 H = \{g_1, g_1 g_2 = a\}, \tag{19}$$
$$(g_1)^2 H = \{g_1^2 = b, g_1^2 g_2 = c\}, \tag{20}$$
$$(g_1)^3 H = \{g_1^3 = d, g_1^3 g_2 = h\}, \tag{21}$$
$$(g_1)^4 H = \{g_1^4 = f, g_1^4 g_2 = j\}. \tag{22}$$

4.3 Normal Subgroups

In our proof, we show how one can get the *left* cosets of a certain subgroup using a given Cayley digraph, but it is also possible to see the *right* cosets of the subgroup as well. In order to produce the right cosets using this process, we need to change our convention of multiplication on the right, to multiplication on the left.

Thus, if we redefine our operation and let each solid edge represent multiplication on the left by generator g_1 and each dashed edge represent multiplication on the left by generator g_2, then we can apply the same process above and be able to see the right cosets of DiH_5. As you can see in the following figure, the underlying digraph structure is the same, but the labeling of the vertices changes slightly:

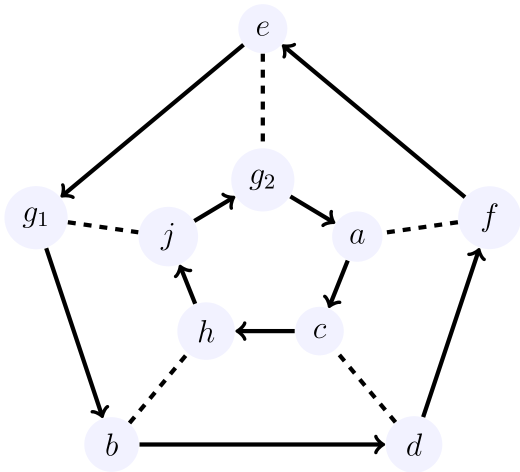

Figure 34: Cayley Digraph of DiH_5 with generating set $\{g_1, g_2\}$ and left multiplication.

Now, let's remove the solid edges representing generator g_1 again:

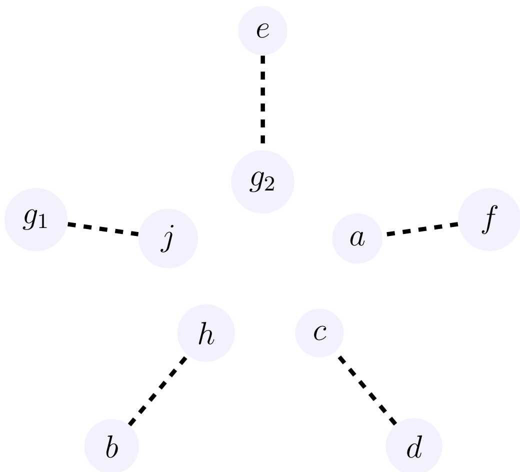

Figure 35: Resulting digraph when g_1 edges are removed.

Now, an argument analogous to the proof of Theorem 4.3 tells us that $H = \{e, g_2\}$ is a subgroup of DiH_5, and the corresponding *right* cosets are:

$$Hg_1 = \{g_1, g_2g_1 = j\}, \tag{23}$$
$$H(g_1)^2 = \{g_1^2 = b, g_2g_1^2 = h\}, \tag{24}$$
$$H(g_1)^3 = \{g_1^3 = d, g_2g_1^3 = c\}, \tag{25}$$
$$H(g_1)^4 = \{g_1^4 = f, g_2g_1^4 = a\}. \tag{26}$$

Not only does this help us visualize the left and right cosets for a group, but we can also use this as a method to test whether or not a group has normal subgroups.

Corollary 4.5. *Given a Cayley digraph $\mathcal{G}$ of a group G, you can apply Theorem 4.3 to obtain a disconnected graph $\mathcal{G}'$ that represents the subgroup H of G and the left cosets of H. Then, you can find the right cosets of H by using left multiplication instead of right multiplication in the application of Theorem 4.3. If the right and left cosets are the same, then H is a normal subgroup of G.*

In our example of the DiH_5 group, we can see that H is not normal since $g_1H = \{g_1, g_1g_2 = a\} \neq Hg_1 = \{g_1, g_2g_1 = j\}$.

4.4 Conjectures

In studying the implications of Theorem 4.3, we investigated a couple conjectures involving the structure of the connected components of the disconnected digraph $\mathcal{G}'$ by following our intuition on a few small examples.

Consider a Cayley digraph of DiH_5 again.

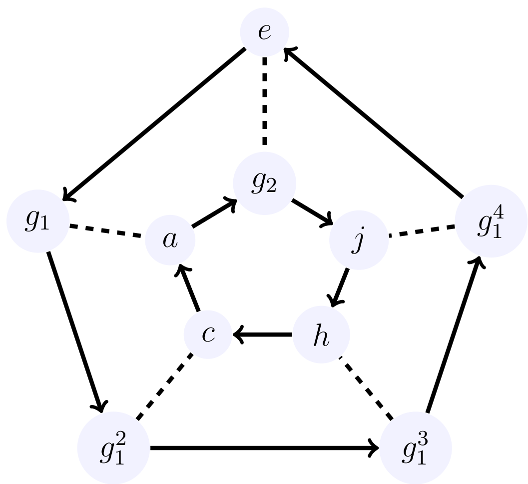

Figure 36: Original Cayley Digraph of DiH_5 with generating set $\{g_1, g_2\}$

And let's remove all g_1 edges from our Cayley digraph.

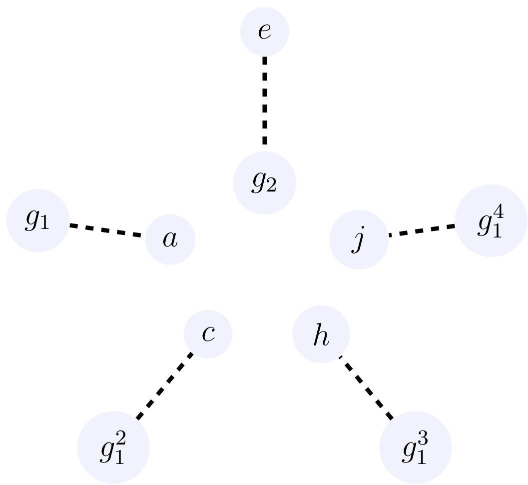

Figure 37: Resulting digraph when g_1 edges are removed.

After we remove all g_1 edges, there is exactly one power of g_1 in each of the connected components in Figure 9, and the number of connected components is five, the order of g_1 in G.

This example, along with a couple others, leads us to the following conjecture.

Conjecture 4.6. *Given a Cayley digraph $\mathcal{G}$ of a group G, when we remove all edges belonging to generator g, and the resulting graph $\mathcal{G}'$ is disconnected, then each connected component contains exactly one power g. Then, the number of connected components in $\mathcal{G}'$ correspond to the order of g.*

But, we find that this is not always true.

Counterexample 4.7. *Consider the Quaternion Group, Q_8:*

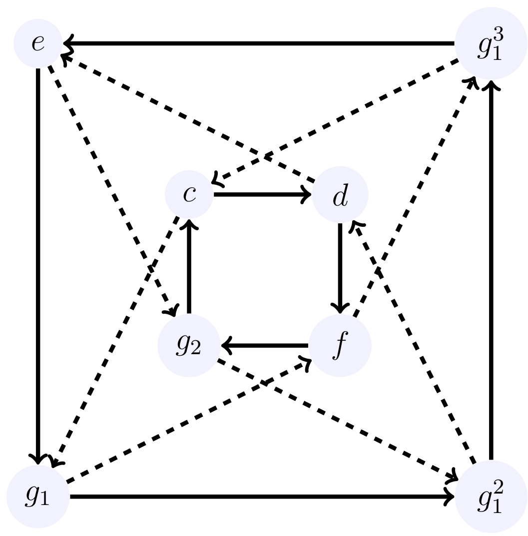

Figure 38: Cayley digraph of Q_8.

If we remove the generator g_1, then we get:

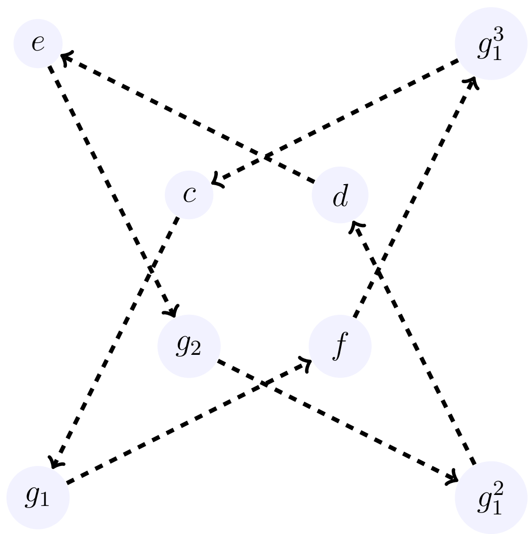

Figure 39: Resulting digraph when generator g_1 is removed.

As you can see, we only have two connected components, even though the order of g_1 is four, and there are two powers of g_1 in each component. Thus, this fails our conjecture.

After we find Conjecture 4.6 to be wrong, we try to reason that there has to be at least one power of the generator removed in each connected component of $\mathcal{G}'$.

Conjecture 4.8. Orphan Problem*: Is it possible, when generator g is removed and the graph becomes disconnected, for there to be an "orphan" connected component that has no power of g in it?*

Several examples, including Q_8, give the impression that no orphan component can exist. However, in trying to prove that this is true, we found another counterexample.

Counterexample 4.9. *Here is a group where we get an "orphan" connected component (actually several) when we remove one generator. This is the Cayley digraph of the group A_4, the alternating group of even permutations on four elements, with generators r_1, represented by the solid black edges, and u_1, represented by the dashed edges.*

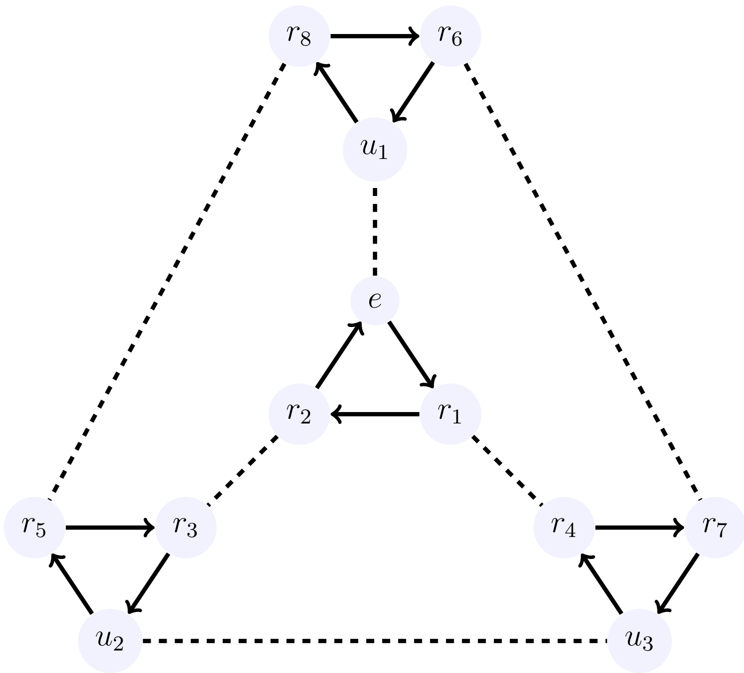

Figure 40: Cayley digraph of A_4.

If we remove the generator u_1 from the Cayley digraph, we get the following disconnected graph:

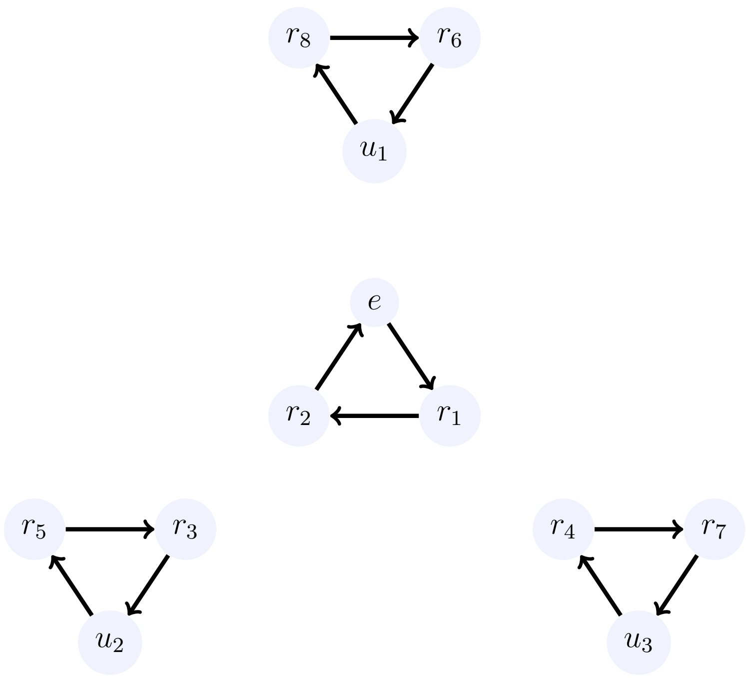

Figure 41: Resulting digraph when all u_1 edges are removed from the Cayley digraph of A_4.

As you can see, only two of the four connected components contain a power of u_1*, the component containing* u_1 *and the component containing* $e = (u_1)^2$*. Thus, the bottom two components are "orphans".*

If one can begin with a given Cayley digraph of some group G and then determine a subgroup H of the group and the corresponding cosets of H, then can we begin with a given group G and proper subgroup H and find a representation of that group such that H and corresponding cosets are visible as in Theorem 4.3? This is the question which sparked the following conjecture:

Conjecture 4.10. *Given a group* G*, suppose we have a proper subgroup* H *of* G*. Then, we can construct the Cayley digraph of* G *in the following way:*

1. *Choose a generating set of* H*. Say* $H = < g_1, \dots, g_k >$.
2. *Construct a Cayley digraph of* H*.*
3. *Make* $n-1$ *copies of* H*, where* n *is the index of* H *in* G*.*
4. *Choose an element* $x \in G \setminus H$*.* [15]

[15] The symbol "\" here means "minus", i.e., $x \in G \setminus H$ means that x is an element of G, but not an element of H.

5. *Then* $G =< g_1, \ldots, g_k, x >$.

But, this conjecture turns out to be untrue.

Counterexample 4.11. *Suppose we are given the group* $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}$. *We choose* H *to be* $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \{e\} \times \{e\}$. *We can follow numbers one through four of the Conjecture 4.10 and choose a generating set, say* $< (1,0,0,0), (0,1,0,0) >$, *construct the corresponding digraph of* H *and 76 other connected components identical to* H, *but the issue comes with the conclusion in step five. Say we had chosen* x *to be* $(0,0,1,0)$, *which is in* $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}$ *but not* $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \{e\} \times \{e\}$. *Then* $G \neq< (1,0,0,0), (0,1,0,0), (0,0,1,0) >$. *For example,* $(1,1,1,1)$ *is in* G, *but not in* $< (1,0,0,0), (0,1,0,0), (0,0,1,0) >$.

However, we believe only a slight alteration to this conjecture is needed. Although it is left unproven, we believe the following to be true:

Conjecture 4.12. *Given a group* G, *suppose we have a proper subgroup* H *of* G. *Then, we can construct the Cayley digraph of a subgroup* H^+ *of* G *for which* H *is also a proper subgroup in the following way:*

1. *Choose a generating set of* H. *Say* $H =< g_1, \ldots, g_k >$.
2. *Construct a Cayley digraph of* H.
3. *Make* $n-1$ *copies of* H, *where* n *is the index of* H *in* G.
4. *Choose an element* $x \in G \setminus H$.
5. *Then* $H^+ =< g_1, \ldots, g_k, x >$, *where* H^+ *is a subgroup of* G.

Thus, we may not always be able to construct the Cayley digraph of G with this method (although we will in some instances), we will always be able to construct the Cayley digraph of a subgroup of G on which we can apply Theorem 4.3 with this method.

5 Further Research

A thorough investigation of the information you can discover about the algebraic properties of a group from a Cayley digraph would take more time and resources than two semesters and an undergraduate education would allow. Therefore, there is much more research to be done on this topic.

Since we were never able to come up with a foolproof way to generate a digraph that satisfied the four properties, one might further investigate ways either to determine if the fourth property is satisfied in a given digraph, having already generated a digraph satisfying the first three properties, or to ensure that the fourth property is satisfied while in the process of generating a digraph.

It would be interesting to investigate if there was a way to easily change a Cayley digraph from right multiplication to left. If this were possible, it would be much easier to implement Corollary 4.5 in order to compare left and right cosets of a subgroup of the corresponding group.

One might also consider other important properties of a group that may be visually determined by a Cayley digraph besides being abelian, being cyclic, and investigating cyclic subgroups and normal subgroups. There are many algebraic properties that mathematicians value in a group that would be interesting to look for in a Cayley digraph.

Furthermore, noting that some of our constructions for visually determining algebraic properties in a Cayley digraph were inefficient to implement for larger groups, one could attempt to find a more practical way of testing Cayley digraphs for cyclic subgroups, for example. Our method works, but uses an inefficient "brute force" approach that could possibly be improved upon.

6 Conclusion

The results of this paper primarily function to present a different perspective in two different fields of mathematics. Graph Theory introduces a unique way of viewing a group; we rely not on multiplication tables or textbooks to tell us if $\mathbb{Z}_2 \times \mathbb{Z}_5$ is abelian, or cyclic, we can confirm these facts for ourselves using graphs and Graph Theory analysis. In addition, we can look at digraphs in a different way; every digraph has the potential to be a Cayley digraph if it fulfills our properties. A careful drawing of dots and arrows can turn into a representation of a group. The combination of these two fields introduces new ideas and connections for both fields to consider. We managed to capture the abstractness of a group and put it into a graph so we could see each element, represent certain cosets, and investigate cyclic subgroups. It creates a new way to experience, and understand, group theory.

7 Acknowledgments

I owe much gratitude to my thesis advisor, Dr. William Higgins, for his many ideas and suggestions throughout all stages of this thesis. His guidance and support was invaluable in this process.

Thanks to Dr. Adam Parker, who provided assistance and knowledge whenever I asked.

I also thank the Mathematics Department at Wittenberg University who provided me with the knowledge and resources necessary for my research.

References

[1] G. L. Alexanderson: *EULER AND KONIGSBERGS BRIDGES: A HISTORICAL VIEW* Bulletin of the American Mathematical Society (2006).

[2] L. Euler: *Solutio Problematis ad Geometriam Situs Pertinentis* (1736).

[3] J. B. Fraleigh: *A First Course In Abstract Algebra* (Seventh Edition) Addison Wesley (2003).

[4] F. Harary: *The bridges of Königsberg/Kaliningrad: A Tale of One City* Math Horizons (2001).

[5] J. Wavrik: *Multiplication tables for groups of small order.* `http://www.math.niu.edu/~beachy/aaol/grouptables1.html`.

[6] D.B. West: *Introduction to Graph Theory* (Second Edition) Prentice Hall (2001).