Honors Thesis: Investigating the Algebraic Properties of Cayley Digraphs

Alexis Byers, Wittenberg University
Mathematics Department

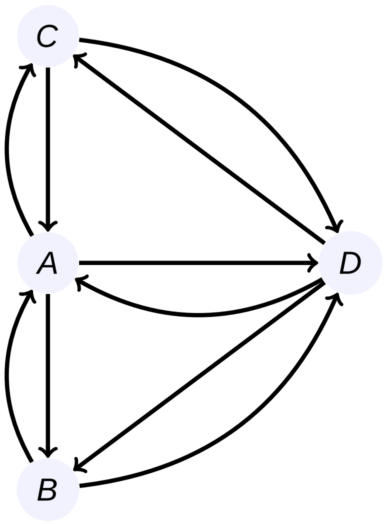
April 30, 2014

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

Contents

1 Introduction

1.1 Graph Theory


C
A
D
B

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 $(z \bmod n) = r$ if r is the remainder when z is divided by n. For elements a, b in $\mathbb{Z}_n$, we define $a + b = (a + b) \bmod n$.*

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 $\{x^n \mid n \in \mathbb{Z}\} = < x >$, [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

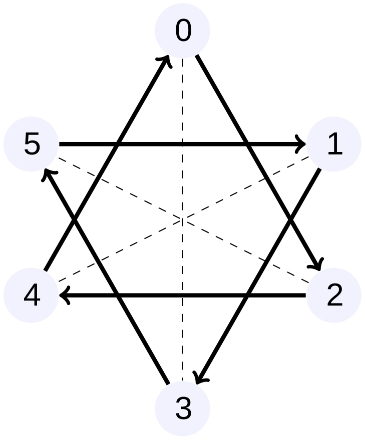


Figure 6: Cayley digraph of$< Z_6; + >$

3. *Every vertex x in 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 G, they should always lead to the same vertex.* [3]

Proof. The first property applies since for elements g

have that the operation we have defined on the vertices of 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

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.

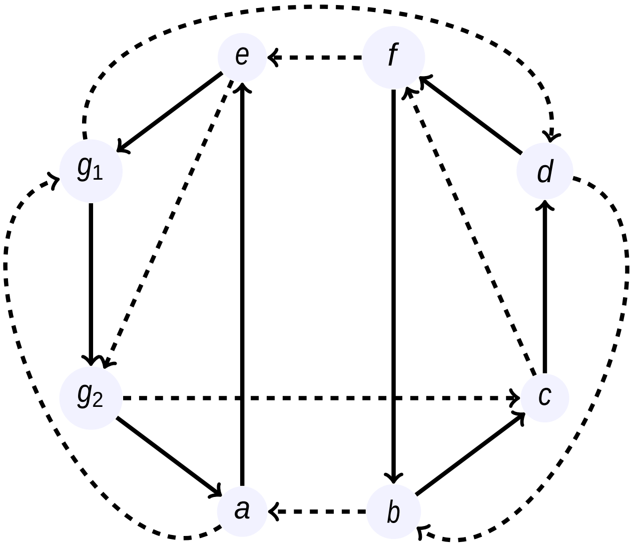
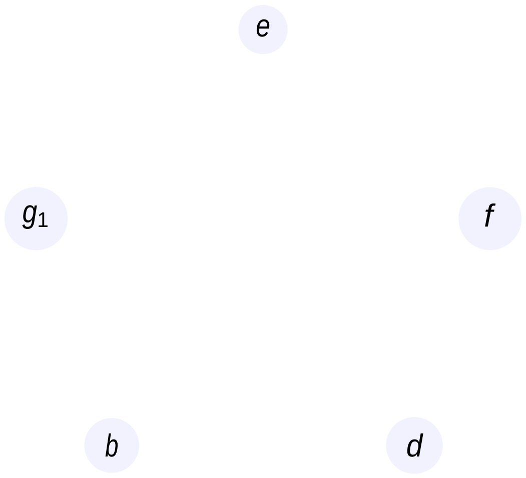


Figure 7:

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]



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 Γ of some group G with generating set $\{g_1; g_2; \dots; g_n\}$.

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 $\{\}$

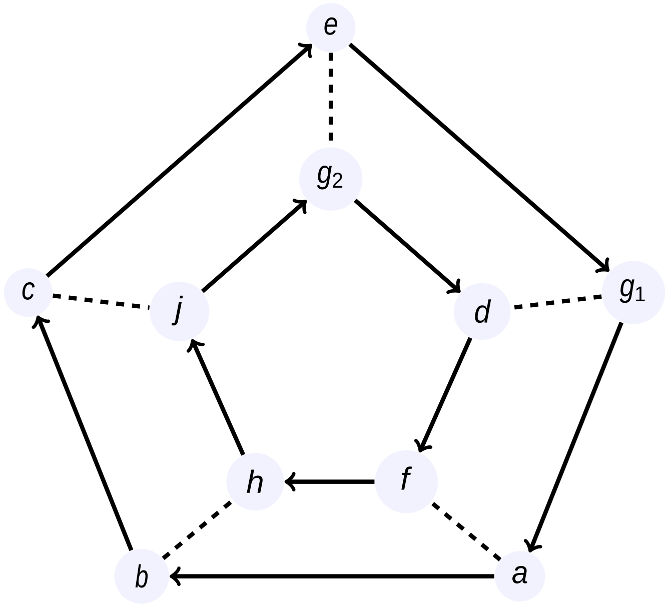


Figure 9: Given a Cayley Digraph$G$.

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 $f g_1; g_2 g$ we will end at vertex d. Similarly, if we start at vertex e and follow the sequence of edges $f g_2; g_1 g$, 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 G is actually a Cayley digraph of $Z_2 \quad Z_5$, with generators $(0; 1)$ and $(1; 0)$ as g_1 and g_2 respectively.

Figure 10:

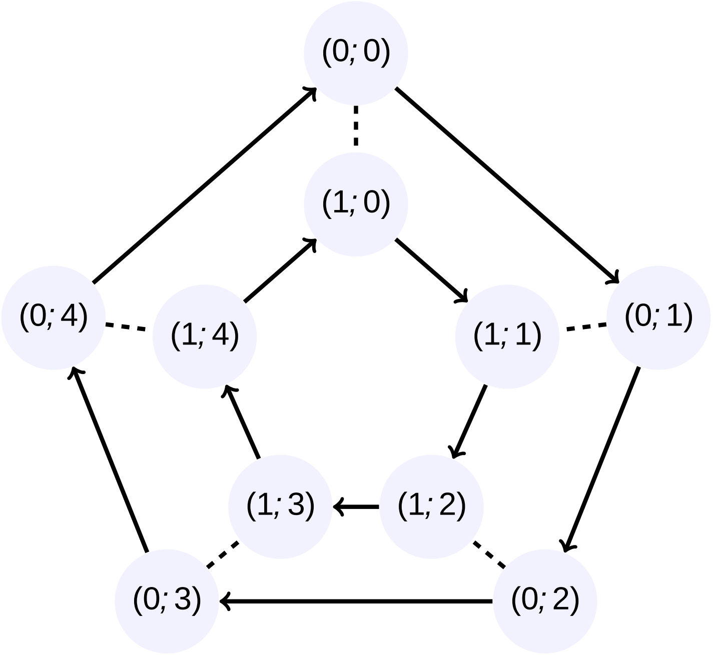
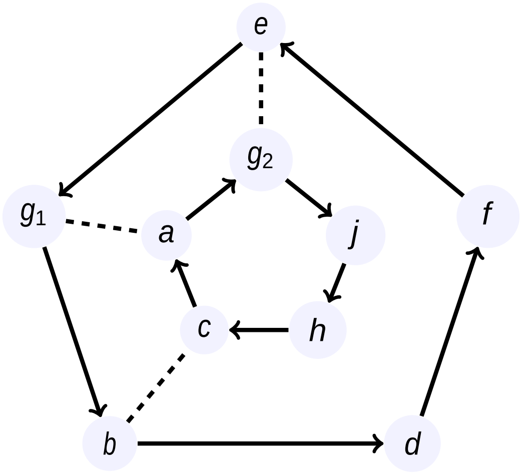


Figure 10: Cayley Digraph ofZ_2 Z_5

Since we know that Z_2 Z_5 *is actually* 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* G^0 *of some group* G^0.



the sequence of edges fg_1

By Proposition 3.4, if we can find a closed walk in G by repeating a sequence of one single path that consists of every vertex and edge of 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 G that is all of 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:

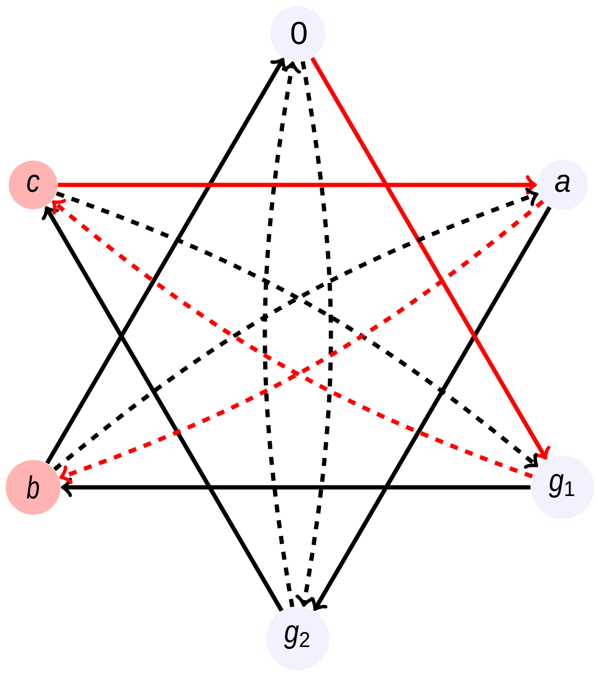


Figure 14: Given Cayley digraph $\mathcal{G}$ of group G after we have traversed the edges in the sequence $\{g_1, g_2\}$ twice.

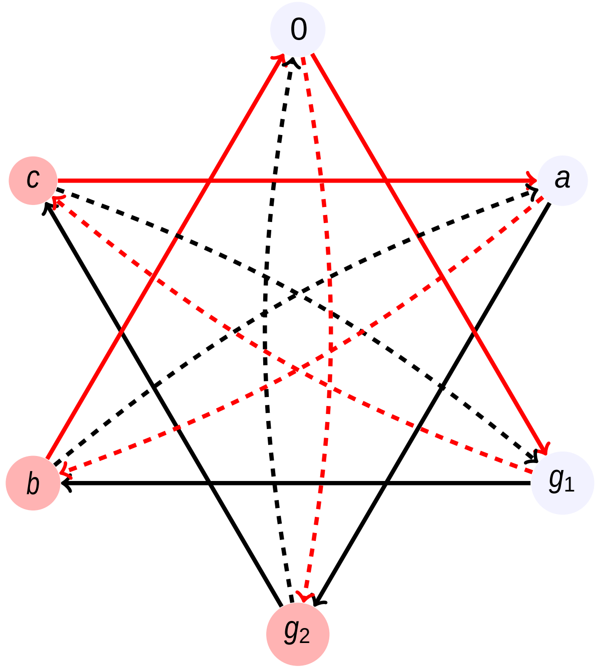


Figure 15: Given Cayley digraph $\mathcal{G}$ of group G after we have traversed the edges in the sequence $\{g_1, g_2\}$ three times.

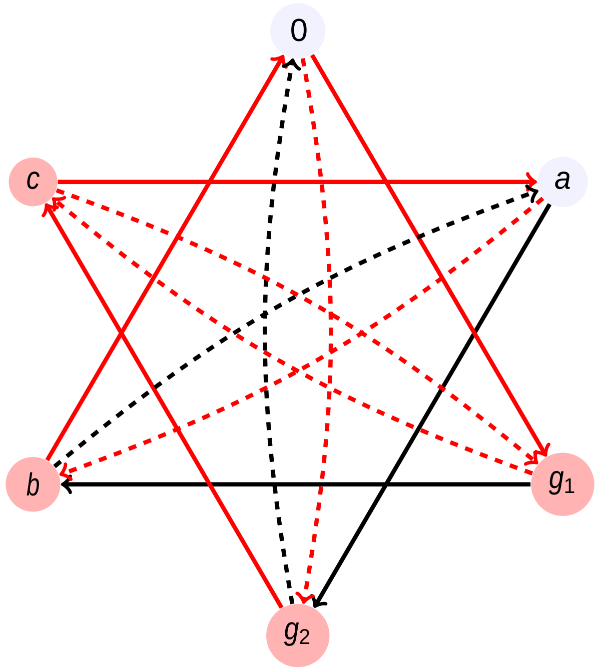


Figure 16: Given Cayley digraph $\mathcal{G}$ of group G after we have traversed the edges in the sequence $\{g_1, g_2\}$ four times.

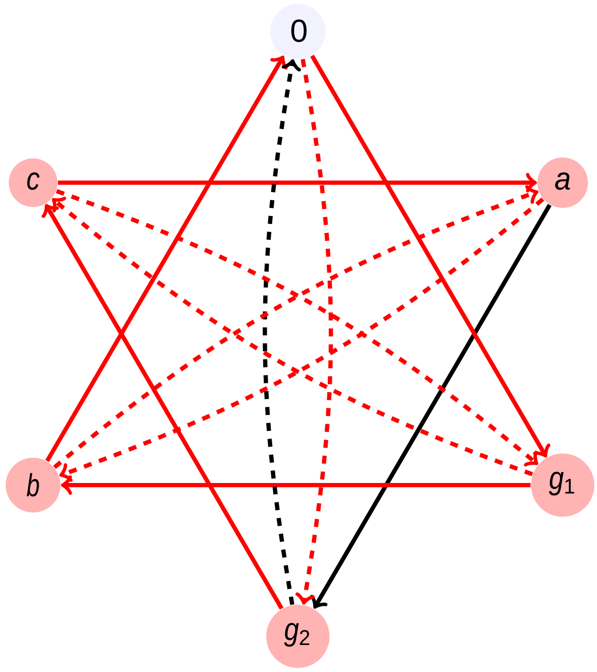


Figure 17: Given Cayley digraph $\mathcal{G}$ of group G after we have traversed the edges in the sequence $\{g_1, g_2\}$ five times.

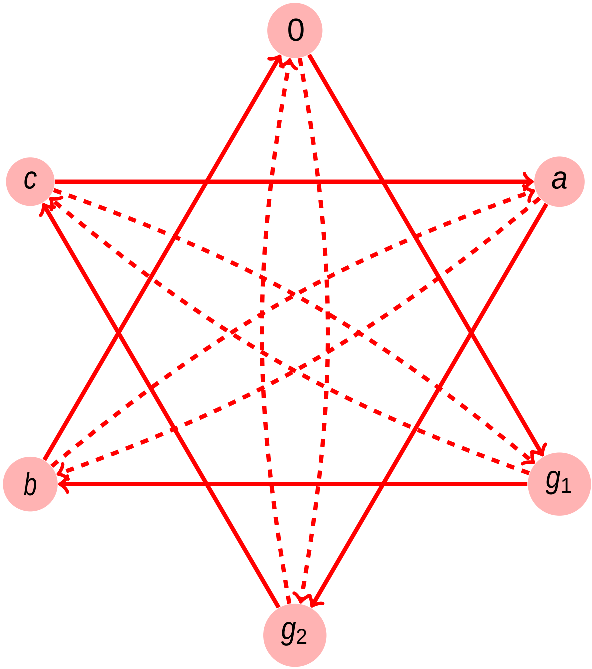


Figure 18: Given Cayley digraph $\mathcal{G}$ of group G after we have traversed the edges in the sequence $\{g_1, g_2\}$ six times.

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 $\mathcal{G}$ 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 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.*

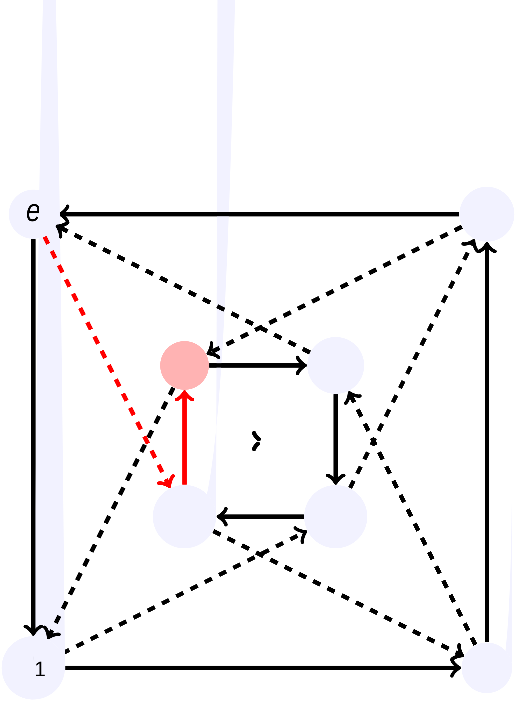


Figure 20: Given Cayley digraph $\hat{G}$ of some group $\hat{G}$ $_2; g_1g$ following the sequence of edges 7 0.56786 0 0.1 0.27522 w [ ] 0.0 $fg_2; g_1g$.

At this point, S contains

At this point, S contains

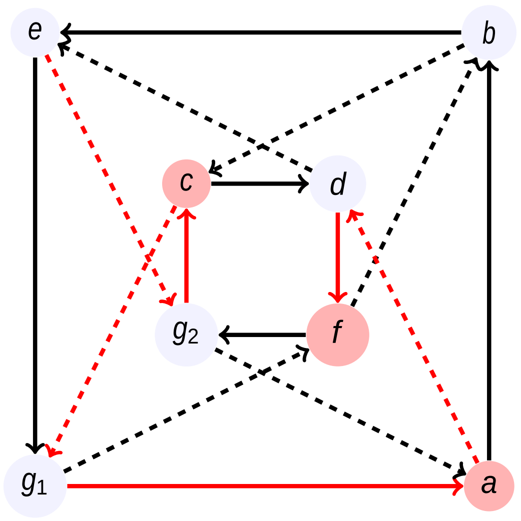


Figure 22: Given Cayley digraph $\hat{G}$ of some group $\hat{G}$, following the sequence of edges $f g_2; g_1 g$.

Now, S contains c, a, and f .

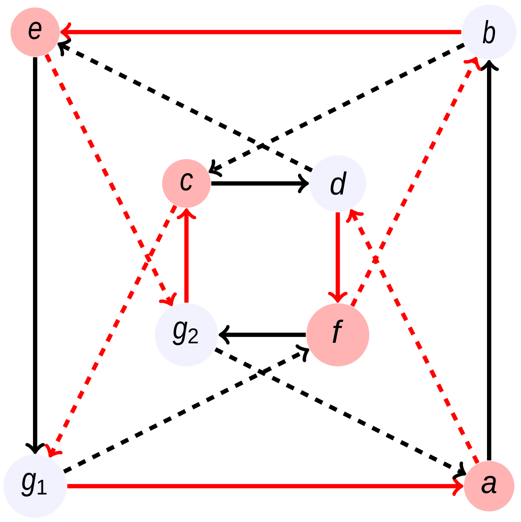


Figure 23: Given Cayley digraph $\hat{G}$ of some group $\hat{G}$, following the sequence of edges $f g_2; g_1 g$.

Thus, we are back at e, and S = fc; a; f; eg. Therefore, by Proposition 3.6, the set S represents the cyclic subgroup generated by c, i.e.,

$$\begin{aligned} < c > &= fc; a; f; eg && (17)\\ &= fc = g_2 g_1; a = (g_2 g_1)^2; f = (g_2 g_1)^3; e = (g_2 g_1)^4 g: && (18) \end{aligned}$$

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

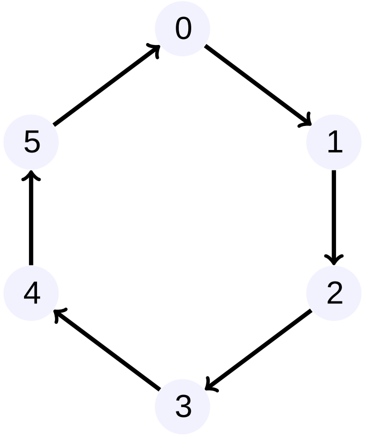


Figure 25: Resulting digraph when generator 2 is removed.

This is still a Cayley digraph of $< Z_6; + >$*, as you can see.*

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

Theorem 4.2. *Let G be a Cayley digraph of a group G. Suppose all edges of one type are removed from G, and the resulting graph G^0 remains connected. Then G^0 remains a Cayley digraph of G.*

Proof. Let G represent a Cayley digraph of a group G. Then G satisfies the four properties.

If we remove one type of edge from G, and the resulting graph G^0 is connected, then we know that G^0 satisfies the first condition.

Since G^0 G, then it is easy to see how properties 2, 3, and 4 hold in G^0. Since the only change made between graphs G and G^0 is the removal of edges, and G satisfied properties 2, 3, and 4, then the following is true: G^0 will not have more than one edge from some vertex x to some vertex y, else G would have failed property two. Every vertex in G^0 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 G^0 that fail the fourth property else those sequences would have failed the fourth property in G as well.

Thus, G^0 satisfies all four properties and must be a Cayley digraph of G by Theorem 2.1. □

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

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

Since this path exists in G, and 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 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 G.

Figure 27: We know that this first edge is adjacent to x because the third property of Cayley digraphs is satisfied in 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.

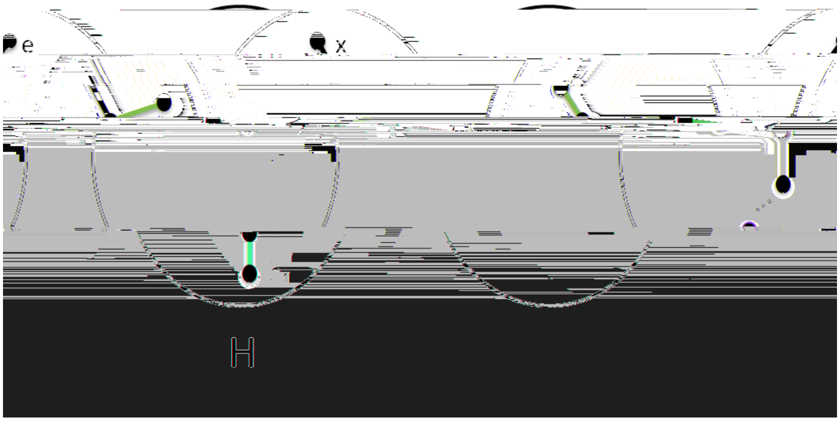


Figure 28: We know that this second edge is incident to the first edge because of the same reason.

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.

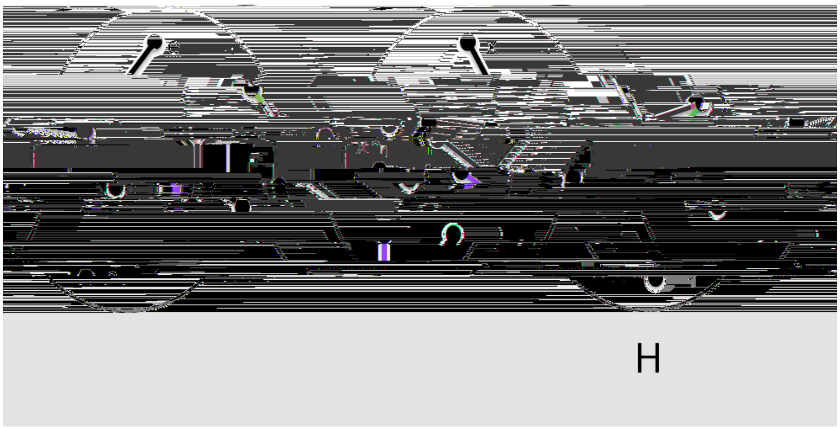


Figure 29: We can construct the path represented by h_1, and we know have xh_1 in the connected component containing x.

Thus, for any element h 2 H, we know xh is in the connected component containing x. Since the set $f xhjh$ 2 Hg 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 G. Let's call this sequence S.

Figure 30: Since x and y are in the same connected component, we know that they are connected by some sequence of edges S in G^{0}.

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

Figure 31: This sequence of edges S exists in H.

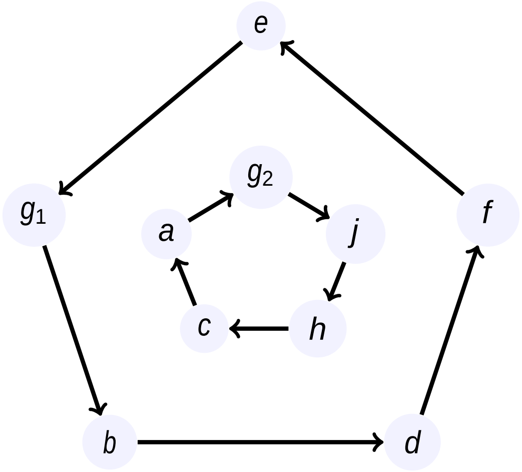
By property four of Cayley digraphs, we know that wherever this sequence S exists, it is equivalent to multiplication on the right by h . Thus, in the connected component containing x, we can interpret y as xh , since if we follow the sequence S (equivalent to h) starting at x, we get to y. Thus, every element of the connected component containing x can be written as xh where h 2 H. Therefore the connected component containing x is a subset of the left coset

In general, we have that each of the connected components G^0 of represent a left coset of H in G. □

By this result, it follows that:

Corollary 4.4. *The number of connected components in G^0 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 groupDiH_5, with generating set$fg_1; g_2g$, 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:



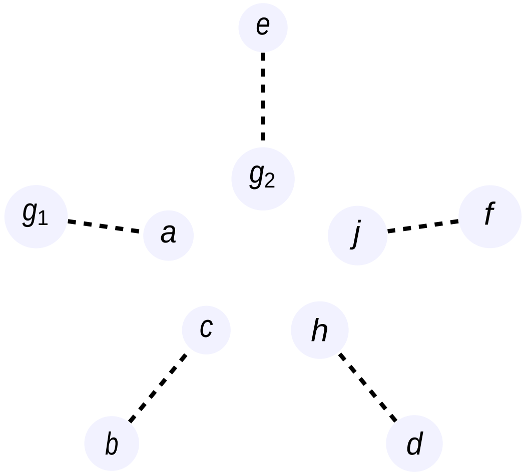


Figure 33: Resulting digraph when g_1 edges are removed.

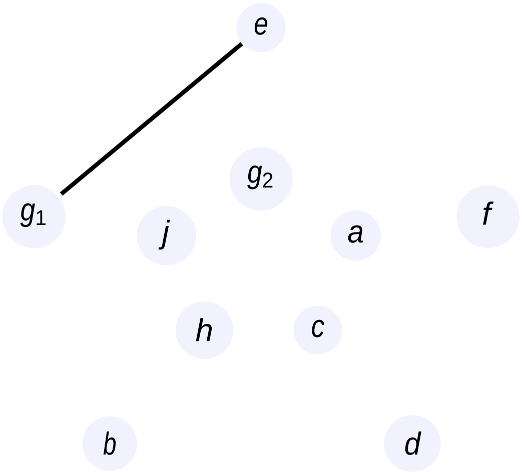
Thus, by our theorem, $H = fe; g_2g$ is a subgroup of DiH_5 and the left cosets are:

$$\begin{aligned} g_1H &= fg_1; g_1g_2 = ag; && (19)\\ (g_1)^2H &= fg_1^2 = b; g_1^2g_2 = cg; && (20)\\ (g_1)^3H &= fg_1^3 = d; g_1^3g_2 = hg; && (21)\\ (g_1)^4H &= fg_1^4 = f; g_1^4g_2 = jg: && (22)\end{aligned}$$

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:


e
g2
g1
j
a
f
h
c
b
d

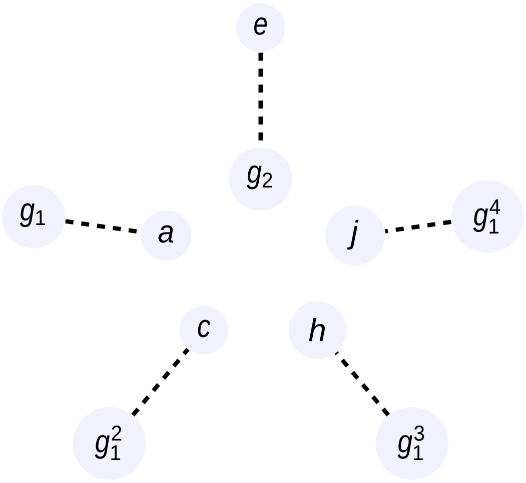


Figure 37:

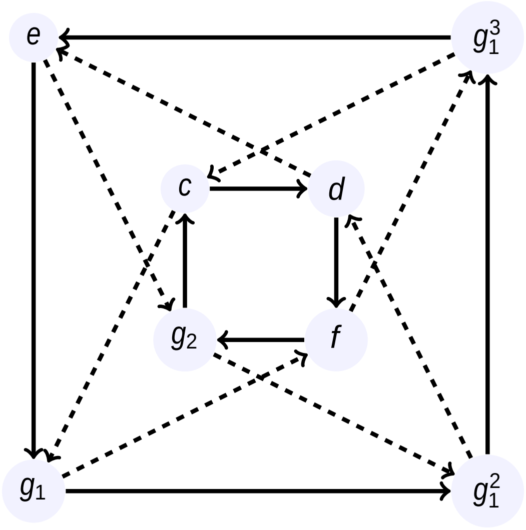


Figure 38: Cayley digraph of Q_8.

If we remove the generator g_1, then we get:

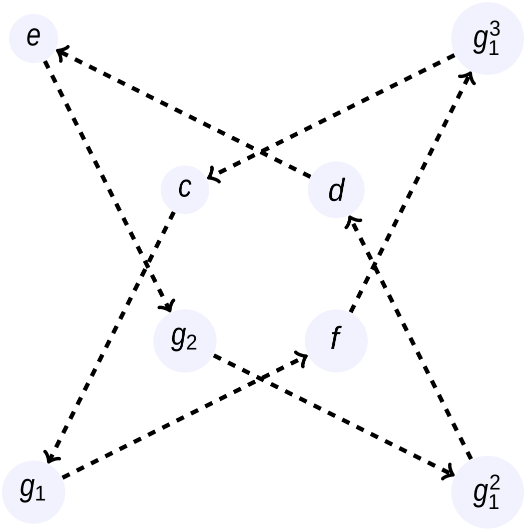
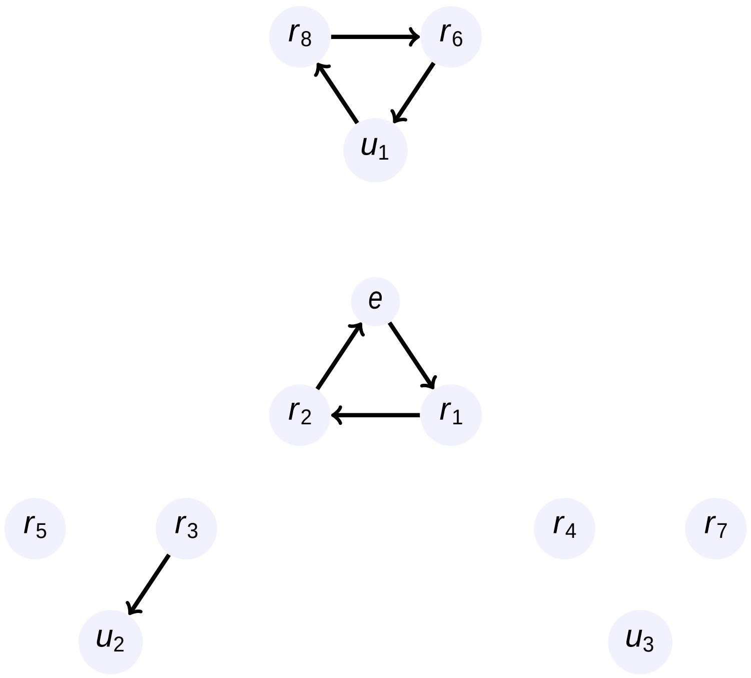


Figure 39: Resulting digraph when generator g_1 is removed.

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 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?*



r_8
r_6
u_1
e
r_2
r_1
r_5
r_3
r_4
r_7
u_2
u_3

5. *Then $G = < g_1; : : : ; g_k; x >$.*

But, this conjecture turns out to be untrue.

Counterexample 4.11. *Suppose we are given the group Z_2 Z_5 Z_7 Z_{11}. We choose H to be Z_2 Z_5 feg feg. 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 Z_2 Z_5 Z_7 Z_{11} but not Z_2 Z_5 feg feg. 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 $H = < g_1; : : : ; g_k >$.*
2. *Construct a Cayley digraph of H.*
3. *Make H.*

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: