



Virginia Commonwealth University
VCU Scholars Compass

Theses and Dissertations


Graduate School

2016

The Automorphism Group of the Halved Cube

Benjamin B. MacKinnon
Virginia Commonwealth University

Follow this and additional works at: <https://scholarscompass.vcu.edu/etd>

 Part of the [Algebra Commons](#), [Discrete Mathematics and Combinatorics Commons](#), and the [Other Mathematics Commons](#)

Ben MacKinnon

Downloaded from

<https://scholarscompass.vcu.edu/etd/4609>

This Thesis is brought to you for free and open access by the Graduate School at VCU Scholars Compass. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of VCU Scholars Compass. For more information, please contact libcompass@vcu.edu.

Copyright ©2016 by Ben MacKinnon
All rights reserved

THE AUTOMORPHISM GROUP OF THE HALVED CUBE

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at Virginia Commonwealth University.

by

Ben MacKinnon
Master of Science

Director: Richard H. Hammack , Professor
Department of Mathematics and Applied Mathematics



Virginia Commonwealth University
Richmond, Virginia
December 2016

Acknowledgements

I can't truly thank anyone before I thank my Lord and Savior Jesus Christ. He is the author of mathematical truth, so He created the topic of this thesis and was gracious enough to give Dr. Hammack and I the necessary insight to fill these pages.

None of this would have been possible without my loving and supportive wife. She has always been my teammate and my best friend. Without her support and encouragement I would be a fraction of the man that I am now, and for that I am eternally grateful.

Finally, I am honored to thank Dr. Hammack for taking me on in this research. Throughout this whole process he has been challenging me, encouraging me, and showing me grace for my shortcomings. I sincerely doubt that I will forget his talent, kindness, and character.

Table of Contents

Acknowledgements	iii
List of Figures	v
Abstract	vi
1 Introduction	1
1.1 Graphs	1
1.2 Halved Cubes and Circulants	4
1.3 Automorphism Groups	10
2 $\text{Aut}(Q'_n)$ Where $n \neq 4$	16
3 The Fourth Dimension	28
4 A Connection Between Halved Cubes And Circulants	44
Bibliography	50
Vita	50

List of Figures

1.1	Two examples of graphs G , and H	2
1.2	A graph G and two of its sub-graphs H and K	3
1.3	Two isomorphic graphs P and Q , and an isomorphism ϕ	3
1.4	Q_2 , Q_3 and Q_4	5
1.5	Γ_2 and Γ_3	6
1.6	Q'_2 , Q'_3 , and Q'_4	9
1.7	The circulant graph $C_6(1, 2)$	9
1.8	An element S_5 , its cycle permutation representation, and its permutation matrix.	11
1.9	A graph K with $\text{Aut}(K) \cong \langle (24), (5678) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$	13
2.1	The graph Q'_3 and Q'_3 with R , an element of $\text{Aut}(Q'_3)$, acting on $V(Q'_3)$. . .	27
3.1	The graph Q'_4 and it's complement.	28
3.2	The graph Q'_4 and Q'_4 with R acting on $V(Q'_4)$	43
4.1	Q'_2 and $C_2(1)$	49
4.2	Q'_3 and $C_4(1, 2)$	49
4.3	Q'_4 and $C_8(1, 2, 3)$	49

Abstract

An n -dimensional **halved cube** is a graph whose vertices are the binary strings of length n , where two vertices are adjacent if and only if they differ in exactly two positions. It can be regarded as the graph whose vertex set is one partite set of the n -dimensional hypercube, with an edge joining vertices at hamming distance two.

In this thesis we compute the automorphism groups of the halved cubes by embedding them in \mathbb{R}^n and realizing the automorphism group as a subgroup of $GL_n(\mathbb{R})$. As an application we show that a halved cube is a circulant graph if and only if its dimension of is at most four.

Chapter 1

Introduction

This thesis will present and discuss the automorphism groups of a family of graphs known as halved cubes. We will use these groups to characterize which halved cubes are isomorphic to circulants. Specifically, we will use characteristics of elements of the automorphism group of halved cubes to show that a halved cube is isomorphic to a circulant graph if and only if the dimension of the halved cube is less than or equal to four. Before this proof can be presented we must first present definitions for the structures used throughout this thesis.

1.1 Graphs

Since this thesis deals largely with graphs, we begin with some fundamental definitions and examples of graphs.

Definition 1. A *graph* G is an ordered pair $(V(G), E(G))$ where $V(G)$ is a finite set called the *vertices* of the graph G , and $E(G)$ is a set of unordered pairs of elements of $V(G)$, which are called *edges*. We call the number of vertices in the graph G the *order* of G , and the number of edges in the graph G the *size* of G . Let u and v be vertices of a graph G . The vertices u and v are *adjacent* if there exists an edge $uv \in E(G)$. If $uv \notin E(G)$ then u and v are *nonadjacent*.

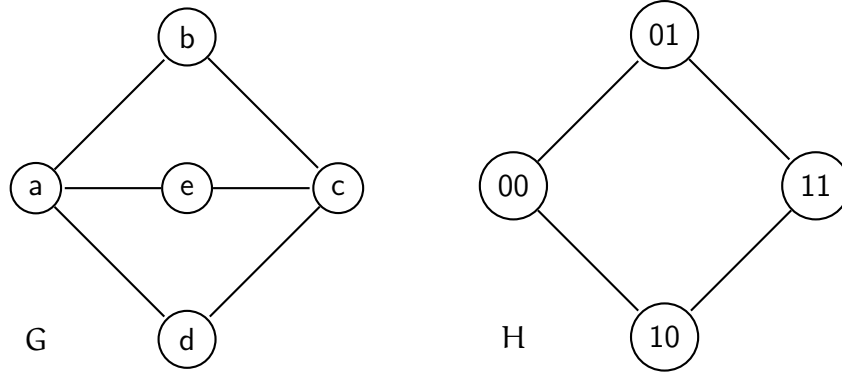


Figure 1.1: Two examples of graphs G, and H.

Similarly, if u and v are adjacent then u is a **neighbor** of v and vice a versa [1] (pg. 3).

Figure 1.1 shows two graphs G and H. Given Definition 1 we see that $V(G) = \{a, b, c, d, e\}$ and $E(G) = \{ab, ac, bc, cd, ae, ce\}$. Observe that G is a graph of order five and size six. Next, observe that $V(H) = \{00, 01, 11, 10\}$ and $E(H) = \{(00, 01), (01, 11), (11, 10), (10, 00)\}$. Also observe that H is of order and size four.

Clearly, vertices do not have to be letters or numbers, but can take on any particular identity. In this thesis we will discuss graphs with vertices which are binary strings of a specified length. Figure 1.1 provides examples of graphs, the last of which has binary strings as the vertices. Constructions of graphs from binary strings will serve as an important idea throughout this thesis.

Definition 2. Let G be a graph, a graph H is a **subgraph** of G , written $G \supseteq H$, if and only if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. The **subgraph induced** by H , denoted $G[H]$ is the subgraph of H where if $u, v \in H$ and $uv \in E(G)$ then $uv \in E(G[H])$.

The bulk of this thesis deals with demonstrating the similarity between graphs using mappings between their vertex sets. In particular, we will examine isomorphisms between graphs.

Definition 3. The graphs G and H are **isomorphic**, written $G \cong H$, if there exists a bijective mapping $\phi : V(G) \rightarrow V(H)$ such that two vertices are adjacent in G if and only if their images are adjacent in H . That is, $xy \in E(G)$ if and only if $\phi(x)\phi(y) \in E(H)$.

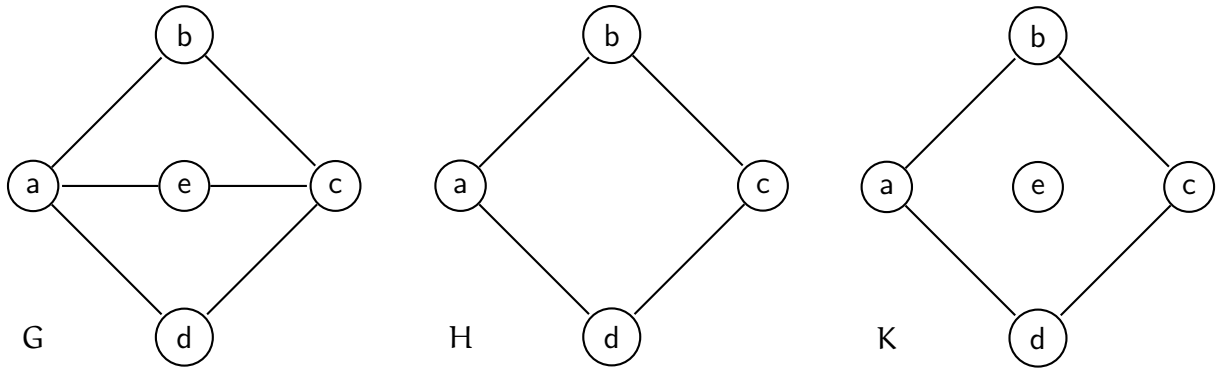


Figure 1.2: A graph G and two of its sub-graphs H and K .

The notion of isomorphism helps avoid the mistake of thinking of graphs as “equal” if they are simply drawn in a different manner. Consider the two different representations of the graphs shown in Figure 1.3 below: the graphs P and Q seem to be the same graph drawn in different ways, but there are edge-crossings in G while no edges cross in Q . While this difference may seem subtle, this is only one example of why “equality” between graphs needs a more abstract definition, hence isomorphism. Figure 3 explicitly presents one of these possible mappings $\phi : V(P) \rightarrow V(Q)$.

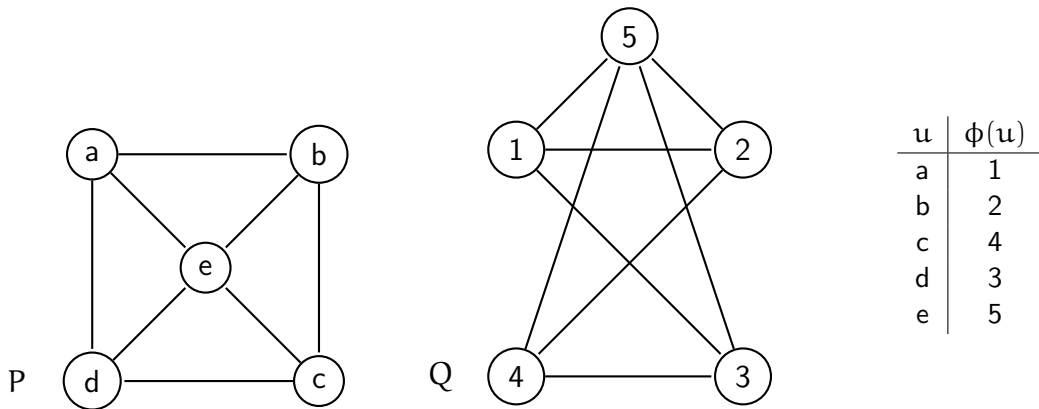


Figure 1.3: Two isomorphic graphs P and Q , and an isomorphism ϕ .

1.2 Halved Cubes and Circulants

This thesis will focus on the graphs known as “halved cubes.” Before these graphs can be discussed we begin with the notion of hamming distance.

Definition 4. Let u and v be binary strings each of length n where n is a positive integer, the *hamming distance* of u and v is the number of digits in which the strings u and v differ. Strings u and v are **binary inverses** if and only if they have a hamming distance of n .

As an example, let u and v be binary strings of length four and $u = 0011$ and $v = 0101$. The strings u and v only differ in the second and third digits, thus the hamming distance between u and v is two. We would say that $w = 1100$ is the binary inverse of u in that u and w have a hamming distance of four.

An example of a construction of a graph from the hamming distance of binary digits is Q_n , or the Hypercube, which is defined below:

Definition 5. An n -dimensional hypercube graph, called Q_n , is constructed by the set of all n -digit binary numbers as $V(Q_n)$ where u and v are adjacent if and only if u and v have a hamming distance of one. [3] (pg. 18).

Before any discussion of Q_n , we define k -regular graphs below:

Definition 6. A graph G is **k -regular** if and only if every vertex of G has exactly k neighbors.

Observe that Q_n is of order 2^n , and is n -regular in that each vertex has n neighbors with a hamming distance of one. From here we see that Q_n is of size $2^{n-1}n$. In Figure 1.4, the graphs Q_2 , Q_3 , and Q_4 are displayed. Notice that the hypercube in the n -th dimension can have a representation reminiscent of an n -th dimensional cube in the geometric sense.

Say that you are now going to define the vertices of a graph to be the set of all n digit binary strings and let two vertices be adjacent if and only if their associated binary strings have a hamming distance of two. Observe that this graph will be of order 2^n

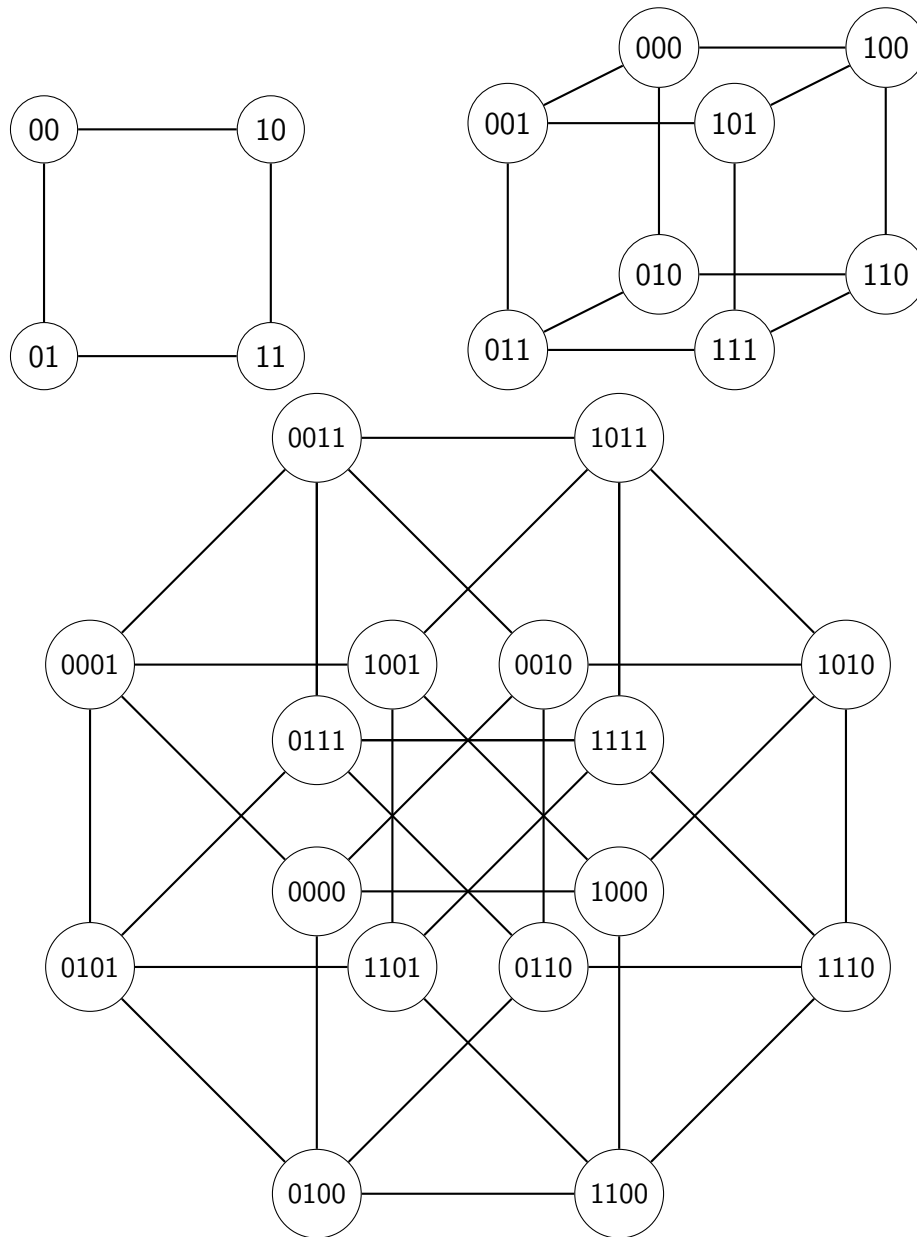


Figure 1.4: Q_2, Q_3 and Q_4

and will be $\binom{n}{2}$ regular. In examining these constructions in the figure below, notice that each construction yields two sub-graphs which share no vertices and edges, and are isomorphic. For a given n , the graph resulting from the above construction is denoted Γ_n .

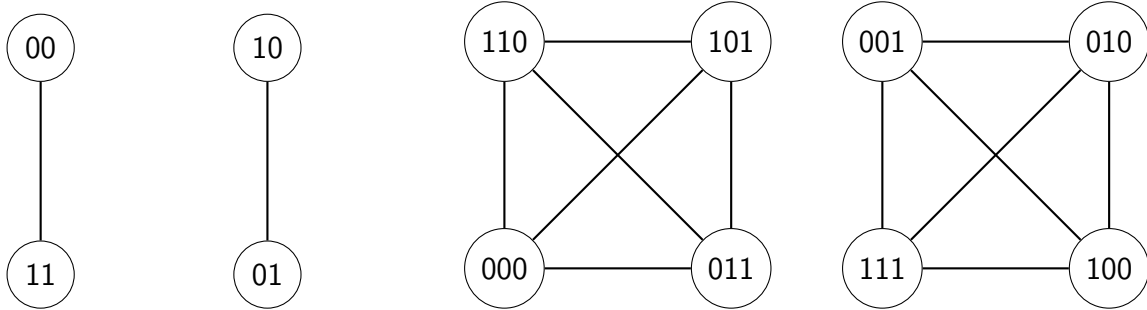


Figure 1.5: Γ_2 and Γ_3

Let u and v be n -digit binary strings with a hamming distance of two. Suppose that the digit sum of u is k . In the two digits where u and v differ, either u has two ones in the digits where v has two zeros (the digit sum of v is two less than k), u has a one in place of a zero in v and u has a zero in place of a one in v (the digit sum of v is k), or u has two zeros in the digits where v has two ones (the digit sum of v is two more than k). Thus, if u has an even digit sum then all of its neighbors will also have even digit sum, and likewise if u had an odd digit sum then all its neighbors will have odd digit sums. Below we will prove that there are exactly two components of Γ_n and they are isomorphic with one another.

Proposition 1. *For all $n \in \mathbb{N}$ there are exactly two components of Γ_n and these components are isomorphic.*

Proof. Let $n \in \mathbb{N}$ and define the sequence $\langle a_0, \dots, a_{2^n-1} \rangle$ such that a_i is the binary expression of i with n digits, thus $i \in \{0, \dots, 2^n - 1\}$, the terms of this sequence will also be the vertex set of Q'_n . Next, define V_0 to be the set binary digits from the sequence above having an even digit sum and V_1 to be the set of binary digits from the sequence above with odd digit sum. We will now show that given a vertex in V_1 and a vertex in

V_0 there will not be a path between them in Γ_n . Let $a_p \in V_1$ and $a_q \in V_2$ and suppose that a_p and a_q are adjacent, then the hamming distance of a_p and a_q is two. Observe that if the digit sum of a_p is k , then the digit sum of a_q is either k or $k \pm 2$. Thus, a_p and a_q have the same parity, a contradiction. From here, it is clear that vertices in V_1 can only be adjacent with vertices of V_1 then there will be no path from a vertex in V_1 to any vertex in V_0 , thus Γ_n is disconnected. Further, by this construction we see that if there were more than two components of Γ_n then the subgraph induced by V_0 or the subgraph induced by V_1 is disconnected.

Consider the subgraph induced by V_0 . Clearly, we have that $a_0 \in V_0$, and for any vertex $a_k \neq a_0$ then there is a $2r$ 1s in a_k where $r \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$. Define a sequence $\langle b_1, \dots, b_{r-1}, 0000 \rangle$ to be the sequence of vertices of V_0 such that b_i is a_k with $2i$ 1s from a_k changed to 0s. Observe that the vertices b_i and b_{i-1} will be adjacent and that this sequence defines a path from a_k to a_0 . Since a_k was chosen arbitrarily then there exists a path from an vertex of V_0 to the vertex a_0 , so there must be a path from any vertex in V_0 to any other vertex in V_0 . Similarly, for $a_m \in V_1$ if we define a similar sequence where $\langle c_1, \dots, c_{r-1} \rangle$ then c_{r-1} would have a singular 1 in its binary expression, thus would either be adjacent to $a_1 = 0\dots1$ or $c_{r-1} = a_1$. By this logic we have also shown that V_1 is connected.

Next we need to show that the subgraph induced by V_0 and the subgraph induced by V_1 are isomorphic. Where n is fixed, define $f : V_0 \rightarrow V_1$ such that $u \rightarrow f(u)$ if and only if $f(u)$ is u with its last digit changed form a 0 to a 1 or from a 1 to a 0. First, we will show that f is a bijection. Suppose that $f(u) = f(v)$, then by changing the last digits in $f(u)$ and $f(v)$ then we have u and v . Obviously, we have that $u = v$ and f is an injection. Clearly, since $|V_0| = |V_1|$ then f is a bijection.

Finally, we need to show that adjacency is preserved under the function f . Let $u, v \in V_0$ such that u and v are adjacent, thus u and v differ in two digits. Suppose they differ in the i -th and j -th digit where $i, j \in \{1, \dots, n\}$. If we suppose that $j = n$ then we have that

u and v differ in their n -th digit, thus $f(u)$ and $f(v)$ differ in their n -th digit as well. Since $f(u)$ and $f(v)$ also differ in their i -th digit, then $f(u)$ and $f(v)$ have a hamming distance of two and thus are adjacent. Further, if neither i nor j are equal to n , then u and v have the same n -th digit, therefore $f(u)$ and $f(v)$ will also have the same n -th digit and differ in the i -th and j -th digit, thus they are adjacent. Next, suppose that $f(u)$ and $f(v)$ are adjacent, and they differ in their n -th digit. Then we have that they also differ in their i -th digit where $i \in \{1, \dots, n - 1\}$, and we have that u and v will differ in their i -th digit and n -th digit, thus u and v will be adjacent. If $f(u)$ and $f(v)$ do not differ in their n -th digit, then u and v will have the same n -th digit, and will differ in the same two places as $f(u)$ and $f(v)$ do, and will be adjacent. Thus, adjacency is preserved by this mapping f . Therefore, the subgraph induced by V_0 is isomorphic with the subgraph induced by V_1 and the proof is complete. \square

From here, we can clearly define a halved cube and we will make a connection between specific dimensions of halved cubes and complete graphs:

Definition 7. Let G with a graph and $V(G)$ be the set containing all n -length binary strings with even digit sum. Next, let $u, v \in V(G)$ and $uv \in E(G)$ if and only if u and v have a hamming distance of two, then G is a **halved cube** with dimension n and is denoted Q'_n .

Definition 8. A graph is a **complete graph** on n vertices and is denoted as K_n if and only if for any arbitrary $u, v \in V(K_n)$ we have that $uv \in E(K_n)$.

Trivially, Q'_1 is a graph of order one, with size of zero. Using the definition above, it's clear from the figure below that Q'_2 and Q'_3 are both complete graphs; more generally $Q'_2 \cong K_2$ and $Q'_3 \cong K_4$. Another interesting connection that will be discussed later in this thesis is the connection between Q'_n and graphs which are called circulants.

Definition 9. Let G be a graph of order n with $V(G) = \{a_1, \dots, a_n\}$. Then G is a **circulant** of the form $C_n(k_1, \dots, k_m)$ if $a_i a_{i+k_j \bmod(n)} \in E(G)$ for all $i, j \in \{1, \dots, n\}$.

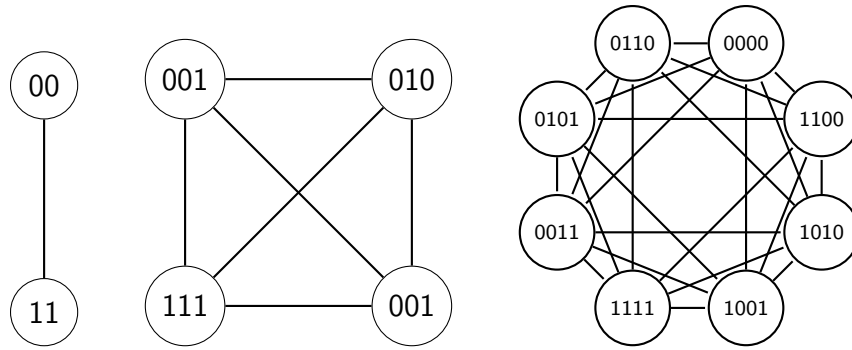


Figure 1.6: Q'_2 , Q'_3 , and Q'_4

As an example, consider the circulant $C_6(1, 2)$. This graph has six vertices, namely a_1 through a_6 . By our definition, we have that $k_1 = 1$ and $k_2 = 2$. The term k_1 induces a cycle consisting of all vertices in the graph with vertices being adjacent if and only if they are of the form $a_{i \bmod(6)}$ and $a_{(i+1) \bmod(6)}$. Next, k_2 induces two cycles of length three on the vertex sets $\{a_1, a_3, a_5\}$ and $\{a_2, a_4, a_6\}$. This graph is pictured in Figure 1.7.

The study of halved cubes is not a new mathematical endeavor. In particular, one paper from Wilfred Imrich, and Sandi Klavzar demonstrates a characterization of all halved cubes [6]. This result gives a specific series of properties that if an arbitrary graph meets, then it is some dimension of a halved cube. These same mathematicians, with the addition of Aleksander Vesel, developed an algorithm for recognition of a halved cube with a constant time per edge as well [7]. Seeing that Q'_n is a highly structured graph then it is not difficult to find powerful results describing the nature of Q'_n .

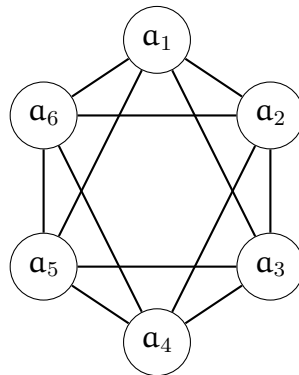


Figure 1.7: The circulant graph $C_6(1, 2)$.

1.3 Automorphism Groups

At its core, this thesis presents a collection of algebraic objects which act on the vertices of Q'_n in such a way that each object permutes the vertices of Q'_n while still preserving the adjacency structure of Q'_n . Background in algebra is required in order to describe the structures of these objects, and the global behavior of the collection of these objects. We will begin with the definition a group and present examples, and finish with a presentation of semidirect products.

Definition 10. *Let A be a non-empty set. A set A together with a binary operation $\star : A \times A \rightarrow A$ is a **group** if the following occur:*

1. *The operation \star is associative in that $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in A$.*
2. *There exists some $I \in A$ such that $I \star a = a \star I = a$ for all $a \in A$. We call this element I the **identity element** of A .*
3. *For any $a \in A$ there exists some element $b \in A$ such that $a \star b = b \star a = I$. The element b is called the **inverse element** of a , and is denoted as a^{-1} .*

A group G is a **abelian** if $x \star y = y \star x$ for all $x, y \in G$ [2] (pg. 6).

Let S_n be the set of all bijections from $\{1, \dots, n\}$ to itself. We will set out to show that this set is a group under the operation of composition.

Proposition 2. *The set S_n forms a group under the operation of composition.*

Proof. As a standard fact, composition of a bijection is a bijection. Thus, S_n is closed under composition. Observe also that the composition operation of functions is associative.

Now we set out to show that there exists an identity element in S_n under composition. Let $I : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ such that for all $x \in \{1, \dots, n\}$ the mapping $I(x) = x$. Clearly, for any $\phi \in S_n$ the mapping $I(\phi(x))$ equals $\phi(x)$ for all $x \in \{1, \dots, n\}$, thus I is the identity element of S_n under composition.

u	$\phi(u)$		
1	1	$\phi = (2345)$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$
2	3		
3	4		
4	5		
5	2		

Figure 1.8: An element S_5 , its cycle permutation representation, and its permutation matrix.

Observe that since ϕ is a bijection, then this function has an inverse ϕ^{-1} which is also a bijection thus, is an element of S_n . From here, we see that ϕ^{-1} is the group inverse of ϕ . □

A useful expression of an element of S_n is a **permutation**. An example of ϕ , a bijection, and its cyclic permutation representation is presented in Figure 1.8. Consider $\phi \in S_n$, then we could think of the element x to be permuted to $\phi(x)$. In this thesis we will be working with an alternate form of S_n , which is the set of permutation matrices, which we will define below:

Definition 11. *The set of permutation matrices, denoted as \mathcal{P}_n , is the set of $n!$ matrices constructed by permuting rows of the $n \times n$ identity matrix.*

In Figure 1.8, the permutation matrix of ϕ is derived from taking the 5×5 identity matrix and permuting the i -th row to the $\phi(i)$ -th row. With the operation of matrix multiplication over \mathcal{P}_n , observe that the groups S_n and \mathcal{P}_n are isomorphic. We will demonstrate an important fact of \mathcal{P}_n below:

Proposition 3. *Let $P \in \mathcal{P}_n$. Then where P^T is the transpose of P we have that $P^{-1} = P^T$.*

Proof. Let $P \in \mathcal{P}_n$. Clearly, $P^T \in \mathcal{P}_n$ and since \mathcal{P}_n is closed under multiplication then we have that $PP^T \in \mathcal{P}_n$.

$$PP^T = \begin{bmatrix} (PP^T)_{11} & \dots & (PP^T)_{1n} \\ \vdots & \dots & \vdots \\ (PP^T)_{n1} & \dots & (PP^T)_{nn} \end{bmatrix}$$

In general, where $i, j \in \{1, \dots, n\}$ we have that $(PP^T)_{ij} = \sum_{k=1}^n P_{ik}P_{kj}^T = \sum_{i=1}^n P_{ik}P_{jk}$. Since $PP^T \in \mathcal{P}_n$ then there exists some $a, b \in \{1, \dots, n\}$ such that $P_{ab} = P_{ba} = 1$. Since every row has only one non-zero entry and every column has only one non-zero entry then we have that $(PP^T)_{ij} = 1$ when $i = j$ and that $(PP^T)_{ij} = 0$ when $i \neq j$. By definition PP^T is the identity matrix, so $P^T = P^{-1}$ so $PP^T = PP^{-1} = P^{-1}P = P^TP = I$. \square

Definition 12. *The group $GL_n(\mathbb{R})$ is the group of invertible $n \times n$ matrices with real-valued entries. This group is called the general linear group. Its operation is standard matrix multiplication.*

For a construction of Q'_n to be presented later, an important fact to observe is that $\mathcal{P}_n \subseteq GL_n(\mathbb{R})$. We will be using the permutation matrices to permute column vectors which will be representative of vertices in Q'_n in an embedding (to be discussed later) in \mathbb{R}^n .

Definition 13. *Let G be a graph, and H be a group. The set $\text{Aut}(G)$ is the collection of all isomorphisms from $G \rightarrow G$. We call an element of $\text{Aut}(G)$ an **automorphism**. Under the operation of composition, this set forms a group (because the composition of two automorphisms is an automorphism) called the **automorphism group** of G [3] (pg. 201).*

Now we will present a graph and its automorphism group. Before we express this graph and its automorphism group, we will set out some critical definitions.

Definition 14. *Let G be a group and $H \subseteq G$. We call H a **subgroup** of G if the elements of H form a group under the operation induced by G . We denote that H is a subgroup of G by $H \leq G$.*

Definition 15. *Let G be a group under multiplication and $S \subseteq G$ where $S = \{s_1, \dots, s_n\}$ then the **subgroup generated by S** is the subgroup consisting of products of powers of elements of S .*

This subgroup is denoted as $G = \langle S \rangle$. If the subgroup generated by S is abelian then each element of $\langle S \rangle$ is of the form $\prod_{i=1}^n s_i^{\alpha_i}$ where $\alpha_i \in \{1, \dots, n\}$.

Definition 16. Let G and H be groups. Then we define the **direct product** of G and H and its group operation as follows:

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

Let $g, g' \in G$ and $h, h' \in H$, then the operation associated with this group is given below:

$$(g, h)(g', h') = (gg', hh')$$

Definition 17. Let G be a group and $g \in G$. The **order** of g , denoted as $|g|$ is the smallest positive integer k such that $g^k = I_G$ where I_G is the identity element of G .

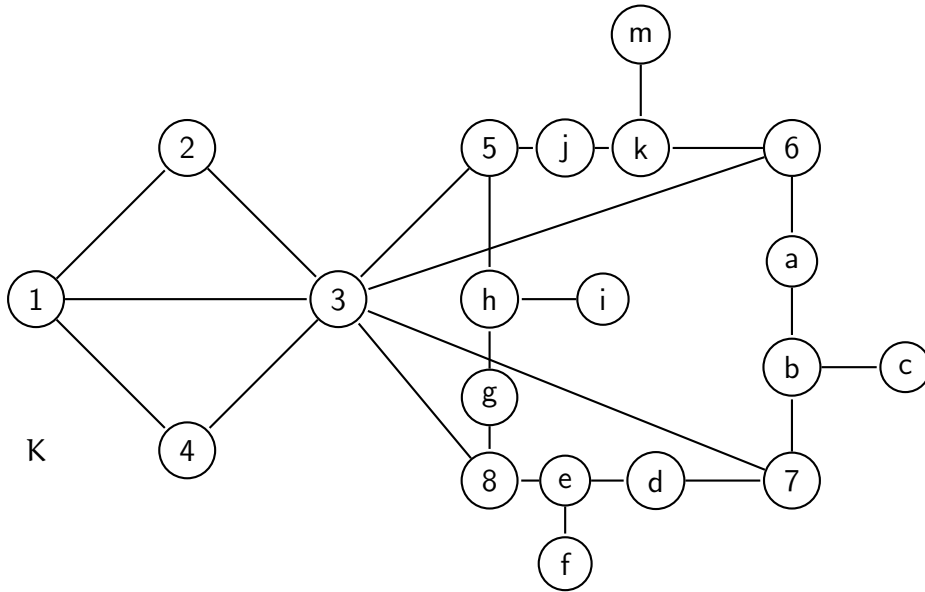


Figure 1.9: A graph K with $\text{Aut}(K) \cong \langle (24), (5678) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

For the graph K in Figure 1.9 we see that in permuting the vertices 2 and 4 that this will form an isomorphism with itself, or more plainly the permutation of these vertices do not change the appearance of K . Similarly, if we permute the collection of vertices 5, 6, 7 and 8 in such a manner that we “rotate” the cycle containing these vertices one position clockwise (along with the respective sets of vertices a, b, c, d, e, f, g, h and i)

then the collection of these four permutations would also be automorphisms. Clearly, these are the only automorphisms of the graph K since an automorphism cannot permute vertices 2 and 4 with any other vertices of degree two. Similarly 5, 6, 7, and 8 are the only vertices of degree three which can be permuted and this can only be done by rotations of the cycle containing these vertices. Similarly, if 5, 6, 7, or 8 permute with 1, b, e, h or k then this wouldn't be an automorphism since none of the vertices 5 – 8, b, e, h or k are adjacent with 2 and 4. By similar logic, since 3 is the only vertex of degree seven, then any permutation of 3 with any other vertex would not be an automorphism.

If we consider S_8 to be the set of all permutations of the vertices of K , then we see that $\text{Aut}(K) = \langle (24), (5678) \rangle$. From here, we see that an element of $\text{Aut}(K)$ is defined to be the set of elements of the form $(24)^\alpha(5678)^\beta$ where $\alpha \in \mathbb{Z}_2$ (since $|(24)| = 2$) and $\beta \in \mathbb{Z}_4$ (since $|(5678)| = 4$). If we fix two elements, say $(24)^{\alpha_1}(5678)^{\beta_1}$ and $(24)^{\alpha_2}(5678)^{\beta_2}$ and compose them, we use the fact that disjointed cycles commute so their composition is $(24)^{\alpha_1+\alpha_2}(5678)^{\beta_1+\beta_2}$. Let the set $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$. Note that the exponents $\alpha_1 + \alpha_2$ and $\beta_1 + \beta_2$ are elements of \mathbb{Z}_2 and \mathbb{Z}_4 respectively. From here it is clear that $\text{Aut}(K) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. Since $\mathbb{Z}_2 \times \mathbb{Z}_4$ is a simpler group to visualize than $\langle (24), (5678) \rangle$ we would say that $\text{Aut}(K) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

While the graph K has a very straightforward automorphism group, $\text{Aut}(Q'_n)$ has an expression which requires a different group product than a direct product. The direct product of groups G and H is a rather non-homogeneous combination of elements of G and H in that they do not interact with each other. We found that $\text{Aut}(Q'_n)$ had an expression which was a semidirect product, which while less intuitive, has more interaction between the elements of the sets in the product. Note that all of these definitions are in the context of groups, and not graphs as previously mentioned.

Definition 18. *Let G and H be groups under multiplication. The mapping $\phi : G \rightarrow H$ is a **homomorphism** if for all $x, y \in G$ we have that $\phi(xy) = \phi(x)\phi(y)$. An **isomorphism** is an injective homomorphism. An **automorphism** of G is an isomorphism from G to itself, and the*

collection of all automorphisms is denoted as $\text{Aut}(G)$ which is a group under composition.

Definition 19. Let G and H be groups and let $\psi : H \rightarrow \text{Aut}(G)$ be a homomorphism. We define the **semidirect product** of G by H via ψ as the following:

$$G \rtimes_{\psi} H = \{(g, h) : g \in G, h \in H\}$$

under the binary operation defined by $(g_1, h_1)(g_2, h_2) = (g_1\psi_{h_1}(g_2), h_1h_2)$ [2] (pg. 177).

Note that if G and H are groups and ψ is the identity mapping, then $G \rtimes_{\psi} H \cong G \times H$. In this regard, the direct product could be referred to as the trivial semidirect product.

Chapter 2

$\text{Aut}(Q'_n)$ Where $n \neq 4$

In constructing the automorphism group of Q'_n , we will first describe an embedding of Q'_n in \mathbb{R}^n which re-expresses the binary strings in the vertex set of Q'_n as vectors. Next, we will define and describe the groups used in the semidirect product which yields our automorphism group. For brevity, whenever addressing Q'_n in this chapter we assume that $n \neq 4$. The case where $n = 4$ will be addressed separately as it is a special case.

Now we can define our embedding of Q'_n in n -dimensional space. First, we let G to be the set of column vectors as follows:

$$G = \{\langle v_1, \dots, v_n \rangle : v_i \in \{-1, 1\}, \forall i \in \{1, \dots, n\}\}$$

Now, let u be an n -digit binary string in $V(Q'_n)$ and let $f : V(Q'_n) \rightarrow G$ be such that $f(u) = \vec{u}$ where every 0 in the i -th position of u is a negative one in the i -th component of \vec{u} and every 1 in the j -th position of u is a 1 in the j -th component of \vec{u} . To demonstrate this mapping, let $u = 010010$ in $V(Q'_6)$, then $\vec{u} = \langle -1, 1, -1, -1, 1, -1 \rangle$ in G . Next, in \mathbb{R}^n we let \vec{u} and \vec{v} be adjacent if and only if u and v are adjacent in Q'_n . Henceforth, when referring to $V(Q'_n)$ we will be referring to the images of the function f .

Before we can describe the necessary groups to define the automorphism group of Q'_n , we must show that with our embedding of Q'_n into n -dimensional space, every automorphism of Q'_n is the restriction of an invertible linear transformation of \mathbb{R}^n . We

will first prove a lemma and then we will have sufficient machinery to prove that that $f \in \text{Aut}(Q'_n)$ is the restriction of $M \in \text{GL}_n(\mathbb{R})$.

Lemma 1. *Suppose $\vec{v} \in \mathbb{R}^n$ and $\mathcal{B} = \{x_1, \dots, x_n\}$ is a basis of \mathbb{R}^n . Then $\vec{v} = 0$ if and only if $\vec{v} \cdot \vec{x}_i = 0$ for all $1 \leq i \leq n$.*

Proof. Let $\vec{v} \in \mathbb{R}^n$ and $\mathcal{B} = \{x_1, \dots, x_n\}$ be a basis of \mathbb{R}^n . It is trivial that if $\vec{v} = 0$ then $\vec{v} \cdot \vec{x}_i = 0$ for all $1 \leq i \leq n$. Suppose now that $\vec{v} \cdot \vec{x}_i = 0$ for all $1 \leq i \leq n$. Then we have that $|\vec{v}|^2 = \vec{v} \cdot \vec{v} = \vec{v} \cdot \sum_{i=1}^n a_i x_i = \sum_{i=1}^n a_i \vec{v} \cdot x_i = 0$. Since the square of the norm of \vec{v} is 0 then it is clear that $\vec{v} = 0$. □

Theorem 1. *Any $f \in \text{Aut}(Q'_n)$ is the restriction of $M \in \text{GL}_n(\mathbb{R})$.*

Proof. First, define $\mathcal{B} \subseteq V(Q'_n)$ where $\mathcal{B} = \{b_1, \dots, b_n\}$ is the set of vectors given below:

$$b_1 = \langle 1, 1, \dots, 1 \rangle$$

$$b_2 = \langle -1, -1, 1, 1, \dots, 1 \rangle$$

$$b_3 = \langle -1, 1, -1, 1, \dots, 1 \rangle$$

$$\vdots \quad \quad \quad \vdots$$

$$b_n = \langle -1, 1, 1, 1, \dots, -1 \rangle$$

We set out to show that \mathcal{B} is a basis of \mathbb{R}^n . To do this, we only need to show that the collection of vectors in \mathcal{B} are linearly independent since a collection of n linearly independent vectors in \mathbb{R}^n spans \mathbb{R}^n . Suppose that $a_1 b_1 + \dots + a_n b_n = 0$. Then we have

the system of equations given below:

$$\begin{aligned}
 0 &= a_1 - a_2 - a_3 - \cdots - a_n \\
 0 &= a_1 - a_2 + a_3 + \cdots + a_n \\
 0 &= a_1 + a_2 - a_3 + \cdots + a_n \\
 &\vdots \qquad \qquad \qquad \vdots \qquad \qquad \qquad \vdots \\
 0 &= a_1 + a_2 + a_3 + \cdots - a_n
 \end{aligned}$$

If we add the first equation to the i -th equation we have that $2(a_1 - a_i) = 0$, so $a_1 = a_i$ for all $i \in \{1, \dots, n\}$. Thus, for all distinct $p, q \in \{1, \dots, n\}$ we have that $a_p = a_q$. By substituting a_i in for every term of the first equation we have that $(n-1)a_i = 0$, therefore $a_i = 0$ and all constants are equal to zero. Thus, the collection of vectors in \mathcal{B} are linearly independent so \mathcal{B} is a basis of \mathbb{R}^n .

We will now prove that the collection $\{f(b_1), \dots, f(b_n)\}$ also forms a basis over \mathbb{R}^n . Let $b_i, b_j \in \mathcal{B}$ be arbitrary; observe that the hamming distance of b_i and b_j is two. Since $f \in \text{Aut}(Q'_n)$ then we have that $f(b_i)$ and $f(b_j)$ have a hamming distance of two. Define each $f(b_k) = \langle p_{k1}, \dots, p_{kn} \rangle$ and let c_1, \dots, c_n be a collection of constants. Then we have the system of equations given below:

$$\begin{aligned}
 0 &= c_1 p_{11} + c_2 p_{21} + \cdots + c_n p_{n1} \\
 0 &= c_1 p_{12} + c_2 p_{22} + \cdots + c_n p_{n2} \\
 0 &= c_1 p_{13} + c_2 p_{23} + \cdots + c_n p_{n3} \\
 &\vdots \qquad \qquad \qquad \vdots \qquad \qquad \qquad \vdots \\
 0 &= c_1 p_{1n} + c_2 p_{2n} + \cdots + c_n p_{nn}
 \end{aligned}$$

Since each $f(b_i)$ and $f(b_j)$ have hamming distance of two, then by subtracting the i -th and j -th equation we have that $2(c_i - c_j) = 0$. By the same argument used to show that \mathcal{B} is a basis, we see that $\{f(b_1), \dots, f(b_n)\}$ forms a basis of \mathbb{R}^n .

Now, given $\vec{x}, \vec{y} \in V(Q'_n)$, then $\text{dist}(x, y) = |\vec{x} - \vec{y}| = 2\sqrt{d(\vec{x}, \vec{y})}$ where $d(\vec{x}, \vec{y})$ is the hamming distance between \vec{x} and \vec{y} . Then we have that $\text{dist}(\vec{x}, \vec{y})^2 = |\vec{x} - \vec{y}|^2 = (\vec{x} - \vec{y}) \cdot (\vec{x} - \vec{y}) = 4d(x, y)$. Now let $f \in \text{Aut}(Q'_n)$ and note that $|f(x)| = |x|$ for all $\vec{x} \in V(Q'_n)$. From here, we compute the square of $\text{dist}(f(\vec{x}), f(\vec{y}))$ to show that $f(\vec{x}) \cdot f(\vec{y}) = \vec{x} \cdot \vec{y}$ for all $x, y \in V(Q'_n)$.

$$\begin{aligned} \text{dist}(f(\vec{x}), f(\vec{y}))^2 &= \text{dist}(\vec{x}, \vec{y})^2 \\ (f(\vec{x}) - f(\vec{y})) \cdot (f(\vec{x}) - f(\vec{y})) &= (\vec{x} - \vec{y}) \cdot (\vec{x} - \vec{y}) \\ f(\vec{x}) \cdot f(\vec{x}) - 2f(\vec{x}) \cdot f(\vec{y}) + f(\vec{y}) \cdot f(\vec{y}) &= \vec{x} \cdot \vec{x} - 2\vec{x} \cdot \vec{y} + \vec{y} \cdot \vec{y} \\ |f(\vec{x})|^2 - 2f(\vec{x}) \cdot f(\vec{y}) + |f(\vec{y})|^2 &= |\vec{x}|^2 - 2\vec{x} \cdot \vec{y} + |\vec{y}|^2 \\ -2f(\vec{x}) \cdot f(\vec{y}) &= -2\vec{x} \cdot \vec{y} \end{aligned}$$

$$f(\vec{x}) \cdot f(\vec{y}) = \vec{x} \cdot \vec{y} \tag{2.1}$$

Now, with $\mathcal{B} = \{b_1, \dots, b_n\}$ as a basis of \mathbb{R}^n then let $M \in \text{GL}_n(\mathbb{R})$ such that $f(\vec{b}_i) = M\vec{b}_i$. Next, let $\vec{v} \in V(Q'_n)$ so $\vec{v} = \sum_{i=1}^n a_i \vec{b}_i$, and we have the following equation:

$$M\vec{v} = \sum_{i=1}^n a_i M\vec{b}_i = \sum_{i=1}^n a_i f(\vec{b}_i) \tag{2.2}$$

Note that $\vec{0} = \vec{v} - \sum_{i=1}^n a_i \vec{b}_i$ and therefore for each $b_i \in \mathcal{B}$ we have that $\vec{0} \cdot \vec{b}_j = (\vec{v} - \sum_{i=1}^n a_i \vec{b}_i) \cdot \vec{b}_j$. Now, we will employ equation 2.1 to show that

$f(\vec{v}) = \sum_{i=1}^n \alpha_i f(\vec{b}_i)$ below; and therefore $f(\vec{v}) = M\vec{v}$ by 2.2.

$$\begin{aligned}\vec{0} &= \vec{v} \cdot \vec{b}_j - \sum_{i=1}^n \alpha_i \vec{b}_i \cdot \vec{b}_j \\ \vec{0} &= f(\vec{v}) \cdot f(\vec{b}_j) - \sum_{i=1}^n \alpha_i f(\vec{b}_i) \cdot f(\vec{b}_j) \\ \vec{0} &= (f(\vec{v}) \cdot f(\vec{b}_j) - \sum_{i=1}^n \alpha_i f(\vec{b}_i) \cdot f(\vec{b}_j))\end{aligned}$$

Since $f(\vec{b}_j) \neq \vec{0}$ then we have that $f(\vec{v}) - \sum_{i=1}^n \alpha_i f(\vec{b}_i) = 0$. From Lemma 1 and the fact that $\{f(\vec{b}_1), \dots, f(\vec{b}_n)\}$ is a basis of \mathbb{R}^n , we have that $f(\vec{v}) = \sum_{i=1}^n \alpha_i f(\vec{b}_i)$. Here we have shown that for any $\vec{v} \in V(Q'_n)$ we have that $f(\vec{v}) = M\vec{v}$ and the proof is complete. \square

Given this embedding, we show (rather trivially) that $\text{Aut}(Q'_2) = \{\pm I\}$ where I is the 2×2 identity matrix below:

Proposition 4. $\text{Aut}(Q'_2) = \{\pm I\}$.

Proof. First, it is obvious that $I \in \text{Aut}(Q'_2)$. Since Q'_2 consists of the adjacent vertices with associated vectors $\langle -1, -1 \rangle$ and $\langle 1, 1 \rangle$, then $-I$ transposes both of these vertices which is clearly the only other automorphism of Q'_2 . \square

Next, we define the set \mathcal{G}_n^e below, which we will later show is $\text{Aut}(Q'_n)$:

Definition 20. Let \mathcal{A}_n be the set of diagonal $n \times n$ matrices with the non-zero entries being either 1 or -1 . Next, let \mathcal{A}_n^e be the subset of \mathcal{A}_n consisting of matrices with an even number of -1 's on their diagonal. Analogously, \mathcal{A}_n^o can be defined as follows:

$$\mathcal{A}_n^e = \{A \in \mathcal{A}_n : \det(A) = 1\}$$

Further, let $\mathcal{G}_n^e = \{AP : A \in \mathcal{A}_n^e, P \in \mathcal{P}_n\}$.

Note that \mathcal{A}_n and \mathcal{A}_n^e are clearly groups under matrix multiplication since matrix multiplication is associative, the set (which contains I , the identity element) is closed under multiplication, and any element of \mathcal{A}_n is its own inverse, or analogously for all $A \in \mathcal{A}_n$, the order of A is two.

Now we will show that \mathcal{G}_n^e forms a group under matrix multiplication, and will proceed to show that \mathcal{G}_n^e is isomorphic with a semidirect product of the groups \mathcal{A}_n^e and \mathcal{P}_n . In order to do this, there will be a few minor results required, which will be proved below.

Proposition 5. *For any $P \in \mathcal{P}_n$ and $A \in \mathcal{A}_n$ the matrix PAP^{-1} is an element of \mathcal{A}_n .*

Proof. Let $A \in \mathcal{A}_n$ and $P \in \mathcal{P}_n$ with $\pi \in S_n$ being the permutation which permuted the rows of I to yield P . Then we have the following:

$$\begin{aligned} P \times \begin{bmatrix} (A)_{11} & \dots & (A)_{1n} \\ \vdots & \dots & \vdots \\ (A)_{n1} & \dots & (A)_{nn} \end{bmatrix} \times P^T &= \begin{bmatrix} (A)_{\pi(1)1} & \dots & (A)_{\pi(1)n} \\ \vdots & \dots & \vdots \\ (A)_{\pi(n)1} & \dots & (A)_{\pi(n)n} \end{bmatrix} \times P^T \\ &= \begin{bmatrix} (A)_{\pi(1)\pi(1)} & \dots & (A)_{\pi(1)\pi(n)} \\ \vdots & \dots & \vdots \\ (A)_{\pi(n)\pi(1)} & \dots & (A)_{\pi(n)\pi(n)} \end{bmatrix} \end{aligned}$$

Since A was a diagonal matrix then $(A)_{ij} = \pm 1$ if and only if $i = j$. Since there exists some $k \in \{1, \dots, n\}$ such that $\pi(k) = i$, then we have that $(A)_{\pi(k)\pi(k)} = \pm 1$ and PAP^T is a diagonal matrix with non-zero entries being either 1 or -1 . \square

Theorem 2. *Every element $G \in \mathcal{G}_n$ has a unique decomposition as $G = AP$ where $A \in \mathcal{A}_n$ and $P \in \mathcal{P}_n$.*

Proof. Let $A, A' \in \mathcal{A}_n$ and $P, P' \in \mathcal{P}_n$ and suppose that $AP = A'P'$. Then we have the

following:

$$AP = A'P'$$

$$A = A'P'P^{-1}$$

$$A'A = P'P^{-1}$$

Since $A'A \in \mathcal{A}_n$ then AA' is a diagonal matrix with non-zero entries equal to either one or negative one and since $P'P^{-1} \in \mathcal{P}_n$ is a permutation matrix then its non-zero entries can only equal one. Thus $AA' = I$, so $P'P^{-1} = I$, and $A = A'$ and $P = P'$. \square

Observe that both of these results apply for \mathcal{A}_n^e and \mathcal{G}_n^e as well. Now we can prove that \mathcal{G}_n^e is a group, and that it is isomorphic to a semidirect product of \mathcal{A}_n^e and \mathcal{P}_n .

Theorem 3. *Under matrix multiplication \mathcal{G}_n^e is a group and it is isomorphic to a semidirect product $\mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n$.*

Proof. First, we set out to show that \mathcal{G}_n^e is a group under matrix multiplication. First, let $AP, BQ \in \mathcal{G}_n^e$ with $A, B \in \mathcal{A}_n^e$ and $P, Q \in \mathcal{P}_n$. Notice that $APBQ = APBPT^T PQ$ and $PBP^T \in \mathcal{A}_n^e$. Since $A(PBP^T) \in \mathcal{A}_n^e$ and $PQ \in \mathcal{P}_n$ then we have that $APBQ \in \mathcal{G}_n^e$, thus \mathcal{G}_n^e is closed by matrix multiplication. Note that matrix multiplication is a binary associative operation.

Next, by definition, $I \in \mathcal{A}_n^e$ where I is the $n \times n$ identity matrix, and $I \in \mathcal{P}_n$, so if $G = AP$ where $A = P = I$ then $I \in \mathcal{G}_n^e$. Finally, let $H \in \mathcal{G}_n^e$ where $H = CR$ where $C \in \mathcal{A}_n^e$ and $R \in \mathcal{P}_n$. Since $C \in \mathcal{G}_n^e$ and $R^T = R^{-1} \in \mathcal{G}_n^e$ then $R^T C = R^{-1}C = (CR)^{-1} \in \mathcal{G}_n^e$ and we have demonstrated that \mathcal{G}_n^e is a group under matrix multiplication.

Let $\psi : \mathcal{P}_n \rightarrow \text{Aut}(\mathcal{A}_n^e)$ where $\psi(X)(Y) = XYX^{-1}$. We claim that $\mathcal{G}_n^e \cong \mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n$.

Now we will show that $|\mathcal{G}_n^e| = |\mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n|$. Since $\mathcal{G}_n^e = AP$ with $A \in \mathcal{A}_n^e$ and $P \in \mathcal{P}_n$ and this decomposition is unique then we have that $|\mathcal{G}_n^e| = |\mathcal{A}_n^e| |\mathcal{P}_n| = 2^{n-1} n!$. Thus,

$$|\mathcal{G}_n^e| = |\mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n|.$$

Next, let $\phi : \mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n \rightarrow \mathcal{G}_n^e$ be $\phi(A, P) = AP$. Let $(B, Q) \in \mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n$. By Theorem 2 and the definition of ϕ we see that if $\phi(A, P) = \phi(B, Q)$ then $A = B$ and $P = Q$, thus $(A, P) = (B, Q)$ and ϕ is injective. Below we demonstrate that ϕ is a homomorphism which completes the proof.

$$\begin{aligned} \phi((P, Q), (R, S)) &= \phi(P\psi(Q)(R), QS) \\ &= \phi(PQRQ^{-1}, QS) \\ &= PQRQ^{-1}QS \\ &= PQRS \\ &= \phi(P, Q)\phi(R, S) \end{aligned}$$

□

Now we remind the reader that we have embedded Q'_n into \mathbb{R}^n , and by Theorem 1 we have that $\text{Aut}(Q'_n) \leq \text{GL}_n(\mathbb{R})$. This result gives us the final employment of structure required to prove that $\text{Aut}(Q'_n) \cong \mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n$. Before we do this, we will prove one lemma which will serve us well in showing that $\text{Aut}(Q'_n) \leq \mathcal{G}_n^e$.

Proposition 6. *If $\{\alpha_1, \dots, \alpha_n\}$ is a collection of real numbers where $n = 3$ or $n > 5$ with the following properties:*

1. $\sum_{i=1}^n \alpha_i = \pm 1$
2. *After negating any two elements of $\{\alpha_1, \dots, \alpha_n\}$ the sum of the elements is ± 1 .*

Then the collection $\{\alpha_1, \dots, \alpha_n\}$ contains $n - 1$ elements equal to zero and one element equal to ± 1 .

Proof. First, let $n = 3$, then we have the following two equations from the properties above:

$$a_1 + a_2 + a_3 = \pm 1 \quad (2.3)$$

$$a_1 - a_2 - a_3 = \pm 1 \quad (2.4)$$

In summing equation 2.3 and equation 2.4 we have that $2a_1 \in \{-2, 0, 2\}$ thus $a_1 \in \{-1, 0, 1\}$. Without loss of generality, we also have that $a_2, a_3 \in \{-1, 0, 1\}$. Observe that if more than one value of a_1, a_2 and a_3 is non-zero and satisfies property 1, then all three must be non-zero. If we suppose that a_1, a_2 and a_3 are all non-zero then by the pigeonhole principle since $a_1, a_2, a_3 \in \{\pm 1\}$ then two of these elements are equal to each other, so without loss of generality let $a_1 = a_2$. By property 1 we have that $a_3 = -a_1$. If we employ property 2 and negate a_1 and a_2 we have that $-3a_1 = \pm 1$, a contradiction. Thus, there is exactly one non-zero element of $\{a_1, a_2, a_3\}$ and that value must be ± 1 .

Next, suppose that $n > 4$ and let $i, j \in \{1, \dots, n\}$ such that $i \neq j$. Given properties 1 and 2 we have the following equations:

$$a_1 + \dots + a_n = \pm 1 \quad (2.5)$$

$$a_1 + \dots - a_i + \dots - a_j + \dots = \pm 1 \quad (2.6)$$

By subtracting equation 2.6 from equation 2.5 then we have that $2(a_i + a_j) \in \{-2, 0, 2\}$, thus $a_i + a_j \in \{-1, 0, 1\}$. Since i and j were chosen arbitrarily then for all $x, y \in \{1, \dots, n\}$ with $x \neq y$ we have that $a_x + a_y \in \{-1, 0, 1\}$. Since $n > 4$ then for unique $m, p, q, r, s \in \{1, \dots, n\}$ where m is fixed, then we have that $a_m + a_p, a_m + a_q, a_m + a_r,$ and $a_m + a_s$ are elements of the set $\{-1, 0, 1\}$. By pigeonhole principle there exists a pair of equations which are equal, without loss of generality let $a_m + a_p = a_m + a_q$. Thus we have that $a_p = a_q$. Since $a_p + a_q \in \{-1, 0, 1\}$ then $a_p = \pm \frac{1}{2}$ or $a_p = a_q = 0$.

Suppose that $a_p = \pm \frac{1}{2}$, then $a_m = \pm \frac{1}{2}$ and for all $z \in \{1, \dots, n\}$ we have that $a_z = \pm \frac{1}{2}$.

From property 1, suppose that $\sum_{i=1}^n a_i = 1$. Observe that in there are $\lceil \frac{n}{2} \rceil - 1$ entries of $\{a_1, \dots, a_n\}$ which equal $-\frac{1}{2}$ and since $n > 4$ there we have at least two of these values. Suppose $a_j, a_k \in \{a_1, \dots, a_n\}$ such that $a_j = a_k = -\frac{1}{2}$, then we have that the sum of the elements of the set $\{a_1, \dots, -a_j, \dots, -a_k, \dots, a_n\}$ is 3, a contradiction. This same argument holds if $\sum_{i=1}^n a_i = -1$ in that if we negate two of the $\lceil \frac{n}{2} \rceil - 1$ entries of $\{a_1, \dots, a_n\}$ which equal $\frac{1}{2}$, then this sum will now be -3 , a contradiction.

Thus, for all $w \neq m$ we have that $a_w = 0$, so for property 1 to hold, we have that $a_m = \pm 1$ and the proof is complete. \square

The proposition above had clear restrictions on n with a sensitivity for the two cases where $n = 2$ and $n = 4$. To cite these, we see that the sets $\{a_1 = \pm\frac{1}{2}, a_2 = \pm\frac{1}{2}\}$ and $\{b_1 = \pm\frac{1}{2}, b_2 = \pm\frac{1}{2}, b_3 = \pm\frac{1}{2}, b_4 = \mp\frac{1}{2}\}$ provide these cases. We will see that the existence of these sets create an important distinction in establishing that when $n = 4$ the automorphism group of Q'_n is not \mathcal{G}_n^e . The case of $n = 2$ can be disregarded since we already have that $\text{Aut}(Q'_2) = \{\pm I\}$. We now have all necessary machinery to show that $\text{Aut}(Q'_n) \cong \mathcal{G}_n^e$ where $n \neq 4$ below:

Theorem 4. *Let $n \neq 4$ and $n > 2$, and define $M \in \mathcal{G}_n^e$ to be the map sending $\vec{v} \in V(Q'_n)$ to $M\vec{v}$, then $\text{Aut}(Q'_n) \cong \mathcal{G}_n^e$.*

Proof. Let $n \in \mathbb{N}$ and $M \in \text{GL}_n(\mathbb{R})$ such that $M = AP$ where $A \in \mathcal{A}_n^e$ and $P \in \mathcal{P}_n$. Define the function $M : \mathbb{R}^n \rightarrow \mathbb{R}^n$ such that where $\vec{a} \in \mathbb{R}^n$ then $M(\vec{a}) = M\vec{a}$. Note that the mapping M is a bijection over $\mathbb{R}^n \rightarrow \mathbb{R}^n$. We must now show that if $\vec{a} \in V(Q'_n)$ that $M\vec{a} \in V(Q'_n)$.

Suppose that $\vec{a} \in V(Q'_n)$. Then we have that $\vec{a} = \langle a_1, \dots, a_n \rangle$ where $|a_i| = 1$ for all $i \in \{1, \dots, n\}$. Further, let p be a non-negative integer and k_1, \dots, k_{2p} be the components of \vec{a} such that where $j \in \{1, \dots, 2p\}$ we have that $a_{k_j} = -1$. Clearly, $P\vec{a} \in V(Q'_n)$ since permuting the coordinates of a vertex of Q'_n will still yield a vertex of Q'_n . Now let q be a non-negative integer (obviously less than or equal to $\lfloor \frac{n}{2} \rfloor$) such that there are a $2q$ entries

of -1 in A . Then we have that $AP\vec{a}$ will have a $2p - 2q$ negative entries. Clearly, for all $r \in \{1, \dots, n\}$ we have that for $r \in \{1, \dots, n\}$ we have that $a'_r = \pm 1$ where $AP\vec{a} = \langle a'_1, \dots, a'_n \rangle$. Thus, we have that $M : V(Q'_n) \rightarrow V(Q'_n)$.

Now, let $\vec{x}\vec{y} \in E(Q'_n)$. In order to prove that $\mathcal{G}_n^e \leq \text{Aut}(Q'_n)$ we need to show that $M\vec{x}M\vec{y} \in E(Q'_n)$. Note that if we permute the coordinates of \vec{x} and \vec{y} then the two vectors will still differ in exactly two positions, thus $P\vec{x}P\vec{y} \in E(Q'_n)$. Next, recall that let A has $2q$ negative ones where $q \in \{0, 1, \dots, \lfloor \frac{n}{2} \rfloor\}$. In negating the $2q$ coordinates of $P\vec{x}$ and $P\vec{y}$ note that the two vectors will still differ in exactly two positions, thus $AP\vec{x}AP\vec{y} \in E(Q'_n)$ so by definition $M\vec{x}M\vec{y} \in E(Q'_n)$ and $\mathcal{G}_n^e \leq \text{Aut}(Q'_n)$.

Now we set out to show that $\text{Aut}(Q'_n) \leq \mathcal{G}_n^e$. Let $\vec{v} \in V(Q'_n)$, then as seen above $M\vec{v} \in V(Q'_n)$. We now set out to show that an arbitrary $M \in \text{Aut}(Q'_n)$ will be an element of \mathcal{G}_n^e , thus $\text{Aut}(Q'_n) \leq \mathcal{G}_n^e$.

Let $[a_{k1} \dots a_{kn}]$ be an arbitrary k -th row of M and $\vec{a} = \langle 1, \dots, 1 \rangle$ then in calculating $M\vec{a}$ we have that $a_{k1} + \dots + a_{kn} = \pm 1$. Notice that in negating any two components of \vec{a} we still have an element of Q'_n . Without loss of generality let \vec{a}' have -1 entries in it's i -th and j -th position, then the k -th entry of $M\vec{a}'$ is $a_{k1} + \dots - a_{ki} + \dots - a_{kj} \dots + a_{kn} = \pm 1$. Observe that both properties of the set outlined in Proposition 6 are met by $\{a_{k1} \dots a_{kn}\}$ so we have that when $n = 3$ or $n > 4$ every row of M has exactly one non-zero entry and that entry is ± 1 .

Since the rows of M are linearly independent by definition, then $M \in \mathcal{G}_n^e$. Note that we also have that we can say the same of columns of M as we can the rows of M since it is obvious that if $M \in \mathcal{G}_n^e$ then $M^T \in \mathcal{G}_n^e$. Therefore, $\text{Aut}(Q'_n) \leq \mathcal{G}_n^e$ so $\text{Aut}(Q'_n) = \mathcal{G}_n^e$ when $n = 3$ and $n \geq 5$ and the proof is complete.

□

In essence, we have shown that the elements of $\text{Aut}(Q'_n)$ can be described as $n \times n$ (of course, when $n \neq 4$) permutation matrices where an even number of 1s are replaced with -1 s. Figure 2.1 demonstrates the vertices Q'_3 being acted upon by an element of

$\text{Aut}(Q'_3)$ by left multiplication.

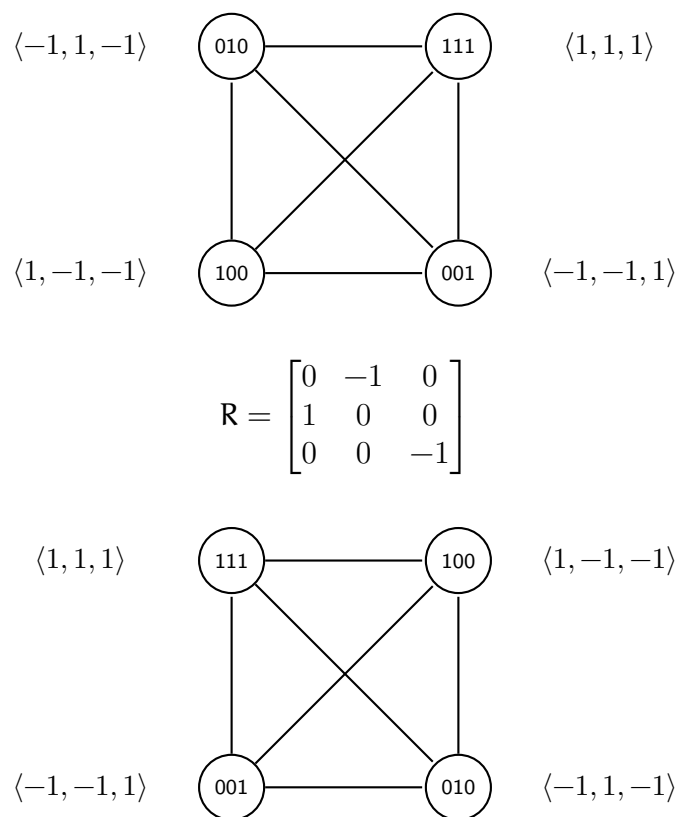


Figure 2.1: The graph Q'_3 and Q'_3 with R , an element of $\text{Aut}(Q'_3)$, acting on $V(Q'_3)$.

Chapter 3

The Fourth Dimension

Observe in Figure 3.1 that each vertex in Q'_4 is adjacent to every other vertex except its binary inverse. It is now obvious that a transposition of a vertex in Q'_4 with its binary inverse is an automorphism. Since there are four pairs of non-adjacent vertices then we have 2^4 automorphisms which transpose pairs of non-adjacent vertices. Similarly, observe that if we permute the vertices 0000 and 1100 then we have also permuted 1111 and 0011 respectively. By extension, any permutation the vertices 0000, 1100, 1010, and 1001 produces an automorphism, and these permutations force a permutation of the vertices not mentioned. Thus, we have $4!$ of these automorphisms which coupled with the transpositions mentioned earlier yields a total of $4!2^4$ automorphisms. This calculation is verified by Brouwer, Cohen, and Neumaier in their text *Distance Regular*

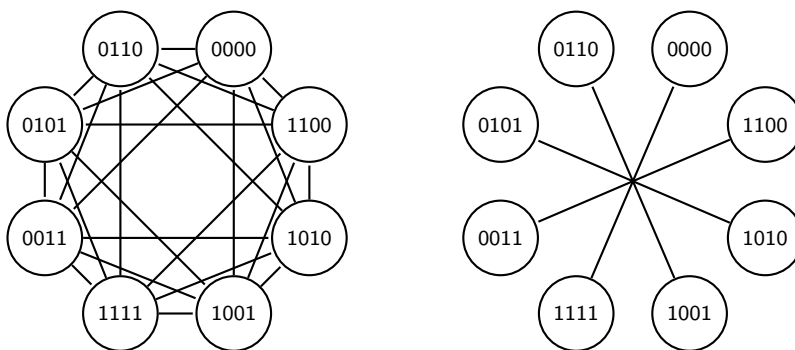


Figure 3.1: The graph Q'_4 and its complement.

Graphs [4].

We will begin the exposition of $\text{Aut}(Q'_4)$ with an embedding in \mathbb{R}^4 . Again, we do this so that we can realize $\text{Aut}(Q'_4) \leq \text{GL}_4(\mathbb{R})$.

First we lay out an embedding of Q'_4 into \mathbb{R}^4 different from our previous embedding. This is done because the automorphism group of Q'_4 in our usual embedding is more complicated in nature and will require machinery which will be laid out later. In \mathbb{R}^4 define the set \mathbb{G} below:

$$\mathbb{G} = \{\pm\langle 1, 0, 0, 0 \rangle, \pm\langle 0, 1, 0, 0 \rangle, \pm\langle 0, 0, 1, 0 \rangle, \pm\langle 0, 0, 0, 1 \rangle\}$$

Next, we define the mapping $f : V(Q'_4) \rightarrow \mathbb{G}$ below:

x	$f(x)$	x	$f(x)$
0000	$\langle 1, 0, 0, 0 \rangle = v_1$	1111	$\langle -1, 0, 0, 0 \rangle = v_5$
1100	$\langle 0, 1, 0, 0 \rangle = v_2$	0011	$\langle 0, -1, 0, 0 \rangle = v_6$
1010	$\langle 0, 0, 1, 0 \rangle = v_3$	0101	$\langle 0, 0, -1, 0 \rangle = v_7$
1001	$\langle 0, 0, 0, 1 \rangle = v_4$	0110	$\langle 0, 0, 0, -1 \rangle = v_8$

Next, we let the images of f be the terminal points on the vectors given in \mathbb{R}^4 . These points will be the vertices of our embedding of Q'_n in \mathbb{R}^4 . Next, let two vectors $\vec{u}, \vec{v} \in \mathbb{G}$ be adjacent if and only if $\vec{u} \neq -\vec{v}$. From here, it is obvious that f is an isomorphism in \mathbb{R}^4 ; from henceforth when referring to $V(Q'_4)$ we will be referring to the images of the function f : Next, define the set \mathcal{G}_4 below:

Definition 21. Let \mathcal{A}_4 be defined as the set of diagonal 4×4 matrices with the non-zero entries being either 1 or -1 . Next, let \mathcal{P}_4 be defined as the set of 4×4 permutation matrices. Further, let $\mathcal{G}_4 = \{AP : A \in \mathcal{A}_4, P \in \mathcal{P}_4\}$. We will call the elements \mathcal{G}_4 signed permutation matrices.

Now we will prove that the set of signed permutation matrices form a group under matrix multiplication and that \mathcal{G}_4 is isomorphic with a semi-direct product of the groups \mathcal{A}_4 and \mathcal{P}_4 . In order to do that, we will first demonstrate that every 4×4 signed per-

mutation matrix has a unique decomposition into a products of an elements of \mathcal{A}_4 and \mathcal{P}_4 .

Theorem 5. *Every element $G \in \mathcal{G}_n$ has a unique decomposition as $G = AP$ where $A \in \mathcal{A}_n$ and $P \in \mathcal{P}_n$.*

Proof. First, G has such a decomposition by the definition of \mathcal{G}_4 . Next, let $A, A' \in \mathcal{A}_n$ and $P, P' \in \mathcal{P}_n$ and suppose that $AP = A'P'$. Then we have the following:

$$AP = A'P'$$

$$A = A'P'P^{-1}$$

$$A'A = P'P^{-1}$$

Since $A'A \in \mathcal{A}_n$ then AA' is a diagonal matrix with non-zero entries equal to either one or negative one and since $P'P^{-1} \in \mathcal{P}_n$ is a permutation matrix then its non-zero entries can only equal one. Thus $AA' = I$, so $P'P^{-1} = I$, and $A = A'$ and $P = P'$. \square

Theorem 6. *Under matrix multiplication \mathcal{G}_4 is a group and it is isomorphic to a semidirect product $\mathcal{A}_4 \rtimes_{\psi} \mathcal{P}_4$.*

Proof. First, we set out to show that \mathcal{G}_4 is a group under matrix multiplication. First, let $A, B \in \mathcal{A}_4$ and $P, Q \in \mathcal{P}_4$ and $AP, BQ \in \mathcal{G}_4$. Notice that $APBQ = APBP^T PQ$ and $PBP^T \in \mathcal{A}_4$. Since $A(PBP^T) \in \mathcal{A}_4$ and $PQ \in \mathcal{P}_4$ then we have that $APBQ \in \mathcal{G}_4$, thus \mathcal{G}_4 is closed by matrix multiplication, which is also known to be an associative, binary operation. Next, by definition, $I \in \mathcal{A}_4$ where I is the 4×4 identity matrix, and $I \in \mathcal{P}_4$, so if $G = AP$ where $A = P = I$ then $I \in \mathcal{G}_4$. Finally, let $H \in \mathcal{G}_4$ where $H = CR$ where $C \in \mathcal{A}_4$ and $R \in \mathcal{P}_4$. Since $C \in \mathcal{G}_4$ and $R^T = R^{-1} \in \mathcal{G}_4$ then $R^T C = R^{-1} C = (CR)^{-1} \in \mathcal{G}_4$ and we have demonstrated that \mathcal{G}_4 is a group under matrix multiplication.

Let $\psi : \mathcal{P}_4 \rightarrow \text{Aut}(\mathcal{A}_4)$ where $\psi(X)(Y) = XYX^T$. We claim that $\mathcal{G}_4 \cong \mathcal{A}_4 \rtimes_{\psi} \mathcal{P}_4$.

Now we will show that $|\mathcal{G}_4| = |\mathcal{A}_4 \rtimes_{\psi} \mathcal{P}_4|$. Since $\mathcal{G}_4 = AP$ with $A \in \mathcal{A}_4$ and $P \in \mathcal{P}_4$ and this decomposition is unique then we have that $|\mathcal{G}_4| = |\mathcal{A}_4||\mathcal{P}_4| = 2^4 4!$. Thus, $|\mathcal{G}_4| = |\mathcal{A}_4 \rtimes_{\psi} \mathcal{P}_4|$.

Next, let $\phi : \mathcal{A}_4 \rtimes_{\psi} \mathcal{P}_4 \rightarrow \mathcal{G}_4$ be $\phi(F, P) = FP$. Let $(H, Q) \in \mathcal{A}_4 \rtimes_{\psi} \mathcal{P}_4$. By Theorem 5 and the definition of ϕ we see that if $\phi(A, P) = \phi(B, Q)$ then $A = B$ and $P = Q$, thus $(A, P) = (B, Q)$ and ϕ is injective. Below we demonstrate that ϕ is a homomorphism which completes the proof.

$$\begin{aligned}
\phi((P, Q), (R, S)) &= \phi(P\psi(Q)(R), QS) \\
&= \phi(PQRQ^{-1}, QS) \\
&= PQRQ^{-1}QS \\
&= PQRS \\
&= \phi(P, Q)\phi(R, S)
\end{aligned}$$

□

Now, let \mathcal{G}_4 act on the vertices of Q'_n by left multiplication. For example, given the signed permutation matrix R below, we will demonstrate how R is a unique representative of an automorphism of Q'_4 .

$$R = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = AP$$

Observe that since the cyclic permutation associated with the given permutation matrix P is (23), then by multiplying each vector in $V(Q'_4)$ on the left by R we permute the second and third components of the vectors. Naturally, the vectors $\pm\langle 1, 0, 0, 0 \rangle$ and

$\pm\langle 0, 0, 0, 1 \rangle$ will not be changed in permuting their second and third components, so the vertices associated with these vectors will not be permuted by P in the decomposition of R . However, the vertices associated with the vectors $\langle 0, 1, 0, 0 \rangle$ and $\langle 0, 0, 1, 0 \rangle$, and the vertices associated with the vectors $\langle 0, -1, 0, 0 \rangle$ and $\langle 0, 0, -1, 0 \rangle$ will be permuted by P in the decomposition of R . Next, when A acts on the vectors associated with the vertices of $V(Q'_4)$ then we will clearly be negating the first and third component. This will leave vertices associated with the vectors $\pm\langle 0, 1, 0, 0 \rangle$ and $\pm\langle 0, 0, 1, 0 \rangle$ unaffected, but will transpose the non-adjacent vertices associated with the vectors $\pm\langle 1, 0, 0, 0 \rangle$ and $\pm\langle 0, 0, 1, 0 \rangle$. Figure 3.2 presents a juxtaposition of the original graph of Q'_4 and Q'_4 with R acting on $V(Q'_4)$.

We will now set out to show that the automorphism group of Q'_4 is isomorphic with \mathcal{G}_4 . Before we do this, first note that we are embedding Q'_4 into \mathbb{R}^4 so that we can realize $\text{Aut}(Q'_4) \leq \text{GL}_4(\mathbb{R})$.

Theorem 7. $\text{Aut}(Q'_4) \cong \mathcal{G}_4$.

Proof. Let $M \in \mathcal{G}_4$ such that $M = AP$ where $A \in \mathcal{A}_4$ and $P \in \mathcal{P}_4$. Next, define the function $M : V(Q'_4) \rightarrow V(Q'_4)$ such that $M(\vec{a}) = M\vec{a}$ where $\vec{a} \in V(Q'_4)$. Let $\vec{a}, \vec{b} \in V(Q'_4)$ such that $M\vec{a} = M\vec{b}$. By multiplying both sides of this result on the left by M^{-1} we have that $\vec{a} = \vec{b}$ which implies the function is injective. Since M maps $V(Q'_4)$ to itself, then we have the set of pre-images of M has the same cardinality as the set of its images, thus M is a bijection. Next, let \vec{u} and \vec{v} be adjacent vertices in $V(Q'_4)$. By the adjacency rule of our embedding since \vec{u} and \vec{v} are adjacent then $\vec{u} \neq -\vec{v}$ so when we multiply both sides of this equation by M we have that $M\vec{u} \neq -M\vec{v}$. Therefore $M\vec{u}$ and $M\vec{v}$ are adjacent. Now suppose that $M\vec{u}$ and $M\vec{v}$ are adjacent. Then we have that $M\vec{v} \neq M\vec{u}$, and by multiplying both sides of this inequality by M^{-1} we have that $\vec{u} \neq \vec{v}$. Therefore we have that \vec{u} and \vec{v} are adjacent. Since adjacency is preserved by the function M then $\mathcal{G}_4 \leq \text{Aut}(Q'_4)$.

Finally, since $|\mathcal{G}_4| = |\text{Aut}(Q'_4)| = 4!2^4$ and $\mathcal{G}_4 \leq \text{Aut}(Q'_4)$ then we have that $\mathcal{G}_4 \cong$

$\text{Aut}(Q'_4)$ and the proof is complete. \square

In the process of finalizing the above results another interesting expression of $\text{Aut}(Q'_4)$ presented itself which allows us to return to the first embedding of Q'_4 into \mathbb{R}^4 . Figuratively speaking, the semidirect product presented in the preceding portion of this chapter is more “heavy handed” in its expression of the automorphisms of Q'_4 in that the product is between the set of objects which flip the P_2 components of $\overline{Q'_4}$ and the set of objects which permute the P_2 components of $\overline{Q'_4}$ (the group \mathcal{P}_4). Before we will expose the nature of this group, we must recall our original expression of the vectors of Q'_4 in \mathbb{R}^4 .

Let $g : V(Q'_4) \rightarrow \mathbb{H}$ where \mathbb{H} is the set of vectors in \mathbb{R}^4 with given below:

$$\mathbb{H} = \{h : h = \langle \pm 1, \pm 1, \pm 1, \pm 1 \rangle, \text{ and } h \text{ has an even number of components that equal } -1\}$$

The function g maps the vertex x to the vector \vec{x} where every 1 in the i -th position of x results in a 1 in the i -th components in \vec{x} and every 0 in the j -th position of x results in a -1 in the j -th component in \vec{x} . This mapping is demonstrated below:

x	$g(x)$	x	$g(x)$
0000	$\langle -1, -1, -1, -1 \rangle = v_1$	1111	$\langle 1, 1, 1, 1 \rangle = v_5$
1100	$\langle 1, 1, -1, -1 \rangle = v_2$	0011	$\langle -1, -1, 1, 1 \rangle = v_6$
1010	$\langle 1, -1, 1, -1 \rangle = v_3$	0101	$\langle -1, 1, -1, 1 \rangle = v_7$
1001	$\langle 1, -1, -1, 1 \rangle = v_4$	0110	$\langle -1, 1, 1, -1 \rangle = v_8$

As in the previous example of the embedding, we will further refer to \mathbb{H} as $V(Q'_4)$. As in the previous embedding we also see that two vertices \vec{u} and \vec{v} are adjacent if and only if $\vec{u} \neq -\vec{v}$.

In order to define the set of objects which transpose sets of non-adjacent vertices in Q'_n we need to establish some machinery. First, let $\mathbb{1}$ be the 4×4 matrix with 1 in every entry. Next, let P_1, P_2 and P_3 be the permutation matrices associated with the cyclic

permutations (12)(34), (13)(24), and (14)(23) respectively. These matrices are shown below:

$$P_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad P_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad P_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Let $\mathbb{P} = \{I, P_1, P_2, P_3\}$ for shorthand.

Now, let $f_1 : V(Q'_4) \rightarrow V(Q'_4)$ be defined as $f_1(\vec{x}) = I - \frac{1}{2}\mathbb{1}\vec{x}$. This mapping is shown below:

\vec{x}	$f_1(\vec{x})$	\vec{x}	$f_1(\vec{x})$
$\langle -1, -1, -1, -1 \rangle$	$\langle 1, 1, 1, 1 \rangle$	$\langle 1, 1, 1, 1 \rangle$	$\langle -1, -1, -1, -1 \rangle$
$\langle -1, -1, 1, 1 \rangle$	$\langle -1, -1, 1, 1 \rangle$	$\langle 1, 1, -1, -1 \rangle$	$\langle 1, 1, -1, -1 \rangle$
$\langle -1, 1, -1, 1 \rangle$	$\langle -1, 1, -1, 1 \rangle$	$\langle 1, -1, 1, -1 \rangle$	$\langle 1, -1, 1, -1 \rangle$
$\langle -1, 1, 1, -1 \rangle$	$\langle -1, 1, 1, -1 \rangle$	$\langle 1, -1, -1, 1 \rangle$	$\langle 1, -1, -1, 1 \rangle$

Observe that f_1 transposed the vertices associated with the vectors $\langle 1, 1, 1, 1 \rangle$ and $\langle -1, -1, -1, -1 \rangle$ and left all over vertices fixed. For shorthand we will let $F_1 = I - \frac{1}{2}\mathbb{1}$, so $f_1(\vec{x}) = F_1\vec{x}$.

Further, we define $F_2, F_3,$ and F_4 below:

$$F_2 = -(P_1 - \frac{1}{2}\mathbb{1}) \quad F_3 = -(P_2 - \frac{1}{2}\mathbb{1}) \quad F_4 = -(P_3 - \frac{1}{2}\mathbb{1})$$

Let $f_2 : V(Q'_4) \rightarrow V(Q'_4)$ be the function $f_2(\vec{x}) = F_2\vec{x}$. This mapping is shown below:

\vec{x}	$f_2(\vec{x})$	\vec{x}	$f_2(\vec{x})$
$\langle -1, -1, -1, -1 \rangle$	$\langle -1, -1, -1, -1 \rangle$	$\langle 1, 1, 1, 1 \rangle$	$\langle 1, 1, 1, 1 \rangle$
$\langle -1, -1, 1, 1 \rangle$	$\langle 1, 1, -1, -1 \rangle$	$\langle 1, 1, -1, -1 \rangle$	$\langle -1, -1, 1, 1 \rangle$
$\langle -1, 1, -1, 1 \rangle$	$\langle -1, 1, -1, 1 \rangle$	$\langle 1, -1, 1, -1 \rangle$	$\langle 1, -1, 1, -1 \rangle$
$\langle -1, 1, 1, -1 \rangle$	$\langle -1, 1, 1, -1 \rangle$	$\langle 1, -1, -1, 1 \rangle$	$\langle 1, -1, -1, 1 \rangle$

In the same way that f_1 only transposed one pair of non-adjacent vertices and fixed the rest of the vertices, f_2 will do the same but the permuted pair of vertices will be the ones with associated vectors $\langle -1, 1, -1, 1 \rangle$ and $\langle 1, -1, 1, -1 \rangle$. Now we define $f_3 : V(Q'_4) \rightarrow V(Q'_4)$ to be $f_3(\vec{x}) = F_3 \vec{x}$ and $f_4 : V(Q'_4) \rightarrow V(Q'_4)$ to be $f_4(\vec{x}) = F_4 \vec{x}$ and display these mappings below:

\vec{x}	$f_3(\vec{x})$	\vec{x}	$f_3(\vec{x})$
$\langle -1, -1, -1, -1 \rangle$	$\langle -1, -1, -1, -1 \rangle$	$\langle 1, 1, 1, 1 \rangle$	$\langle 1, 1, 1, 1 \rangle$
$\langle -1, -1, 1, 1 \rangle$	$\langle -1, -1, 1, 1 \rangle$	$\langle 1, 1, -1, -1 \rangle$	$\langle 1, 1, -1, -1 \rangle$
$\langle -1, 1, -1, 1 \rangle$	$\langle 1, -1, 1, -1 \rangle$	$\langle 1, -1, 1, -1 \rangle$	$\langle -1, 1, -1, 1 \rangle$
$\langle -1, 1, 1, -1 \rangle$	$\langle -1, 1, 1, -1 \rangle$	$\langle 1, -1, -1, 1 \rangle$	$\langle 1, -1, -1, 1 \rangle$

\vec{x}	$f_4(\vec{x})$	\vec{x}	$f_4(\vec{x})$
$\langle -1, -1, -1, -1 \rangle$	$\langle -1, -1, -1, -1 \rangle$	$\langle 1, 1, 1, 1 \rangle$	$\langle 1, 1, 1, 1 \rangle$
$\langle -1, -1, 1, 1 \rangle$	$\langle -1, -1, 1, 1 \rangle$	$\langle 1, 1, -1, -1 \rangle$	$\langle 1, 1, -1, -1 \rangle$
$\langle -1, 1, -1, 1 \rangle$	$\langle -1, 1, -1, 1 \rangle$	$\langle 1, -1, 1, -1 \rangle$	$\langle 1, -1, 1, -1 \rangle$
$\langle -1, 1, 1, -1 \rangle$	$\langle 1, -1, -1, 1 \rangle$	$\langle 1, -1, -1, 1 \rangle$	$\langle -1, 1, 1, -1 \rangle$

From the mappings above we see that f_3 only permuted the vertices associated with the vectors $\langle -1, 1, -1, 1 \rangle$, and $\langle 1, -1, 1, -1 \rangle$, and similarly f_4 only permuted the pair of vertices associated with the vectors $\langle -1, 1, 1, -1 \rangle$, and $\langle 1, -1, -1, 1 \rangle$. In order to use the matrices F_1, \dots, F_4 to form a group, we establish relations between these matrices below:

Proposition 7. *The matrices F_1, F_2, F_3 and F_4 are all of order two.*

Proof. Let $F_i = \pm(P - \frac{1}{2}\mathbb{1})$ where $P \in \mathbb{P}$ and $i \in \{1, \dots, 4\}$. Since $P \in \mathbb{P}$ then we have that

$P^2 = I$. Now we complete the proof by calculating $(F_i)^2$ below:

$$\begin{aligned}
 (F_i)^2 &= (P - \frac{1}{2}\mathbf{1})(P - \frac{1}{2}\mathbf{1}) \\
 &= P^2 - \frac{1}{2}P\mathbf{1} - \frac{1}{2}\mathbf{1}P + \frac{1}{4}\mathbf{1}\mathbf{1} \\
 &= I - \frac{1}{2}\mathbf{1} - \frac{1}{2}\mathbf{1} + \mathbf{1} \\
 &= I
 \end{aligned}$$

□

Now, if the set $\{F_1, \dots, F_4\}$ is used as generators coupled with the relations that $|F_i| = 2$ and that $F_i F_j = F_j F_i$ for all $i, j \in \{1, \dots, 4\}$ then we can define the group \mathcal{F} , and with another definition characterize its elements:

Definition 22. Let $\mathcal{F} = \langle \{F_1, F_2, F_3, F_4\} \rangle$. A matrix $F \in \mathcal{F}$ is called a *flip matrix*.

Definition 23. A matrix X is *symmetric* if and $X = X^T$.

We will now demonstrate relationships between flip matrices which will serve in presenting another representation of $\text{Aut}(Q'_4)$, this one using the embedding we first presented in Chapter 2.

Proposition 8. The matrices F_1, F_2, F_3 and F_4 commute with one another.

Proof. Let and $k_1, k_2 \in \mathbb{P}$, so $k_1 k_2 = k_2 k_1$. Let i and j be distinct elements of $\{1, \dots, 4\}$ and

define $F_i = \pm(k_1 - \frac{1}{2}\mathbb{1})$ and $F_j = \pm(k_2 - \frac{1}{2}\mathbb{1})$, then we complete the proof below:

$$\begin{aligned}
F_i F_j &= \pm(k_1 - \frac{1}{2}\mathbb{1})(k_2 - \frac{1}{2}\mathbb{1}) \\
&= \pm(k_1 k_2 - \frac{1}{2}k_1 \mathbb{1} - \frac{1}{2}\mathbb{1} k_2 + \frac{1}{4}4\mathbb{1}) \\
&= \pm(k_1 k_2 - \frac{1}{2}\mathbb{1} - \frac{1}{2}\mathbb{1} + \mathbb{1}) \\
&= \pm(k_1 k_2) \\
&= \pm(k_2 k_1 - \frac{1}{2}\mathbb{1} - \frac{1}{2}\mathbb{1} + \mathbb{1}) \\
&= \pm(k_2 k_1 - \frac{1}{2}k_2 \mathbb{1} - \frac{1}{2}\mathbb{1} k_1 + \frac{1}{4}4\mathbb{1}) \\
&= \pm(k_2 - \frac{1}{2}\mathbb{1})(k_1 - \frac{1}{2}\mathbb{1}) \\
&= F_j F_i
\end{aligned}$$

□

Since the matrices F_1, \dots, F_4 commute with one another, then \mathcal{F} is abelian. Thus each element of \mathcal{F} is of the form $\prod_{i=1}^n F_i^{\alpha_j}$ where $i \in \{1, \dots, 4\}$ and $\alpha_j \in \mathbb{Z}_2$. This expression of flip matrices will serve us in the proposition below:

Proposition 9. *Every flip matrix is symmetric.*

Proof. First, we will show that for all F_i where $i \in \{1, \dots, 4\}$ that $F_i = F_i^T$. In the case of F_1 we have that $F_1^T = (I - \frac{1}{2}\mathbb{1})^T = I^T - \frac{1}{2}\mathbb{1}^T = F_1$. Note that P_1, P_2 , and P_3 are their own inverses and since they are permutation matrices then their inverses are their transpositions. Thus for $i \in \{1, \dots, 3\}$ we have the following:

$$-(P_i - \frac{1}{2}\mathbb{1})^T = -(P_i^T - \frac{1}{2}\mathbb{1}^T) = -(P_i - \frac{1}{2}\mathbb{1})^T$$

Let $F \in \mathcal{F}$ such that $F = F_1^{\alpha_1} F_2^{\alpha_2} F_3^{\alpha_3} F_4^{\alpha_4}$ where $\alpha_j \in \{0, 1\}$ for all $j \in \{1, \dots, 4\}$. We

complete the proof below:

$$\begin{aligned}
 F^T &= (F_1^{\alpha_1} F_2^{\alpha_2} F_3^{\alpha_3} F_4^{\alpha_4})^T \\
 &= (F_4^{\alpha_4})^T (F_3^{\alpha_3})^T (F_2^{\alpha_2})^T (F_1^{\alpha_1})^T \\
 &= F_4^{\alpha_4} F_3^{\alpha_3} F_2^{\alpha_2} F_1^{\alpha_1} \\
 &= F_1^{\alpha_1} F_2^{\alpha_2} F_3^{\alpha_3} F_4^{\alpha_4} = F
 \end{aligned}$$

□

From here, we now set out to show that for all $P \in \mathcal{P}_4$, the element PPF^T where $F \in \mathcal{F}$ is contained in \mathcal{F} . Before we do this, we will show that the set $\{I, P_1, P_2, P_3\}$ forms a normal subgroup in \mathcal{P}_4 by showing that their associated permutations form a normal subgroup in S_4 .

Definition 24. Let G be a group and $N \leq G$. The subgroup N is a **normal subgroup** of G if $gng^{-1} \in N$ for all $n \in N$ and all $g \in G$.

Proposition 10. The set $K = \{I, (12)(34), (13)(24), (14)(23)\}$ forms a normal subgroup in S_4 .

Proof. First, we will show that the set K is closed under composition. We will demonstrate this with the Cayley Table below:

	I	(12)(34)	(13)(24)	(14)(23)
I	I	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	I	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	I	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	I

Now we set out to show that for any $k \in K$ and $g \in G$ that $gkg^{-1} \in K$. Clearly, if $k = I$ then $gIg^{-1} = gg^{-1} = I \in K$. Now suppose that $k \neq I$. Let $k = (ab)(cd)$ where $a, b, c,$ and d are unique elements of $\{1, \dots, 4\}$. Then we have that $gkg^{-1} = (g(a) \ g(b))(g(c) \ g(d))$.

Since $g \in S_4$ then $g(a), g(b), g(c)$, and $g(d)$ are unique elements of the set $\{1, \dots, 4\}$ and $gkg^{-1} \in K$. \square

From this result we can conclude that the set $\mathbb{P} = \{I, P_1, P_2, P_3\}$ forms a normal subgroup of \mathcal{P}_4 under matrix multiplication. We will use this fact in the proposition below:

Proposition 11. *For all $P \in \mathcal{P}_4$ and $F \in \mathcal{F}$ the matrix $PF P^T$ is contained in \mathcal{F} .*

Proof. First, let $P \in \mathcal{P}_4$, then we will prove that $PF_i P^T \in \{F_1, \dots, F_4\}$ for all $i \in \{1, \dots, 4\}$. In the case that $i = 1$ we have that $PF_1 P^T = P(I - \frac{1}{2}\mathbb{1})P^T = (PP^T - \frac{1}{2}\mathbb{1}) = F_1$. Note from proposition 8 we have that $PP_{i-1} P^T = P_k \in \mathbb{P}$ where $k \in \{2, 3, 4\}$ and $i \neq 1$. Now we calculate $PF_i P^T$ below:

$$\begin{aligned} P[-(P_{i-1} - \frac{1}{2}\mathbb{1})P^T] &= -(PP_{i-1} P^T - \frac{1}{2}P\mathbb{1}P^T) \\ &= -(P_k - \frac{1}{2}\mathbb{1}) \end{aligned}$$

Since $P_k \in \mathbb{P}$ where $k \in \{2, 3, 4\}$ then we have that $PF_i P^T \in \{F_1, \dots, F_4\}$ for all $P \in \mathcal{P}_4$. Now we will show that where for some $F \in \mathcal{F}$ where $F = F_1^{\alpha_1} F_2^{\alpha_2} F_3^{\alpha_3} F_4^{\alpha_4}$ where $\alpha_j \in \{0, 1\}$ for all $j \in \{1, \dots, 4\}$. We calculate $PF P^T$ below:

$$\begin{aligned} P(F_1^{\alpha_1} F_2^{\alpha_2} F_3^{\alpha_3} F_4^{\alpha_4})P^T &= PF_1^{\alpha_1} P^T PF_2^{\alpha_2} P^T PF_3^{\alpha_3} P^T PF_4^{\alpha_4} P^T \\ &= (PF_1^{\alpha_1} P^T)(PF_2^{\alpha_2} P^T)(PF_3^{\alpha_3} P^T)(PF_4^{\alpha_4} P^T) \end{aligned}$$

Since $PF_i^{\alpha_i} P^T \in \{F_1, \dots, F_4\}$ for all $i \in \{1, \dots, 4\}$ and $\alpha_i \in \{0, 1\}$ and \mathcal{F} is closed under multiplication then we have that $PF P^T \in \mathcal{F}$ for all $P \in \mathcal{P}_4$ and $F \in \mathcal{F}$. \square

We can now examine the specific elements of \mathcal{F} as products of F_1, F_2, F_3 and F_4 . From Proposition 7 we see that $F_i F_j = \pm k_i k_j$ where $k_i, k_j \in \mathbb{P}$ and i, j are unique elements of $\{1, \dots, 4\}$. Thus, for all $P \in \mathbb{P}$, the matrices P and $-P$ are matrices in \mathcal{F} . Using this, we see that the matrices of \mathcal{F} which are products of three of the matrices F_1, \dots, F_4 is

calculated below (let $m \in \{1, \dots, 4\}$ with $m \neq i \neq j$):

$$\begin{aligned} F_i F_j F_m &= \pm(k_i k_j)(k_m - \frac{1}{2}\mathbb{1}) \\ &= \pm(k_i k_j k_m - \frac{1}{2}k_i k_j \mathbb{1}) \\ &= \pm(k_i k_j k_m - \frac{1}{2}\mathbb{1}) \end{aligned}$$

Here we see that the product of three of the matrices of F_1, \dots, F_4 is either one of the F_1, \dots, F_4 matrices or it's negation, so for all $w \in \{1, \dots, 4\}$ we have that $\pm F_w \in \mathcal{F}$. Finally, observe that the product of all four matrices F_1, \dots, F_4 will be equal to $-(k_1 k_2 k_3 k_4) = -I$. In short, we can exhaustively list all sixteen elements of \mathcal{F} accordingly:

$$\mathcal{F} = \{\pm I, \pm F_1, \pm F_2, \pm F_3, \pm F_4, \pm P_1, \pm P_2, \pm P_3\}$$

From here, we can now define \mathcal{H}_4 , which we will eventually prove is isomorphic to $\text{Aut}(Q'_4)$.

Definition 25. Let $\mathcal{H}_n = \{FP : F \in \mathcal{F}, P \in \mathcal{P}_n\}$ be the set of *dihedral matrices*.

We now set out to show that every element of \mathcal{H}_n has a unique decomposition of a flip matrix and a permutation matrix. This will be an important result in showing that $\mathcal{H}_4 \cong \mathcal{F} \rtimes_{\psi} \mathcal{P}_4$. This result will also be pivotal in showing that $\mathcal{H}_4 \cong \text{Aut}(Q'_4)$ in that we will be able to use the fact that $|\mathcal{H}_4| = |\mathcal{F} \rtimes_{\psi} \mathcal{P}_4| = 4!2^4$.

Theorem 8. Every element $G \in \mathcal{H}_4$ has a unique decomposition as $G = FP$ where $F \in \mathcal{F}$ and $P \in \mathcal{P}_4$.

Proof. Let $F, F' \in \mathcal{F}$ and $P, P' \in \mathcal{P}_4$ and suppose that $FP = F'P'$. Then we have the following:

$$FP = F'P'$$

$$P^T FP = P^T F'P'$$

Since $P^T F P \in \mathcal{F}$ then $P^T F' P' \in \mathcal{F}$, thus $P^T F' P'$ is symmetric. Since $P^T F' P'$ is symmetric then $P' = (P^T)^T = P$. Thus we have that $F = F'$ and the proof is complete. \square

Theorem 9. *Under matrix multiplication \mathcal{H}_4 is a group and it is isomorphic to a semidirect product $\mathcal{F} \rtimes_{\psi} \mathcal{P}_4$.*

Proof. First, we set out to show that \mathcal{H}_4 is a group under matrix multiplication. First, let $F, H \in \mathcal{F}$ and $P, Q \in \mathcal{P}_4$ and $FP, HQ \in \mathcal{H}_4$. Notice that $FPHQ = FPHP^T P Q$ and $PHP^T \in \mathcal{F}$. Since $F(PHP^T) \in \mathcal{F}$ and $PQ \in \mathcal{P}_4$ then we have that $FPHQ \in \mathcal{H}_4$, thus \mathcal{H}_4 is closed by matrix multiplication, which is also known to be an associative, binary operation. Next, by definition, $I \in \mathcal{F}$ where I is the 4×4 identity matrix, and $I \in \mathcal{P}_4$, so if $G = FP$ where $F = P = I$ then $I \in \mathcal{H}_4$. Finally, let $H \in \mathcal{F}$ where $H = CR$ where $C \in \mathcal{F}$ and $R \in \mathcal{P}_4$. Since $C \in \mathcal{H}_4$ and $R^T = R^{-1} \in \mathcal{H}_4$ then $R^T C = R^{-1} C = (CR)^{-1} \in \mathcal{H}_4$ and we have demonstrated that \mathcal{H}_4 is a group under matrix multiplication.

Let $\psi : \mathcal{P}_4 \rightarrow \text{Aut}(\mathcal{F})$ where $\psi(X)(Y) = XYX^T$. We claim that $\mathcal{H}_4 \cong \mathcal{F} \rtimes_{\psi} \mathcal{P}_4$.

Now we will show that $|\mathcal{H}_4| = |\mathcal{F} \rtimes_{\psi} \mathcal{P}_4|$. Since $\mathcal{H}_4 = FP$ with $F \in \mathcal{F}$ and $P \in \mathcal{P}_4$ and this decomposition is unique then we have that $|\mathcal{H}_4| = |\mathcal{F}| |\mathcal{P}_4| = 4! 2^4$. Thus, $|\mathcal{G}_4| = |\mathcal{A}_4 \rtimes_{\psi} \mathcal{P}_4|$.

Next, let $\phi : \mathcal{F} \rtimes_{\psi} \mathcal{P}_4 \rightarrow \mathcal{H}_4$ be $\phi(F, P) = FP$. Let $(H, Q) \in \mathcal{F} \rtimes_{\psi} \mathcal{P}_4$. By Theorem 8, and the definition of ϕ we see that if $\phi(A, P) = \phi(B, Q)$ then $F = H$ and $P = Q$, thus $(F, P) = (H, Q)$ and ϕ is injective. Let $J, K \in \mathcal{F}$ and $L, M \in \mathcal{P}_4$. Below we demonstrate

that ϕ is a homomorphism which completes the proof.

$$\begin{aligned}
\phi((J, L), (K, M)) &= \phi(J\psi(L)(K), LM) \\
&= \phi(JLKL^{-1}, LM) \\
&= JLKL^{-1}LM \\
&= JLKM \\
&= \phi(J, L)\phi(K, M)
\end{aligned}$$

□

We now show that $\mathcal{H}_4 \cong \text{Aut}(Q'_4)$ below:

Theorem 10. $\text{Aut}(Q'_4) \cong \mathcal{G}_4$.

Proof. Let $M \in \mathcal{H}_4$ such that $M = FP$ where $F \in \mathcal{F}$ and $P \in \mathcal{P}_4$. Next, define the function $M : V(Q'_4) \rightarrow V(Q'_4)$ such that where $\vec{\alpha} \in V(Q'_n)$, $M(\vec{\alpha}) = M\vec{\alpha}$. Since $M \in \text{GL}_4(\mathbb{R})$ then we have that the function M is injective. Since M maps $V(Q'_4)$ to itself, then we have the set of pre-images of M has the same cardinality as the set of its images, thus M is a bijection. Next, let \vec{u} and \vec{v} be adjacent vertices in $V(Q'_4)$. By the adjacency rule of our embedding since \vec{u} and \vec{v} are adjacent then $\vec{u} \neq -\vec{v}$. From here, we multiply both sides of this equation by M we have that $M\vec{u} \neq -M\vec{v}$, therefore $M\vec{u}$ and $M\vec{v}$ are adjacent. Now suppose that $M\vec{u}$ and $M\vec{v}$ are adjacent. Then we have that $M\vec{v} \neq M\vec{u}$, and by multiplying both sides of this inequality by M^{-1} we have that $\vec{u} \neq \vec{v}$. Therefore we have that \vec{u} and \vec{v} are adjacent. Since adjacency is preserved by the function M then $\mathcal{H}_4 \leq \text{Aut}(Q'_4)$.

Finally, since $|\mathcal{H}_4| = |\text{Aut}(Q'_4)| = 4!2^4$ and $\mathcal{H}_4 \leq \text{Aut}(Q'_4)$ then we have that $\mathcal{H}_4 \cong \text{Aut}(Q'_4)$ and the proof is complete. □

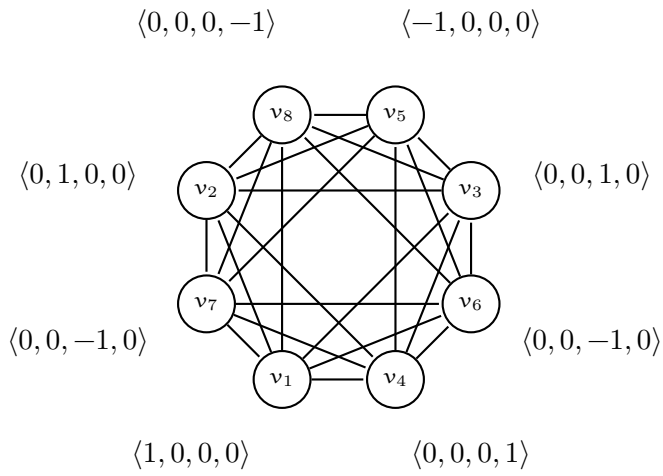
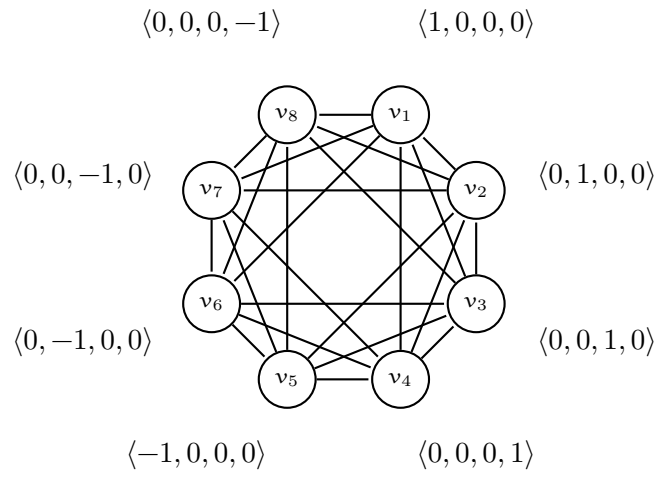


Figure 3.2: The graph Q'_4 and Q'_4 with R acting on $V(Q'_4)$.

Chapter 4

A Connection Between Halved Cubes And Circulants

An interesting relationship between halved cubes and circulants can be proven given our representation of $\text{Aut}(Q'_n)$. The forthcoming theorem states that Q'_n is a circulant if and only if $n \leq 4$.

Proving the converse requires only depictions of the specific circulants which have an isomorphism to Q'_n when $n \in \{1, 2, 3, 4\}$. The proof of the forward direction of this theorem is more involving: the core idea of the proof is that the order of an element in $\text{Aut}(Q'_n)$ never gets large enough to equal the number of vertices in Q'_n when $n > 4$. Given research from Eric Weisstein [5] we have the following:

A graph G is a circulant if and only if the automorphism group of G contains at least one permutation consisting of a minimal cycle of length $|V(G)|$.

Using this result we will show that when $n > 4$ there is no $M \in \text{Aut}(Q'_n)$ such that $|M| = 2^{n-1}$. This will require proving a few key lemmas which will give structure to the maximal orders of elements of $\text{Aut}(Q'_n)$ where $n > 4$ which will provide the necessary machinery to prove that Q'_n is a circulant if and only if $n \leq 4$.

Theorem 11. *The halved cube Q'_n is a circulant if and only if $n \leq 4$.*

Proof. First, we prove that if Q'_n is a circulant then $n \leq 4$ by proving its contrapositive. First, we suppose that $n > 4$, and we set out to show that Q'_n is not a circulant. Let $(A, P) \in \mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n$, then will show that the order of (A, P) is either $|P|$ or $2|P|$ below.

Lemma 2. *Let $(A, P) \in \mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n$ such that $|P| = k$, then $|(A, P)| = k$ or $|(A, P)| = 2k$. Consequently, if $AP \in G_n^e$ then $|AP| = |P|$ or $|AP| = 2|P|$.*

Proof. First, let $A \in \mathcal{A}_n^e$ and $P \in \mathcal{P}_n$ and let $r \leq n$. First, we will show by induction that $(A, P)^r = ((AP)^{r-1}AP^{1-r}, P^r)$.

Beginning $r = 1$, we trivially have the following:

$$\begin{aligned} (A, P)^1 &= ((AP)^{1-1}AP^{1-1}, P^1) \\ &= (A, P) \end{aligned}$$

Next, suppose that for all $r > 1$, $(A, P)^r = ((AP)^{r-1}AP^{1-r}, P^r)$. Now we check the $(r+1)$ -st case below:

$$\begin{aligned} (A, P)^{r+1} &= (A, P)[(A, P)^r] \\ &= (A, P)((AP)^{r-1}AP^{1-r}, P^r) \\ &= (A\phi_P((AP)^{r-1}AP^{1-r}), P^{r+1}) \\ &= (AP[(AP)^{r-1}AP^{1-r}]P^{-1}, P^{r+1}) \\ &= ((AP)^rAP^{-r}, P^{r+1}) \\ &= ((AP)^{(r+1)-1}AP^{1-(r+1)}, P^{r+1}) \end{aligned}$$

and this portion of the proof is complete.

Note: $(AP)^{r-1}A = A(PA)^{r-1}$ so we also have that $(A, P)^r = (A(PA)^{r-1}P^{1-r}, P^r)$. Now, let $|P| = k$ then we see that $P^{1-k} = P$, so we have the following:

$$(A, P)^k = (A(PA)^{k-1}P^{1-k}, P^k) = (A(PA)^{k-1}P, I)$$

In the case that $(PA)^{1-k} = AP^{k-1}$ we have that $(A, P)^k = (I, I)$ and the order of (A, P) is k . Rather, we have that if $(PA)^{1-k} = AP^{k-1}$ then the order of (A, P) will be the same as the order of P . We will now show that any element of $\mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n$ raised to the $2k$ power is the identity element. This implies that any element of $\mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n$ which isn't of order $|P|$ is of order $2|P|$.

We now prove that $(A, P)^{2k}$ is the identity. We calculate $(A, P)^{2k}$ below (note that $P^{1-2k} = PP^{-2k} = P(P^{-2})^k = P$):

$$\begin{aligned} (A, P)^{2k} &= (A(PA)^{2k-1}P^{1-2k}, P^{2k}) \\ &= (A(PA)^{2k-1}P, I) \\ &= ((AP)^{2k}, I) \end{aligned}$$

We now set out to show that $(AP)^{2k} = I$. Below, we calculate $(AP)^{2k}$ and re-express our calculation in such a way that we have a product of elements of \mathcal{A}_n^e .

$$\begin{aligned} (AP)^{2k} &= A(PAP^{-1})(P^2AP^{-2})(P^3AP^{-3})\dots(P^kAP^{-k})\dots(P^{2k-1}AP^{1-2k})P^{2k} \\ &= A(PAP^{-1})(P^2AP^{-2})(P^3AP^{-3})\dots(P^kAP^{-k})\dots(P^{2k-1}AP^{1-2k}) \end{aligned}$$

By Proposition 3 we have that $P^rAP^{-r} \in \mathcal{A}_n^e$ for all $r \in \{1, \dots, k\}$ and \mathcal{A}_n^e is commutative (since every element of \mathcal{A}_n^e is of order two), then we can commute all of the terms of the product above. We commute the terms in parentheses in such a way that we have the terms PAP^{-1} next to P^kAP^{-k} , P^2AP^{-2} next to $P^{k+1}AP^{-k-1}$, and for we continue this process such that where $t \in \{3, \dots, 2k-1\}$ we have terms P^tAP^{-t} commuted to be next to

$P^{k+t}AP^{-k-t}$. Note that underlined terms are multiplied in the proceeding line:

$$\begin{aligned}
(A, P)^{2k} &= A(P^kAP^{-k})(PAP^{-1})(P^{k+1}AP^{-k-1})\dots(P^tAP^{-t})(P^{k+t}AP^{-k-t})\dots \\
&= \underline{A(A)}(\underline{P^1AP^{-1}})(\underline{P^{k+1}AP^{-k-1}})(\underline{P^2AP^{-2}})(\underline{P^{k+2}}\dots(\underline{P^tAP^{-t}})(\underline{P^{k+t}AP^{-k-t}})\dots \\
&= P(AP^k)(AP^{-k+1})(AP^k)(AP^{-k+1})\dots(AP^{-k+1}) \\
&= P(A)(AP^{-k+1})(A)(AP^{-k+1})\dots(AP^{-k+1}) \\
&= P(AA)P^{-k+1}(AA)P^{-k+1}\dots(AA)P^{-k+1} \\
&= P(P^{-k+1})^{2k-1} \\
&= P(P)^{2k-1} \\
&= P^{2k} \\
&= I
\end{aligned}$$

Therefore, given a permutation matrix of order k , in multiplying this permutation matrix by an element of \mathcal{A}_n^e then either the order of the initial permutation matrix is preserved, or the the order of the resulting matrix is twice that of the initial permutation matrix. \square

Next, we set out to show that the any element of \mathcal{P}_n with a power of two order will have an order less than or equal to n , so the any element of $\mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n$ will have order less than or equal to $2n$. This fact, coupled with the previous lemma, gives us critical information about the order of elements of $\mathcal{A}_n^e \rtimes_{\psi} \mathcal{P}_n$ where $n > 4$ to complete this proof.

Lemma 3. *Let $\pi \in \mathcal{P}_n$, such that there exists some $k \in \mathbb{N}$ where $|\pi| = 2^k$. Then $2^k \leq n$.*

Proof. Let $\pi \in S_n$ such that $|\pi| = 2^k$ where $k \in \mathbb{N}$ with $2^k > n$. Since $\pi \in S_n$, if π is a single cycle then we have a contradiction in that the length of the cycle is larger than n . Suppose instead that π has a cycle decomposition of t cycles (where $t > 1$) with cycle lengths $|a_1|, \dots, |a_t|$ respectively. Since $\pi \in S_n$ then $|\pi| = 2^k = \text{lcm}(|a_1|, \dots, |a_t|)$ then for

some $a_i \in \{a_1, \dots, a_t\}$, we have that $|a_i| = 2^k$. Thus, there is some cycle of length 2^k in the cycle decomposition of π with order larger than n , a contradiction. Observe that equality holds when n is a power of two and $k \in \mathbb{N}$, such that $n = 2^k$. \square

By Lemma 1, and Lemma 2, we have that given an element of \mathcal{G}_n^e with a power of two order can have an order of at most $2n$. Lemma 4 states that where $n > 4$ then $2n < 2^{n-1}$. Contextually, a proof of Lemma 4 demonstrates that the maximal order of an element of $\text{Aut}(Q'_n)$ is less than the order of the graph Q'_n . Thus, where $n > 4$ we have that Q'_n will not be isomorphic to a circulant. In proving Lemma 4 we complete the proof below:

Lemma 4. *If $n \in \mathbb{N}$ and $n > 4$, then $2n < 2^{n-1}$*

Proof. We will prove this by induction. First, consider the case where $n = 5$, then trivially $10 < 16$ and the base case holds. For our induction hypothesis suppose that $2n < 2^{n-1}$ for all $n > 5$. Now we set out to show that $2(n + 1) < 2^n$. Since $2(n + 1) = 2n + 2$ and $2 < 2^{n-1}$ then by induction hypothesis we have that $2n + 2 < 2^{n-1} + 2 < 2^{n-1} + 2^{n-1} = 2^n$ and the lemma has been proven and the proof is complete. \square

First, in proving the converse, note that Q'_1 is trivially a circulant. In examining Figures 4.1, 4.2, and 4.3 we see that the graphs Q'_2 , Q'_3 , and Q'_4 are isomorphic with the circulant graphs $C_2(1)$, $C_4(1, 2)$, and $C_8(1, 2, 3)$ respectively. \square

Though this is a negative result, it serves as an example of an application of the automorphism groups of a graph. In particular, a more intuitive and streamlined expression of the automorphism groups of a family of graphs could aid in demonstrating a connection to a separate family of graphs. The advent of an algorithmic calculus for determining the automorphism group of any arbitrary graph would help draw parallels between specific families of graphs which otherwise would remain undiscovered. Unfortunately, the question of how to find an arbitrary graph's automorphism group is one which hasn't yet been answered. Further, this problem fits into a category of problems

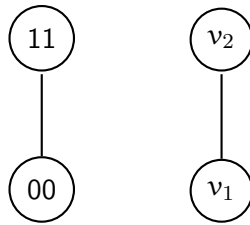


Figure 4.1: Q'_2 and $C_2(1)$

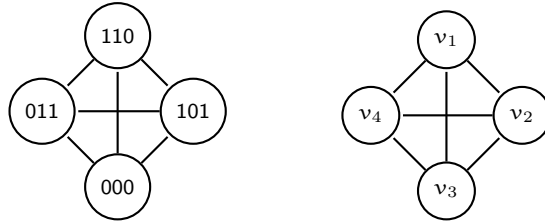


Figure 4.2: Q'_3 and $C_4(1, 2)$

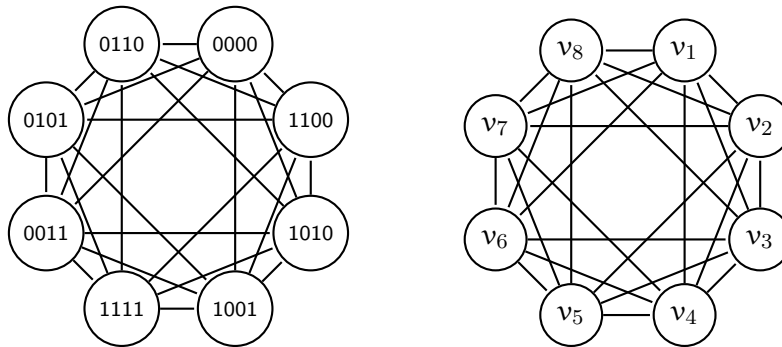


Figure 4.3: Q'_4 and $C_8(1, 2, 3)$

in mathematics which cannot be solved without significant progress in the field of algorithmic graph theory. While our result is a specific representation of the automorphism group of a very specific and structured family of graphs, Charles Caleb Colton, the English cleric and writer once said: *“the study of mathematics, like the Nile begins in minuteness but ends in magnificence.”*

Bibliography

- [1] Diestel, R. (1997). *Graph theory*. New York: Springer.
- [2] Dummit, D. S., and Foote, R. M. (2004). *Abstract Algebra* (3rd edition). Hoboken, NJ: Wiley.
- [3] Chartrand, G., Lesniak, L., and Zhang, P. (2011). *Graphs and digraphs* (5th ed.). Boca Raton, FL: CRC Press.
- [4] Brouwer, A. E., Cohen, A. M., and Neumaier, A. (1989). *Distance regular graphs*. Berlin: Springer.
- [5] Circulant Graph – from Wolfram Mathworld. (n.d.). Retrieved June/July, 2016, from <http://www.oalib.com/references/19757466>
- [6] W. Imrich, S. Klavzar and A. Vesel, *A characterization of halved cubes*, *Ars Combin.* 48 (1998),27–32.
- [7] Imrich, W., Klavzar, S., and Vesel, A. (1995). *Recognizing halved cubes in a constant time per edge*. *European Journal of Combinatorics*, 16(6), 617-621.

Vita

Ben MacKinnon came from humble beginnings, has maintained these humble circumstances, and will more than likely have a humble demise. Upon graduating from University of Delaware in 2010 he set his hand to teaching mathematics at a public high-school just outside of Richmond, VA. Shortly after he began his careers he discovered that teaching is an endeavor far worthy of his life's commitment. As a true glutton for punishment, Ben also finds a passion in mathematics and hopes to spend the rest of his life as a students of the subject.

Kate MacKinnon, Ben's saint of a wife, encouraged him to return to school to study Mathematics in order to pursue his dream of post-secondary teaching. With much trepidation, he returned to academic mathematics as a student at Virginia Commonwealth University. After three semesters of rigorous coursework he obtained a Masters in Mathematics in the fall of 2016.

While the profession of teaching may have enjoyed the year-and-a-half moratorium from Ben MacKinnon, he will be returning to the profession. His dog, Reepicheep, looks forward to seeing less of his adoptive father throughout the day.