2012-01-01

Dihedral Cayley Directed Strongly Regular Graphs

Jose Jonathan Gamez
University of Texas at El Paso, jonathan.gamez@ymail.com

DIHEDRAL CAYLEY DIRECTED STRONGLY REGULAR GRAPH

JOSE JONATHAN GAMEZ

Department of Mathematics

APPROVED:

Art Duval, Chair, Ph.D.

Joe A. Guthrie, Ph.D.

Vladik Kreinovich, Ph.D.

Benjamin Flores, Ph.D.
Interim Dean of the Graduate School

to my

MOTHER and FATHER

with love

DIHEDRAL CAYLEY DIRECTED STRONGLY REGULAR GRAPH

By

JOSE JONATHAN GAMEZ

THESIS

Presented to the Faculty of the Graduate School of

The University of Texas at El Paso

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE

Department of Mathematics

THE UNIVERSITY OF TEXAS AT EL PASO

MAY 2012

Acknowledgements

I would like to thank my advisor Dr. Art Duval for his constant support throughout my two years here at UTEP. He always pushed me to go further in my work, and always did so with a smile knowing that I was able to handle the challenge, even though I thought at times that I was going to die. His response to my constant worried look on my face when I felt like everything was going down hill was, "it's ok Jonathan, you can do this." My desire to his future student(s) is to also experience fully what I have experienced in these past two years. I believe that I have learned more about mathematics in these past two years under his supervision, then in previous years.

I would like to also thank the other members of my committee, Dr. Joe. Guthrie of the Mathematics Department, and Dr. Vladik Kreinovich of the Computer Science Department for their suggestions, comments, and addtitional guidance throughout the completion of the thesis. Words cannot express my graditude for their expertise, experience, and concerns for my success.

I would like to also thank my peers for helping me clear the ideas in my head as I wrote them down when structuring the thesis. Their inputs, suggestions, and time as I explained my work to them to better understand it myself was a huge help towards the completion of the thesis and presentation. This includes (but certainly is not limited to) the following individuals: Arturo Callias, Adrian Delgado, John Appiah Kubi, Christopher Dodoo, Angelica Monarrez, Berenice Salazar, Pavel Bezdek, Sameera Viswakula, Maduranga Kasun Dassanayake, Rebecca Davis, Francis Biney, and Adel Bedoui.

Additionally, I want to thank the Mathematics Department professors and staff from UTEP for their hard and dedication, providing me the means to complete my masters degree and prepare me for a career as a Mathematician. My education here at UTEP will forever have me in a competative advantage in the job market.

Finally, I want to thank my family and friends for always believing in me and helping me throughout these past two years here at UTEP.

Abstract

A graph is a directed strongly regular graph (DSRG) if and only if the number of paths of length 2 from vertex x to vertex y is: λ, if there is an edge from x to y; μ, if there is not an edge from x to y (with x not equal to y); and t, if $x = y$. For every vertex in G, the in-degree and out-degree is k. The number of vertices in G is denoted by v. If G is a group and S a subset of G, then the Cayley graph is the directed graph whose vertices are the elements of G, and directed edges are (g, sg) for every g in G and for every s in S.

If w is any natural number and $n = 4w + 2$, then we construct a family of DSRGs with parameters $v = 8w + 4,\ k = 4w,\ t = 2w,\ \mu = 2w,\ and\ \lambda = 2w - 2$ utilizing Cayley graphs of the dihedral group D_{2n}.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Strongly regular graphs are well known graphs in graph theory and have been studied by many people [1]. Directed strongly regular graphs (DSRGs) are a directed version of Strongly Regular Graphs [2]. They were defined and first studied by A. M. Duval [3]. A graph is a DSRG with parameters (v, k, t, μ, λ) if and only if the number of paths of length two from vertex x to vertex y is: λ, if there is an edge from x to y; μ, if there is not an edge from x to y (with x not equal to y); and t, if $x = y$. For every vertex in G, the in-degree and out-degree is k. The number of vertices in G is denoted by v.

Let G be a group and S a subset of G. Then the Cayley graph is a directed graph whose vertices are the elements of G, and whose directed edges are (g, sg) for every g in G and every s in S. The first authors who searched for DSRGs after [3] were [4, 11] who found DSRGs as Cayley graphs over dihedral groups with certain parameters. They made a table of different constructions of DSRGs [4, p. 106]. Motivated by [11], S. A. Hobart and T. J. Shaw [8] found a new infinite family of DSRGs using dihedral Cayley graphs. They found if n is even, then one can construct dihedral Cayley graphs as DSRGs with parameters $(2n, n-1, n/2, n/2-1, n/2-1)$. A list of DSRGs are in [5].

Since DSRGs were found before as Cayley graphs over dihedral groups, we took this same empirical approach to search for more DSRGs. We found a strong characteristic that Cayley DSRGs must have, and as consequence used that to refine the search. We were able to determine exactly how many rotations and reflections set S needs, to have DSRGs. This additional approach reduced the number of Cayley sets S to fewer sets to test. Once we found the first few DSRGs, we constructed an infinite family of DSRGs with parameters $n = 4w + 2, k = 4w, t = 2w, \mu = 2w$, and $\lambda = 2w - 2$, where w is a natural number.

C. D. Godsil, S. A. Hobart, and W. J. Martin have found graphs with these parameters, but they were not dihedral Cayley graphs [2].

Chapter 2 begins with a brief review of definitions on dihedral groups, dihedral Cayley graphs, DSRGs, and adjacency matrices. Section 2.2 covers results of other DSRGs that have been previously found. Chapter 3 proceeds with a search for dihedral Cayley sets S, and is broken down into four sections. Section 3.1 focuses on paths of length two from e to a rotation. Section 3.2 focuses on paths of length two from e to a reflection. Section 3.3 focuses on dihedral Cayley sets S. Finally Section 3.4 focuses on parameter sets that satified the computer search for dihedral Cayley sets and definition of DSRG. Chapter 4 is composed of four sections. Sections 4.1, 4.2, and 4.3 verify that there are λ paths of length two from the identity to elements in S, μ paths of length two from the identity to elements not in S, and t paths of length two from the identity back to itself, respectively. In Section 4.4, we have the proof of the main result, and finally the computer search in the appendix, which is in Chapter 5.

Chapter 2

Background

We review in this section well known concepts and include details of these concepts for the sake of completeness.

2.1 Dihedral Group

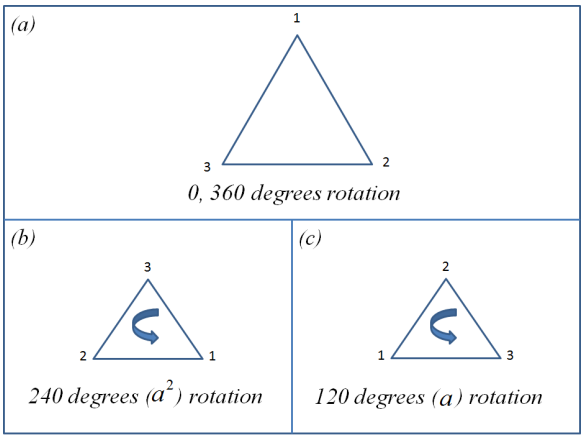
The *dihedral group* is the (non-commutative) symmetry group of a n-sided regular polygon for $n > 1$. This group plays an important role in many areas in mathematics such as algebra (e.g., group theory), geometry, and graph theory [6, 7]. We use (2.1) to define D_{2n}, where n represents the rotations and also reflections [6, 7]. So we have

$$\begin{aligned} D_{2n} &= \left\langle a, x \mid a^n = e,\ x^2 = e,\ xa = a^{-1}x \right\rangle \\ &= \left\{ e,\ a,\ a^2, \ldots,\ a^{n-1},\ x,\ ax, \ldots, a^{n-1}x \right\}, \end{aligned} \tag{2.1}$$

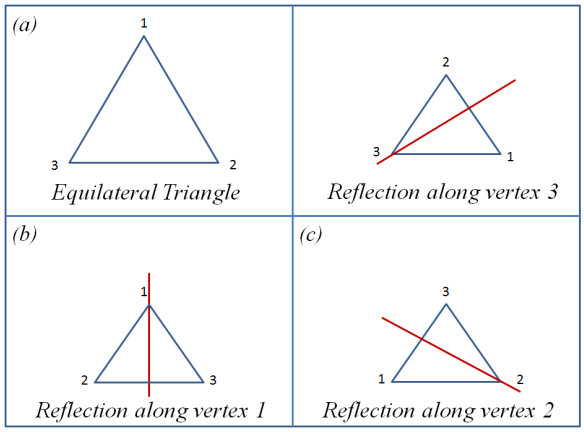
where the rotation element, a, and reflection element, x, together generate D_{2n} (e is the identity element). The elements of the form a^k are called rotations, and the elements of the form $a^k x$ are called reflections. We define the rotation of a polygon in a counter-clockwise direction.

If one rotates the n-sided regular polygon n times, the polygon returns to its original position ($a^n = e$). If one reflects the polygon twice along a given vertex, the polygon also returns to its original position ($x^2 = e$). If one reflects a polygon and then rotates it, it is the same as rotating the polygon clockwise and then reflecting it ($xa = a^{-1}x$), which we demonstrate in the following example.

Example



(a) Rotations



(b) Reflections

Figure 2.1: Rotations and reflections of an equilateral triangle

Let $n = 3$, then we have an equilateral triangle. The triangle has six movements composed of rotations and reflections. We rotate counter-clockwise the triangle along the center at 0, 120, and 240 degrees (see Figure 2.1a). We reflect the triangle by choosing a vertex and rotate at 180 degrees along the axis that goes through the chosen vertex. This movement switches the placement of the two remaining vertices (see Figure 2.1b).

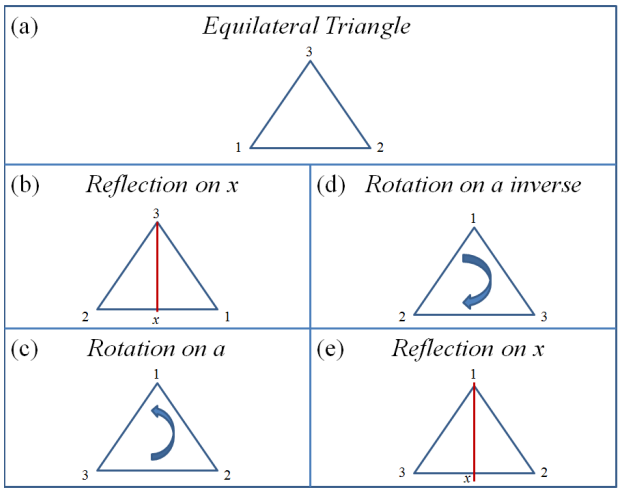


Figure 2.2: $xa = a^{-1}x$

Let us consider Figure 2.2. If we flip along the axis that crosses through the top part of the triangle followed by a rotation counter-clockwise along the center at 120 degrees (Figure 2.2b and Figure 2.2c), we have the same result if we rotate along the center at 120 degrees clockwise followed by a flip through the crosses through the top part of the triangle ($xa = a^{-1}x = a^2x$).

To end with Figure 2.2c or Figure 2.2e of Figure 2.2a, we take the reflection that crosses vertex 2. This axis is called a^2x, as how it is shown in Figure 2.3. Now to obtain axis ax, we start with Figure 2.2a. Then rotate the triangle counter-clockwise along the center at 120 degrees followed by a flip along vertex 2. This gives the same result if we reflect the triangle along vertex 1. The reflections are drawn in Figure 2.3.

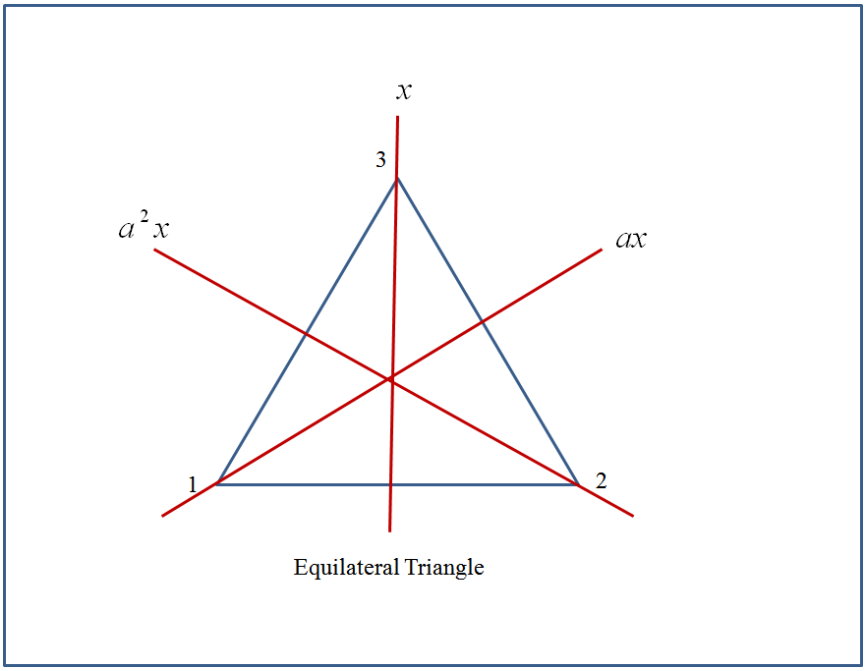


Figure 2.3: Reflections

Now if we rotate the triangle along the center at 360 degrees it is the same as rotating at 0 degrees ($a^3 = e$). Moreover, the 120 degrees rotation and 240 degrees rotation are each other's inverse ($a^2 = a^{-1},\ a = a^{-2}$). Furthermore, each flip is its own inverse ($x^2 = e,\ (ax)^2 = e,\ (a^2x)^2 = e$).

2.2 Cayley Graphs

Let G be a group and $\emptyset \neq S \subseteq G$, then the *Cayley graph*, $C(G, S)$, is a directed graph whose vertices are the group elements of G, and directed edges are (g, gs) for each $s \in S$ and each $g \in G$ [10, 8].

Cayley graphs are high in symmetry and have been used many times to search for DSRGs. Here are references to read more about these graphs [4, 5, 8].

Example

Let $G = D_6$ and $S = \{a, x\}$, and let us construct the Cayley graph with this group.

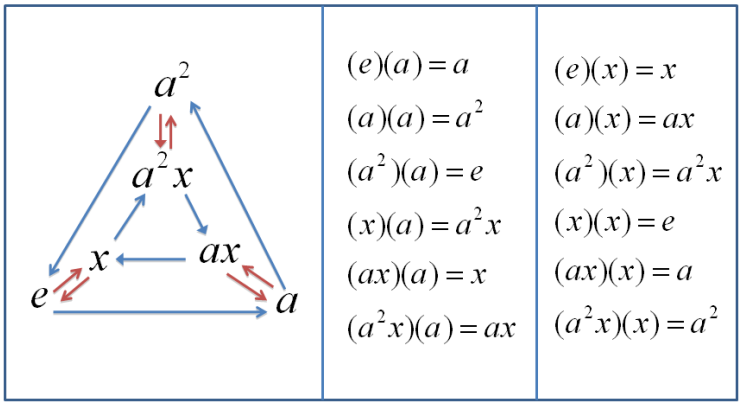


Figure 2.4: Cayley graph over D_6

For a given vertex g, each element of S generates a directed edge from g. Furthermore, since each vertex from the graph has the same in- and out-degree (namely $|S|$), then the Cayley graph is also a regular graph.

2.3 Directed Strongly Regular Graphs

A directed graph, G with v vertices is a *directed strongly regular graph* (*DSRG*) with parameters (v, k, μ, λ, t) [10, 8, 3] if:

1. For every vertex in G, the in-degree and out-degree is equal to k. This means that our graph G is a regular graph.
2. If there is an edge from x to y, then there are λ paths of length two from x to y.
3. If there is not an edge from x to y, then there are μ paths of length two from x to y.
4. There are t paths of length two from vertex x back to itself.

Many DSRGs have been found using different constructions. To see a list of these contructions of DSRGs and nonexistent parameter sets see [5].

A lot has been done with Cayley graphs of dihedral group. Furthermore, many have found DSRGs with these two concepts [4, 5, 8]. Thus, we have also used Dihedral Cayley graphs as our empiricial approach to find our family of DSRGs.

Example

Let us verify that Figure 2.4 is a DSRG with parameters (6, 2, 1, 0, 1) (the parameter set for this example is from [3]).

Since there is a directed edge from e to a, and since $\lambda = 0$, then we will have 0 paths of length two from e to a. Note that by Figure 2.4, the only other vertex e is adjacent to is x, but since $\lambda = 0$ then it will have 0 paths of length two from e to x.

Now let us verify μ paths of length two, and still consider vertex e. Since there is not a directed edge from e to a, and $\mu = 1$, then there exists a path of length two from e to a. This path of length two is from a to a^2 to e.

Considering this further, there isn't an edge from e to a^2x. However $\mu = 1$, which means that the graph should have a path of length two from e to a^2x. This path of length two is from e to a, and from a to a^2x.

Moreover, there isn't an edge from e to ax, but because $\mu = 1$, then our path of length two from e to ax is from e to x, and then from x to ax.

Furthermore, since $t = 1$, then each vertex from the graph should have one path of length two coming back to it. To see this, let us continue to take vertex e. Notice that the only two vertices that are adjacent to vertex e, is vertex x and vertex a. However, since $t = 1$, then there should only be one edge coming back to vertex e. The edge that comes back to e is from vertex x. There is no edge coming back from a. Thus, there is a path of length two from vertex e back to itself from vertex x. Now notice the graph is high in symmetry. Then it is easy to check that any other vertex in G will have λ paths of length two to its neighboring vertices, μ paths of length two with its non-neighboring vertices, and t paths of length two to itself.

Thus, this Dihedral Cayley graph is a DSRG.

2.4 Adjacency Matrix

The *adjacency matrix* A, of a graph G, is a $v \times v$ $(0,1)$-matrix (matrix of 0's and 1's) such that the (i,j)- entry is 1 if there is an edge from v_i to v_j, and 0 if there is not an edge from v_i to v_j [3].

Let J be a $v \times v$ matrix whose entires are 1's, and I the identity matrix. Then if A^2 counts paths of length two from v_1 to v_2 [3, 9], and there is a directed edge from v_1 to v_2, then there are λ paths of length two from v_1 to v_2 contributing to λA in equation 2.2. Moreover, if $v_1 \not\to v_2$, then there are μ paths of length two from v_1 to v_2 contributing to $\mu\,(J - I - A)$ in equation 2.2, where $(J - I - A)$ is the compliment of A. Furthermore, choosing v_1, it has t paths of length two back to itself, which contributes to tI. Then a graph is a (v,k,t,λ,μ)-DSRG whose adjacency matrix A satisfies

$$\begin{aligned} A^2 &= tI + \lambda A + \mu(J - I - A) \\ AJ &= JA = kJ, \end{aligned} \tag{2.2}$$

and with a little bit of algebra, we have the following equivalent matrix equation

$$\begin{gathered} A^2 + (\mu - \lambda)A - (t - \mu)I = \mu J \\ AJ = JA = kJ. \end{gathered} \tag{2.3}$$

Example

Let us use Figure 2.4, since it is a (6, 2, 1, 0, 1)-DSRG and $S = \{a, x\}$. Then the adjacency matrix, A, is

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Figure 2.5: Adjacency matrix of a dihedral Cayley DSRG when $n = 3$

Notice that each entry of Figure 2.5 corresponds with whether we have an edge from one vertex to another. For example, since there is a directed edge from e to a, then we have a 1 in entry position $(1, 2)$, and since we are not considering loops, then we have 0's along the diagonal.

Now that we have the adjacency matrix A of our DSRG, we can check A with the matrix equation (it is the matrix definition version of the defintion of a DSRG). It follows

$$A^2 = tI + \lambda A + \mu(J - I - A).$$

$$A^2 = 1I + 0A + 1(J - I - A).$$

$$A^2 + A = J$$

and

$$AJ = JA = 2J.$$

Notice, it is easy to work with these equations, ans so we have used this approach with the computer program Mathematica as we searched for DSRGs.

Chapter 3

In Search For Cayley Set S

We were in search for a Cayley set S that satisfied the definition of a DSRG, and did so through a careful search to see how many rotations and reflections set S needed, in order to have a possible dihedral Cayley DSRG. We let p repesent the number of reflections, and q the number of rotations in S. So, by knowing how our Cayley set S needs to look, will allow us to further refine the computer search by adding this restriction along with what k, λ, μ, and t are.

3.1 Paths of Length Two from e to a Rotation

The first thing we did was look at the number of ways we can have a rotation and a reflection. We came up with the following ways to count paths of length two from e to a rotation, and from e to some reflection.

If we use a rotation followed by another rotation from set S, then the number of paths of length two from e to some rotation is q^2. We also end with a rotation, if we start with a reflection followed by another reflection. This gives p^2 paths of length two. So, the total count of paths of length two from e to some rotation is

$$q^2 + p^2. \tag{3.1}$$

There are n rotations and n reflections. Now let $A = \{a_1, a_2, \ldots, a_q\}$ be the set of rotations that e is adjacent to (see Figure 3.1). Then there are λ paths of length two from e to each vertex in A. So, we have $q\lambda$ paths of length two from e to a, where $a \in A$.

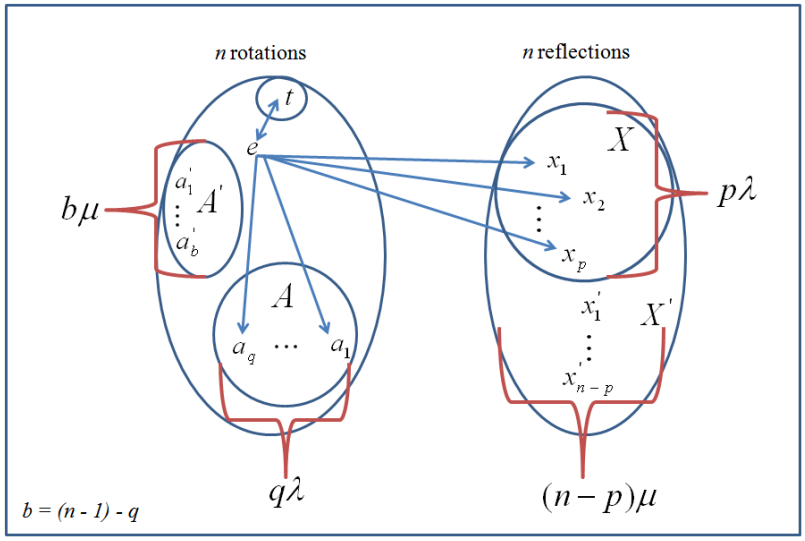


Figure 3.1: Paths of length two from the identity to rotations and reflections

Let $A' = \left\{a'_1, a'_2, \ldots, a'_{(n-1)-q}\right\}$ be the set of rotations that e is not adjacent to, since A' has (n - 1) $-$ q elements. This implies, for each vertex that e is *not* adjacent to will have μ paths of length two to that vertex in A'. So, we have $((n-1)-q)\,\mu$ paths of length two from e to a', where $a' \in A'$. Finally, since we also have t paths of length two from a given vertex back to itself, then e will have t paths of length two back to itself.

Thus, the three possible ways of having paths of length two from e to a rotation give a total of

$$((n-1)-q)\mu + q\lambda + t \tag{3.2}$$

paths of length two from e to a rotation. Note that (3.1) and (3.2) both give the same count of paths of length two from e to a rotation. So, it follows

$$((n-1)-q)\mu + q\lambda + t = p^2 + q^2 \tag{3.3}$$

3.2 Paths of Length Two From *e* to a Reflection

We came up with the following ways to count paths of length two from e to a reflection. If we start with e from S and want to end with a reflection from G, then we can have a

rotation first followed by a reflection to end with a reflection. On the other hand, we can start with a reflection followed by a rotation to have a reflection. Then the number of ways to have a reflection from e is

$$2pq \tag{3.4}$$

Let us consider a different way of having paths of length two from e to a reflection. Note that there are n rotations and n reflections. Let $X = \{x_1, x_2, \ldots, x_i, \ldots, x_p\}$ be the set of reflection e is adjacent to. Then there are λ paths of length two from e to each vertex in X. So, we have $p\lambda$ paths of length two from e to x, where $x \in X$.

Let $X' = \left\{x'_1, x'_2, \ldots, x'_{(n-p)}\right\}$ be the set of reflections that e is not adjacent to. Then, for each vertex that e is *not* adjacent to will have μ paths of length two to that vertex in X'. So, we have $(n-p)\,\mu$ paths of length two from e to x', where $x' \in X'$. Thus, the two possible ways of having paths of length two from e to a reflection give a total of

$$(n-p)\,\mu + p\lambda. \tag{3.5}$$

Since both (3.4) and (3.5) count the same number of paths of length two from e to a reflection, then it follows

$$(n-p)\,\mu + p\lambda = 2pq. \tag{3.6}$$

3.3 Dihedral Cayley Set S

So equations (3.3) and (3.6) tells us how many rotations and reflections set S needs in order to have a possible DSRG. Moreover this observation adds an additional restriction to the computer search for the family of Dihedral Cayley DSRGs. Two examples are provided below to see how this analysis works.

Example 1

Consider a Dihedral Cayley Graph on six vertices, and show that in order for it to be a DSRG with parameters $(12, 4, 2, 0, 2)$, S needs to have two rotations and two reflections.

$$p + q = 4 \tag{3.7}$$

$$12 - 2p = 2pq \tag{3.8}$$

$$12 - 2q = p^2 + q^2 \tag{3.9}$$

The only solution set that satisfies all three equations are $p = q = 2$ (Solution set $q = 1$ and $p = 3$ gives a contradiction making $t > 2$). Thus, S will have two rotations and reflections, in order to have a possible DSRG.

Example 2

Now consider a Dihedral Cayley Graph on 28 vertices and use the analysis to see what S needs to be to have a DSRG with parameters (28, 7, 2, 1, 2). This can be a possible Dihedral Cayley DSRG. Notice $t = 2$. Then we have at most two reflections, since t is defined as a vertex having a path of length two back to itself. This means that five rotations cannot be inverses of each other. We have $n = 14, k = 7, t = 2, \lambda = 1, \mu = 2$. Then using equations (3.3) and (3.6), we have

$$p + q = 7 \tag{3.10}$$

$$28 - p = 2pq \tag{3.11}$$

$$28 - q = p^2 + q^2 \tag{3.12}$$

The only solution to this system of equations is when $q = 3$ and $p = 4$, but since $p \leq 2$, we do not have a DSRG with these parameters.

3.4 Parameters

Let the parameter set be $(4w + 2,\ 4w,\ 2w, 2w - 2, 2w)$ and w a natural number. Now, in order to have a possible DSRG, $2w$ rotations and $2w$ reflections in S are needed. In total, we have $\binom{4w+2}{2w}$ ways to choose $2w$ reflections, and $\binom{4w+2}{2w}$ ways to choose $2w$ rotations, and together $\binom{4w+2}{2w}\binom{4w+2}{2w} = y$ Cayley sets S.

However, some of these y sets have at least one rotation joined with its inverse causing $t > 2w$. So, we narrow the search by considering the rotations. Since $t = 2w$, implies we use at most $2w$ reflections, which we do, and as a result will have no more elements with their inverses in set S.

Furthermore, since $n = 4w + 2$, then we have rotations $a,\ \ldots,\ a^{4w+1}$. Note that e is not included, and a^{2w+1} is its own inverse. So we do not include e and a^{2w+1} in the count. Now pair the rotations with their inverse, and have

$$\left\{a,\ a^{4w+1}\right\},\ \left\{a^2,\ a^{4w}\right\},\ \left\{a^3,\ a^{4w-1}\right\}, \ldots,\ \left\{a^{2w},\ a^{2w+2}\right\}. \tag{3.13}$$

Then selecting one element from $\{a,\ a^{4w+1}\}$, one element from $\{a^2,\ a^{4w}\}$, one element from $\{a^3,\ a^{4w-1}\}$, and continuing with this pattern, one element from $\{a^{2w},\ a^{2w+2}\}$ implies there are two ways to choose an element from each set. Since each set is independent, then we have 2^{2w} ways to choose $2w$ rotations. So we narrow the search to $2^{2w}\binom{4w+2}{2w} = y'$ Dihedral Cayley sets S to test in the computer search.

The significance about y' is each one of these sets will *not* have a rotation joined with its inverse. This is a more sufficient search for a possible Dihedral Cayley DSRG verses y because y has sets that *will* have at least one rotation joined with its inverse forcing $t > 2w$. Let us consider $\binom{4w+2}{2w}$ and 2^{2w}. We know $\binom{4w+2}{2w}$ dominates 2^{2w} and as a consequence,

$\binom{4w+2}{2w}\binom{4w+2}{2w}$ will dominate $2^{2w}\binom{4w+2}{2w}$. This makes $2^{2w}\binom{4w+2}{2w}$ a more efficient search for a possible Dihedral Cayley DSRG.

We have used this approach with many different parameter sets from website [5]. The parameter sets in Table 3.1 satisfy the p and q test. The parameter sets with $v = 12,\ 16,\ \ldots,\ 4z$, where $z \geq 5$, do not give a DSRG in the computer search, whereas Table 3.2 and Table 3.3, is a list of parameter sets that give a family of DSRGs, (these two tables are subsets of Table 3.1, when z is odd).

Table 3.1: Parameters that satisfied the $p,\ q$ test.

v	n	k	t	λ	μ	p	q
12	6	4	2	0	2	2	2
16	8	6	3	1	3	3	3
20	10	8	4	2	4	4	4
24	12	10	5	3	5	5	5
28	14	12	6	4	6	6	6
32	16	14	7	5	7	7	7
36	18	16	8	6	8	8	8
			$\vdots$				
$4z$	$2z$	$2z-2$	$z-1$	$z-3$	$z-1$	$z-1$	$z-1$

Table 3.2: Family of DSRGs, when $z \geq 3$, and when $z = 2w + 1$

v	n	k	t	λ	μ	p	q
12	6	4	2	0	2	2	2
20	10	8	4	2	4	4	4
28	14	12	6	4	6	6	6
36	18	16	8	6	8	8	8
44	22	20	10	8	10	10	10
52	26	24	12	10	12	12	12
				$\vdots$			
$4z$	$2z$	$2z-2$	$z-1$	$z-3$	$z-1$	$z-1$	$z-1$

Table 3.3: Family of DSRGs, when w is a natural

v	n	k	t	λ	μ	p	q
12	6	4	2	0	2	2	2
20	10	8	4	2	4	4	4
28	14	12	6	4	6	6	6
36	18	16	8	6	8	8	8
44	22	20	10	8	10	10	10
52	26	24	12	10	12	12	12
				$\vdots$			
$8w+4$	$4w+2$	$4w$	$2w$	$2w-2$	$2w$	$2w$	$2w$

Example

Consider parameter set (10, 8, 4, 2, 4) from Table 3.2 and go through the steps in search for DSRGs. Now to have a possible DSRG, $p = 4$ and $q = 4$. This means that we will need four rotations and four reflections in S. In total, we have $\binom{10}{4}$ ways to choose four reflections, and $\binom{10}{4}$ ways to choose four rotations, having a total of $\binom{10}{4}\binom{10}{4} = 44,100$ Cayley sets S.

As an observation, in this count, there will be many sets S that will have at least one rotation joined with its inverse causing $t > 4$. So, we narrow the search by taking the rotations into consideration. Since $t = 4$, this means that we use exactly four reflections, this way we know that we will not use an element with its inverse.

Since $n = 10$, then we have rotations $a,\ \ldots,\ a^9$. Note that e and a^5 are not included in the count. Now, pairing the rotations with their inverse, we have

$$\left\{a,\ a^9\right\},\ \left\{a^2,\ a^8\right\},\ \left\{a^3,\ a^7\right\},\ \left\{a^4,\ a^6\right\}. \tag{3.14}$$

So, choosing one element from $\{a,\ a^9\}$, one element from $\{a^2,\ a^8\}$, one element from $\{a^3,\ a^7\}$, and one element from $\{a^4,\ a^6\}$ implies that there are two ways to choose an element from the first set, two ways to choose an element from the second set, two ways to choose an element from the third set, and two ways to choose an element from the fourth set. Moreover, since each pair is independent, then we have 2^4 ways to have four rotations. So, we have narrowed the search to $2^4\binom{10}{4} = 3360$ dihedral Cayley sets S to test in the computer search.

The 3360 Dihedral Cayley sets S will *not* have a rotation joined with its inverse, which makes this into a more sufficient search for a possible Dihedral Cayley DSRG verses the 44,100 Cayley sets S. The 44,100 Cayley sets S have 40,740 sets that *have* at least one rotation joined with its inverse causing $t > 4$.

Table 3.3 gives a small list of DSRGs from the computer search for parameter set (10, 8, 4, 2, 4). A pdf of DSRGs from the computer search is provided in the appendix section.

Table 3.4: Dihedral Cayley DSRGs

Parameter Set (10, 8, 4, 2, 4)	
$\{a, a^2, a^6, a^7, x, ax, a^5x, a^6x\}$	$\{a, a^2, a^6, a^7, x, a^4x, a^5x, a^9x\}$
$\{a, a^2, a^6, a^7, a^3x, a^4x, a^8x, a^9x\}$	$\{a, a^3, a^6, a^8, x, a^2x, a^5x, a^7x\}$
$\{a, a^3, a^6, a^8, ax, a^4x, a^6x, a^9x\}$	$\{a, a^3, a^6, a^8, a^2x, a^4x, a^7x, a^9x\}$
$\{a^2, a^4, a^7, a^9, ax, a^3x, a^6x, a^8x\}$	$\{a^2, a^4, a^7, a^9, ax, a^4x, a^6x, a^9x\}$
$\{a^3, a^4, a^8, a^9, x, a^4x, a^5x, a^9x\}$	$\{a^3, a^4, a^8, a^9, ax, a^2x, a^6x, a^7x\}$

3.5 Previously Found Results

In this section we briefly give a summary of past results done with Cayley graphs over dihedral groups.

Letting n be odd, [11, 4, Lemma 6.1] found dihedral Cayley DSRGs with parameters $(2n, n-1+\epsilon, \frac{n-1}{2}+\epsilon, \frac{n-1}{2}+\epsilon, \frac{n-3}{2}+\epsilon)$, where $\epsilon \in \{0,\ 1\}$. In the case when n even, [4] found dihedral Cayley DSRGs with parameters $(2n,\ n-1, \frac{n}{2},\ \frac{n}{2}-1,\ \frac{n}{2}-1)$. The conditions for these two lemmas are found in [4, p. 97 - 99]. Moreover examples and summary table of these results, are provided in [4, p. 106 - 111].

Motivated by [4], S. A. Hobart and T. J. Shaw found if n is even and

$$S = \left\{a, a^2 \ldots, a^{\frac{n}{2}-1}, x, xa, \ldots, xa^{\frac{n}{2}-1}\right\},$$

then the dihedral Cayley graph is a $(2n, n-1, \frac{n}{2}, \frac{n}{2}-1, \frac{n}{2}-1)$ - DSRG, where x is a reflection and a a rotation. Also [8] mentions if n is odd and $S = \left\{a, a^2 \ldots, a^{\frac{n-1}{2}}, x, xa, \ldots, xa^{\frac{n-1}{2}}\right\}$, then we have dihedral Cayley DSRGs that are found in [11].

Chapter 4

Main Result

The following result is a theorem about the existence of an infinite family of dihedral Cayley DSRGs with parameters in terms of w. This chapter is devoted to the neccessary lemmas verifying that there are λ paths of length two from the identity to elements in S, there are μ paths of length two from the identity to elements in S, and that there are t paths of length two from e back to itself, but the proof of the main result is found in Section 4.4.

Theorem 1. *Let* $n = 4w + 2,\ w \geq 1,\ G = D_{2n}$, *and take* $U_1 = \{a^i \colon 1 \leq i \leq w\}$, $U_2 = \{a^i \colon 2w+2 \leq i \leq 3w+1\}$, $U_3 = \{a^i x \colon 0 \leq i \leq w-1\}$, $U_4 = \{a^i x \colon 2w+1 \leq i \leq 3w\}$, *and also let* $S = \cup_{i=1}^{4} U_i$. *Then* $C(D_{2n},\ S)$ *is a* $(8w+4,\ 4w,\ 2w,\ 2w-2,\ 2w)$*-DSRG.*

C. D. Godsil, S. A. Hobart, and W. J. Martin have found graphs with these parameters, but they were not dihedral Cayley graphs [2].

4.1 Verifying that there are λ paths of length two from e to elements in S

We verify in this section that there are λ paths of length two from the identity to each element in S. The proof is divided into eight lemmas, where each lemma has four cases. We verify in lemmas 1, 3, 5, and 7 that the elements from these lemmas are the only list of elements that give $s \in S$, and verify in lemmas 2, 4, 6, and 8 that the elements from these lemmas do not give $s \in S$.

4.1.1 Finding the λ paths of length two from e to elements in U_1

Lemma 1. *Take $a^r \in U_1$, then the sum of the following paths of length two to a^r is λ.*

Case 1 Let $g = a^p x \in U_3$ and $h = a^q x \in U_3$ where $q = p - r$. Then $gh = a^r$ is a path of length two to a^r if and only if $p \in [r, w-1]$. So the complete list is

$$(a^r x)\,(a^0 x), \ldots, , (a^p x)\,(a^{p-r} x) \ldots \left(a^{w-1} x\right)\,(a^{(w-1-r} x).$$

The total count is $w - r$. If $r = w$, then we have an empty list.

Case 2 Let $g = a^p x \in U_4$ and $h = a^q x \in U_4$ where $q = p - r$. Then $gh = a^r$ is a path of length two to $a^r \in U_1$ if and only if $p \in [r + 2w + 1, 3w]$. Hence the complete list is

$$\left(a^{r+2w+1} x\right)\,(a^{2w+1} x), \ldots, (a^p x)\,(a^{p-r} x), \ldots, \left(a^{3w} x\right)\,(a^{3w-r} x).$$

The total count is $w - r$. If $r = w$, then we have an empty list.

Case 3 Let $g = a^p \in U_1$ and $h = a^q \in U_1$ where $q = r - p$. Then $gh = a^r$ is a path of length two to $a^r \in U_1$ if and only if $p \in [1, r-1]$. So the complete list is

$$(a)\left(a^{r-1}\right), \ldots, (a^p)\,(a^{r-p}), \ldots, \left(a^{r-1}\right)(a)\,.$$

The total count is $r - 1$. If $r = 1$, then we have an empty list.

Case 4 Let $g = a^p \in U_2$ and $h = a^q \in U_2$ where $q = r + n - p$. Then $gh = a^r$ is a path of length two to $a^r \in U_1$ if and only if $p \in [2w + 2, r + 2w]$. So,the complete list is

$$\left(a^{2w+2}\right)\left(a^{r+2w}\right), \ldots, (a^p)\,(a^{r+n-p}), \ldots, \left(a^{r+2w}\right)\left(a^{2w+2}\right).$$

The total count is $r - 1$. If $r = 1$, then we have an empty list.

By inspection, we have $2(w-r)+2(r-1)=2w-2=\lambda$.

Proof. Now, we will show that each one of these cases of elements are the only list of elements that give us $a^r \in U_1$.

Consider Case 1 and take $g, h \in U_3$ where $g = a^p x$ and $h = a^q x$. Note that $0 \leq p \leq w-1$ and $0 \leq q \leq w-1$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.1}$$

Now, suppose by way of contradiction $p \notin [r, w-1]$. So, $p < r$ or $p > w-1$. Since $p \in U_3$, then $p \not> w-1$, so $p < r$ and so $p \leq r-1$. Since $a^q x \in U_3$, then $q \geq 0$. It follows

$$p - q \leq (r-1) - 0 < r. \tag{4.2}$$

Now notice that $p \geq 0$ and $q \leq w-1$. Since also $w \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq 0 - (w-1) = -w+1 > -3w-2 = w - (4w+2) \geq r - n. \tag{4.3}$$

Hence, combining (4.2) and (4.3), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.1). Hence, this completes Case 1.

Consider Case 2 and take $g, h \in U_4$ where $g = a^p x$ and $h = a^q x$. Note that $2w+1 \leq p \leq 3w$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.4}$$

Now, suppose by way of contradiction $p \notin [r+2w+1, 3w]$. So, $p < r+2w+1$ or $p > 3w$. Since $p \in U_4$, then $p \not> 3w$, so $p < r+2w+1$ and so $p \leq r+2w$. Since $a^q x \in U_4$, then $q \geq 2w+1$. It follows

$$p - q \leq (r+2w) - (2w+1) = r - 1 < r. \tag{4.5}$$

Now notice that $p \geq 2w+1$ and $-q \geq -3w$. Since also $w \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+1) - 3w = -w+1 > -3w-2 = w - (4w+2) \geq r - n. \tag{4.6}$$

Hence, combining (4.5) and (4.6), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.4). Hence, this completes Case 2.

Consider Case 3 and take $g, h \in U_1$ where $g = a^p$ and $h = a^q$. Note that $1 \leq p \leq w$ and $1 \leq q \leq w$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.7}$$

Now, suppose by way of contradiction $p \notin [1, r-1]$. So, $p < 1$ or $p > r - 1$. Since $p \in U_1$, then $p \not< 1$, so $p > r - 1$ and so $p \geq r$. Since $a^q \in U_1$, then $q \geq 1$. It follows

$$p + q \geq r + 1 > r. \tag{4.8}$$

Now notice that $p \leq w$ and $q \leq w$. Since also $w \geq r,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \leq w + w = 2w < 5w + 2 = w + (4w + 2) \leq r + n. \tag{4.9}$$

Hence, combining (4.8) and (4.9), $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.7). Hence, this completes Case 3.

Consider Case 4 and take $g, h \in U_2$ where $g = a^p$ and $h = a^q$. Note that $2w + 2 \leq p \leq 3w + 1$ and $2w + 2 \leq q \leq 3w + 1$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.10}$$

Now, suppose by way of contradiction $p \notin [2w + 2, r + 2w]$. So, $p < 2w + 2$ or $p > r + 2w$. Since $p \in U_2$, then $p \not< 2w + 2$, so $p > r + 2w$ and so $p \geq r + 2w + 1$. Since $a^q \in U_1$, then $q \geq 2w + 2$. It follows

$$p + q \geq (r + 2w + 1) + (2w + 2) = r + (4w + 2) + 1 > r + n \tag{4.11}$$

Now notice that $p \leq 3w + 1$ and $q \leq 3w + 1$. Since also $w \geq r,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \leq (3w + 1) + (3w + 1) = 6w + 2 < 9w + 4 = w + 2(4w + 2) \leq r + 2n. \tag{4.12}$$

Hence, combining (4.11) and (4.12), $r + n < p + q < r + 2n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.10). Hence, this completes Case 4. □

4.1.2 There are no other paths of length two from e to elements in U_1

Lemma 2. *The elements listed in Lemma 1 are the only paths of length two from e to elements in U_1.*

Proof. We now check the cases that do not give λ paths of length two from e to $a^r \in U_1$. They are the following.

Let $g \in U_4$ and $h \in U_3$ where $g = a^p x$ and $h = a^q x$. Note that $2w+1 \leq p \leq 3w$ and $0 \leq q \leq w-1$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.13}$$

Since $a^p x \in U_4$, then $p \leq 3w$. Moreover, since $a^q x \in U_3$, then $q \geq 0$. It follows

$$p - q \leq 3w - 0 = 3w < w + (4w+2) = r + n. \tag{4.14}$$

On the other hand, $p \geq 2w+1$ and $q \leq w-1$. Since also $r \leq w,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+1) - (w-1) = w + 2 > 1 \geq r. \tag{4.15}$$

Hence, combining (4.14) and (4.15) give us $r < p - q < r + n$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.13). This completes this case.

Let $g \in U_3$ and $h \in U_4$ where $g = a^p x$ and $h = a^q x$. Note that $0 \leq p \leq w-1$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.16}$$

Since $a^p x \in U_3$, then $p \leq w-1$. Moreover, since $a^q x \in U_4$, then $q \geq 2w+1$. It follows

$$p - q \leq w - 1 - (2w+1) = -w - 2 < w \leq r. \tag{4.17}$$

Also, $p \geq 0$ and $q \leq 3w$. Since also $r \leq w,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq 0 - 3w > -3w - 2 = w - (4w+2) \geq r - n. \tag{4.18}$$

Hence, combining (4.17) and (4.18) give us $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.16). This completes this case.

Now let $g \in U_1$ and $h \in U_2$ where $g = a^p$ and $h = a^q$. Note that $1 \leq p \leq w$ and $2w + 2 \leq q \leq 3w + 1$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.19}$$

Since $a^p \in U_1$, then $p \leq w$. Moreover, since $a^q \in U_2$, then $q \leq 3w + 1$. It follows

$$p + q \leq w + (3w + 1) = 4w + 1 < w + (4w + 2) \leq r + n. \tag{4.20}$$

On the other hand $p \geq 1$ and $q \geq 2w + 2$. Since also $r \leq w,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \geq 1 + (2w + 2) = 2w + 3 > w \geq r. \tag{4.21}$$

Hence, combining (4.20) and (4.21) has $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.19). This completes this case.

Now let $g \in U_2$ and $h \in U_1$ where $g = a^p$ and $h = a^q$. Note that $1 \leq q \leq w$ and $2w + 2 \leq p \leq 3w + 1$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.22}$$

Note that since we are still considering elements from U_1 and from U_2, we are still using the same rotation elements as in the previous case. This means that the proof for this case is the same proof as in the previous case. Hence $p + q \not\equiv r \pmod{n}$, which contradicts (4.22). This completes this case.

Thus, this shows that each one of the cases provided in Lemma 1 are the only set of elements that give $a^r \in U_1$. □

4.1.3 Finding the λ paths of length two from e to elements in U_2

Lemma 3. *Now let us take $a^r \in U_2$ and integer p, then the sum of the following counts of paths of length two to a^r is λ.*

Case 1 Let $g = a^p x \in U_4$ and $h = a^q x \in U_3$ where $q = p - r$. Then $gh = a^r$ is a path of length two to $a^r \in U_2$ if and only if $p \in [r, 3w]$. So the complete list is

$$(a^r x)(a^0 x), \ldots, (a^p x)(a^{p-r} x), \ldots, (a^{3w} x)(a^{3w-r} x).$$

The total count is $3w - r + 1$. Note that if $r = 3w + 1$, then we have an empty list.

Case 2 Let $g = a^p x \in U_3$ and $h = a^q x \in U_4$ where $q = p - r + n$. Then $gh = a^r$ is a path of length two to $a^r \in U_2$ if and only if $p \in [r - 2w - 1, w - 1]$. The complete list is

$$(a^{r-2w-1} x)(a^{2w+1} x), \ldots, (a^p x)(a^{p-r+n} x), \ldots, (a^{w-1} x)(a^{5w-r+1} x).$$

The total count is $3w - r + 1$. If we take $r = 3w + 1$, then we will have an empty list.

Case 3 Let $g = a^p \in U_2$ and $h = a^q \in U_1$ where $q = r - p$. Then $gh = a^r$ is a path of length two to $a^r \in U_2$ if and only if $p \in [r - 1, 2w + 2]$. Hence the complete list is

$$(a^{r-1})(a), \ldots, (a^p)(a^{r-p}), \ldots, (a^{2w+2})(a^{r-2w-2}).$$

The total count is $r - 2w - 2$. If we choose $r = 2w + 2$, then we will have an empty list.

Case 4 Let $g = a^p \in U_1$ and $h = a^q \in U_2$ where $q = r - p$. Then $gh = a^r$ is a path of length two to $a^r \in U_2$ if and only if $p \in [1, r - 2w - 2]$. Thus the complete list is

$$(a)(a^{r-1}), \ldots, (a^p)(a^{r-p}), \ldots, (a^{r-2w-2})(a^{2w+2}).$$

The total count is $r - 2w - 2$. if $r = 2w + 2$, then we have an empty list.

Notice that by inspection, we have $2(3w - r + 1) + 2(r - 2w - 2) = 2w - 2 = \lambda$.

Proof. Now, we will show that each one of these cases of elements are the only list of elements that give us $a^r \in U_2$.

Consider Case 1 and let $g \in U_4$ and $h \in U_3$ where $g = a^p x$ and $h = a^q x$. Note that $2w+1 \leq p \leq 3w$ and $0 \leq q \leq w-1$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.23}$$

Now, suppose by way of contradiction $p \notin [r, 3w]$. So, $p < r$ or $p > 3w$. Since $p \in U_4$, then $p \not> 3w$, so $p < r$ and so $p \leq r-1$. Also $q \geq 0$. It follows

$$p - q \leq (r-1) - 0 < r. \tag{4.24}$$

Now notice that $p \geq 2w+1$ and $-q \geq -(w-1)$. Since also $2w+2 \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+2) - (w-1) = w+2 > -w-1 = (3w+1) - (4w+2) \geq r - n. \tag{4.25}$$

Hence, combining (4.25) and (4.24), $r-n < p-q < r$, which means that $p-q \not\equiv r \pmod{n}$, which contradicts (4.23). Hence, this completes Case 1.

Consider Case 2 and take $g \in U_3$ and $h \in U_4$ where $g = a^p x$ and $h = a^q x$. Note that $0 \leq p \leq w-1$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.26}$$

Now, suppose by way of contradiction $p \notin [r-2w-1, w-1]$. So, $p < r-2w-1$ or $p > w-1$. Since $p \in U_3$, then $p \not> w-1$, so $p < r-2w-1$ and thus $p \leq r-2w-2$. Since $a^q x \in U_4$, then $-q \leq -(2w+1)$. It follows

$$p-q \leq (r-2w-2)-(2w+1) = r-4w-3 = r-(4w+2)-1 < r-(4w+2) = r-n. \tag{4.27}$$

Now notice that $p \geq 1$ and $-q \geq -3w$. Since also $3w+1 \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq 1 - 3w > -5w - 3 \geq 3w + 1 - 2(4w+2) \geq r - 2n. \tag{4.28}$$

Hence, combining (4.27) and (4.28), $r - 2n < p - q < r - n$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.26). Hence, this completes Case 2.

Consider Case 3 and take $g \in U_1$ and $h \in U_2$ where $g = a^p$ and $h = a^q$. Note that $1 \leq p \leq w$ and $2w + 2 \leq q \leq 3w + 1$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.29}$$

Now, suppose by way of contradiction $p \notin [1, r - 2w - 2]$. So, $p < 1$ or $p > r - 2w - 2$. Since $p \in U_1$, then $p \not< 1$, so $p > r - 2w - 2$ and so $p \geq r - 2w - 1$. Since $a^q \in U_2$, then $q \geq 2w + 2$. It follows

$$p + q \geq (r - 2w - 1) + (2w + 2) = r + 1 > r. \tag{4.30}$$

Now notice that $p \leq w$ and $q \leq 3w + 1$. Since also $3w + 1 \geq r,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \leq w + (3w + 1) < 6w + 4 = (2w + 2) + (4w + 2) \leq r + n. \tag{4.31}$$

Hence, combining (4.29) and (4.30), $r < p+q < r+n$, which means that $p+q \not\equiv r \pmod{n}$, which contradicts (4.28). Hence, this completes Case 3.

Consider case 4 and take $g = a^p \in U_1$ and $h = a^q \in U_2$ where $q = r - p$. Note that $1 \leq p \leq w$ and $2w + 2 \leq q \leq 3w + 1$. Then we have

$$a^r = hg = (a^q)(a^p) = a^{q+p}. \tag{4.32}$$

Note that since we are using the same rotation elements as in the previous case, then $q + p = p + q$. This means that the proof for this case is the same proof as in the previous case. Hence $p+q \not\equiv r \pmod{n}$, which contradicts (4.32). Hence, this completes case 4. □

4.1.4 There are no other paths of length two from e to elements in U_2

Lemma 4. *The elements listed in Lemma 3 are the only paths of length two from e to elements in U_2.*

Proof. Now we will check the cases that do not give λ paths of length two. They are the following.

Let $g, h \in U_3$ where $g = a^p x$ and $h = a^q x$. Note that $2w+2 \leq r \leq 3w+1$, $0 \leq p \leq w-1$ and $0 \leq q \leq w-1$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.33}$$

Since $a^p x, a^q x \in U_3$, then $p \leq w-1$ and $q \geq 0$. It follows

$$p - q \leq (w-1) - 0 = w - 1 < 2w + 2) \leq r. \tag{4.34}$$

Also we know that $p \geq 0$ and $q \leq w-1$. We also know that $r \leq 3w+1,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq 0 - (w-1) = -w + 1 > -w - 1 = (3w+1) - (4w+2) \geq r - n. \tag{4.35}$$

Hence, (4.35) and (4.34), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which means contradicts (4.33). This completes this case.

Let $g, h \in U_4$ where $g = a^p x$ and $h = a^q x$. Note that $2w+1 \leq p \leq 3w$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.36}$$

Since $a^p x, a^q x \in U_4$, then $p \leq 3w$ and $q \geq 2w+1$. It follows

$$p - q \leq 3w - (2w+1) = w - 1 < 2w + 2 \leq r. \tag{4.37}$$

On the other hand $p \geq 2w+1$ and $q \leq 3w$. Since also $r \leq w,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+1) - 3w = -w + 1 > -2w = (2w+2) - (4w+2) \geq r - n. \tag{4.38}$$

Hence, combining (4.38) and (4.37) we have $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.36). This completes this case.

Let $g \in U_2$ and $h \in U_2$ where $g = a^p$ and $h = a^q$. Note that $2w+2 \leq p \leq 3w+1$ and $2w+2 \leq q \leq 3w+1$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.39}$$

Since $a^p, a^q \in U_2$, then $p \leq 3w+1$ and $q \leq 3w+1$. It follows

$$p+q \leq (3w+1)+(3w+1) = 6w+2 < 7w+3 = (3w+1)+(4w+2) \leq r+n. \tag{4.40}$$

Also $p \geq 2w+2$ and $q \geq 2w+2$. Since also $r \leq 3w+1,\ w \geq 1$, and $n = 4w+2$, we have

$$p+q \geq (2w+2)+(2w+2) = 4w+4 > 2w+2 \geq r. \tag{4.41}$$

Hence, by (4.40) and (4.41), $r < p+q < r+n$, which means that $p+q \not\equiv r \pmod{n}$, which contradicts (4.39). This completes this case.

Let $g, h \in U_1$ where $g = a^p$ and $h = a^q$. Note that $1 \leq p \leq w$ and $1 \leq q \leq w$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.42}$$

Since $a^p, a^q \in U_1$, then $p \leq w$ and $q \leq w$. It follows

$$p+q \leq w+w = 2w < 2w+2 \leq r. \tag{4.43}$$

On the other hand, $p \geq 1$ and $q \geq 1$. Since also $r \leq 2w+2,\ w \geq 1$, and $n = 4w+2$, we have

$$p+q \geq 1+1 = 2 > -2w = 2w+2-(4w+2) \geq r-n. \tag{4.44}$$

Hence, combining (4.43) and (4.44) we have $r-n < p+q < r$, which means that $p+q \not\equiv r \pmod{n}$, which contradicts (4.42). This completes this case.

Thus, this shows that each one of the cases provided in Lemma 3 are the only set of elements that give $a^r \in U_2$. □

4.1.5 Finding the λ paths of length two from e to elements in U_3

Lemma 5. *Take $a^r x \in U_3$, then the sum of the following paths of length two to $a^r x$ is λ.*

Case 1 Let $g = a^p \in U_1$ and $h = a^q x \in U_3$ where $q = r - p$, then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [1, r]$. So the complete list is

$$(a)(a^{r-1}x), \ldots, (a^p)(a^{r-p}x), \ldots, (a^r)(a^0 x).$$

The total count is r. Note that if $r = 0$, then our count is 0. This means that we have an empty list.

Case 2 Let $g = a^p x \in U_3$ and $h = a^q \in U_1$ where $q = p - r$, then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [r + 1, w - 1]$. So the complete list is

$$(a^{r+1}x)(a), \ldots, (a^p x)(a^{p-r}), \ldots, (a^{w-1}x)(a^{w-(r+1)}).$$

The total count is $w - (r + 1)$. If $r = w - 1$, then we have an empty list.

Case 3 Let $g = a^p \in U_2$ and $h = a^q x \in U_4$ where $q = p - r$, then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [2w + 2 + r, 3w]$. So the complete list is

$$(a^{2w+2+r}x)(a^{2w+2}), \ldots, (a^p x)(a^{p-r}), \ldots, (a^{3w}x)(a^{3w-r}).$$

The total count is $w - (r + 1)$. If $r = w - 1$, then we have an empty list.

Case 4 Let $g = a^p \in U_2$ and $h = a^q x \in U_4$ where $q = r - p + n$, then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [2w + 2, r + 2w + 1]$. So the complete list is

$$(a^{2w+2})(a^{r+2w}x), \ldots, (a^p)(a^{r-p+n}x), \ldots, (a^{r+2w+1})(a^{2w+1}x).$$

The total count is r. If $r = 0$, then we have an empty list.

By inspection, we have $2r + 2(w - (r + 1)) = 2w - 2 = \lambda$

Proof. Now, we will show that each one of these cases of elements are the only list of elements that give us $a^r x \in U_3$.

Consider Case 1 and take $g \in U_1$ and $h \in U_3$ where $g = a^p$ and $h = a^q x$. Note that $1 \leq p \leq w$ and $0 \leq q \leq w - 1$. Then we have

$$a^r x = gh = (a^p x)(a^q x) = a^{p+q} x. \tag{4.45}$$

Now, suppose by way of contradiction $p \notin [1, r]$. So, $p < 1$ or $p > r$. Since $p \in U_1$, then $p \not< 1$, so $p > r$ and so $p \geq r + 1$. Since $a^q x \in U_3$, then $q \geq 0$. It follows

$$p + q \geq (r + 1) + 0 > r. \tag{4.46}$$

Now notice that $p \leq w$ and $q \leq w - 1$. Since also $r \geq 0,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \leq w + (w - 1) = 2w - 1 < 4w + 2 \leq r + (4w + 2) = r + n. \tag{4.47}$$

Hence, combining (4.47) and (4.46), $r < p+q < r+n$, which means that $p+q \not\equiv r \pmod{n}$, which contradicts (4.45). Hence, this completes Case 1.

Consider Case 2 and take $g \in U_3$ and $h \in U_1$ where $g = a^p x$ and $h = a^q$. Note that $0 \leq p \leq w - 1$ and $1 \leq q \leq w$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.48}$$

Now, suppose by way of contradiction $p \notin [r + 1, w - 1]$. So, $p < r + 1$ or $p > w - 1$. Since $p \in U_3$, then $p \not> w - 1$, so $p < r + 1$ and so $p \leq r$. Also since $a^q \in U_1$, then $q \geq 1$. It follows

$$p - q \leq r - 1 < r. \tag{4.49}$$

Now notice that $p \geq 0$ and $q \leq w$. Since also $w - 1 \geq r,\ w \geq 1$, and $n = 4w + 2$, we have

$$p - q \geq 0 - w = -w > -3w - 3 = w - 1 - (4w + 2) \geq r - n. \tag{4.50}$$

Hence, combining (4.50) and (4.49), $r-n < p-q < r$, which means that $p-q \not\equiv r \pmod{n}$, which contradicts (4.48). Hence, this completes Case 2.

Consider Case 3 and take $g \in U_4$ and $h \in U_2$ where $g = a^p x$ and $h = a^q$. Note that $2w+1 \leq p \leq 3w$ and $2w+2 \leq q \leq 3w+1$ such that

$$a^r x = gh = (a^p)x(a^q) = a^{p-q}x. \tag{4.51}$$

Now, suppose by way of contradiction $p \notin [2w+2+r, 3w]$. So, $p < 2w+2+r$ or $p > 3w$. Since $p \in U_4$, then $p \not> 3w$, so $p < 2w+2+r$ and so $p \leq 2w+1+r$. Moreover, since $a^q \in U_2$, then $q \geq 2w+2$. Then we have

$$p - q \leq (2w+r+1) - (2w+2) = r - 1 < r. \tag{4.52}$$

Furthermore, notice that $p \geq 2w+1$ and $q \leq 3w+1$. Since also $w-1 \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+1) - (3w+1) = -w > -3w-3 = (w-1) - (4w+2) \geq r - n. \tag{4.53}$$

Hence, combining (4.52) and (4.53), $r-n < p-q < r$, which means that $p+q \not\equiv r \pmod{n}$, which contradicts (4.51). Hence, this completes Case 3.

Consider Case 4 and take $g \in U_2$ and $h \in U_4$ where $g = a^p$ and $h = a^q x$. Moreover, notice that $2w+2 \leq p \leq 3w+1$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r x = gh = (a^p)(a^q)x = a^{p+q}x. \tag{4.54}$$

Now, suppose by way of contradiction $p \notin [2w+2, r+2w+1]$. So, $p < 2w+2$ or $p > r+2w+1$. Since $p \in U_2$, then $p \not< 2w+2$, so $p > r+2w+1$ and $p \geq r+2w+2$. Furthermore, since $a^q x \in U_4$, then $q \geq 2w+1$. It follows

$$p + q \geq (r+2w+2) + (2w+1) = r + (4w+2) + 1 > r + n \tag{4.55}$$

Moreover, notice that $p \leq 3w+1$ and $q \leq 3w$. Also since $w-1 \geq r,\ w \geq 1$, and $n = 4w+2$, then we have

$$p + q \leq (3w+1) + 3w = 6w + 1 < 8w + 2 = 2(4w+2) \leq r + 2n. \tag{4.56}$$

Hence, combining (4.55) and (4.56), $r + n < p + q < r + 2n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.54). Hence, this completes Case 4. □

4.1.6 There are no other paths of length two from e to elements in U_3

Lemma 6. *The elements listed in Lemma 5 are the only paths of length two from e to elements in U_3.*

Proof. Now we will check the cases that do not give λ paths of length two from e to $a^r x$. They are the following.

Let $g \in U_1$ and $h \in U_4$ where $g = a^p$ and $h = a^q x$. Note that $1 \leq p \leq w$ and $2w + 1 \leq q \leq 3w$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.57}$$

Since $a^p \in U_1$, then $p \leq w$. Moreover, since $h \in U_4$, then $q \leq 3w$. It follows

$$p + q \leq w + 3w = 4w < 5w + 1 = (w - 1) + (4w + 2) \leq r + n. \tag{4.58}$$

Also $p \geq 1$ and $q \geq 2w + 1$. Since also $r \leq w - 1,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \geq 1 + (2w + 1) = 2w + 2 > w - 1 \geq r. \tag{4.59}$$

Hence, by (4.58) and (4.59), $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.57). This completes this case.

Now $g \in U_4$ and $h \in U_1$ where $g = a^p x$ and $h = a^q$. Note that $1 \leq q \leq w$ and $2w + 1 \leq p \leq 3w$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.60}$$

Since $g \in U_4$, then $p \leq 3w$. Moreover, since $h \in U_4$, then $q \geq 1$. It follows

$$p - q \leq 3w - 1 < 4w + 2 \leq r + n. \tag{4.61}$$

On the other hand, $q \leq w$ and $p \geq 2w+1$. Since also $r \leq w-1,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+1) - w = w + 1 > w - 1 \geq r. \tag{4.62}$$

Hence, by (4.62) and (4.61), $r < p - q < r + n$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.60). This completes this case.

Let $g \in U_3$ and $h \in U_2$ where $g = a^p x$ and $h = a^q$. Note that $0 \leq p \leq w-1$ and $2w+2 \leq q \leq 3w+1$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.63}$$

Since $g \in U_3$, then $p \leq w-1$. Moreover, since $h \in U_2$, then $q \geq 2w+2$. It follows

$$p - q \leq w - 1 - (2w+2) = -w - 3 < 0 \leq r. \tag{4.64}$$

Also, $p \geq 0$ and $q \leq 3w+1$. Since also $r \leq w-1,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq 0 - (3w+1) = -3w - 1 > -3w - 3 = w - 1 - (4w+2) \geq r - n. \tag{4.65}$$

Hence, combining (4.65) and (4.64) we have $r - n < p - q < r$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.63). This completes this case.

Let $g \in U_2$ and $h \in U_3$ where $g = a^p$ and $h = a^q x$. Note that $2w+2 \leq p \leq 3w+1$ and $0 \leq q \leq w-1$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.66}$$

Since $g \in U_2$, then $p \leq 3w+1$. Moreover, since $h \in U_3$, then $q \leq w-1$. It follows

$$p + q \leq (3w+1) + (w-1) = 4w < 4w + 2 = 0 + (4w+2) \leq r + n. \tag{4.67}$$

On the other hand, we see that $q \geq 0$ and $p \geq 2w+2$. Since also $r \leq w-1,\ w \geq 1$, and $n = 4w+2$, we have

$$p + q \geq (2w+2) + 0 = 2w + 2 > w - 1 \geq r. \tag{4.68}$$

Hence, by (4.67) and (4.68), $r < p+q < r+n$, which means that $p-q \not\equiv r \pmod{n}$, which contradicts (4.66). This completes this case.

Thus, this shows that each one of the cases provided in Lemma 5 are the only set of elements that give $a^r x \in U_3$. □

4.1.7 Finding the λ paths of length two from e to elements in U_4

Lemma 7. *Take $a^r x \in U_4$, then the sum of the following of paths of length two to $a^r x$ is λ.*

Case 1 Let $g = a^p \in U_2$ and $h = a^q x \in U_3$ where $q = r - p$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [r, 2w+2]$. Thus the list complete list is

$$(a^{2w+2})(a^{r-(2w+2)}x), \ldots, (a^p)(a^{r-p}x), \ldots, (a^r)(a^0 x).$$

The total count is $r - 2w - 1$. If $r = 2w+1$, then we have an empty list.

Case 2 Take $g = a^p x \in U_4$ and $h = a^q \in U_1$ with $q = p - r$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [r, 2w+2]$. Then the complete list is

$$(a^{r+1}x)(a), \ldots, (a^p x)(a^{p-r}), \ldots, (a^{3w}x)(a^{3w-r}).$$

The total count is $3w - r$. If $r = -3w$, then we have an empty list.

Case 3 Let $g = a^p \in U_1$ and $h = a^q x \in U_4$ where $q = r - p$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [1, r-(2w+1)]$. Then the complete list is

$$(a)(a^{r-1}x), \ldots, (a^p)(a^{r-p}x), \ldots, (a^{r-(2w+1)})(a^{2w+1}x).$$

The total count is $r - 2w - 1$. If we take $r = 2w+1$, then we will have an empty list.

Case 4 Let $g = a^p x \in U_3$, and $h = a^q \in U_2$ where $q = p - r + n$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [r - 2w, w - 1]$. Then the complete list is

$$(a^{r-2w}x)(a^{2w+2}), \ldots, (a^p x)(a^{p-r+n}), \ldots, (a^{w-1}x)(a^{5w-r+1}).$$

The total count is $3w - r$. If $r = -3w$, then we have an empty list.

So, by inspection, we have $2(3w - r) + 2(r - 2w - 1) = 2w - 2 = \lambda$.

Proof. Now, we will show that each one of these cases of elements are the only list of elements that give us $a^r x \in U_4$.

Consider Case 1 and take $g \in U_2$ and $h \in U_3$ where $g = a^p$ and $h = a^q x$. Note that $2w + 2 \leq p \leq 3w + 1$ and $0 \leq q \leq w - 1$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.69}$$

Now, suppose by way of contradiction $p \notin [2w + 2, r]$. So, $p < 2w + 2$ or $p > r$. Since $g \in U_2$, then $p \not< 2w + 2$, so $p > r$, and so $p \geq r + 1$. Furthermore, since $a^q x \in U_3$, then $q \geq 0$. It follows

$$p + q \geq (r + 1) + 0 > r. \tag{4.70}$$

Now notice that $p \leq 3w + 1$ and $q \leq w - 1$. Since also $r \geq 2w + 2,\ 1 \leq w$, and $n = 4w + 2$, we have

$$p + q \leq (3w + 1) + (w - 1) = 4w < (6w + 2) = (2w + 2) + (4w + 2) \leq r + n. \tag{4.71}$$

Hence, combining (4.71) and (4.70) we have $r < p + q < r + n$, which means $p + q \not\equiv r \pmod{n}$, which contradicts (4.69). Hence, this completes Case 1.

Consider Case 2 and take $g \in U_4$ and $h \in U_1$ where $g = a^p x$ and $h = a^q$. Note that $2w + 1 \leq p \leq 3w$ and $1 \leq q \leq w$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.72}$$

Now, suppose by way of contradiction $p \notin [r+1, 3w]$. So, $p < r+1$ or $p > 3w$. Since $p \in U_4$, then $p \not> 3w$, so $p < r+1$ and so $p \leq r$. Also since $a^q \in U_1$, then $q \geq 1$. It follows

$$p - q \leq r - 1 < r. \tag{4.73}$$

Now notice that $p \geq 2w+1$ and $q \leq 1$. Since also $2w+1 \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+1) - 1 = 2w > -2w - 1 = (2w+1) - (4w+2) \geq r - n. \tag{4.74}$$

Hence, combining (4.73) and (4.74), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.72). Hence, this completes Case 2.

Consider Case 3 and take $g \in U_1$ and $h \in U_4$ where $g = a^p$ and $h = a^q x$. Note that $2w+1 \leq p \leq 3w$ and $2w+2 \leq q \leq 3w+1$ such that

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.75}$$

Now, suppose by way of contradiction $p \notin [1, r-2w-1]$. So, $p < 1$ or $p > r - 2w - 1$. Since $p \in U_1$, then $p \not< 1$, so $p > r - 2w - 1$ and so $p \geq r - 2w$. Moreover, since $a^q \in U_4$, then $q \geq 2w+1$. Then we have

$$p + q \geq (r - 2w) + (2w+1) = r + 1 > r. \tag{4.76}$$

Furthermore, notice that $p \leq 3w$ and $q \leq 3w+1$. Since also $2w+1 \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p + q \leq 3w + (3w+1) = 6w + 1 < 6w + 3 = (2w+1) + (4w+2) \leq r + n. \tag{4.77}$$

Hence, combining (4.76) and (4.77), $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.75). Hence, this completes Case 3.

Consider Case 4 and take $g \in U_3$ and $h \in U_2$ where $g = a^p x$ and $h = a^q$. Moreover, notice that $0 \leq p \leq w - 1$ and $2w+2 \leq q \leq 3w+1$. Then we have

$$a^r x = gh = (a^p)x(a^q) = a^{p-q} x. \tag{4.78}$$

Now, suppose by way of contradiction $p \notin [r-2w, w-1]$. So, $p < r-2w$ or $p > w-1$. Since $p \in U_3$, then $p \not> w-1$, so $p < r-2w$ and hence $p \leq r-2w-1$. Furthermore, since $a^q \in U_2$, then $q \geq 2w+2$. It follows

$$p - q \leq (r-2w-1) - (2w+2) = r - (4w+2) - 1 < r - n \tag{4.79}$$

Moreover, notice that $p \geq 0$ and $q \leq 3w+1$. Also since $2w+1 \geq r,\ w \geq 1$, and $n = 4w+2$, then we have

$$p - q \geq 0 - (3w+1) = -3w - 1 > -5w - 4 = 3w - 2(4w+2) \geq r - 2n. \tag{4.80}$$

Hence, combining (4.80) and (4.79), $r - 2n < p - q < r - n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.78). Hence, this completes Case 4. □

4.1.8 There are no other paths of length two from e to elements in U_4

Lemma 8. *The elements listed in Lemma 7 are the only paths of length two from e to elements in U_4.*

Proof. We now check the cases that do not give λ paths of length two from e to $a^r x \in U_4$. They are the following.

Let $g \in U_1$ and $h \in U_4$ where $g = a^p$ and $h = a^q x$. Note that $1 \leq p \leq w$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.81}$$

Since $a^p \in U_1$, then $p \leq w$. Moreover, since $h \in U_4$, then $q \leq 3w$. It follows

$$p + q \leq w + 3w = 4w < 4w + 2 \leq r + n. \tag{4.82}$$

On the other hand, $p \geq 1$ and $q \geq 2w+1$. Since also $r \leq w-1,\ w \geq 1$, and $n = 4w+2$, we have

$$p + q \geq 1 + (2w + 1) = 2w + 2 > w - 1 \geq r. \tag{4.83}$$

Hence, by (4.82) and (4.83), $r < p+q < r+n$, which means that $p+q \not\equiv r \pmod{n}$, which contradicts (4.81). This completes this case.

Let $g \in U_3$ and $h \in U_1$ where $g = a^p x$ and $h = a^q$. Note that $0 \leq p \leq w-1$ and $1 \leq q \leq w$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.84}$$

Since $g \in U_3$, then $p \leq w - 1$. Moreover, since $h \in U_1$, then $q \geq 1$. It follows

$$p - q \leq (w - 1) - 1 = w - 2 < 2w + 1 \leq r. \tag{4.85}$$

Also, we see that $q \leq w$ and $p \geq 0$. Since also $r \leq 3w,\ w \geq 1$, and $n = 4w + 2$, we have

$$p - q \geq 0 - w = -w > -w - 2 = 3w - (4w + 2) \geq r - n. \tag{4.86}$$

Hence, by (4.86) and (4.85), $r-n < p-q < r$, which means that $p-q \not\equiv r \pmod{n}$, which contradicts (4.84). This completes this case.

Let $g \in U_1$ and $h \in U_3$ where $g = a^p$ and $h = a^q x$. Note that $1 \leq p \leq w$ and $0 \leq q \leq w-1$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.87}$$

Since $g \in U_1$, then $p \leq w$. Moreover, since $h \in U_3$, then $q \leq w - 1$. It follows

$$p + q \leq w + (w - 1) = 2w - 1 < 2w + 1 \leq r. \tag{4.88}$$

On the other hand, it is clear that $q \geq 0$ and $p \geq 1$. Since also $r \leq 3w,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \geq 0 + 1 = 1 > -w - 2 = 3w - (4w + 2) \geq r - n. \tag{4.89}$$

Hence, combining (4.88) and (4.89), $r-n < p+q < r$, which means that $p+q \not\equiv r \pmod{n}$, which contradicts (4.87). This completes this case.

Let $g \in U_4$ and $h \in U_2$ where $g = a^p x$ and $h = a^q$. Note that $2w+1 \leq p \leq 3w$ and $2w+2 \leq q \leq 3w+1$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.90}$$

Since $g \in U_4$, then $p \leq 3w$. Moreover, since $h \in U_2$, then $q \geq 2w+2$. It follows

$$p - q \leq 3w - (2w+2) = w - 2 < 2w + 1 \leq r. \tag{4.91}$$

Also, we know that $q \leq 3w+1$ and $p \geq 2w+1$. Since also $r \leq 3w,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+1) - (3w+1) = -w > -w - 2 = 3w - (4w+2) \geq r - n. \tag{4.92}$$

Hence, combining (4.91) and (4.92), $r-n < p-q < r$, which means that $p-q \not\equiv r \pmod{n}$, which contradicts (4.90). This completes this case.

Let $g \in U_2$ and $h \in U_4$ where $g = a^p$ and $h = a^q x$. Note that $2w+2 \leq p \leq 3w+1$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.93}$$

Since $g \in U_2$, then $p \leq 3w+1$. Moreover, since $h \in U_4$, then $q \leq 3w$. It follows

$$p + q \leq (3w+1) + 3w = 6w + 1 < 7w + 2 \leq 3w + (4w+2) \leq r + n. \tag{4.94}$$

On the other hand, we see that $q \geq 2w+1$ and $p \geq 2w+2$. Since also $r \leq 3w,\ w \geq 1$, and $n = 4w+2$, we have

$$p + q \geq (2w+2) + (2w+1) = 4w + 3 > 3w \geq r. \tag{4.95}$$

Hence, combining (4.94) and (4.95), $r < p+q < r+n$, which means that $p+q \not\equiv r \pmod{n}$, which contradicts (4.93). This completes this case.

Thus, this shows that each one of the cases provided in Lemma 7 are the only set of elements that give $a^r x \in U_4$.

Therefore, we have λ paths of length two from e to each element in S. □

4.2 Verifying that there are μ paths of length two from e to elements in S'

Lemma 9 defines the following set of elements that are not in S. We use this lemma to proof Theorem 1 in the following lemmas of this section.

Lemma 9. *Using the notation from Theorem 1, let* $U_1' = \{a^i \colon w+1 \leq i \leq 2w+1\}$, $U_2' = \{a^i \colon 3w+2 \leq i \leq 4w+1\}$, $U_3' = \{a^i x \colon w \leq i \leq 2w\}$, $U_4' = \{a^i x \colon 3w+1 \leq i \leq 4w+1\}$ *so that* $S' = \cup_{i=1}^{4} U_i'$. *Then these elements are not in* S.

We verify in this section μ paths of length two from e to each element in S' using elements from S. The proof is divided into eight lemmas, where each lemma has four cases. We verify in lemmas 9, 11, 13, and 15 that the elements from these lemmas are the list of elements that give $s' \in S'$. We verify in lemmas 10, 12, 14, and 16 that the elements from these lemmas do not give $s' \in S'$.

4.2.1 Finding the μ paths of length two from e to elements in U_1'

Lemma 10. *Take* $a^r \in U_1'$ *where* $w+1 \leq r \leq 2w+1$. *Then the sum of the following paths of length two to* a^r *is* μ

Case 1 Let $g = a^p \in U_1$ and $h = a^q \in U_1$ where $q = r - p$. Then, $gh = a^r$ is a path of length two to $a^r \in U_1'$ if and only if $p \in [r-w, w]$. The complete list is

$$(a^{r-w})(a^w), \ldots, (a^p)(a^{r-p}), \ldots, (a^w)(a^{r-w}).$$

The total count is $2w - r + 1$. If $r = 2w+1$, then we will have an empty list.

Case 2 Let $g = a^p \in U_2$ and $h = a^q \in U_2$ where $q = r + n - p$. Then $gh = a^r$ is a path of length two to $a^r \in U_2'$ if and only if $p \in [r+w+1, 3w+1]$. The complete list is

$$(a^{r+w+1})(a^{3w+1}), \ldots, (a^{p})(a^{r+n-p}), \ldots, (a^{3w+1})(a^{r+w+1}).$$

The total count is $2w - r + 1$. If $r = 2w + 1$, then we will have an empty list.

Case 3 Let $g = a^p x \in U_4$ and $h = a^q x \in U_3$ where $q = p - r$. Then $gh = a^r$ is a path of length two to $a^r \in U_1'$ if and only if $p \in [2w + 1, r + w - 1]$. The complete list is

$$(a^{2w+1}x)(a^{2w+1-r}x), \ldots, (a^{p}x)(a^{p-r}x), \ldots, (a^{r+(w-1)}x)(a^{w-1}x).$$

The total count is $r - w - 1$. If $r = w + 1$, then we will have an empty list.

Case 4 Let $g = a^p x \in U_3$ and $h = a^q x \in U_4$ where $q = p - r + n$. Then $gh = a^r$ is a path of length two to $a^r \in U_1'$ if and only if $p \in [0, r - w - 2]$. The complete list is

$$(a^{0}x)(a^{4w+2-r}x), \ldots, (a^{p}x)(a^{p-r+n}), \ldots, (a^{r-w-2)}x)(a^{3w}x).$$

The total count is $r - w - 1$. If $r = w + 1$, then we will have an empty list.

By inspection, we have $2(2w - r + 1) + 2(r - 1 - w) = 2w = \mu$.

Proof. Now, we show that each one of these cases of elements are the only list of elements that give $a^r \in U_1'$.

Consider Case 1 and take $g, h \in U_1$ where $g = a^p$ and $h = a^q$. Note that $1 \leq p \leq w$ and $1 \leq q \leq w$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.96}$$

Now, suppose by way of contradiction $p \notin [r - w, w]$. So, $p < r - w$ or $p > w$. Since $p \in U_1$, then $p \not> w$, so $p < r - w$, and thus $p \leq r - w - 1$. Furthermore, since $a^q \in U_1$, then $q \leq w$. It follows

$$p + q \leq (r - w - 1) + w = r - 1 < r. \tag{4.97}$$

Now notice that $p \geq 1$ and $q \geq 1$. Since also $2w+1 \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p + q \geq 1 + 1 = 2 > -2w - 1 = (2w+1) - (4w+2) \geq r - n. \tag{4.98}$$

Hence, combining (4.97) and (4.98), $r - n < p + q < r$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.95). Hence, this completes Case 1.

Consider Case 2 and take $g, h \in U_2$ where $g = a^p$ and $h = a^q$. Note that $2w+2 \leq p \leq 3w+1$ and $2w+2 \leq q \leq 3w+1$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.99}$$

Now, suppose by way of contradiction $p \notin [r+w+1, 3w+1]$. So, $p < r+w+1$ or $p > 3w+1$. Since $p \in U_2$, then $p \not> 3w+1$, so $p < r+w+1$, and thus $p \leq r+w$. Furthermore, since $a^q \in U_2$, then $q \leq 3w+1$. It follows

$$p + q \leq (r+w) + (3w+1) = r + (4w+1) < r + (4w+2) = r + n. \tag{4.100}$$

Now notice that $p \geq 2w+2$ and $q \geq 2w+2$. Since also $2w+1 \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p + q \geq (2w+2) + (2w+2) = 4w+4 > 2w+1 \geq r. \tag{4.101}$$

Hence, combining (4.100) and (4.101), $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.99). Hence, this completes Case 2.

Consider Case 3 and take $g \in U_4$ and $h \in U_3$ where $g = a^p x$ and $h = a^q x$. Note that $2w+1 \leq p \leq 3w$ and $0 \leq q \leq w-1$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.102}$$

Now, suppose by way of contradiction $p \notin [r+w+1, 2w+1]$. So, $p < r+w+1$ or $p > 2w+1$. Since $p \in U_4$, then $p \not< 2w+1$, so $p > r+w-1$, and thus $p \geq r+w$. Furthermore, since $a^q \in U_3$, then $q \leq w-1$. It follows

$$p - q \geq (r+w) - (w-1) = r+1 > r. \tag{4.103}$$

Now notice that $p \leq 3w$ and $q \geq 0$. Since also $2w+1 \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \leq 3w - 0 = 3w < 5w + 3 = (w+1) + (4w+2) \leq r + n. \tag{4.104}$$

Hence, combining (4.103) and (4.104), $r < p - q < r + n$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.102). Hence, this completes Case 3.

Consider case 4 and take $g \in U_3$ and $h \in U_4$ where $g = a^p x$ and $h = a^q x$. Note that $0 \leq p \leq w - 1$ and $2w + 1 \leq q \leq 3w$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.105}$$

Now, suppose by way of contradiction $p \notin [0, r - w - 2]$. So, $p < 0$ or $p > r - w - 2$. Since $p \in U_3$, then $p \not< 0$, so $p > r - w - 2$, and thus $p \geq r - w - 1$. Furthermore, since $a^q \in U_4$, then $q \leq 3w$. It follows

$$p - q \geq (r - w - 1) - 3w = r - (4w + 1) > r - (4w + 2) = r + n. \tag{4.106}$$

Now notice that $p \leq w - 1$ and $q \geq 2w + 1$. Since also $2w + 1 \geq r,\ w \geq 1$, and $n = 4w + 2$, we have

$$p - q \leq (w - 1) - (2w + 1) = -w - 2 < w + 1 \leq r. \tag{4.107}$$

Hence, combining (4.106) and (4.107), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.105). Hence, this completes Case 4. □

4.2.2 There are no other paths of length two from e to elements in U_1'

Lemma 11. *The elements listed in Lemma 10 are the only paths of length two from e to elements in U_1'.*

Proof. Now we will check the cases that do not give μ paths of length two. They are the following.

Let $g \in U_1$ and $h \in U_2$ where $g = a^p$ and $h = a^q$. Note that $1 \leq p \leq w$ and $2w + 2 \leq q \leq 3w + 1$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.108}$$

Since $g \in U_1$, then $p \leq w$. Moreover, since $h \in U_2$, then $q \leq 3w + 1$. It follows

$$p + q \leq w + (3w + 1) = 4w + 1 < 5w + 3 = (w + 1) + (4w + 2) \leq r + n. \tag{4.109}$$

On the other hand, we see that $q \geq 2w + 2$ and $p \geq 1$. Since also $r \leq 2w + 1,\ w \geq 1$, we have

$$p + q \geq 1 + (2w + 2) = 2w + 3 > 2w + 1 \geq r. \tag{4.110}$$

Hence, by (4.110) and (4.109), $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.108). This completes this case.

Let $g \in U_1$ and $h \in U_2$ where $g = a^p$ and $h = a^q$. Note that $1 \leq p \leq w$ and $2w + 2 \leq q \leq 3w + 1$. Then we have

$$a^r = hg = (a^q)(a^p) = a^{q+p}. \tag{4.111}$$

Note that since we are using the same rotation elements as in the previous case, then $q + p = p + q$. This means that the proof for this case is the same proof as in the previous case. Hence $p + q \not\equiv r \pmod{n}$, which contradicts (4.111). This completes this case.

Let $g,\ h \in U_3$ where $g = a^p x$ and $h = a^q x$. Note that $0 \leq p \leq w - 1$ and $0 \leq q \leq w - 1$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.112}$$

Since $g \in U_3$, then $p \leq w - 1$. Moreover, since $h \in U_3$, then $q \geq 0$. It follows

$$p - q \leq (w - 1) - 0 = w - 1 < w + 1 \leq r. \tag{4.113}$$

On the other hand, we see that $q \leq w - 1$ and $p \geq 0$. Since also $r \leq 2w + 1,\ w \geq 1$, and $n = 4w + 2$, we have

$$p - q \geq 0 - (w - 1) = -w + 1 > -2w - 1 = (2w + 1) - (4w + 2) \geq r - n. \tag{4.114}$$

Hence, combining (4.113) and (4.114), we have $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.112). This completes this case.

Let $g,\ h \in U_4$ where $g = a^p x$ and $h = a^q x$. Note that $2w + 1 \leq p \leq 3w$ and $2w + 1 \leq q \leq 3w$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.115}$$

Since $g \in U_4$, then $p \leq 3w$. Moreover, since $h \in U_4$, then $q \geq 2w + 1$. It follows

$$p - q \leq 3w - (2w + 1) = w - 1 < w + 1 \leq r. \tag{4.116}$$

On the other hand, we see that $q \leq 3w$ and $p \geq 2w + 1$. Since also $r \leq 2w + 1,\ w \geq 1$, and $n = 4w + 2$, we have

$$p - q \geq (2w + 1) - 3w = -w + 1 > -2w - 1 = (2w + 1) - (4w + 2) \geq r - n. \tag{4.117}$$

Hence, by (4.116) and (4.117), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.115). This completes this case.

Thus, this shows that each one of the cases provided in Lemma 10 are the only set of elements that give $a^r \in U_1'$ □

4.2.3 Finding the μ paths of length two from e to elements in U_2'

Lemma 12. *Take $a^r \in U_2'$ where $3w + 2 \leq r \leq 4w + 1$. Then the sum of the following paths of length two to a^r is μ.*

Case 1 Let $g = a^p \in U_1$ and $h = a^q \in U_2$ where $q = r - p$. Then $gh = a^r$ is a path of length two to a^r if and only if $p \in [r - 3w - 1, w]$. The complete list is

$$(a^{r-3w-1))(a^{3w+1}),\ldots,(a^p)(a^{r-p}),\ldots,(a^w)(a^{r-w}).$$

The total count is $4w - r + 2$. If $r = 4w + 2$, then we will have an empty list.

Case 2 Let $g = a^p \in U_2$ and $h = a^q \in U_1$ where $q = r - p$. Then $gh = a^r$ is a path of length two to a^r if and only if $p \in [w, r - 3w - 1]$. The complete list is

$$(a^w)(a^{r-w}), \ldots, (a^p)(a^{r-p}), \ldots, (a^{3w+1})(a^{r-3w-1}).$$

The total count is $4w - r + 2$. If $r = 4w + 2$, then we will have an empty list.

Case 3 Let $g = a^p x \in U_3$ and $h = a^q x \in U_3$ where $q = p - r + n$. Then $gh = a^r$ is a path of length two to a^r if and only if $p \in [0, r - 3w - 3]$. The complete list is

$$(a^0 x)(a^{4w+2-r}), \ldots, (a^p x)(a^{p-r+n} x), \ldots, (a^{r-3w-3} x)(a^{w-1} x).$$

The total count is $r - 3w - 2$. If $r = 3w + 2$, then we will have an empty list.

Case 4 Let $g = a^p x \in U_4$ and $h = a^q x \in U_4$ where $q = p - r + n$. Then $gh = a^r$ is a path of length two to $a^r \in U_2'$ if and only if $p \in [2w + 1, r - w - 2]$. The complete list is

$$(a^{2w+1} x)(a^{6w+3-r} x), \ldots, (a^p x)(^{p-r+n} x), \ldots, (a^{r-w-2} x)(a^{3w} x).$$

The total count is $r - 3w - 2$. If $r = 3w + 2$, then we will have an empty list.

So, by inspection we have $2(4w + 2 - r) + 2(r - 2 - 3w) = 2w = \mu$.

Now, we show that each one of these cases of elements are the only list of elements that give $a^r \in U_2'$.

Proof. Consider Case 1 and take $g = a^p \in U_1$ and $h = a^q \in U_2$ where $1 \leq p \leq w$ and $2w + 2 \leq q \leq 3w + 1$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.118}$$

Now, suppose by way of contradiction $p \notin [r - 3w - 1, w]$. So, $p < r - 3w - 1$ or $p > w$. Since $p \in U_1$, then $p \not> w$, so $p < r - 3w - 1$, and thus $p \leq r - 3w - 2$. Furthermore, since

$a^q \in U_2$, then $q \leq 3w+1$. It follows

$$p+q \leq (r-3w-2)+(3w+1) = r-1 < r. \tag{4.119}$$

Now notice that $p \geq 1$ and $q \geq 2w+2$. Since also $4w+1 \geq r,\ w \geq 1$, and $n = 4w+2$, we have

$$p+q \geq 1+(2w+2) = 2w+3 > -1 = (4w+1)-(4w+2) \geq r-n. \tag{4.120}$$

Hence, combining (4.119) and (4.120), $r-n < p+q < r$, which means that $p+q \not\equiv r \pmod{n}$, which contradicts (4.118). Hence, this completes Case 1.

Consider case 2 and take $g \in U_1$ and $h \in U_2$ where $g = a^p$ and $h = a^q$. Note that $1 \leq p \leq w$ and $2w+2 \leq q \leq 3w+1$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.121}$$

Note that since we are still considering elements from U_1 and from U_2, we are still using the same rotation elements as in the previous case. This means that the proof for this case is the same proof as in the previous case. Hence $p+q \not\equiv r \pmod{n}$, which contradicts with (4.119). This completes this case.

Consider Case 3 and take $g = a^p x \in U_3$ and $h = a^q x \in U_3$ where $0 \leq p \leq w-1$ and $0 \leq q \leq w-1$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.122}$$

Now, suppose by way of contradiction $p \notin [0, r-3w-3]$. So, $p < 0$ or $p > r-3w-3$. Since $a^p x \in U_3$, then $p \not< 0$, so $p > r-3w-3$, and thus $p \geq r-3w-2$. Furthermore, since $a^q x \in U_3$, then $q \leq w-1$. Moreover, recall $n = 4w+2$. It follows

$$p-q \geq (r-3w-2)-(w-1) = r-4w-1 > r-n. \tag{4.123}$$

Now notice that $p \leq w-1$ and $q \geq 0$. Since also $r \geq 3w+2,\ w \geq 1$, we have

$$p-q \leq (w-1)-0 = w-1 < 3w+2 \leq r. \tag{4.124}$$

Hence, combining (4.123) and (4.124), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.122). Hence, this completes Case 3.

Consider Case 4 and take $g,\ h \in U_4$ where $g = a^p x$ and $h = a^q x$. Note that $2w + 1 \leq p \leq 3w$ and $2w + 1 \leq q \leq 3w$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.125}$$

Now, suppose by way of contradiction $p \notin [2w + 1, r - w - 2]$. So, $p < 2w + 1$ or $p > r - w - 2$. Since $a^p x \in U_4$, then $p \not< 2w + 1$, so $p > r - w - 2$, and thus $p \geq r - w - 1$. Furthermore, since $a^q x \in U_4$, then $q \leq 3w$. It follows

$$p - q \geq (r - w - 1) - 3w = r - (4w + 1) > r - (4w + 2) = r - n. \tag{4.126}$$

Now notice that $p \leq 3w$ and $q \geq 2w + 1$. Since also $r \geq 3w + 2,\ w \geq 1$, we have

$$p - q \leq 3w - (2w + 1) = w - 1 < 3w + 2 \leq r. \tag{4.127}$$

Hence, combining (4.124) and (4.125), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.123). Hence, this completes Case 4. □

4.2.4 There are no other paths of length two from e to elements in U_2'

Lemma 13. *The elements listed in Lemma 12 are the only paths of length two from e to elements in U_2'.*

Proof. Now we check cases that do not give μ paths of length two. They are the following.

Let $g,\ h \in U_1$ where $g = a^p$ and $h = a^q$. Note that $1 \leq p \leq w$ and $1 \leq q \leq w$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.128}$$

Since $g, h \in U_1$, then $p \leq w$ and $q \leq w$. Moreover, $r \geq 3w + 2$. It follows

$$p + q \leq w + w = 2w < 3w + 2 \leq r. \tag{4.129}$$

On the other hand, we see that $q \geq 1$ and $p \geq 1$. Since also $r \leq 4w+1,\ w \geq 1$, and $n = 4w+2$, we have

$$p + q \geq 1 + 1 = 2 > -1 = (4w+1) - (4w+2) \geq r - n. \tag{4.130}$$

Hence, by (4.129) and (4.130), $r - n < p + q < r$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.128). This completes this case.

Let $g,\ h \in U_2$ where $g = a^p$ and $h = a^q$. Note that $2w+2 \leq p \leq 3w+1$ and $2w+2 \leq q \leq 3w+1$. Then we have

$$a^r = gh = (a^p)(a^q) = a^{p+q}. \tag{4.131}$$

Since $g, h \in U_2$, then $p \geq 2w+2$ and $q \geq 2w+2$. Moreover, $4w+1 \geq r$. It follows

$$p + q \geq (2w+2) + (2w+2) = 4w+4 > 4w+1 \geq r. \tag{4.132}$$

On the other hand, we see that $q \leq 3w+1$ and $p \leq 3w+1$. Since also $r \geq 3w+2,\ w \geq 1$, and $n = 4w+2$, we have

$$p + q \leq (3w+1) + (3w+1) = 6w+2 < 7w+4 = (3w+2) + (4w+2) \leq r + n. \tag{4.133}$$

Hence, combining (4.132) and (4.133), $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.131). This completes this case.

Let $g = a^p x \in U_3$ and $h = a^q x \in U_4$. Note that $0 \leq p \leq w-1$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.134}$$

Since $g \in U_3$, then $p \leq w-1$ and $q \geq 2w+1$. Moreover, $r \leq 4w+1$. It follows

$$p - q \leq (w-1) - (2w+1) = -w-2 > -1 = 4w+1-4w-2 \geq r - n. \tag{4.135}$$

On the other hand, we see that $p \geq 0$ and $q \leq 3w$. Since also $r \leq 4w+1,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq 0 - 3w = -3w > -4w-3 = (4w+1) - 2(4w+2) \geq r - 2n. \tag{4.136}$$

Hence, by (4.135) and (4.136), $r-2n < p-q < r-n$, which means that $p-q \not\equiv r \pmod{n}$, which contradicts (4.134) This completes this case.

Let $g = a^p x \in U_4$ and $h = a^q x \in U_3$. Note that $2w+1 \leq p \leq 3w$ and $0 \leq q \leq w-1$. Then we have

$$a^r = gh = (a^p x)(a^q x) = a^{p-q}. \tag{4.137}$$

Since $g \in U_4$, then $p \leq 3w$ and $q \geq 0$. Moreover, $3w+2 \leq r$. It follows

$$p - q \leq 3w - 0 = 3w < 3w + 2 \leq r. \tag{4.138}$$

On the other hand, we see that $q \leq w-1$ and $p \geq 2w+1$. Since also $r \leq 4w+1,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+1) - (w-1) = w + 2 > -1 = (4w+1) - (4w+2) \geq r - n. \tag{4.139}$$

Hence, by (4.138) and (4.139), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.137). This completes this case.

Thus, this shows that each one of the cases provided in Lemma 12 are the only set of elements that give $a^r \in U_2'$ □

4.2.5 Finding the μ paths of length two from e to elements in U_3'

Lemma 14. *Take $a^r x \in U_3'$ where $w \leq r \leq 2w$. Then the sum of the following paths of length two to a^r is μ.*

Case 1 Let $g = a^p \in U_1$ and $h = a^q x \in U_3$ where $q = r - p$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [r-w+1, w]$. The complete list is

$$(a^{r-w+1})(a^{w-1}x), \ldots, (a^p)(a^{r-p}x), \ldots, (a^w)(a^{r-w}x).$$

The total count is $2w - r$. If $r = 2w$, then we will have an empty list.

Case 2 Let $g = a^p \in U_2$ and $h = a^q x \in U_4$ where $q = r + n - p$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [r + w + 2, 3w + 1]$. The complete list is

$$(a^{r+w+2})(a^{3w}x), \ldots, (a^p)(a^{r+n-p}x), \ldots, (a^{3w+1})(a^{r-w-1)}).$$

The total count is $2w - r$. If $r = 2w$, then we will have an empty list.

Case 3 Let $g = a^p x \in U_4$ and $h = a^q \in U_1$ where $q = p - r$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [2w + 1, r + w]$. The complete list is

$$(a^{2w+1}x)(a^{2w+1-r}), \ldots, (a^p x)(a^{p-r}), \ldots, (a^{r+w}x)(a^w).$$

The total count is $r - w$. If $r = w$, then we will have an empty list.

Case 4 Let $g = a^p x \in U_3$ and $h = a^q \in U_2$ where $q = p - r + n$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [0, r - w - 1]$. The complete list is

$$(a^{r-w-1}x)(a^{3w+1}), \ldots, (a^p x)(a^{p-r+n}), \ldots, (a^0 x)(a^{4w+2-r}).$$

The total count is $r - w$. If $r = w$, then we will have an empty list.

So by inspection, we have $2(r - w) + 2(2w - r) = 2w = \mu$.

Now, we will show that each one of these cases of elements are the *only* list of elements that give $a^r x \in U_3'$.

Proof. Let us consider Case 1 and take $g = a^p \in U_1$ and $h = a^q x \in U_3$. Note that $1 \leq p \leq w$ and $0 \leq q \leq w - 1$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.140}$$

Now, suppose by way of contradiction $p \notin [r - w + 1, w]$. So, $p < r - w + 1$ or $p > w$. Since $a^p \in U_1$, then $p \not> w$, so $p < r - w + 1$, and thus $p \leq r - w$. Furthermore, since $a^q x \in U_3$,

then $q \leq w - 1$. It follows

$$p + q \leq (r - w) + (w - 1) = r - 1 < r. \tag{4.141}$$

Now notice that $p \geq 1$ and $q \geq 0$. Since also $r \leq 2w,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \geq 1 + 0 = 1 > -2w - 2 = 2w - (4w + 2) \geq r - n. \tag{4.142}$$

Hence, combining (4.141) and (4.142), $r - n < p + q < r$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.140). Hence, this completes Case 1.

Consider Case 2 and take $g = a^p \in U_2$ and $h = a^q x \in U_4$. Note that $2w+2 \leq p \leq 3w+1$ and $2w + 1 \leq q \leq 3w$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.143}$$

Now, suppose by way of contradiction $p \notin [r + w + 2, 3w + 1]$. So, $p < r + w + 2$ or $p > 3w + 1$. Since $a^p \in U_2$, then $p \not> 3w + 1$, so $p < r + w + 2$, and thus $p \leq r + w + 1$. Furthermore, since $a^q x \in U_4$, then $q \leq 3w$. It follows

$$p + q \leq (r + w + 1) + 3w = r + (4w + 1) < r + (4w + 2) = r + n. \tag{4.144}$$

Now notice that $p \geq 2w + 2$ and $q \geq 2w + 1$. Since also $r \leq 3w,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \geq (2w + 2) + (2w + 1) = 4w + 3 > 3w \geq r. \tag{4.145}$$

Hence, combining (4.144) and (4.145), $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.143). Hence, this completes Case 2.

Consider Case 3 and take $g = a^p x \in U_4$ and $h = a^q \in U_1$. Note that $2w + 1 \leq p \leq 3w$ and $1 \leq q \leq w$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.146}$$

Now, suppose by way of contradiction $p \notin [2w + 1, r + w]$. So, $p < 2w + 1$ or $p > r + w$. Since $a^p x \in U_4$, then $p \not< 2w + 1$, so $p > r + w$, and thus $p \geq r + w + 1$. Furthermore, since

$a^q \in U_1$, then $q \leq w$. It follows

$$p - q \geq (r + w + 1) - w = r + 1 > r. \tag{4.147}$$

Now notice that $p \leq 3w$ and $q \geq 1$. Since also $r \geq w,\ w \geq 1$, and $n = 4w + 2$, we have

$$p - q \leq 3w - 1 < 5w + 2 = w + (4w + 2) \leq r + n. \tag{4.148}$$

Hence, combining (4.147) and (4.148), $r < p - q < r + n$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.146). Hence, this completes Case 3.

Consider Case 4 and take $g = a^p x \in U_3$ and $h = a^q \in U_2$. Note that $0 \leq p \leq w - 1$ and $2w + 2 \leq q \leq 3w + 1$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.149}$$

Now, suppose by way of contradiction $p \notin [0, r - w - 1]$. So, $p < 0$ or $p > r - w - 1$. Since $a^p x \in U_3$, then $p \not< 0$, so $p > r - w - 1$, and thus $p \geq r - w$. Furthermore, since $a^q \in U_2$, then $q \leq 3w + 1$. It follows

$$p - q \geq (r - w) - (3w + 1) = r - (4w + 1) > r - (4w + 2) = r - n. \tag{4.150}$$

Now notice that $p \leq w - 1$ and $q \geq 2w + 2$. Since also $r \geq w,\ w \geq 1$, and $n = 4w + 2$, we have

$$p - q \leq (w - 1) - (2w + 2) = -w - 3 < w \leq r. \tag{4.151}$$

Hence, combining (4.150) and (4.151), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.149). Hence, this completes Case 4. □

4.2.6 There are no other paths of length two from e to elements in U_3'

Lemma 15. *The elements listed in Lemma 14 are the only paths of length two from e to elements in U_3'.*

Proof. Now we check cases that do not give μ paths of length two. They are the following.

Let $g = a^p x \in U_3$ and $h = a^q \in U_1$. Note that $0 \leq p \leq w-1$ and $1 \leq q \leq w$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q}x. \tag{4.152}$$

Since $g \in U_3$, then $p \leq w-1$. Moveover, since $q \in U_1$, then $q \geq 1$. Furthermore, $r \geq w$. Then, it follows

$$p - q \leq (w-1) - 1 = w - 2 < w \leq r. \tag{4.153}$$

On the other hand, we see that $q \leq w$ and $p \geq 0$. Since also $r \leq 2w,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq 0 - w = -w > -2w - 2 = 2w - (4w+2) \geq r - n. \tag{4.154}$$

Hence, combining (4.153) and (4.154), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.152). This completes this case.

Let $g = a^p x \in U_4$ and $h = a^q \in U_2$. Note that $2w+1 \leq p \leq 3w$ and $2w+2 \leq q \leq 3w+1$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q}x. \tag{4.155}$$

Since $g \in U_4$, then $p \leq 3w$ and $q \geq 2w+2$. Moreover, $w \leq r$. It follows

$$p - q \leq 3w - (2w+2) = w - 2 < w \leq r. \tag{4.156}$$

On the other hand, we see that $q \leq 3w+1$ and $p \geq 2w+1$. Since also $r \leq 2w,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+1) - (3w+1) = -w > -2w - 2 = 2w - (4w+2) \geq r - n. \tag{4.157}$$

Hence, combining (4.156) and (4.157), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.155). This completes this case.

Let $g = a^p \in U_1$ and $h = a^q x \in U_4$. Note that $1 \leq p \leq w$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q}x. \tag{4.158}$$

Since $g \in U_1$, then $p \leq w$. Moreover, since $h \in U_4$, then $q \leq 3w$. Also, $w \leq r$. It follows

$$p + q \leq w + 3w = 4w < 5w + 2 = w + (4w + 2) \leq r + n. \tag{4.159}$$

On the other hand, we see that $q \geq 2w + 1$ and $p \geq 1$. Since also $r \leq 2w,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \geq 1 + (2w + 1) = 2w + 2 > 2w \geq r. \tag{4.160}$$

Hence, combining (4.159) and (4.160), we have $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.158). This completes this case.

Let $g = a^p \in U_2$ and $h = a^q x \in U_3$. Note that $2w + 2 \leq p \leq 3w + 1$ and $0 \leq q \leq w - 1$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.161}$$

Since $g \in U_2$, then $p \leq 3w + 1$. Moreover, since $h \in U_3$, then $q \leq w - 1$. Also, $r \geq w$. It follows

$$p + q \leq (3w + 1) + (w - 1) = 4w < 5w + 2 = w + (4w + 2) \leq r + n. \tag{4.162}$$

On the other hand, we see that $p \geq 2w + 2$ and $q \geq 0$. Since also $r \leq 2w,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \geq (2w + 2) + 0 = 2w + 2 > 2w \geq r. \tag{4.163}$$

Hence, combining (4.162) and (4.163), we have $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.161). This completes this case.

Thus, this shows that each one of the cases provided in Lemma 14 are the only set of elements that give $a^r x \in U_3'$ □

4.2.7 Finding the μ paths of length two from e to elements in U_4'

Lemma 16. *Take $a^r x \in U_4'$ where $3w + 1 \leq r \leq 4w + 1$. Then the sum of the following paths of length two from e to $a^r x$ is μ*

Case 1 Let $g = a^p \in U_2$ and $h = a^q x \in U_3$ where $q = r - p$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [r - w + 1, 3w + 1]$. The complete list is

$$(a^{r-w+1})(a^{w-1}x), \ldots, (a^p)(a^{r-p}x), \ldots, (a^{3w+1})(a^{r-(3w+1)}).$$

The total count is $4w - r + 1$. If $r = 4w + 1$, then we will have an empty list.

Case 2 Let $g = a^p \in U_1$ and $h = a^q x \in U_4$ where $q = r - p$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [r - 3w, w]$. The complete list is

$$(a^{r-3w})(a^{3w}x), \ldots, (a^p)(a^{r-p}x), \ldots, (a^w)(a^{r-w}x).$$

The total count is $4w - r + 1$. If $r = 4w + 1$, then we will have an empty list.

Case 3 Let $g = a^p x \in U_3$ and $h = a^q \in U_1$ where $q = p - r + n$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [0, r - 3w - 2]$. The complete list is

$$(a^0 x)(a^w), \ldots, (a^p x)(a^{p-r+n}), \ldots, (a^{r-3w-2}x)(a^w).$$

The total count is $r - 3w - 1$. If $r = 3w + 1$, then we will have an empty list.

Case 4 Let $g = a^p x \in U_4$ and $h = a^q \in U_2$ where $q = p - r + n$. Then $gh = a^r x$ is a path of length two to $a^r x$ if and only if $p \in [2w + 1, r - w - 1]$. The complete list is

$$(a^{2w+1}x)(a^{6w+3-r}), \ldots, (a^p x)(a^{p-r+n}), \ldots, (a^{r-w-1}x)(a^{3w+1}).$$

The total count is $r - 3w - 1$. If $r = 3w + 1$, then we will have an empty list.

So by inspection, we have $2(4w - r + 1) + 2(r - 3w - 1) = 2w = \mu$.

Proof. Now, we will show that each one of these cases of elements are the only list of elements that give $a^r x \in U_4'$.

Consider Case 1 and take $g = a^p \in U_2$ and $h = a^q x \in U_3$. Note that $2w+2 \leq p \leq 3w+1$ and $0 \leq q \leq w-1$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.164}$$

Now, suppose by way of contradiction $p \notin [r-w+1, 3w+1]$. So, $p < r-w+1$ or $p > 3w+1$. Since $a^p \in U_2$, then $p \not> 3w+1$, so $p < r-w+1$, and thus $p \leq r-w$. Furthermore, since $a^q x \in U_3$, then $q \leq w-1$. It follows

$$p + q \leq (r-w) + (w-1) = r-1 < r. \tag{4.165}$$

Now notice that $p \geq 2w+2$ and $q \geq 0$. Since also $r \leq 4w+1,\ w \geq 1$, and $n = 4w+2$, we have

$$p + q \geq (2w+2) + 0 = 2w+2 > -1 = (4w+1) - (4w+2) \geq r - n. \tag{4.166}$$

Hence, combining (4.165) and (4.166), $r - n < p + q < r$, which means $p + q \not\equiv r \pmod{n}$, which contradicts (4.164). Hence, this completes Case 1.

Consider Case 2 and let $g = a^p \in U_1$ and $h = a^q x \in U_4$. Note that $1 \leq p \leq w$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.167}$$

Now, suppose by way of contradiction $p \notin [r-3w, w]$. So, $p < r-3w$ or $p > w$. Since $g \in U_1$, then $p \not> w$, so $p < r-3w$, and thus $p \leq r-3w-1$. Furthermore, since $h \in U_4$, then $q \leq 3w$. It follows

$$p + q \leq (r-3w-1) + 3w = r-1 < r. \tag{4.168}$$

Now notice that $p \geq 1$ and $q \geq 2w+1$. Since also $r \leq 4w+1,\ w \geq 1$, and $n = 4w+2$, we have

$$p + q \geq 1 + (2w+1) = 2w+2 > -1 = (4w+1) - (4w+2) \geq r - n. \tag{4.169}$$

Hence, combining (4.168) and (4.169), $r - n < p + q < r$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.167). Hence, this completes Case 2.

Consider Case 3 and take $g = a^p x \in U_3$ and $h = a^q \in U_1$. Note that $0 \leq p \leq w - 1$ and $1 \leq q \leq w$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.170}$$

Now, suppose by way of contradiction $p \notin [0, r - 3w - 2]$. So, $p < 0$ or $p > r - 3w - 2$. Since $a^p x \in U_3$, then $p \not< 0$, so $p > r - 3w - 2$, and thus $p \geq r - 3w - 1$. Furthermore, since $a^q \in U_1$, then $q \leq w$. It follows

$$p - q \geq (r - 3w - 1) - w = r - (4w + 1) > r - (4w + 2) = r - n. \tag{4.171}$$

Now notice that $p \leq w - 1$ and $q \geq 1$. Since also $r \geq 3w + 1,\ w \geq 1$, and $n = 4w + 2$, we have

$$p - q \leq (w - 1) - 1 = w - 2 < 3w + 1 \leq r. \tag{4.172}$$

Hence, combining (4.171) and (4.172), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.170). Hence, this completes Case 3.

Consider Case 4 and take $g = a^p x \in U_4$ and $h = a^q \in U_2$. Note that $2w + 1 \leq p \leq 3w$ and $2w + 2 \leq q \leq 3w + 1$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.173}$$

Now, suppose by way of contradiction $p \notin [2w + 1, r - w - 1]$. So, $p < 2w + 1$ or $p > r - w - 1$. Since $a^p x \in U_4$, then $p \not< 2w + 1$, so $p > r - w - 1$, and thus $p \geq r - w$. Furthermore, since $a^q \in U_2$, then $q \leq 3w + 1$. It follows

$$p - q \geq (r - w) - (3w + 1) = r - (4w + 1) > r - (4w + 2) = r - n. \tag{4.174}$$

Now notice that $p \leq 3w$ and $q \geq 2w + 2$. Since also $r \geq 3w + 1,\ w \geq 1$, and $n = 4w + 2$, we have

$$p - q \leq 3w - (2w + 2) = w - 2 < 3w + 1 \leq r. \tag{4.175}$$

Hence, combining (4.174) and (4.175), $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.173). Hence, this completes Case 4. □

4.2.8 There are no other paths of length two from e to elements in U_4'

Lemma 17. *The elements listed in Lemma 16 are the only paths of length two from e to elements in U_4'.*

Proof. We now check cases that do not give μ paths of length two. They are the following.

Let $g = a^p x \in U_3$ and $h = a^q \in U_2$. Note that $0 \leq p \leq w-1$ and $2w+2 \leq q \leq 3w+1$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.176}$$

Since $g \in U_3$, then $p \leq w-1$. Moreover, since $h \in U_2$, then $q \geq 2w+2$. Also, $r \geq 3w+1$. It follows

$$p - q \leq (w-1) - (2w+2) = -w-3 < -w-1 = (3w+1) - (4w+2) \leq r - n. \tag{4.177}$$

On the other hand, we see that $p \geq 0$ and $q \leq 3w+1$. Since also $r \leq 4w+1,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq 0 - (3w+1) = -3w-1 > -4w-3 = (4w+1) - 2(4w+2) \geq r - 2n. \tag{4.178}$$

Hence, combining (4.177) and (4.178), we have $r - 2n < p - q < r - n$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.176). This completes this case.

Let $g = a^p x \in U_4$ and $h = a^q \in U_1$. Note that $2w+1 \leq p \leq 3w$ and $1 \leq q \leq w$. Then we have

$$a^r x = gh = (a^p x)(a^q) = a^{p-q} x. \tag{4.179}$$

Since $g \in U_4$, then $p \leq 3w$. Moreover, since $h \in U_1$, then $q \geq 1$. Also, $r \geq 3w+1$. It follows

$$p - q \leq 3w - 1 < 3w + 1 \leq r. \tag{4.180}$$

On the other hand, we see that $p \geq 2w+1$ and $q \leq w$. Since also $r \leq 4w+1,\ w \geq 1$, and $n = 4w+2$, we have

$$p - q \geq (2w+1) - w = w + 1 > -1 = (4w+1) - (4w+2) \geq r - n. \tag{4.181}$$

Hence, combining (4.180) and (4.181), we have $r - n < p - q < r$, which means that $p - q \not\equiv r \pmod{n}$, which contradicts (4.179). This completes this case.

Let $g = a^p \in U_1$ and $h = a^q x \in U_3$. Note that $1 \leq p \leq w$ and $0 \leq q \leq w - 1$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.182}$$

Since $g \in U_1$, then $p \leq w$. Moreover, since $h \in U_3$, then $q \leq w - 1$. Also, $r \geq 3w + 1$. It follows

$$p + q \leq w + (w - 1) = 2w - 1 < 3w + 1 \leq r. \tag{4.183}$$

On the other hand, we see that $p \geq 1$ and $q \geq 0$. Since also $r \leq 4w + 1,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \geq 1 + 0 = 1 > -1 = (4w + 1) - (4w + 2) \geq r - n. \tag{4.184}$$

Hence, combining (4.183) and (4.184), we have $r - n < p + q < r$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.182). This completes this case.

Let $g = a^p \in U_2$ and $h = a^q x \in U_4$. Note that $2w+2 \leq p \leq 3w+1$ and $2w+1 \leq q \leq 3w$. Then we have

$$a^r x = gh = (a^p)(a^q x) = a^{p+q} x. \tag{4.185}$$

Since $g \in U_2$, then $p \leq 3w + 1$. Moreover, since $h \in U_1$, then $q \leq 3w$. Also, $r \geq 3w + 1$. It follows

$$p + q \leq (3w + 1) + 3w = 6w + 1 < (3w + 1) + (4w + 2) \leq r + n. \tag{4.186}$$

On the other hand, we see that $p \geq 2w + 2$ and $q \geq 2w + 1$. Since also $r \leq 4w + 1,\ w \geq 1$, and $n = 4w + 2$, we have

$$p + q \geq (2w + 2) + (2w + 1) = 4w + 3 > 4w + 1 \geq r. \tag{4.187}$$

Hence, combining (4.186) and (4.187), we have $r < p + q < r + n$, which means that $p + q \not\equiv r \pmod{n}$, which contradicts (4.185). This completes this case.

Thus, this shows that each one of the cases provided in Lemma 16 are the only set of elements that give $a^r x \in U_4'$.

Therefore, we have μ paths of length two from e to each element not in S. □

4.3 Verifying that there are t paths of length two from e back to itself

We verify in this section that there are t paths of length two from the identity back to itself.

Lemma 18. *There are exactly t paths of length two from the identity, e, back to itself.*

Proof. Notice that each of sets U_3 and U_4 has w reflections, giving a total of $2w = \mu$ reflections in S.

Now we will show that there is no other element joined with its inverse. Lets take $a^p \in U_1$ and show that $a^{n-p} \notin U_1$ or in U_2. Since $a^p \in U_1$, then we have

$$\begin{aligned} 1 \leq p \leq w \\ n-1 \leq n-p \leq n-w \\ 3w+2 \leq n-p \leq 4w+1. \end{aligned} \tag{4.188}$$

So, from (4.188), we have that $a^{n-p} \notin U_1$ and that $a^{n-p} \notin U_2$.

Now let us take $a^p \in U_2$ and show that $a^{n-p} \notin U_1$ or in U_2. Since $a^p \in U_2$, then we have

$$\begin{aligned} 2w+2 \leq p \leq 3w+1 \\ n-2w-2 \geq n-p \geq n-3w-1. \end{aligned} \tag{4.189}$$

Since $n = 4w+2$, then we have

$$\begin{aligned} 4w+2-2w-2 \geq n-p \geq 4w+2-3w-1 \\ 2w \leq n-p \leq w+1 \end{aligned} \tag{4.190}$$

So, from (4.194), we have that $a^{n-p} \notin U_1$ and that $a^{n-p} \notin U_2$. So we have shown that a rotation is not joined with its inverse, have exactly $2w = t$ paths of length two from e back to itself. □

4.4 Proof of Main Result

In this section we proof Main Result using Sections 4.1, 4.2, and 4.3.

Lemma 19. *If $h \in S$, then we have λ paths of length two from e to h.*

Proof. Section 4.1 □

Lemma 20. *If $b, m \in G$ and there exist an edge from b to m, then we have λ paths of length two from b to m.*

Proof. Since $b \to m$, there exists an $s \in S$ such that $bs = m$ so $s = b^{-1}m \in S$). By Lemma 19, we have λ paths of length two from e to $b^{-1}m$. Let us take $J = \{j_i \mid 1 \leq i \leq \lambda\}$, then we have

$$\begin{aligned} (j_1)(j_1') &= b^{-1}m \\ &\vdots \\ (j_\lambda)(j_\lambda') &= b^{-1}m \end{aligned} \tag{4.191}$$

So, we have $b(j_i)(j_i') = m$ for $i = 1,\ldots, \lambda$. So, we have λ paths of length two from b to m.

Lemma 21. *If $h \notin S$, then we have μ paths of length two from e to h.*

Proof. Section 4.2 □

Lemma 22. *If $b, m \in G$ and there does not exist an edge from b to m, then we have μ paths of length two from b to m.*

Proof. Since $b \not\to m$, then for every $s \in S,\ bs \neq m$ i.e., $s \neq b^{-1}m \in S$. By Lemma 21, if $h \notin S$, then we have μ paths of length two from e to h. Let us take $C = \{c_i \mid 1 \leq i \leq \mu\}$ and have

$$\begin{aligned}(c_1)(c_1') &= b^{-1}m \\ &\vdots \\ (c_\mu)(c_\mu') &= b^{-1}m\end{aligned} \tag{4.192}$$

So, we have $b(c_i)(c_i') = m$ for $i = 1, \ldots, \mu$. So, we have μ paths of length two from b to m. □

Lemma 23. *If $b \in G$, then there are t paths of length two from b back to itself.*

Proof. By Theorem 18, there exist t paths of length two from e back to itself. So, let's take $O = \{o_i \mid 1 \leq o_i \leq t\}$ and have

$$\begin{aligned}(o_1)(o_1') &= e \\ &\vdots \\ (o_t)(o_t') &= e.\end{aligned} \tag{4.193}$$

So by choosing $o_i \in O$ and multiplying by b to both sides, we have

$$b(o_i)(o_i') = b. \tag{4.194}$$

So we have t paths of length two from b back to itself for $i = 1, \ldots,\ t$. □

Proof. (of main result, Theorem 1)

Suppose $G = C\,(D_{2n},\ S)$ and let $x \in G$. If $y \in G$ and there is a directed edge from x to y, then there are λ paths of length from x to y, by Lemma 20. Moreover, if there isn't a directed edge from x to y, then there are μ paths of length two from from x to y, by Lemma 22. Finally, choosing x, there are t paths of length two from x back to itself, by Lemma 23. Therefore, $C\,(D_{2n},\ S)$ is a Directed Strongly Regular Graph. □

References

[1] P. J. Cameron, *Strongly Regular Graphs,* L.W. Beineke, R.J. Wilson (Eds.), Selected Topics in Graph Theory, Academic Press, New York (1978), pp. 337–360.

[2] C. D. Godsil, S. A. Hobart, and W. J. Martin, *Representations of directed strongly regular graphs,* Europ. J. Comb. 28 (2007), pp. 1980–1993.

[3] A. M. Duval, *A directed graph version of strongly regular graphs,* Journal of Combinartorial Theory (Series A) 47 (1988), pp. 71–100.

[4] F. Fiedler, M. H. Klin, and M. Muzychuk, *Small vertex-transitive directed strongly regular graphs,* Discr. Math. 255 (2002), pp. 87–115.

[5] A. E. Brouwer and S. A. Hobart, *Parameters of directed strongly regular graphs,* http://homepages.cwi.nl/ aeb/math/dsrg/dsrg.html

[6] D. S. Dummit and R. M. Foote, *Abstract algebra*, John Wiley and Sons, Inc. Third Edition;(2003).

[7] O. E. Nicodemi, M. A. Sutherland, and G. W. Towsley, *An Introduction to Abstract Algebra with Notes to the Future Teacher,* Upper Saddle River, New Jersey, (2007), pp. 198–200.

[8] S. A. Hobart and T. J. Shaw, *A note on a family of directed strongly regular graphs,* Europ. J. Combin. 20 (1999), pp. 819–820.

[9] K. H. Rosen, *Discrete Mathematics and Its Applications,* McGraw-Hill Companies, (2007), pp. 628–629.

[10] A. M. Duval and D. Iourinski, *Semidirect product constructions of directed strongly regular graphs,* Journal of Combinatorial Theory (Series A) 104 (2003), pp. 157–167. Preprint, 2000.

[11] M. Klin, A. Munemasa, M. Muzychuk, and P. H. Zeischang, *Directed strongly regular graphs coherent (cellular) algebras,* Lin. Alg. Appl. 377 (2004), pp. 83–109; Preprint Kyushu-MPS-1997-12, Kyushu University, 1997.

Chapter 5

Appendix

The computer search was written in Mathematica, and it searched for dihedral Cayley DSRGs where $n = 10$.

```
(* Jonathan Gamez *)

(* DSRG Parameters *)

w = 2;
n = 4 * w + 2; (*2*n*)
k2 = 4 * w;
t = 2 * w;
mu = 2 * w;
lamda = 2 * w - 2;

(*--------------------------------------------------------------------------*)

k = 2;
J = Table[1, {2 * n}, {2 * n}];
Dn = Sort[Flatten[Table[{{a^i}, {a^i * x}}, {i, 0, n - 1}]]];

(*Programs*)

mult[e_, u_] := y[p[foo[e], foo[u]]];
foo[variable_] :=
  {Mod[Exponent[variable, a], n], Mod[Exponent[variable, x], k]};
p[{c_, d_}, {r_, t_}] := If[d == 1, {c - r, d + t}, {c + r, d + t}];
y[{c_, d_}] := a^Mod[c, n] * x^Mod[d, k];

(*Testing Function*)

TestingS[S_] := Module[{G, i, j},
  edges = Flatten[Table[Dn[[j]] → mult[S[[i]], Dn[[j]]], {i, 1, k2}, {j, 1, 2 * n}]];
  G = Graph[edges, VertexLabels → "Name"];
  A = AdjacencyMatrix[G]; A.A + (mu - lamda) * A == mu * J]

(*Construction of Sets*)

(*--------------------------------------------------------------------------*)

(*Local Variables*)

n2 = Binomial[n, t];
X1 = Flatten[Table[{a^i * x}, {i, 0, n - 1}]];
X2 = Subsets[X1, {t}];
H1 = Flatten[Table[{i}, {i, 1, t}]];
H2 = Flatten[Table[{i}, {i, t + 2, n - 1}]];
T2 = Subsets[H2];
Length[T2];
n1 = Length[T2];
```

```
T3 = Table[Mod[n, Complement[H2, T2[[u]]]], {u, 1, n1}];
T4 = a^Table[Union[T2[[j]], T3[[j]]], {j, 1, n1}];
T5 = Flatten[Table[Flatten[{T4[[j]], X2[[i]]}], {j, 1, n1}, {i, 1, n2}], 1];

(*------------------------------------------------------------------------*)

(* Testing Dihedral Cayley sets S*)

Select[T5, TestingS]

(*Dihedral Cayley DSRGs when n = 10*)
```

$$\{\{a, a^2, a^6, a^7, x, a\,x, a^5\,x, a^6\,x\}, \{a, a^2, a^6, a^7, x, a^4\,x, a^5\,x, a^9\,x\},$$
$$\{a, a^2, a^6, a^7, a\,x, a^2\,x, a^6\,x, a^7\,x\}, \{a, a^2, a^6, a^7, a^2\,x, a^3\,x, a^7\,x, a^8\,x\},$$
$$\{a, a^2, a^6, a^7, a^3\,x, a^4\,x, a^8\,x, a^9\,x\}, \{a, a^3, a^6, a^8, x, a^2\,x, a^5\,x, a^7\,x\},$$
$$\{a, a^3, a^6, a^8, x, a^3\,x, a^5\,x, a^8\,x\}, \{a, a^3, a^6, a^8, a\,x, a^3\,x, a^6\,x, a^8\,x\},$$
$$\{a, a^3, a^6, a^8, a\,x, a^4\,x, a^6\,x, a^9\,x\}, \{a, a^3, a^6, a^8, a^2\,x, a^4\,x, a^7\,x, a^9\,x\},$$
$$\{a^2, a^4, a^7, a^9, x, a^2\,x, a^5\,x, a^7\,x\}, \{a^2, a^4, a^7, a^9, x, a^3\,x, a^5\,x, a^8\,x\},$$
$$\{a^2, a^4, a^7, a^9, a\,x, a^3\,x, a^6\,x, a^8\,x\}, \{a^2, a^4, a^7, a^9, a\,x, a^4\,x, a^6\,x, a^9\,x\},$$
$$\{a^2, a^4, a^7, a^9, a^2\,x, a^4\,x, a^7\,x, a^9\,x\}, \{a^3, a^4, a^8, a^9, x, a\,x, a^5\,x, a^6\,x\},$$
$$\{a^3, a^4, a^8, a^9, x, a^4\,x, a^5\,x, a^9\,x\}, \{a^3, a^4, a^8, a^9, a\,x, a^2\,x, a^6\,x, a^7\,x\},$$
$$\{a^3, a^4, a^8, a^9, a^2\,x, a^3\,x, a^7\,x, a^8\,x\}, \{a^3, a^4, a^8, a^9, a^3\,x, a^4\,x, a^8\,x, a^9\,x\}\}$$

```
(*------------------------------------------------------------------------*)
```

Curriculum Vitae

Jose Jonathan Gamez was born on April 10, 1984 at Saint Joseph's Hospital. His parents are Jose Alicio Gamez and Tavita Gamez. Jonathan graduated from Aldine Senor High School in 2003, and attended the University of Houston Downtown graduating in 2008 with a B.S in Applied Mathematics and a minor in Applied Statistics.

In the fall of 2009, he was admitted to the Graduate School at The University of Texas at El Paso, but did not enter until the spring 2010 as a receipient of the Bridge to the Doctorate Fellowship. While pursuing a master's degree in Mathematics, he worked as an Assistant Researcher for Dr. Art Duval.

Permanent address: 411 Sulky Trail
Houston, Texas 77060