APPROVAL PAGE FOR GRADUATE THESIS OR PROJECT

GS-13

SUBMITTED IN PARTIAL FULFILLMENT OF REQUIREMENTS FOR DEGREE OF MASTER OF SCIENCE AT CALIFORNIA STATE UNIVERSITY, LOS ANGELES BY

Preston T. Smith
Candidate

Mathematics
Department

TITLE: **UTILIZING WREATH PRODUCTS TO CONSTRUCT A SEQUENCE OF CAYLEY GRAPHS WITH LOGARITHMIC DIAMETER**

APPROVED:

Dr. Mike Krebs Committee Chairperson	Signature
Dr. Anthony Shaheen Faculty Member	Signature
Dr. Daphne Liu Faculty Member	Signature
Dr. Grant Fraser Department Chairperson	Signature

DATE: **June 12, 2013**

UTILIZING WREATH PRODUCTS TO CONSTRUCT A SEQUENCE OF CAYLEY GRAPHS WITH LOGARITHMIC DIAMETER

A Thesis

Presented to

The Faculty of the Department of Mathematics

California State University, Los Angeles

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

By

Preston T. Smith

June 2013

ACKNOWLEDGMENTS

Preparing this thesis has definitely been my most memorable learning experience at CSULA. I am truly grateful Dr. Krebs, my thesis advisor, gave me the opportunity to work with him during the 2012/2013 academic year. I certainly appreciated all the comments and suggestions Dr. Krebs provided while I was working on this thesis. Most of all, I am grateful he encouraged me to write a mathematical paper.

I would like to also thank Dr. Liu and Dr. Shaheen for serving as committee members and for all their wonderful comments as well. I want to also thank all of the professors at CSULA who taught me mathematics, plus all of the students who studied mathematics with me. I would like to also thank Gustavo A. Gordillo for helping me with figures. They look amazing!

Most of all, I want to say thanks to my family for all of their love and support throughout the years.

ABSTRACT

Utilizing Wreath Products to Construct a

Sequence of Cayley Graphs with Logarithmic Diameter

By

Preston T. Smith

In this thesis, we will recursively construct a sequence of groups using semidirect products. Using it, we will then construct a sequence of symmetric multi-subsets to generate a sequence of 3-regular Cayley graphs with logarithmic diameter. We will then show that our sequence of Cayley graphs is not an expander family.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

CHAPTER 1

Introduction

If we think of graphs as communication networks, then an expander family is considered a quick, inexpensive and reliable communication networks, that is, they are good communication network (see Definition 2.29). Throughout the past few decades, numerous applications of expander families has occurred in computer science, so mathematicians are currently searching for necessary and sufficient conditions to construct expander families with d-regular Cayley graphs, which do in fact exists for each integer $d \geq 3$; Moreover, if a sequence of d-regular Cayley graphs is randomly selected, it will more than likely be an expander family, but constructing an expander family is nontrivial.

According to [3], no sequence of finite abelian groups yields an expander family. Also, solvable groups with bounded derived length does not yield an expander family (§2.4). The optimal diameter growth rate for a sequence of graphs is logarithmic (§2.2). Expander families do in fact have logarithmic diameter; however, if a sequence of d-regular Cayley graphs has logarithmic diameter, it is not necessarily an expander family [3]. For instance, the sequence of cube-connected cycle graphs has logarithmic diameter but it is not an expander family, and this sequence of 3-regular Cayley graphs was constructed by applying wreath products [3].

In Chapter 3, we will also utilize wreath products to construct a sequence of 3-regular Cayley graphs with logarithmic diameter; nevertheless, Proposition 3.6 shows us that this sequence of Cayley graphs is not an expander family. Currently, there is no evidence that shows us a sequence of groups formed by iterating semidirect products with $\mathbb{Z}_2$ can possibly yield an expander family, and this serves as a notable research project.

CHAPTER 2

Preliminaries

2.1 Cayley Graphs

In this section we begin by stating a general definition of a graph, and we will introduce some basic terminology from graph theory that will be applied throughout this paper. However, in this paper, we will mainly be interested in Cayley graphs (see Definition 2.14). Cayley graphs are constructed by elements of a finite group, so we can derive properties of a graph from properties of the group. Proposition 2.16 will provided us with a couple of useful facts about Cayley graphs.

We will use the dihedral group D_n throughout this paper, so see Appendix A for notational conventions and facts about the dihedral group.

Definition 2.1. *A* **multiset** *is, roughly speaking, a set in which elements are allowed to be repeated. The number of times a particular element is listed in a multiset is called the* **multiplicity** *of that element. The* **order** *of a finite multiset S, denoted by $|S|$, is defined to be the number of elements in S, including multiplicity.*

From the definition of a multiset, we see that multisets generalize sets. For example, if $X = \{\alpha, \beta, \xi\}$ and $Y = \{\alpha, \alpha, \alpha, \beta, \beta, \xi\}$ are viewed as sets, then $X = Y$; however, if X and Y are seen as multisets, then $X \neq Y$ since $\alpha \in X$ is of multiplicity 1 while $\alpha \in Y$ is of multiplicity 3. Also, notice that the order of the set Y is 3, but the order of the multiset Y is 6.

Definition 2.2. *A* **graph** X *consists of a vertex set* V *and an edge multiset* E*. The vertex set* V *can be any collection of objects. The elements of the edge multiset* E *are sets of the form* $\{v, w\}$ *where* v *and* w *are distinct vertices, or* $\{v\}$ *where* $v \in V$*. An edge of the form* $\{v\}$ *is referred to as a* **loop***. Two distinct vertices* v *and* w *are* **adjacent** *or* **neighbors** *if* $\{v, w\} \in E$*, in which case we say the edge* $\{v, w\}$ *is incident to the vertices* v *and* w*. A vertex* v *is adjacent to itself if* $\{v\} \in E$*, and we say the loop* $\{v\}$ *is incident to* v*.*

We can easily sketch a graph because they do not require any artistic skills or even a straightedge and compass. To do so, begin by drawing a dot or a circle for each vertex anywhere on a piece of paper. If two vertices are adjacent, draw an arc between their corresponding dots. If a vertex is adjacent to itself, draw a circle at its corresponding dot.

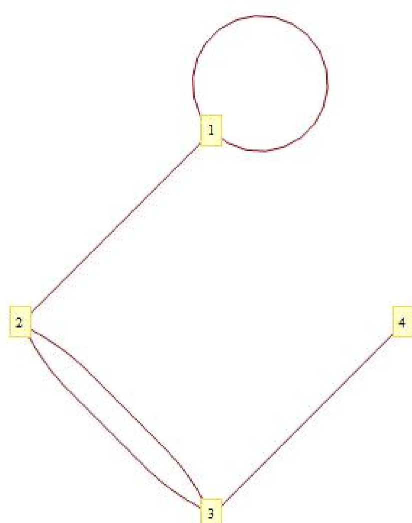

Figure 2.1: A Graph That is Not Regular

In our definition of a graph, we allow our graphs to have multiple edges since E is a multiset; however, some authors refer to a graph with multiple edges as a multigraph. The main focus of this paper will be graphs with no multiple edges, but we have stated a general definition so we can observe various examples throughout this chapter to help us visualize the definitions.

Also, the edges in our definition have no direction because they are defined as sets. If we were interested in directed graphs in this paper, we could simply define an edge to be an ordered pair, say, (v, w) where v is called the initial point and w is called the terminal point, or (v, v) where v is both the initial and terminal point (that is, a loop). However, we will not be using directed graphs in this paper.

Remark 2.3. The graph in Figure 2.1 has vertex set $V = \{1, 2, 3, 4\}$. Notice that the vertex 1 has a loop, and the vertices 2 and 3 are adjacent. Also, the edge $\{2, 3\}$ is of multiplicity 2, that is, there are two edges $\{2, 3\}$ in the edge set that are incident to 2 and 3.

Definition 2.4. *The* **degree** *of a vertex v, denoted by* $\deg(v)$, *is the number of edges incident to v.*

Definition 2.5. *The* **order of a graph** X, *denoted by* $|X|$, *equals the cardinality of the vertex set.*

Remark 2.6. In figure 2.1, $\deg(4) = 1$ and $\deg(3) = 3$, and the order of the graph is 4. The order of the graph is figure 2.2 is 8.

Definition 2.7. *A graph is said to be* d**-regular** *when every vertex has degree d.*

Remark 2.8. The graph in Figure 2.1 is not a regular graph since $\deg(4) = 1$ and $\deg(3) = 3$. The graphs in Figures 2.2 and 2.5 are both 3-regular graphs. The graph in Figure 2.3 is 2-regular. The graph in Figure 2.4 is 4-regular.

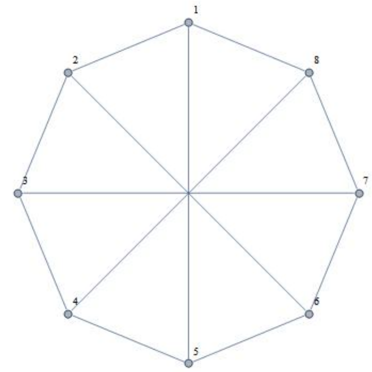

Figure 2.2: Cay($\mathbb{Z}_8, \{1, 4, 7\}$)

Definition 2.9. *Let X be a graph with vertex set V, and let $v_0, v_n \in V$. A* **walk of length** *n from v_0 to v_n in X is a finite sequence in the form*

$$w = (v_0, v_1, \dots, v_n)$$

where v_i is adjacent to v_{i+1} for $i = 0, 1, \dots, n-1$.

Definition 2.10. *A graph X with vertex set V is* **connected** *if for any $x, y \in V$ there is a walk from x to y. Otherwise, the graph is said to be* **disconnected***.*

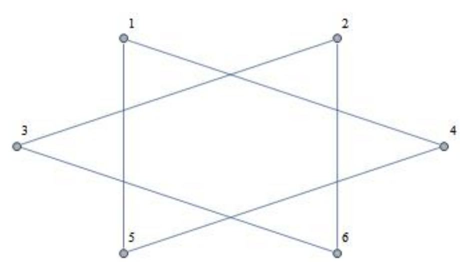

Figure 2.3: A Disconnected Graph

Remark 2.11. The graph in Figure 2.3 is disconnected since there is no walk from vertex 1 to the vertex 2. The graphs in Figures 2.2 and 2.4 are connected.

Definition 2.12. *Let X be a graph with vertex set V. The* **distance** *between two vertices $x, y \in V$, denoted by* $\operatorname{dist}(x, y)$*, is defined to be the minimal length of all walks from x to y; however, if there is no walk from x to y in X, we will define* $\operatorname{dist}(x, y) = \infty$*. The* **diameter** *of X is given by*

$$\operatorname{diam}(X) = \max_{x,y\in V} \operatorname{dist}(x, y).$$

According to our definition, note that $\operatorname{diam}(X) = \infty$ if X is disconnected.

Definition 2.13. *Let G be a group. A subset Γ of G is called a* **symmetric subset** *of G if $\gamma^{-1} \in \Gamma$ for each $\gamma \in \Gamma$. We will write $\Gamma \Subset G$ to denote that Γ is a symmetric subset of G.*

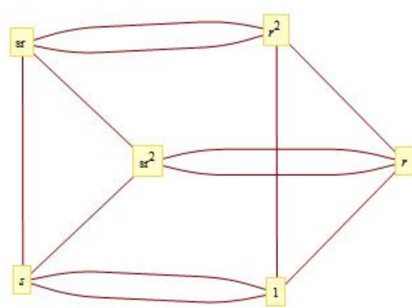

Figure 2.4: $\operatorname{Cay}(D_6, \{s, s, r, r^2\})$

Definition 2.14. *Let G be a group and $\Gamma \Subset G$. The* **Cayley graph** *of G with respect to Γ, denoted* $\operatorname{Cay}(G, \Gamma)$*, is defined as follows:*

(1) *G is the vertex set.*

(2) *Two vertices $g, h \in G$ are adjacent if and only if there exists $\gamma \in \Gamma$ such that $x = y\gamma$.*

Remark 2.15. The graphs in Figures 2.2, 2.4, and 2.5 are examples of Cayley graphs.

Proposition 2.16. *Suppose G is a group and $\Gamma \Subset_{s} G$. Then the following statements are true:*

(1) $\mathrm{Cay}(G,\Gamma)$ *is $|\Gamma|$-regular, and*

(2) $\mathrm{Cay}(G,\Gamma)$ *is connected if and only if Γ generates G as a group.*

Proof of (1). Suppose $g \in G$ is a vertex of $\mathrm{Cay}(G,\Gamma)$, and suppose $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_d\}$. Then by definition, the neighbors of g are the vertices $g\gamma_1, g\gamma_2, \ldots, g\gamma_d$, which includes multiplicity since each element of Γ is listed above and γ_i's are not necessarily distinct. Hence, g is adjacent to exactly d vertices, so there are exactly d edges incident to g, and so the vertex g has degree $d = |\Gamma|$. Since g was arbitrary and $\deg(g) = d$, we see that $\mathrm{Cay}(G,\Gamma)$ is $|\Gamma|$-regular as claimed. $\square$

Proof of (2). Let 1_G be the identity element of the group G and let $g \in G$. Suppose $\mathrm{Cay}(G,\Gamma)$ is a connected graph, then there is a walk from 1_G to g, and so there exist $\gamma_1, \ldots, \gamma_n \in \Gamma$ such that

$$g = (1_G\gamma_1 \cdots \gamma_{n-1})\gamma_n = \gamma_1 \cdots \gamma_n.$$

Since g is written as a finite product of elements of Γ, this shows us that Γ generates G as a group.

Conversely, suppose Γ generates G. Let $g \in G$. Then there exist $\gamma_1, \ldots, \gamma_n \in \Gamma$ so that $g = \gamma_1 \cdots \gamma_n = 1_G\gamma_1 \cdots \gamma_n$. Notice that $1_G\gamma_1 \cdots \gamma_n$ gives the walk

$$(1_G, 1_G\gamma_1, 1_G\gamma_1\gamma_2, \ldots, 1_G\gamma_1 \cdots \gamma_n) = (1_G, 1_G\gamma_1, \ldots, g).$$

So, for any $g \in G$ there is a walk from 1_G to g. Thus, for every $h, g \in G$, there is a walk from g to h; it can easily be obtained by reversing the order of the walk from g

to 1_G and then traversing the walk from 1_G to h. Therefore, $\mathrm{Cay}(G, \Gamma)$ is a connected graph. □

2.2 Diameters of Cayley Graphs

According to [3], the best possible diameter growth rate for a sequence d-regular Cayley graphs is logarithmic. We begin this section by introducing the type of sequence we desire. But, the main purpose of this section is to discuss how we can find the diameter of a Cayley graph in terms of the underlying group structure in Proposition 2.22.

Definition 2.17. *Let f and g be real-valued functions defined on the set of natural numbers. If there exists a positive real number C and a natural number N such that $|f(n)| \leq C|g(n)|$ for every $n > N$, we will write $f(n) = O(g(n))$. Otherwise, we will write $f(n) \neq O(g(n))$.*

The "big oh" notation tells us the behavior of a function f for large enough values of n. That is, we will use "big oh" notation to help us estimate the end behavior of a function $f(n)$ as n tends to ∞ compared to a standard function that is familiar to us. More precisely, for the purpose of this paper, we will search for a sequence of graphs whose diameters have a growth rate less than or equal to the growth rate of a constant multiple of the logarithmic function of the order for sufficiently large values of n.

Definition 2.18. *A sequence (X_n) of graphs is said to have* **logarithmic diameter** *if*

$$\mathrm{diam}(X_n) = O(\log |X_n|).$$

Definition 2.19. *Let (G_n) be a sequence of finite groups. If a sequence of d-regular Cayley graphs* $\mathrm{Cay}(G_n, \Gamma_n)$ *has logarithmic diameter, then (G_n) is said to have* **logarithmic diameter**.

Definition 2.20. *Let Γ be some set. If $n \geq 1$, then a* **word of length** *n in Γ is an element of the Cartesian product*

$$\Gamma \times \cdots \times \Gamma = \Gamma^n.$$

If G is a group, $\Gamma \subset_s G$, and $w = (w_1, ..., w_n) \in \Gamma^n$, then we say w **evaluates** *to $g \in G$ if $g = w_1 \cdots w_n$.*

Definition 2.21. *Let G be a group and $\Gamma \subset G$. If $g \in G$ can be written as a word in Γ, we define the* **word norm** *of g in Γ to be the minimal length of any word in Γ that evaluates to g. If $g \in G$ can not be expressed as a word in Γ, we define the word norm of g in Γ to be ∞.*

According to [3], "the standard convention is to say that the word of length 0 evaluates to the identity element. So the identity element has word norm 0."

Proposition 2.22. *Suppose G is a finite group and $\Gamma \subset_s G$. Let $X = \mathrm{Cay}(G, \Gamma)$. Then the following statements are true:*

(1) *X is a connected graph if and only if each element of G can be expressed as a word in Γ.*

(2) *Suppose $a, b \in G$ and there exists a walk in X from a to b. Then the distance from a to b is the word norm of $a^{-1}b \in \Gamma$.*

(3) *The diameter of X is equal to the maximum of all the word norms in Γ of elements in G.*

Proof. (1) The details of this proof are equivalent to part (2) of Proposition 2.16.

(2) Suppose $(g_0, g_1, \ldots, g_n)$ is a walk of length n in X from a to b. Note that $g_0 = a$ and $g_n = b$. Since g_{i-1} and g_i are adjacent vertices for each $i = 1, \ldots, n$, $g_{i-1}^{-1} g_i \in \Gamma$. So, let $\gamma_i = g_{i-1}^{-1} g_i$ for each $i = 1, \ldots, n$. Then notice that

$$\gamma_1 \gamma_2 \cdots \gamma_n = g_0^{-1} g_1 g_1^{-1} g_2 \cdots g_{n-1}^{-1} g_n = g_0^{-1} g_n = a^{-1} b,$$

and so we see that the word $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ of length n in Γ evaluates to $a^{-1}b$.

Conversely, if we are given a word of length n in Γ that evaluates to $a^{-1}b$ and we reverse the procedure above, we will see that there is a corresponding walk of length n in X from a to b.

Recall that the distance from a to b in X is equal to the minimal length of all walks in X from a to b, which is equivalent to saying the distance from a to b in X equals the minimal length of any word on Γ that evaluates to $a^{-1}b$. Therefore, the distance from a to b in X is equal to the word norm of $a^{-1}b \in \Gamma$.

(3) Recall that

$$\operatorname{diam}(X) = \max_{x,y \in G} \operatorname{dist}(x, y).$$

By (2) $\operatorname{dist}(x, y)$ equals the word norm of $x^{-1}y \in \Gamma$, and so $\operatorname{diam}(X)$ equals the maximum of word norms in Γ of elements in G as desired. $\square$

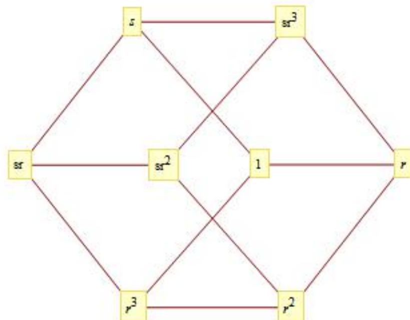

Figure 2.5: $\text{Cay}(D_4, \{s, r, r^3\})$

Remark 2.23. Let $X = \text{Cay}(D_4, \{s, r, r^3\}$ as shown in Figure 2.5. Notice that the word norm of sr^2 in Γ is 3 since (s, r, r) is a word of minimal length in Γ that evaluates to sr^2, and in fact, $\text{diam}(X) = 3$.

2.3 Isopermetric Constants and Expander Families

The objective of this section is to define the isopermetric constant of a graph, define an expander family, plus make reference to the Quotients Nonexpansion Principle. Intuitively speaking, the isopermetric constant is a quantity that measures the rate information flows through the graph, and according to [3], "the isoperimetric constant provides some measure of connectivity in a graph." Roughly speaking, expander families are good communication networks. We will use the Quotients Nonexpansion Principle in Chapter 3 to show that the sequence of Cayley graphs we will construct is not an expander family.

Definition 2.24. *Let X be a graph with vertex set V and edge set E. Let $F \subset V$. The set*

$$\partial F = \{\{v, w\} \in E \mid v \in F, w \in V - F\}$$

is called the **boundary** *of F.*

Notice that ∂F is the set of edges in X connecting F to $V-F$, that is, the set of edges incident to a vertex of F and a vertex of $V-F$. Also, note that $\partial F = \partial(V-F)$.

Definition 2.25. *The* **isoperimetric constant** *of a graph X with vertex set V is defined to be*

$$\begin{aligned} h(X) &= \min\left\{\frac{|\partial F|}{|F|} : F \subset V, |F| \leq \frac{|V|}{2}\right\} \\ &= \min\left\{\frac{|\partial F|}{\min\{|F|, |V-F|\}} : F \subset V\right\}. \end{aligned}$$

The isoperimetric constant has various names throughout the literature such as the expansion constant, the edge expansion constant, the conductance, or the Cheeger constant.

Remark 2.26. *Suppose X is a graph with vertex set V. If $F \subset V$ with $|F| \leq \frac{|V|}{2}$, then by definition $|\partial F| \geq h(X)|F|$, and so we see that the size of the boundary of F is at least $h(X)$ times the size of F.*

Definition 2.27. *Suppose (α_n) is a sequence of nonzero real numbers. Then (α_n) is said to be* **bounded away from zero** *if there exists a real number $\epsilon > 0$ so that $\alpha_n \geq \epsilon$ for every n.*

Example 2.28. *The sequence $\left(\frac{1}{2^n}\right)$ is not bounded away from zero, but the sequence $\left(\frac{2n+3}{5n+7}\right)$ is bounded away from zero.*

Definition 2.29. *Suppose d is a positive integer. Suppose (X_n) is a sequence of d-regular graphs such that $|X_n| \to \infty$ as $n \to \infty$. If the sequence $(h(X_n))$ is bounded away from zero, then (X_n) is called an* **expander family**.

Definition 2.30. *Let (G_n) and (Q_n) be sequences of finite groups. If for each n there* *exists* $H_n \trianglelefteq G_n$ *such that* $G_n/H_n \cong Q_n$*, we will say* (G_n) **admits** (Q_n) **as a sequence of quotients**.

Definition 2.31. *A sequence* (G_n) *of finite groups* **yields an expander family** *if for some* $d \in \mathbb{N}$ *there is a sequence* (Γ_n)*, where for each* n *we have that* $\Gamma_n \subseteq_s G_n$ *with* $|\Gamma_n| = d$*, such that the sequence of Cayley graphs* $\mathrm{Cay}(G_n, \Gamma_n)$ *is an expander family.*

The next proposition, called the Quotients Nonexpansion Principle, was found in [3], and it is an extremely important result which we will apply in the proof of Proposition 3.6.

Proposition 2.32 (Quotients Nonexpansion Principle)**.** *Let* (G_n) *be a sequence of finite groups. If* (G_n) *admits* (Q_n) *as a sequence of quotients,* $|Q_n| \to \infty$*, and* (Q_n) *does not yield an expander family, then* (G_n) *does not yield an expander family.*

The details for the proof of the Quotients Nonexpansion Principle can be found in [3] on page 54.

2.4 Solvable Groups and Derived Length

In this section, we being by reviewing the definition of a commutator subgroup, plus we will remind ourselves of a few properties in Proposition 2.34 and Proposition 2.36. Then we will discuss the definition of a solvable group with derived length. In Example 2.40, we will see that the dihedral group D_n is solvable with derived length. The highlight of this section is Theorem 2.41, which is an important result from [4]; in short, it states that a sequence of solvable groups with bounded derived length is not an expander family. We take advantage of Theorem 2.41 by applying it in Example 2.42.

Definition 2.33. *Let G be a group and let $g, h \in G$. The* **commutator** *of g and h is defined by $[g, h] = g^{-1}h^{-1}gh$. The* **commutator subgroup** *of G, denoted G', is the subgroup of G generated by all commutators in G, that is, $G' = \langle [g, h] \mid g, h \in G \rangle$.*

Notice that $[g, h] = g^{-1}h^{-1}gh = 1$ if and only if $gh = hg$; that is $[g, h] = 1$ if and only if g and h commute, which explains the name "commutator." Moreover, a group G is abelian if and only if $[g, h] = 1$ for every $g, h \in G$, and so G is abelian if and only if $G' = 1$.

Now, we will introduce some useful statements regarding commutator subgroups.

Proposition 2.34. *If G is a group, then $G' \trianglelefteq G$.*

Proof. Let $g \in G$ and let $[\alpha, \beta] \in G'$. Then

$$\begin{aligned} g[\alpha, \beta]g^{-1} &= g\alpha^{-1}\beta^{-1}\alpha\beta g^{-1} \\ &= g\alpha^{-1}g^{-1}g\beta^{-1}g^{-1}g\alpha g^{-1}g\beta g^{-1} \\ &= (g\alpha g^{-1})^{-1}(g\beta g^{-1})^{-1}(g\alpha g^{-1})(g\beta g^{-1}) \in G'. \end{aligned}$$

Therefore, $gG'g^{-1} \subset G'$ for every $g \in G$, and so $G' \trianglelefteq G$. □

Lemma 2.35. *Let G be a group. Then G/G' is abelian.*

Proof. Let $\alpha H, \beta H \in G/G'$. Then

$$\begin{aligned}
(\alpha G')(\beta G') &= (\alpha\beta)G' \\
&= (\beta\beta^{-1}\alpha\beta)G' \\
&= (\beta\alpha\alpha^{-1}\beta^{-1}\alpha\beta)G' \\
&= (\beta\alpha[\alpha,\beta])G' \\
&= ((\beta\alpha)G')([\alpha,\beta]G') \\
&= (\beta\alpha)G' && \text{since } [\alpha,\beta] \in G' \\
&= (\beta G')(\alpha G').
\end{aligned}$$

Ergo, G/G' is an abelian group. □

Proposition 2.36. *Suppose G is a group. If $H \trianglelefteq G$, then G/H is abelian if and only if $G' \leq H$.*

Proof. Let $H \trianglelefteq G$, and suppose G/H is an abelian group. Then for every $\alpha, \beta \in G$, $(\alpha H)(\beta H) = (\beta H)(\alpha H)$, and so

$$\begin{aligned}
1H &= (\alpha H)^{-1}(\beta H)^{-1}(\alpha H)(\beta H) \\
&= (\alpha^{-1}\beta^{-1}\alpha\beta)H \\
&= [\alpha,\beta]H.
\end{aligned}$$

Hence $1H = [\alpha,\beta]H$ for every $\alpha, \beta \in G$, which implies that $[\alpha,\beta] \in H$ for every $\alpha, \beta \in G$. Therefore, $G' \leq H$ as claimed.

Conversely, suppose $G' \leq H$. By Lemma 2.35, G/G' is an abelian group, which implies that every subgroup of G/G' is normal. So, $H/G' \trianglelefteq G/G'$. According to the Lattice Isomorphism Theorem [2], $H \trianglelefteq G$, and according to the Third Isomorphism

Theorem [2],

$$G/H \cong (G/G')/(H/G').$$

Since G/G' is an abelian group, the quotient $(G/G')/(H/G')$ is also an abelian group.

Therefore, G/H is abelian as desired. $\square$

Definition 2.37. *Let G be a group. Define the commutator of two subgroups H and K of G by $[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle$.*

Definition 2.38. *Let G be a group. Recursively define a sequence of subgroups of G as follows:*

$$G^{(0)} = G, \quad G^{(1)} = [G, G], \quad \textit{and} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad \textit{for each } i \geq 1.$$

This sequence of subgroups is called the **derived** *or* **commutator series** *of G, and we say $G^{(i)}$ is the i^{th}* **derived subgroup** *of G.*

Definition 2.39. *A group G is said to be* **solvable with derived length** *n if $G^{(m)} = 1$ for some integer m, and n is the smallest nonnegative number such that $G^{(n)} = 1$.*

For a nontrivial group G, notice that $G^{(1)} = G'$, and so G is abelian if and only if $G^{(1)} = 1$; that is, G is abelian if and only if G is solvable with derived length 1.

Example 2.40. In this example we will find the derived length of the dihedral group

$$D_n = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle \quad \text{for each } n \geq 1.$$

Recall that $D_1 \cong \mathbb{Z}_2$ and $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and so we see that D_1 and D_2 are solvable of derived length 1 since $\mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are abelian groups.

Next, suppose $n \geq 3$. Notice that $s^{-1}r^{-1}sr = s^{-1}srr = r^2 \in D_n'$, and so $\langle r^2 \rangle \leq D_n'$.

If n is even, let $\phi\colon D_n \to \mathbb{Z}_2 \times \mathbb{Z}_2$ be defined by $\phi(r^j s^k) = (j,k)$. Clearly, ϕ maps D_n onto $\mathbb{Z}_2 \times \mathbb{Z}_2$. Let's show ϕ is a homomorphism. Let $x, y \in D_n$. Then $x = r^i s^j$ and $y = r^k s^l$ for some $i,j,k,l \in \mathbb{Z}$. So,

$$\begin{aligned}
\phi(xy) &= \phi(r^i s^j r^k s^l) \\
&= \phi(r^i r^{-k} s^j s^l) \\
&= \phi(r^{i-k} s^{j+l}) \\
&= (i-k, j+l) \\
&= (i,j) + (-k,l) \\
&= (i,j) + (k,l) && \text{since } -k \equiv_2 k \\
&= \phi(r^i s^j) + \phi(r^k s^l) \\
&= \phi(x) + \phi(y).
\end{aligned}$$

So, ϕ is a homomorphism from D_n onto $\mathbb{Z}_2 \times \mathbb{Z}_2$. Note that $\ker \phi = \langle r^2 \rangle$, and so by the first isomorphism theorem, $\langle r^2 \rangle \trianglelefteq D_n$ and $D_n/\langle r^2 \rangle \cong \phi(D_n) = \mathbb{Z}_2 \times \mathbb{Z}_2$. So, we see that $D_n/\langle r^2 \rangle$ is abelian, and so $D_n' \leq \langle r^2 \rangle$ by Proposition 2.36. Now, suppose n is odd. Let $\phi\colon D_n \to \mathbb{Z}_2$ be defined by $\phi(r^i s^j) = j$. Clearly, ϕ is a surjective map. Let's show ϕ is a homomorphism. Let $x, y \in D_n$. Then $x = r^i s^j$ and $y = r^k s^l$ for some $i, j, k, l \in \mathbb{Z}$, and so

$$\begin{aligned}
\phi(xy) &= \phi(r^i s^j r^k s^l) \\
&= \phi(r^{i-k} s^{j+k}) \\
&= j + k \\
&= \phi(r^i s^j) + \phi(r^k s^l) \\
&= \phi(x) + \phi(y).
\end{aligned}$$

Hence, ϕ is a surjective homomorphism from D_n onto $\mathbb{Z}_2$, and so by the first isomorphism theorem, $\ker \phi = \langle r \rangle = \langle r^2 \rangle \cong D_n$ and $G/\langle r^2 \rangle \cong \mathbb{Z}_2$. Hence $G/\langle r^2 \rangle$ is abelian, so $D_n' \leq \langle r^2 \rangle$ by Proposition 2.36.

Therefore, $D_n' = \langle r^2 \rangle$ for each $n \geq 3$, and since $\langle r^2 \rangle$ is abelian, we see that $D_n^{(2)} = \langle r^2 \rangle' = 1$. Ergo, D_n is solvable with derived length 2 for each $n \geq 3$.

The next theorem was acquired from [4] and it is a remarkable result in graph theory because it tells us that a sequence of solvable groups, where each group has derived length less than or equal to some fix natural number, never yields an expander family.

Theorem 2.41. *Let (G_n) be a sequence of finite nontrivial groups such that $|G_n| \to \infty$. Let k be a positive integer. For each n, suppose that G_n is solvable with derived length $\leq k$. Then (G_n) does not yield an expander family.*

We will omit the proof of Theorem 2.41, but we highly encourage an eager reader to see [4] for the details. The authors of [3] apply Theorem 2.41 to show that the sequence of cube-connected cycle graphs is not an expander family.

Example 2.42. According to Example 2.40 and Theorem 2.41, the sequence (D_n)

of dihedral groups does not yield an expander family.

We will refer back to Example 2.42 in the proof of Proposition 3.6.

2.5 Semidirect Products

In this section we begin by recalling the definition of an automorphism of a group. Then we will define the semidirect products of two groups, which is a generalization of the direct products of two groups. Plus, we will state some useful facts about semidirect products to help us achieve our objective. Furthermore, we will consider a special type of semidirect product called the wreath product.

Definition 2.43. *An isomorphism from a group G to itself is called an* **automorphism**. *The set of all automorphisms of a group G is denoted* $\mathrm{Aut}(G)$. *The set* $\mathrm{Aut}(G)$ *under function composition is called the* **automorphism group** *of G.*

According to [2], the automorphism group is in fact a group since function composition is associative, the identity element $\mathrm{Aut}(G)$ is precisely the identity function on G, and there exists an inverse function for each function in $\mathrm{Aut}(G)$.

Definition 2.44. *Let H and K be groups. Let θ be a homomorphism from K to* $\mathrm{Aut}(H)$. *Let $G = \{(h,k) \mid h \in H, k \in K\}$. Define the binary operation $*$ on G by*

$$(h_1, k_1) * (h_2, k_2) = (h_1[\theta(k_1)](h_2), k_1k_2).$$

The **semidirect product** *of the groups G and K with respect to θ, denoted by $H \rtimes_\theta K$, is the set G under the binary operation $*$.*

When no confusion will arise, we will sometimes omit θ from the subscript. Before we state some useful facts about semidirect products, let's make note of a couple of observations that will be quite useful in the proofs to come. Firstly, because

θ is a homomorphism, notice that

$$[\theta(k_1k_2)](h) = [\theta(k_1)\theta(k_2)](h) = [\theta(k_1)]([\theta(k_2)](h)) \tag{2.1}$$

for each $k_1, k_2 \in K$ and $h \in H$.

Secondly, because $\theta(k)$ for each $k \in K$ is a homomorphism,

$$[\theta(k)](h_1h_2) = [\theta(k)](h_1)[\theta(k)](h_2) \tag{2.2}$$

for every $h_1, h_2 \in H$.

Theorem 2.45. *Let H and K be groups, and let $\theta\colon K \to \mathrm{Aut}(H)$ be a homomorphism. Then $H \rtimes K$ is a group.*

Proof. Let $G = \{(h,k) \mid h \in H, k \in K\}$. Let's begin by verifying the associative law. Let $(h_1,k_1),(h_2,k_2),(h_3,k_3) \in G$. Since θ is a homomorphism, we have the following

$$\begin{aligned}
[(h_1,k_1) * (h_2,k_2)] * (h_3,k_3) &= (h_1[\theta(k_1)](h_2), k_1k_2) * (h_3,k_3) \\
&= (h_1[\theta(k_1)](h_2)[\theta(k_1k_2)](h_3), k_1k_2k_3) \\
&= (h_1[\theta(k_1)](h_2)[\theta(k_1)]([\theta(k_2)](h_3)), k_1k_2k_3) \\
&= (h_1[\theta(k_1)](h_2[\theta(k_2)](h_3)), k_1k_2k_3) \\
&= (h_1,k_1) * (h_2[\theta(k_2)](h_3), k_2k_3) \\
&= (h_1,k_1) * [(h_2,k_2) * (h_3,k_3)].
\end{aligned}$$

Hence, for each $(h_1,k_1),(h_2,k_2),(h_3,k_3) \in G$,

$$[(h_1,k_1) * (h_2,k_2)] * (h_3,k_3) = (h_1,k_1) * [(h_2,k_2) * (h_3,k_3)],$$

and so the binary operation $*$ on G is associative.

Next, let $1_H, 1_K$ be the identity elements of H and K, respectively. We now show that $(1_G, 1_K)$ is the identity element of G. Let $(h, k) \in G$. Since θ is a homomorphism, we see that

$$(1_H, 1_K) * (h, k) = (1_H[\theta(1_K)](h), 1_H k) = ([\theta(1_K)](h), k) = (h, k).$$

Thus, $(1_H, 1_K) * (h, k) = (h, k)$ for every $(h, k) \in G$, and therefore $(1_H, 1_K) \in G$ is the identity element.

Finally, let's show that $(h, k)^{-1} = ([\theta(k^{-1})](h^{-1}), k^{-1})$ for every $(h, k) \in G$. So,

$$\begin{aligned}
([\theta(k^{-1})](h^{-1}), k^{-1}) * (h, k) &= ([\theta(k^{-1})](h^{-1})[\theta(k^{-1})](h), k^{-1}k) \\
&= ([\theta(k^{-1})](h^{-1}h), 1_K) \\
&= ([\theta(k^{-1})](1_H), 1_K) \\
&= (1_H, 1_K).
\end{aligned}$$

Hence, $([\theta(k^{-1})](h^{-1}), k^{-1}) * (h, k) = (1_H, 1_K)$ for each $(h, k) \in G$, and so

$$(h, k)^{-1} = ([\theta(k^{-1})](h^{-1}), k^{-1}).$$

Therefore, the semidirect product of the groups H and K with respect to homomorphism θ is a group. □

As seen in the proof of Theorem 2.45, the computation can easily become cluttered with excess notation, so we will omit the binary operation $*$ from further computations. Plus, we will omit the subscripts on the identity elements of H and K.

Proposition 2.46. *Suppose H, K and θ are defined as in Definition 2.44. Let $\overline{H} = \{(h,1) \mid h \in H\} \subset H \rtimes K$, and let $\overline{K} = \{(1,k) \mid k \in K\} \subset H \rtimes K$. Then $\overline{H}$ and $\overline{K}$ are subgroups of $H \rtimes K$. Moreover, for each $h \in H$, the map $h \mapsto (h,1)$ is an isomorphism between H and $\overline{H}$. Similarly, for each $k \in K$, the map $k \mapsto (1,k)$ is an isomorphism between K and $\overline{K}$.*

Proof. Clearly, $\overline{H}$ and $\overline{K}$ are nonempty sets because H and K are groups. Let $(h_1,1),(h_2,1) \in \overline{H}$. Then

$$\begin{aligned}(h_1,1)(h_2,1)^{-1} &= (h_1,1)([\theta(1)](h_2^{-1}),1)\\ &= (h_1,1)(h_2^{-1},1)\\ &= (h_1[\theta(1)](h_2^{-1}),1)\\ &= (h_1h_2^{-1},1).\end{aligned}$$

Since H is a group, $h_1h_2^{-1} \in H$, and so $(h_1,1)(h_2,1)^{-1} \in \overline{H}$. Hence, $\overline{H}$ is a subgroup of $H \rtimes K$ by the subgroup criterion. Furthermore, a similar computation shows us that the map $h \mapsto (h,1)$ is a homomorphism from H to $\overline{H}$. Notice that the kernel of the map is the set

$$\ker = \{h \mid h \mapsto (1,1)\} = \{1\}.$$

Since the map is a homomorphism and $\ker = \{1\}$, the map is injective (see Corollary A.2). Clearly, by the definition of $\overline{H}$, the map is surjective. Therefore, the map defines an isomorphism between H and $\overline{H}$ as claimed.

Similarly, suppose $(1, k_1), (1, k_2) \in \overline{K}$. Then

$$\begin{aligned}(1, k_1)(1, k_2)^{-1} &= (1, k_1)([\theta(k_2^{-1})](1), k_2^{-1}) \\ &= (1, k_1)(1, k_2^{-1}) \\ &= (1[\theta(k_1)](1), k_1 k_2^{-1}) \\ &= (1, k_1 k_2^{-1}).\end{aligned}$$

Thus, $(1, k_1)(1, k_2)^{-1} \in \overline{K}$ since $k_1 k_2^{-1} \in K$. Ergo, $\overline{K}$ is also a subgroup of $H \rtimes K$. Moreover, a similar argument shows that the map $k \mapsto (1, k)$ is an isomorphism from K to $\overline{K}$. $\square$

With Proposition 2.46 in mind, we may occasionally be imprecise and refer to H as a subgroup of $H \rtimes K$ when we really mean its isomorphic copy $\overline{H}$, and we sometimes abuse notation and write h for $(h, 1)$. Likewise, we will regard K as a subgroup of $H \rtimes K$ and sometimes abuse notation by writing k for $(1, k)$.

Suppose θ is defined as in Definition 2.44. To simplify computation, we denote $[\theta(k)](h)$ by ${}^k h$, and applying this notation to (2.1), we have the following

$$ {}^{k_1 k_2} h = {}^{k_1}({}^{k_2} h). \tag{2.3}$$

Similarly, applying our new notation to (2.2), we see that

$$ {}^{k}(h_1 h_2) = ({}^{k} h_1)({}^{k} h_2). \tag{2.4}$$

Lemma 2.47. *Let $h \in H$ and $k \in K$. Then $khk^{-1} = {}^k h$ in $H \rtimes K$.*

Proof. Let $h \in H$ and $k \in K$. Then

$$\begin{aligned} khk^{-1} &= [(1,k)(h,1)](1,k^{-1}) \\ &= (1[\theta(k)](h), k1)(1,k^{-1}) \\ &= ([\theta(k)](h), k)(1,k^{-1}) \\ &= ([\theta(k)](h)[\theta(k)](1), kk^{-1}) \\ &= ([\theta(k)](h)1, 1) \\ &= ([\theta(k)](h), 1) \\ &= ({}^{k}h, 1). \end{aligned}$$

Hence, $khk^{-1} = {}^{k}h$ in $H \rtimes K$ for every $h \in H$ and $k \in K$. □

Lemma 2.47 will be quite useful in the proof of Proposition 3.4.

Proposition 2.48. *Suppose H, K and θ are defined as in Definition 2.44. Then H is a normal subgroup of $H \rtimes K$.*

Proof. By Proposition 2.46, $\overline{H} = \{(h,1) \mid h \in H\}$ is a subgroup of $H \rtimes K$ and $H \cong \overline{H}$. So, to prove the proposition, let's show $g\overline{H}g^{-1} \subset \overline{H}$ for each $g \in H \rtimes K$. Let $(h,1) \in \overline{H}$. Let $g \in H \rtimes K$, then $g = (h_1, k)$ for some $h_1 \in H$ and $k \in K$. Recall that $(h_1,k)^{-1} = ([\theta(k^{-1})](h_1^{-1}, k^{-1})$ according to Theorem 2.45. Also, notice that

$(h_1, 1)(1, k) = (h_1, k)$, and $(1, k^{-1})(h^{-1}, 1) = ([\theta(k^{-1})](h_1^{-1}), k^{-1}) = (h_1, k)^{-1}$. So,

$$\begin{aligned} g(h,1)g^{-1} &= (h_1, k)(h, 1)(h_1, k)^{-1} \\ &= (h_1, 1)(1, k)(h, 1)(1, k^{-1})(h_1^{-1}, 1) \\ &= (h_1, 1)([\theta(k)](h), 1)(h_1^{-1}, 1) \\ &= (h_1[\theta(k)](h), 1)(h_1^{-1}, 1) \\ &= (h_1[\theta(k)](h)h_1^{-1}, 1). \end{aligned}$$

Since θ maps K to $\mathrm{Aut}(H)$, $[\theta(k)](h) \in H$, and so $h_1[\theta(k)](h)h_1^{-1} \in H$ because H is a group.

Hence, $g(h, 1)g^{-1} = (h_1[\theta(k)](h)h_1^{-1}, 1) \in \overline{H}$. Therefore $g\overline{H}g^{-1} \subset \overline{H}$ for every $g \in H \rtimes K$. Ergo, $\overline{H}$ is a normal subgroup of $H \rtimes K$ as claimed. □

According to [2], we use the notation $\rtimes$ in $H \rtimes K$ to tell us that the copy of H is the normal "factor" in the semidirect product of H and K with respect to θ because K is not necessarily normal in $H \rtimes K$. In fact, K is normal in $H \rtimes K$ if and only if θ is the trivial homomorphism from K to $\mathrm{Aut}(H)$. Also, the semidirect product of H and K with respect to the identity homomorphism from K into $\mathrm{Aut}(H)$ is identical to the direct product of H and K, and so we see that direct products are a special case of semidirect products; that is, semidirect products are a generalization of direct products where the condition of both sets being normal in the product has been reduced to one set being normal in the product [2].

Proposition 2.49. $(H \rtimes K)/H \cong K$.

Proof. Suppose $\varphi\colon H \rtimes K \to K$ is defined by $\varphi(h, k) = k$. We begin by showing φ is a homomorphism. Let $(h_1, k_1), (h_2, k_2) \in H \rtimes K$. Then

$$\begin{aligned}
\varphi((h_1, k_1)(h_2, k_2)) &= \varphi(h_1[\theta(k_1)](h_2), k_1k_2) \\
&= k_1k_2 \\
&= \varphi(h_1, k_1)\varphi(h_2, k_2).
\end{aligned}$$

Thus φ is a homomorphism. Clearly, by definition of $H \rtimes K$, φ maps $H \rtimes K$ onto K.

Next, notice that

$$\begin{aligned}
\ker \phi &= \{(h, k) \mid \varphi((h, k)) = 1\} \\
&= \{(h, 1) \mid h \in H\} \\
&= \overline{H}.
\end{aligned}$$

So, by the First Isomorphism Theorem, $(H \rtimes K)/H \cong \varphi(H \rtimes K)$.

Therefore $(H \rtimes K)/H \cong K$ as claimed. $\square$

2.5.1 Wreath Products

Next, let's introduce a special type of semidirect product called the wreath product. It will be useful when we construct certain Cayley graphs in Chapter 3. Let J be a finite set. Let H and K be groups. Let $H^J = \oplus_{j \in J} H$ be the direct product of $|J|$ copies of H. Notice that the elements of H^J are $|J|$-tuples $(h_j)_{j \in J}$, where $h_j \in H$ for each j. Let θ be an action of K on J. Then θ induces a homomorphism form K to $\mathrm{Aut}(H^J)$ defined by $(h_j)_{j \in J} \mapsto (h_{\theta(j)})_{j \in J}$. This map is also denoted by θ. Using this notation, we can now formally define the wreath product.

Definition 2.50. *The* **wreath product** *of H and K, denoted $H \wr_\theta K$, is defined by*

$$H \wr_\theta K := H^J \rtimes_\theta K.$$

When θ is understood, we'll usually omit the subscript.

CHAPTER 3

Constructing a Sequence of 3-Regular Cayley Graphs with Logarithmic Diameter

At last, we have finally developed enough machinery to accomplish our goal. In this chapter we begin by recursively constructing a sequence (K_n) of groups by iterating semidirect products of $\mathbb{Z}_2$. The ideas to construct such a sequence were obtained from [1]. Then, we will apply wreath products to construct a sequence (Λ_n) of 3-regular Cayley graphs. In Proposition 3.4, the proof requires precise bookkeeping skills and a fair amount of patience. In Corollary 3.5, we will show that the sequence (Λ_n) has logarithmic diameter. On a final note, we will show that the sequence (Λ_n) is not an expander family.

In this chapter we will use the following notational convention. An element of $\mathbb{Z}_2^n = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ will be written as a string of zeros and ones of length n. For example, the element $(1, 0, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ will be represented by 101. Let $\mathbf{e}_i$ denote the element of $\mathbb{Z}_2^n$ with a 1 in the ith coordinate and zeros elsewhere. Let $\mathbf{0} = 0 \cdots 0$ denote the identity element in $\mathbb{Z}_2^n$.

We begin by recursively taking semidirect products of $\mathbb{Z}_2$ to construct a sequence of groups (K_n) as stated in [1]. Later, we will use (K_n) to construct our desired sequence of wreath products. Let $K_1 = \mathbb{Z}_2$ and let $K_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$. Now define $\theta_2 \colon \mathbb{Z}_2 \to \mathrm{Aut}(K_2)$ by $\theta_2(1) \colon (a, b) \mapsto (b, a)$, and let $K_3 = K_2 \rtimes_{\theta_2} \mathbb{Z}_2$. Notice that $K_3 \cong D_4$. Define $\tau \colon \mathbb{Z}_2 \to \mathrm{Aut}(D_n)$ by $\tau(1) \colon r \mapsto r^{-1}, s \mapsto rs$. For each $n \geq 4$, let

$K_n = D_{2^{n-2}} \rtimes_\tau \mathbb{Z}_2$. According to [1], the mapping defined by

$$r \mapsto (s, 1), \qquad s \mapsto (1, 1)$$

shows us that K_n is isomorphic to $D_{2^{n-1}}$. Thus $|K_n| = 2 \cdot 2^{n-1} = 2^n$. Observe that we have constructed the sequence (K_n) of groups by iterating semidirect products of $\mathbb{Z}_2$. Now, let's define the sequence of Cayley graphs we wish to show has logarithmic diameter.

Definition 3.1. *Define an action θ of K_n on $I = K_n$ by $[\theta(a)][b] = ab$. With this action define the the wreath product*

$$G_n = \mathbb{Z}_2 \wr_\theta K_n = \mathbb{Z}_2^I \rtimes_\theta K_n.$$

Let $\Gamma_n = \{(\mathbf{e}_1, 1), \gamma_1, \gamma_2\} \subset G_n$, where $\gamma_1 = (0, sr)$ and $\gamma_2 = (0, s)$. Define Λ_n to be the Cayley graph $\mathrm{Cay}(G_n, \Gamma_n)$.

Remark 3.2. *Notice that Γ_n is a symmetric subset of G_n. So, by Proposition* 2.16*, the Cayley graph Λ_n is* 3*-regular. Also, note that*

$$\gamma_2\gamma_1 = (\mathbf{0}, s)(\mathbf{0}, sr) = (\mathbf{0}, r),$$

$$(\gamma_2\gamma_1)^k = (\mathbf{0}, r)^k = (\mathbf{0}, r^k), \text{ and}$$

$$\gamma_2(\gamma_2\gamma_1)^k = (\mathbf{0}, s)(\mathbf{0}, r^k) = (\mathbf{0}, sr^k).$$

Before we state and prove Proposition 3.4, let's introduce some new notation to simplify our computations, and make a few observations. Let $\mathbf{f}_i = \mathbf{e}_{i+2^{n-1}}$ for $1 \leq i \leq 2^{n-1}$.

Lemma 3.3. *Let θ be the action as in Definition* 3.1*. For each integer $1 \leq k \leq 2^{n-1}$, ${}^{r^{1-k}}\mathbf{e}_1 = \mathbf{e}_k$, and ${}^{sr^{k-1}}\mathbf{e}_1 = \mathbf{f}_k$.*

Proof. To show ${}^{r^{1-k}}\mathbf{e}_1 = \mathbf{e}_k$ for $1 \leq k \leq 2^{n-1}$, let's write $[\theta(r^{1-k})](b)$ in row notation:

$$r^{1-k} \mapsto \begin{pmatrix} 1 & \cdots & r^{k-1} & r^k & \cdots & r^{2^{n-1}-1} & s & \cdots & sr^{2^{n-1}-1} \\ r^{1-k} & \cdots & 1 & r & \cdots & r^{-k} & sr^{k-1} & \cdots & sr^{k-2} \end{pmatrix}.$$

So, the row notation shows us that the first coordinate of $\mathbf{e}_1$ is shifted to the k^{th} coordinate; that is,

$${}^{r^{1-k}}\mathbf{e}_1 = {}^{r^{1-k}}(1, 0, \ldots, 0) = (0, \ldots, 1, \ldots, 0) = \mathbf{e}_k.$$

Similarly, let's write $[\theta(sr^{k-1})](b)$ in row notation:

$$sr^{k-1} \mapsto \begin{pmatrix} 1 & \cdots & r^{2^{n-1}-1} & s & \cdots & sr^{k-1} & sr^k & \cdots & sr^{2^{n-1}-1} \\ sr^{k-1} & \cdots & sr^{k-2} & r^{1-k} & \cdots & 1 & r & \cdots & r^{-k} \end{pmatrix}.$$

So, we see that the 1^{st} coordinate of $\mathbf{e}_1$ is shifted to the $(k+2^{n-1})^{\text{th}}$ coordinate. Thus,

$${}^{sr^{k-1}}\mathbf{e}_1 = \mathbf{e}_{k+2^{n-1}} = \mathbf{f}_k$$

as claimed. □

Proposition 3.4. *For each n,* $\operatorname{diam}(\Lambda_n) \leq 3 \cdot 2^{n+1} - 5$.

Proof. An arbitrary element of G_n is of the form $(\mathbf{e}_{j_1}\mathbf{e}_{j_2}\cdots\mathbf{e}_{j_k}\mathbf{f}_{l_1}\mathbf{f}_{l_2}\cdots\mathbf{f}_{l_m}, x)$, where

$$1 \leq j_1 < j_2 < \cdots < j_k \leq 2^{n-1},$$

$$1 \leq l_1 < l_2 < \cdots < l_m \leq 2^{n-1},$$

$$1 \leq k, m \leq 2^{n-1}, \text{ and } x \in D_{2^{n-1}}.$$

According to Proposition 2.22, it suffices to show that the word norm of $(\mathbf{e}_{j_1}\mathbf{e}_{j_2}\cdots\mathbf{e}_{j_k}\mathbf{f}_{l_1}\mathbf{f}_{l_2}\cdots\mathbf{f}_{l_m}, x)$ in Γ_n is less than or equal to $3 \cdot 2^{n+1} - 5$.

Let $\mathbf{e} = (\mathbf{e}_1, 1)$. Then by Lemma 2.47 and Lemma 3.3,

$$(\gamma_2\gamma_1)^{1-j}\mathbf{e}(\gamma_2\gamma_1)^{j-1} = ({}^{r^{1-j}}\mathbf{e}_1, 1) = (\mathbf{e}_j, 1) \qquad \text{for } 1 \leq j \leq 2^{n-1},$$

and

$$\gamma_2(\gamma_2\gamma_1)^{k-1}\mathbf{e}(\gamma_2\gamma_1)^{1-k}\gamma_2^{-1} = ({}^{sr^{k-1}}\mathbf{e}_1, 1) = (\mathbf{f}_k, 1) \qquad \text{for } 1 \le k \le 2^{n-1}.$$

So,

$$\begin{aligned}
&(\mathbf{e}_{j_1}\mathbf{e}_{j_2}\cdots\mathbf{e}_{j_k}\mathbf{f}_{l_1}\mathbf{f}_{l_2}\cdots\mathbf{f}_{l_m}, x)\\
&= \left[\prod_{p=1}^{k}(\mathbf{e}_{j_p}, 1)\right]\left[\prod_{s=1}^{m}(\mathbf{f}_{l_s}, \mathbf{0})\right](\mathbf{0}, x)\\
&= \left[\prod_{p=1}^{k}(\gamma_2\gamma_1)^{1-j_p}\mathbf{e}(\gamma_2\gamma_1)^{j_p-1}\right]\left[\prod_{s=1}^{m}\gamma_2(\gamma_2\gamma_1)^{l_s-1}\mathbf{e}(\gamma_2\gamma_1)^{1-l_s}\gamma_2^{-1}\right](\mathbf{0}, x)\\
&= \left((\gamma_2\gamma_1)^{1-j_1}\left[\prod_{p=1}^{k-1}\mathbf{e}(\gamma_2\gamma_1)^{j_p-j_{p+1}}\right]\mathbf{e}(\gamma_2\gamma_1)^{j_k-1}\gamma_2(\gamma_2\gamma_1)^{l_1-1}\right)\\
&\times\left(\left[\prod_{s=1}^{m-1}\mathbf{e}(\gamma_2\gamma_1)^{l_{s+1}-l_s}\right]\mathbf{e}(\gamma_2\gamma_1)^{1-l_m}\gamma_2^{-1}(\mathbf{0}, x)\right).
\end{aligned}$$

We now find an upper bound for the length of the final expression as a word in Γ_n. We see that $\mathbf{e}$ appears precisely $k+m$ times, and γ_2 and γ_2^{-1} both appear alone exactly one time each. Since γ_2 is a element of order 2, technically $\gamma_2 = \gamma_2^{-1}$, but since this is a counting argument, we count them separately to help us with the bookkeeping. Likewise, $\gamma_1 = \gamma_1^{-1}$, but we will count them separately as well.

Next, let's consider $x \in D_{2^{n-1}}$. If $x = r^p$ for $1 \le p \le 2^{n-1}$, then $x = (\gamma_2\gamma_1)^p$. If $x = sr^p$ for $1 \le p \le 2^{n-1}$, then $x = \gamma_2(\gamma_2\gamma_1)^p$. So, in either case, x can be expressed as a word in $\{\gamma_1, \gamma_2\}$ with γ_2 appearing no more than $p+1$ times, and γ_1 appearing no more than p times.

To determine the number of times $(\gamma_2\gamma_1)^{-1}$ appears, first note that $1 - l_m < 0$ since $l_m > 1$, and $j_i - j_{i+1} < 0$ because $j_i < j_{i+1}$ for each $1 \le i \le k-1$. Also,

$1 - j_1 \leq 0$ since $1 \leq j_1$, and so $(\gamma_2\gamma_1)^{-1}$ appears exactly

$$(j_1 - 1) + (j_2 - j_1) + \cdots + (j_k - j_{k-1}) + (l_m - 1) = j_k + l_m - 2$$

times.

Finally, let's determine the number of times $(\gamma_2\gamma_1)$ is listed above. Notice that $j_k - 1 > 0$, and $l_{i+1} - l_i > 0$ for each $i = 1, \ldots, m-1$. Also, $1 - l_1 \leq 0$ because $1 \leq l_1$, and so $(\gamma_2\gamma_1)$ appears exactly

$$(l_1 - 1) + (l_2 - l_1) + \cdots + (l_m - l_{m-1}) + (j_k - 1) = l_m + j_k - 2$$

times. Hence, we can express $(e_{j_1} \cdots e_{j_k} f_{l_1} \cdots f_{l_m}, x)$ as a word in Γ_n where γ_1 appears no more than $j_k + l_m + p - 2$ times, γ_2 appears no more than $j_k + l_m + p$ times, γ_1^{-1} appears $j_k + l_m - 2$ times, γ_2^{-1} appears $j_k + l_m - 1$ times, and $\mathbf{e}$ appears $k + m$ times. Therefore, the word norm of $(e_{j_1} \cdots e_{j_k} f_{l_1} \cdots f_{l_m}, x)$ is less than or equal to

$$\begin{aligned} 4j_k + 4l_m + k + m + 2p - 5 &\leq \ 4 \cdot 2^{n-1} + 4 \cdot 2^{n-1} + 2^{n-1} + 2^{n-1} + 2 \cdot 2^{n-1} - 5 \\ &= 12 \cdot 2^{n-1} - 5 \\ &= 3 \cdot 2^{n+1} - 5. \end{aligned}$$

Therefore, $\operatorname{diam}(\Lambda_n) \leq 3 \cdot 2^{n+1} - 5$. $\square$

Corollary 3.5. *The sequence (Λ_n) of Cayley graphs has logarithmic diameter.*

Proof. Recall that $|G_n| = |\mathbb{Z}_2^I||K_n| = 2^{2^n}2^n$, and so $\log|G_n| = 2^n \log 2 + n \log 2$. Let

$C = \frac{6}{\log 2}$. By Proposition 3.4, the following holds for each n:

$$\begin{aligned}
\operatorname{diam}(\Lambda_n) &\leq 3 \cdot 2^{n+1} - 5 \\
&= 6 \cdot 2^n - 5 \\
&\leq 6 \cdot 2^n + 6n \\
&= \frac{6}{\log 2}(2^n \log 2 + n \log 2) \\
&= \frac{6}{\log 2} \log |G_n|.
\end{aligned}$$

Therefore, $\operatorname{diam}(\Lambda_n) \leq C \log |G_n|$ for each n; hence the sequence (Λ_n) of Cayley graphs has logarithmic diameter. $\square$

Proposition 3.6. *The sequence (Λ_n) is not an expander family.*

Proof. According to Proposition 2.48, $\mathbb{Z}_2^I \trianglelefteq G_n$ for each $n \geq 1$. By Proposition 2.49,

$$G_n/\mathbb{Z}_2^I \cong K_n \cong D_{2^{n-1}} \quad \text{for each } n \geq 1.$$

So, (G_n) admits $(D_{2^{n-1}})$ as a sequence of quotients. According to Example 2.42, the sequence $(D_{2^{n-1}})$ of dihedral groups does not yield an expander family. Hence by Proposition 2.32, the sequence (G_n) does not yield an expander family, and a fortiori the sequence (Λ_n) of Cayley graphs is not an expander family. $\square$

REFERENCES

[1] M. Aivazian and M. Krebs, *Solvable Groups, Semidirect Products, and A Necessary Condition For Expansion*, Preprint.

[2] D. S. Dummit and R. M. Foote, *Abstract Algebra,* John Wiley and Sons, Inc., 2004.

[3] M. Krebs and A. Shaheen, *Expander Families and Cayley Graphs,* Oxford University Press, Inc., 2011.

[4] A. Lubotzky and B. Weiss, *Groups and Expanders*, Expanding Graphs, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 10, American Mathematical Society, 1993, pp. 95-109.

APPENDIX A

Notations and Conventions from Group Theory

If A is a subset of a set B not necessarily proper, it will be denoted by $A \subset B$ throughout this paper. $H \leq G$ will denote that H is a subgroup of G. If N is a normal subgroup of G, this fact will be denoted by $N \trianglelefteq G$. The integers mod n will be denoted by $\mathbb{Z}_n$.

The set of natural numbers will be denoted by $\mathbb{N} = \{1, 2, 3, \ldots\}$ and $\mathbb{Z}$ will represent the set of integers.

$D_n = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$ will denote the dihedral group of order $2n$.

The following isomorphism theorems will be referred to throughout the paper. The proofs of the isomorphism theorems can be found in [2], which is where the statements were acquired.

Theorem A.1 (The First Isomorpism Theorem)**.** *Let G and H be groups. Let $\phi\colon G \to H$ be a homomorphism. Then* $\ker \varphi \trianglelefteq G$ *and* $G/\ker \phi \cong \phi(G)$*.*

Corollary A.2. *If $\varphi\colon G \to H$ is a homomorphism, then ϕ is a one-to-one map if and only if* $\ker \phi = 1$*.*

Theorem A.3 (The Second or Diamond Isomorphism Theorem)**.** *Let G be a group, and let $A, B \leq G$. Suppose $A \leq N_G(B)$. Then $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.*

Theorem A.4 (The Third Isomorphism Theorem)**.** *Suppose G is a group. Let $H, K \trianglelefteq G$ so that $H \leq K$. Then $K/H \trianglelefteq G/H$ and*

$$(G/H)/(K/H) \cong G/K.$$

Theorem A.5 (The Fourth or Latice Isomorphism Theorem)**.** *Suppose G is a group and $N \trianglelefteq G$. Let $X = \{A \leq G \mid N \leq A\}$ and $Y = \{A/N \mid A/N \leq G/N\}$. Then there is a bijection from X onto Y. In particular, every subgroup of G/N is of the form A/N where A is a subgroup of G containing N. This bijection has the following properties for each $A, B \leq G$ with $N \leq A$ and $N \leq B$.*

(1) *$A \leq B$ if and only if $A/N \leq B/N$.*

(2) *If $A \leq B$, then $|B\colon A| = |B/N\colon A/N|$.*

(3) *$\langle A, B\rangle/N = \langle A/N, B/N\rangle$.*

(4) *$(A \cap B)/N = A/N \cap B/N$.*

(5) *$A \trianglelefteq G$ if and only if $A/N \trianglelefteq G/N$.*