On the Cogrowth Series of Free Products of Finite Groups

by

Heng (Haggai) Liu

B.Sc. (Computer Science), University of Victoria, 2017
B.Sc. (Mathematics), University of Victoria, 2017

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Spring 2021

Declaration of Committee

Name: **Heng (Haggai) Liu**

Degree: **Master of Science (Mathematics)**

Thesis title: **On the Cogrowth Series of Free Products of Finite Groups**

Committee: **Chair:** Weiran Sun
Associate Professor, Mathematics

Marni Mishna
Supervisor
Professor, Mathematics

Tamon Stephen
Committee Member
Associate Professor, Mathematics

Jake Levinson
Examiner
Assistant Professor, Mathematics

Abstract

Given a group G with a finite set of generators, S, it is natural to ask if the product of n generators from S evaluate to the identity. The enumerative version of this problem, known as the *cogrowth* problem, counts the number of such products and studies the associated counting sequence. Many cogrowth sequences are known. This thesis focuses on the free products of finite groups: Specifically, cyclic and dihedral groups. Such groups have the property that their cogrowth generating functions are algebraic functions, and thus, are solutions to implicit polynomial equations. Using algebraic elimination techniques and free probability theory, we establish upper bounds on the degrees of the polynomial equations that they satisfy. This has implications for asymptotic enumeration, and makes it theoretically possible to determine the functions explicitly.

Keywords: cogrowth, free product, dihedral, free probability, polynomial, Cayley graph

Acknowledgements

Thank you, Dr. Marni Mishna for enthusiastically taking me as a student very late in my degree program, and helping me advance in my academic career. Dr. Mishna saw the potential in my abilities and gave me great encouragement, motivating me to work hard on my research.

Thank you, Dr. Jake Levinson for making me an offer in the PhD. program here at Simon Fraser University, despite me being a beginner in your area of expertise. Dr. Levinson decided to work with me on account of Dr. Mishna speaking highly of my aptitude.

Thank you, Dr. Tamon Stephen, for being on my committee and very supportive of my goals. During casual conversations, Dr. Stephen always appears to be highly interested in my future goals and plan, and he often gives me advice to help me be at my best. Dr. Stephen gives me comments and feedback in a way that is more detail oriented than any other professor I've ever seen.

Thank you, Dr. Zhaosong Lu, for being my initial advisor. Upon hearing that I have greater interests in other research areas, Dr. Lu selflessly suggested that I talk to other potential advisors and consider switching before I graduate.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

The word problem on finitely generated groups is a fundamental problem that is well studied [4, 18]. The problem is as follows: Given a finitely generated group, G, with a finite generating set $S \subseteq G$, not containing the identity, decide if the product of a finite sequence of elements in S is equal to the identity $1 \in G$. This problem is *decidable* for many classes of groups, meaning that there is an algorithm that correctly checks whether or not a given sequence of elements evaluate to the group identity. Free groups and free products of free groups are two example of such classes. Quenell [18] studied the Cayley graphs of these two classes of groups, and discussed the spectrums of these graphs. There are groups for which the word problem cannot be solved. One example of a group with an unsolvable word problem is given by Novikov [15].

Formal language theory gives a useful framework for this problem. We refer to the finite set of symbols as an *alphabet*. Here, we shall consider the generating set as an alphabet. A *word* is a finite sequence of elements from S. The set of all words on S is denoted as S^*. A *language* on S is a subset of S^*. Languages are organized into complexity classes. These include the *regular* languages; *context free* languages; and decidable languages. Given a language $L \subseteq S^*$, we say that L is regular if it can be *recognized* by a *finite automata*; L is context free if it can be recognized by a *pushdown automata*; L is decidable if it can be *decided* by a Turing machine. Every regular language is also context free. Every context free language is decidable. See [10] for more information on languages and automatas. If S is a generating set for a group G, we consider the language,

$$L(G,S) := \{s_1 s_2 \dots s_n : n \geq 1,\ s_i \in S,\ s_1 \cdot s_2 \cdot \dots \cdot s_n = 1 \in G\}.$$

Here, we use "$\cdot$" to denote group multiplication and distinguish it from word concatenation. Thus, we characterize the word problem on groups as a problem of identifying words in a given language. It is natural to ask: "Is there any connection between the language complexity of a group, and its group properties?" It is known that $L(G,S)$ is regular if and only if G is finite [1]; $L(G, S)$ is context free if and only if G has a finite-index subgroup [13] isomorphic to a free group, meaning that G is *virtually free*. We will see in this thesis, that free products of finitely many finite groups are virtually free. For $n \geq 0$, we let S^n denote the set of words in S^* of length n.

Given $L \subseteq S^*$, it is often possible to gain insight into the complexity of L by considering the generating function for the number of words in L of length n, which is $|L \cap S^n|$. Generating functions, like languages, also have their own complexity classes. The simplest kind of are rational functions, which are contained in algebraic functions, which are in turn, contained in D-finite series. A series is called *D-finite* if it solves a linear homogeneous ordinary differential equation where its coefficients are rational functions. If the language, $L(G, S)$, is regular, then its generating function is rational. If $L(G, S)$ is context free, then its series is algebraic. The converse of either statement, however, is not true. The counterexample below is provided in [4]. The language,

$$\{a^n b^n c^n : n \geq 0\} \subseteq \{a, b, c\}^*,$$

can be proven to be not context free via the well known pumping lemma [10], but however, has a rational generating function $\frac{1}{1-t^3}$.

We now introduce the main problem considered in this thesis. Let G be a finitely generated group, and $S \subseteq G \setminus \{1\}$ be a generating set. The sequence, $\{|L(G, S) \cap S^n|\}_{n \geq 0}$, is called the *cogrowth*, or the *cogrowth sequence* of G with respect to S. The corresponding series,

$$\sum_{n \geq 0} |L(G, S) \cap S^n| \, t^n \in \mathbb{Z}_{\geq 0}[[t]],$$

is known as the *cogrowth series* of G with respect to S. Asymptotic properties [8] of cogrowth sequences gives knowledge about the radius of convergence of their associated series. There exist groups with cogrowth series that are not algebraic, and also ones that are not D-finite. Bell and Mishna [4] showed that the amenable groups that are not polynomially bounded do not have D-finite cogrowth series.

In this thesis, we only consider free products of finite groups, which have algebraic cogrowth series. These are series, $F(t)$, that satisfy $P(t, F(t)) = 0$ for some nonzero polynomial $P(t, z) \in \mathbb{Z}[t, z]$. Once P is determined, we are able to theoretically determine the series, $F(t)$, via guess and check; and gain some insight on certain asymptotic properties [8, 2] of $F(t)$. However, such a polynomial, P, is difficult to compute in general. The purpose of this thesis is to give bounds on P to make it theoretically guessable. We continue the study of Bell and Mishna [4] on free products of finite groups. We analyze the case where G is a free product of finite cyclic and finite dihedral groups. Additional classes of groups such as amenable groups, and Lamplighter groups have been studied, as well as gap results on radii of convergence. However, we will not provide these details here.

We briefly summarize the contents of this thesis: Chapter 2 provides some background knowledge in topics from abstract algebra, enumeration, free probability, computer algebra, and asymptotic analysis, that are useful for our problem. In Chapter 3, we bound the degree of the implicit equations of the cogrowth series for free products of finite cyclic groups. This chapter contains the main results in this thesis: Theorem 3.3 for the case of two distinct cyclic factors; and Theorem 3.12 for the case of an arbitrary number of distinct cyclic factors. In Chapter 4, we treat the general case involving a mixture of cyclic and dihedral groups. We give a major conjecture, Conjecture 4.3, regarding the case of identical dihedral factors, and end with a conjecture involving the free product of an arbitrary combination of finite cyclic and finite dihedral groups.

Chapter 2

Background

Prior to discussing the main topics of this thesis, we first recall some useful background topics to help us visualize and motivate our problem at hand. The finite groups that we consider are the cyclic and dihedral groups. We start out in Section 2.1 recalling the structure of a Cayley graph and explain how it provides a visualization of certain cogrowth sequences. We then discuss briefly on algebraic generating functions, which help us analyze the cogrowth generating functions, which are algebraic for the specific class of groups studied in this thesis. The theory of combinatorial classes [12, 8] is useful in deriving a system of equations that can be solved for the cogrowth generating function, provided that the underlying group is finitely generated. Such systems are derived from combinatorial grammar and can grow rapidly as the group become increasingly complex. For this reason, we make use of free probability to obtain a system that is structurally much simpler. Upon obtaining an implicit equation for a cogrowth series, we often wish to seek the dominant singularities of this system, which gives insight to the radius of convergence of this series. Using an implicit equation for a cogrowth series, we may use an iterative technique to generate the first few terms of the underlying sequence of coefficients. This iterative technique is known [19] to converge to a unique solution under certain assumptions of the constant term. We also derive a method to verify, at any given iteration, the number of terms that are correctly approximated. With the help of representation theory, we state a degree bound which applies to any finite groups, and compare this result to other ones in this section for cyclic and dihedral groups.

2.1 Cayley Graphs

Products in a group can be visualized as walks on a particular graph. As before, let G be group, and let $S \subseteq G \setminus \{1\}$ be a generating set. We define the *Cayley graph* of G with respect to S, denoted $\chi(G, S)$, to be the directed graph (V, E), with vertex set $V = G$ and arc set $E = \{(g, g \cdot s) : g \in G,\ s \in S\}$. It is important to note that Cayley graphs are vertex transitive; and since S generates G, $\chi(G, S)$ is strongly connected. We consider two main types of generating sets: minimal and inverse closed. The generating set S is *minimal* if for each $s \in S$, $S \setminus \{s\}$ is not a generating set. The set S is *inverse closed* if the group inverse of each element in S, is again in S. That is, $S = S^{-1}$. If S is inverse closed, the $\chi(G, S)$ can be viewed as an undirected graph. A *walk* on a directed graph is a finite sequence of arcs, $(u_1, v_1), (u_2, v_2), \ldots, (u_n, v_n)$, where consecutive arcs are adjacent in the sense that, $v_i = u_{i+1}$ for each $i = 1, 2, \ldots, n-1$. Such a walk is said to start at u_1 and end at v_n. Observe that elements of S^* are in bijection with the walks on $\chi(G, S)$ starting at $1 \in G$. Each $s_1 s_2 \ldots s_n \in S^*$ corresponds with the walk

$$(1,\ s_1), (s_1,\ s_1 \cdot s_2), \ldots, (s_1 \cdot s_2 \cdot \ldots \cdot s_{n-1},\ s_1 \cdot s_2 \cdot \ldots \cdot s_n).$$

An *excursion* on $\chi(G, S)$ is a walk that starts and ends at the same vertex. We will only consider excursions that start and end at 1. Such walks are in bijective correspondence with elements with $L(G, S)$. For the remainder of this thesis, we identify elements of S^* and the corresponding walk on the Cayley graph. In particular, we use words and walks interchangeably.

For $n \geq 0$, define $a_n := |S^n \cap L(G, S)|$ as the number of such excursions of length n. For fixed G and S, we define the associated generating function to this counting sequence

$$F_{G;S}(t) = F(t) := \sum_{n \geq 0} a_n t^n.$$

If G is finite, then $\chi(G, S)$ is a finite automata accepting $L(G, S)$. By classic theory [8, Proposition V.6.], $F(t)$ is the Taylor series of a rational function. This result on finite groups can be proven using powers of the adjacency matrices and vertex transitivity of the relevant Cayley graph. In this case, $\{a_n\}$ satisfies a linear recurrence with constant coefficients. We give the example of a finite cyclic group below.

Example 2.1. Let $G = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order $n > 1$ with a set $S = \{x\}$ consisting of a single generator. Then $L(G, S) = \{\epsilon, x^n, x^{2n}, x^{3n}, \ldots\}$ and $a_k = \delta_{0,(k \bmod n)}$[1]. Thus, $F(t) = \frac{1}{1-t^n}$. In this case, the Cayley graph, $\chi(G, S)$, is a directed cycle of length n. Figure 2.1 gives a few examples of such Cayley graphs.

[1] $\delta_{i,j}$ denotes the Kronecker Delta function; $(k \bmod n)$ denotes the unique integer $0 \leq r < n$ where $k \equiv r \pmod{n}$.

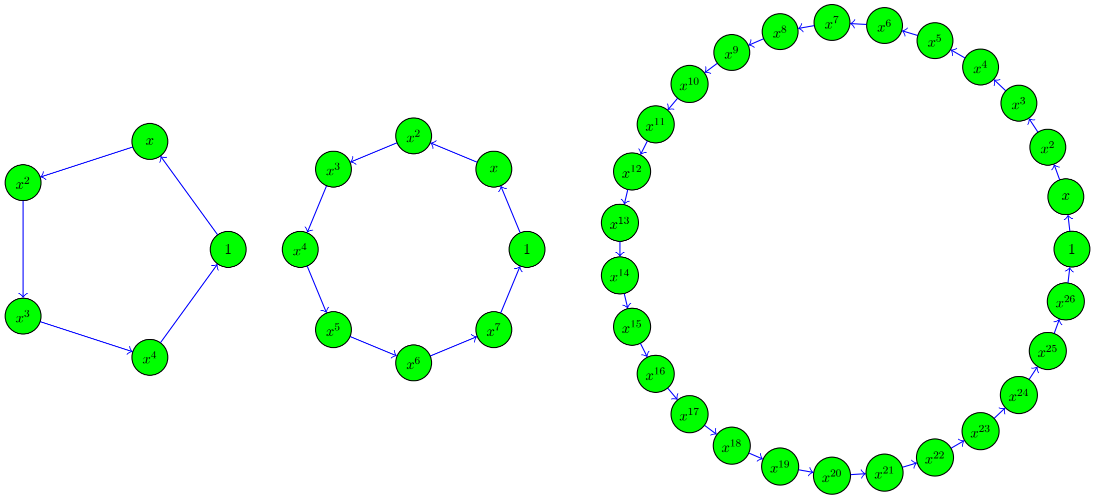


Figure 2.1: Cayley graphs of $\mathbb{Z}_n = \langle x | x^n - 1\rangle$ with respect to $\{x\}$ for $n = 5, 8, 27$ respectively.

Notice that we are using ϵ to denote the empty word in S^*. For $k > 0$, we use x^k to denote the word in S^* that is the concatenation of k occurrences of x, as well as the product of k occurrences of x, as an element of G.

Another classic example of a finite, noncyclic group is the dihedral group: the group of symmetries of a regular polygon. For $n \geq 3$, let D_n denote the dihedral group on n vertices. We give D_n with the presentation $\langle r, f : r^n - 1, f^2 - 1, rf - fr^{-1}\rangle$, where r is a basic rotation by an angle of $\frac{2\pi}{n}$, and f is a flip across an arbitrary axis containing a vertex and the center. We consider the minimal generating set of D_n, $S = \{r, f\}$.[2] The following result gives a formula for the cogrowth series of D_n with generating set S. The example below shows the Cayley graph of D_3 with respect to this generating set.

Example 2.2. Consider the case of $n = 3$ vertices, $G = D_3$, with $S = \{r, f\}$ as described above. In this case, we have

$$L(G, S) = \{\epsilon, ff, rrr, ffff, rfrf, frfr, ffrrr, rrrff, rffrr, rrffr, frrrf, \ldots\},$$

where the elements explicitly listed, are all the words of length up to five. In fact, it is true that $L(G, S) = C^*$, where

$$C = \{ff, rrr, rfrf, frfr, rrfrrf, rfrrfr, frrfrr\}$$

is the set of all excursions of G with respect to S where the nonempty prefixes evaluate to distinct elements of G. The Cayley graph, $\chi(D_3, S)$ has the structures of 2 disjoint directed

[2] Some authors, such as Dummit and Foote [7], use D_{2n} to refer to this group.

triangles, with bidirectional arcs across corresponding vertices. Notice that the elements of C are precisely the directed cycles in $\chi(G,S)$ containing $1 \in G$.

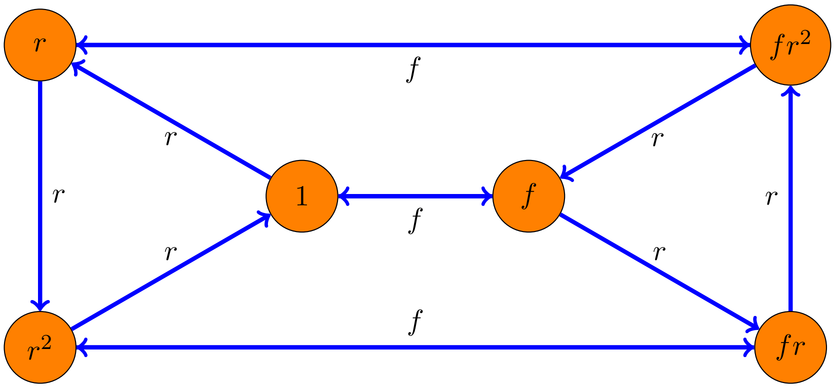


Figure 2.2: The graph, $\chi(D_3,S)$ with $S = \{r,f\}$.

$\diamond$

The cogrowth series for a dihedral group is the Maclaurin series of a rational function, of which the explicit formula is given in the proposition below.

Proposition 2.3. *For each $m \geq 3$, let $F_m(t)$ denote the cogrowth series of D_m with the generating set $S = \{r,f\}$, as described above. Then*

$$F_m(t) = \frac{1}{2} + \frac{1}{2m}\sum_{j=0}^{m-1} \frac{1}{1-2\cos(\frac{2\pi j}{m})t}. \tag{2.1}$$

Proof. List the elements of D_m in the order,

$$g_1 = 1, g_2 = r, g_3 = r^2, \ldots, g_{m-1} = r^{m-1}, g_m = f, g_{m+1} = fr^{m-1}, \ldots, g_{2m} = fr.$$

Let $A = (a_{ij})_{i,j=1}^n$ be the adjacency matrix of the Cayley graph, $\chi(D_m,S)$, so that $a_{ij} = 1$ if $g_i^{-1} \cdot g_j \in S$, and $a_{ij} = 0$ otherwise. Let I_k denote the $k \times k$ identity matrix. Then A has the block structure,

$$A = \begin{bmatrix} \begin{bmatrix} \vec{0} & I_{m-1} \\ 1 & \vec{0}^T \end{bmatrix} & I_m \\ I_m & \begin{bmatrix} \vec{0}^T & 1 \\ I_{m-1} & \vec{0} \end{bmatrix} \end{bmatrix}.$$

After applying a sequence of row and column operations, each of which correspond to elementary matrices of unit determinant, to $tI_{2m} - A$, we obtain the block matrix,

$$\begin{bmatrix} B & I_m \\ O & tI_m \end{bmatrix}$$

where O is an all zeros matrix of the appropriate dimensions, and

$$B = \begin{bmatrix} t & -1 & 0 & \dots & 0 & 0 & -1 \\ -1 & t & -1 & \ddots & \vdots & \vdots & 0 \\ 0 & -1 & t & \ddots & 0 & \vdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & \ddots & t & -1 & 0 \\ 0 & \dots & \dots & 0 & -1 & t & -1 \\ -1 & 0 & 0 & \dots & 0 & -1 & t \end{bmatrix}$$

is $m \times m$, with t's on the diagonal, -1's on the superdiagonal, subdiagonal, the upper right corner, the lower left corner, and has 0's everywhere else. Let $\omega = e^{\frac{2\pi i}{m}} \in \mathbb{C}$. Observe that B is a circular matrix, as each subsequent row of B can be obtained for the previous row by rotating each entry one position to the right with the last entry becoming the first entry. Consequently, $\det B$ can be calculated by computing the scalar product of its last row, with the column vector,

$$[\omega^{j(m-1)}, \omega^{j(m-2)}, \dots, \omega^{j}, 1]^T$$

for each $j = 0, 1, \dots, m-1$, and multiplying the m expressions. Hence,

$$\begin{aligned} \det(tI_{2m} - A) &= t^m \det B \\ &= t^m \prod_{j=0}^{m-1} \left(t - \omega^j - \omega^{j(m-1)}\right) \\ &= t^m \prod_{j=0}^{m-1} \left(t - 2\cos\left(\frac{2\pi j}{m}\right)\right). \end{aligned}$$

This gives us that for $n \geq 1$,

$$\operatorname{tr} A^n = \sum_{j=0}^{m-1} 2^n \cos^n \left(\frac{2\pi j}{m}\right).$$

Since $\chi(D_m, S)$ is vertex transitive, we have that the number of length n excursions starting at $1 \in D_m$ is $\frac{\operatorname{tr} A^n}{|D_m|} = \frac{\operatorname{tr} A^n}{2m}$, yielding

$$F_m(t) = 1 + \frac{1}{2m} \sum_{j=0}^{m-1} \sum_{n \geq 1} 2^n \cos^n \left(\frac{2\pi j}{m}\right) t^n,$$

which simplifies to Equation (2.1) as desired. □

The proof technique used above can be used on any finite groups [8]. As mentioned earlier, for any finite group G and generating set, $S \subseteq G \setminus \{1\}$, we can construct the adjacency matrix of $\chi(G, S)$ and use vertex transitivity to relate the cogrowth sequence with traces of matrices. Notice that, for example, Equation (2.1) for $m = 3$ simplifies to

$$F_3(t) = 1 + \frac{t^2}{(1-2t)(1+t)}.$$

The table below documents the cogrowth series of D_m for a few values of m.

m	Cogrowth series of $D_m,\ S = \{r, f\}$
3	$\frac{1-t-t^2}{(1-2t)(1+t)}$
4	$\frac{1-3t^2}{(1-2t)(1+2t)}$
5	$\frac{1-t-2t^2+t^3}{(1-2t)(1+t-t^2)}$
6	$\frac{1-4t^2+2t^4}{(1-2t)(1-t)(1+t)(1+2t)}$
8	$\frac{1-5t^2+5t^4}{(1-2t)(1+2t)(1-2t^2)}$
9	$\frac{1-t-4t^2+3t^3+3t^4-t^5}{(1-2t)(1+t)(1-3t^2+t^3)}$
10	$\frac{(1-2t^2)(1-4t^2+t^4)}{(1-2t)(1+2t)(1-t-t^2)(1+t-t^2)}$
12	$\frac{1-7t^2+14t^4-7t^6}{(1-2t)(1-t)(1+t)(1+2t)(1-3t^2)}$
16	$\frac{(1-3t^2)(1-6t^2+9t^4-3t^6)}{(1-2t)(1+2t)(1-2t^2)(1-4t^2+2t^4)}$
18	$\frac{(1-2t^2)(1-8t^2+19t^4-12t^6+t^8)}{(1-2t)(1-t)(1+t)(1+2t)(1-3t^2+t^3)(1-3t^2-t^3)}$
20	$\frac{1-11t^2+44t^4-77t^6+55t^8-11t^{10}}{(1-2t)(1+2t)(1-t-t^2)(1+t-t^2)(1-5t^2+5t^4)}$
24	$\frac{1-13t^2+65t^4-156t^6+182t^8-91t^{10}+13t^{12}}{(1-2t)(1-t)(1+t)(1+2t)(1-3t^2)(1-2t^2)(1-4t^2+t^4)}$
32	$\frac{1-17t^2+119t^4-442t^6+935t^8-1122t^{10}+714t^{12}-204t^{14}+17t^{16}}{(1-2t)(1+2t)(1-2t^2)(1-4t^2+2t^4)(1-8t^2+20t^4-16t^6+2t^8)}$
36	$\frac{1-19t^2+152t^4-665t^6+1729t^8-2717t^{10}+2508t^{12}-1254t^{14}+285t^{16}-19t^{18}}{(1-t)(1+2t)(1-2t)(1+t)(1-3t^2)(1-6t^2+9t^4-3t^6)(1-3t^2+t^3)(1-3t^2-t^3)}$

Table 2.1: Cogrowth generating function for the dihedral groups D_m for various values of m with respect to generating set $S = \{r, f\}$.

The following corollary is a consequence of the expression given in (2.1) and classical properties of the cosine function.

Corollary 2.4. *For each $m \geq 3$, there are polynomials $p, q \in \mathbb{Z}[t]$ with $\deg p = \deg q \leq d_m$ so that $F_m(t)$ is the Taylor series of $\frac{p(t)}{q(t)}$, where $p(0) = q(0) = 1$ and*

$$d_m := \begin{cases} \frac{m+1}{2}, & m \text{ is odd} \\ 2\lceil \frac{m}{4} \rceil, & m \text{ is even} \end{cases}. \tag{2.2}$$

Proof. We obtain p and q by simplifying Equation (2.1). Let

$$q^*(t) := \prod_{j=0}^{m-1} \left(1 - 2\cos\left(\frac{2\pi j}{m}\right) t\right) \in \mathbb{R}[t] \tag{2.3}$$

be a common denominator of the expression in (2.1). By factoring out the t as before,

$$q^*(t) = t^m \prod_{j=0}^{m-1} \left(t^{-1} - 2\cos\left(\frac{2\pi j}{m}\right)\right) = t^m \det(M + t^{-1} I_m)$$

for some explicit matrix M with integer entries. Thus, $q^* \in \mathbb{Z}[t, t^{-1}]$. Combining this result with Equation (2.3), we have $q^* \in \mathbb{Z}[t]$. Next, we define

$$S(t) := \sum_{j=0}^{m-1} \frac{1}{1 - 2\cos(\frac{2\pi j}{m})t}$$

as the sum that appears in the right hand side of Equation (2.1). Notice that, applying classical properties of the cosine function, we can rewrite $S(t)$ as

$$S(t) = \begin{cases} \dfrac{1}{1-2t} + 2\displaystyle\sum_{j=1}^{d_m - 1} \dfrac{1}{1 - 2\cos(\frac{2\pi j}{m})t}, & m \equiv 1 \pmod 2 \\ \dfrac{2}{1-4t^2} + 4\displaystyle\sum_{j=1}^{\frac{1}{2}d_m - 1} \dfrac{1}{1 - 4\cos^2(\frac{2\pi j}{m})t^2}, & m \equiv 2 \pmod 4 \\ 4 + \dfrac{2}{1-4t^2} + 4\displaystyle\sum_{j=1}^{\frac{1}{2}d_m - 1} \dfrac{1}{1 - 4\cos^2(\frac{2\pi j}{m})t^2}, & m \equiv 0 \pmod 4 \end{cases}.$$

Let $q \in \mathbb{R}[t]$ be the degree d_m polynomial that is the product of all the denominators that appear in the above expression for $S(t)$ under the appropriate case for m. Notice that $q(0) = 1$. It is not difficult to verify that $q^*(t) = q(t)a(t)$, for some $a \in \mathbb{Q}[t]$, so $q \in \mathbb{Q}[t]$.

Recall that the set of *algebraic integers*, roots of monic polynomials over $\mathbb{Z}$, form a ring. For each $k \in \mathbb{Z}$, let $\alpha_k = 2\cos\left(\frac{2\pi k}{m}\right)$. Observe that $\alpha_k = e^{\frac{2\pi k i}{m}} + e^{-\frac{2\pi k i}{m}}$ is a sum of two m-th roots of unity, and hence α_k and α_k^2 are algebraic integers. Thus, the coefficients of q are rational algebraic integers, so $q \in \mathbb{Z}[t]$. Since $F_m \in \mathbb{Z}[[t]]$ and $F_m(0) = 1$, we have $p(t) := F_m(t)q(t) \in \mathbb{Z}[[t]]$ and so $p(0) = 1$. Since $F_m(t) = \frac{1}{2} + \frac{1}{2m}S(t)$ and $S(t)$ is a rational function of negative degree, and since $q(t)$ is a common denominator of the above expression for $S(t)$, we have that $p(t) \in \mathbb{Z}[t]$ with $\deg p = \deg q$, which completes our proof. □

In the examples given in Table 2.1, the upper bounds, d_m, in Corollary 2.4, appear to hold with equality. Hence, it is unlikely that these upper bound can be tighter. It is apparent that the cogrowth series for dihedral groups are not as simple as for finite cyclic groups. In later chapters, we add to the examples of Bell and Mishna [4] by considering the dihedral groups as factors in a free product.

2.1.1 Cayley Graphs of Free Products of Finite Groups

We start by recalling the definition of a free product, which is stated in [14, Definition 5.8].

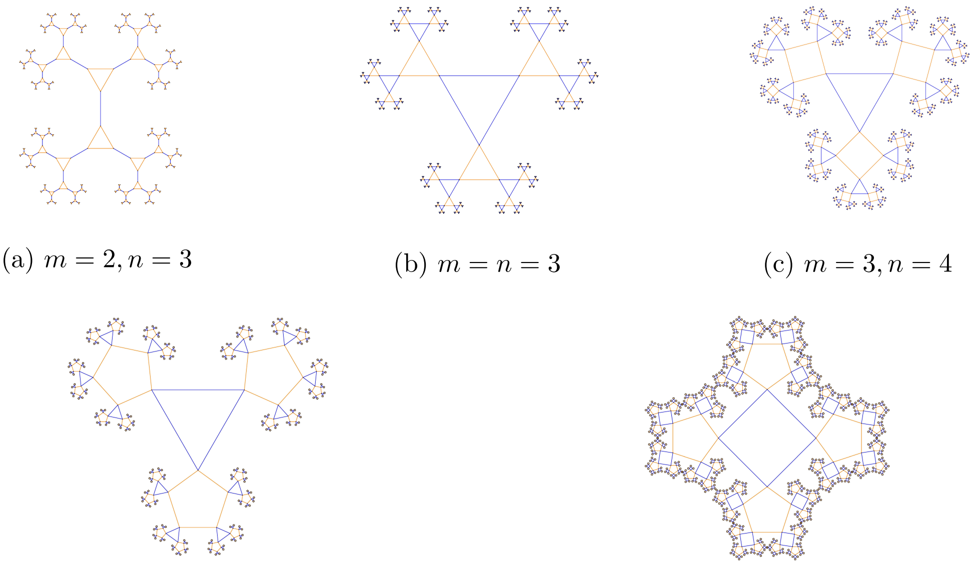
Definition 2.5. Let $G_1, G_2, \ldots, G_m$ be groups. The *free product*, of $G_1, G_2, \ldots, G_m$, denoted as $G := G_1 * G_2 * \ldots * G_m = \coprod_{i=1}^m G_i$, is the group generated by $\cup_{i=1}^m G_i$, subject to the relations in each G_i, and the identity element in each G_i is identified with $1 \in G$.

If K is any group and $m \geq 0$, we define K^{*m} as a shorthand for $\underbrace{K * K * \ldots * K}_{m \text{ factors}}$.

In this thesis, we consider the case where G is a free product of finitely many finite groups, in which case the Cayley graph has the structure of an infinite fractal. Figure 2.3 provides examples of Cayley graphs in the case where G is a free product of two finite cyclic groups, where we take S to be the set containing a generator of each cyclic factor as well as its inverse. Let us consider the case of two cyclic groups. Formally,

$$G := \mathbb{Z}_m * \mathbb{Z}_n = \langle x, y | x^m = 1, y^n = 1\rangle = \langle x | x^m = 1\rangle * \langle y | y^n = 1\rangle$$

and $S = \{x, x^{-1}, y, y^{-1}\}$. The blue edges indicate the "x" direction, and the orange edges indicate the "y" direction. Since S is inverse closed, arrows indicating the direction of the edges are not needed.



(a) $m = 2, n = 3$

(b) $m = n = 3$

(c) $m = 3, n = 4$

(d) $m = 3, n = 5$

(e) $m = 4, n = 5$

Figure 2.3: Cayley graphs for free products of two cyclic groups $\mathbb{Z}_m * \mathbb{Z}_n = \langle x, y | x^m = 1, y^n = 1 \rangle$ with generating set $\{x, x^{-1}, y, y^{-1}\}$.

2.2 Algebraic Generating Functions

The cogrowth series, $F(t)$, for free products of finite groups, converges to an algebraic function that is analytic around $t = 0$ [4, 11]. Consequently, $F(t)$, is a solution of a non-trivial implicit polynomial equation [2]. In other words, there is a polynomial $Q(t, z) \in \mathbb{Z}[t, z] \setminus \{0\}$ so that $Q(t, F(t)) = 0 \in \mathbb{Z}[t]$. For convenience, we make the following definition:

Definition 2.6. Let $F(t) \in \mathbb{Z}[[t]]$ be an algebraic series. Let $Q(t, z) \in \mathbb{Z}[t, z]$ be a nonzero polynomial. We say that $z = F(t)$ *satisfies* $Q(t, z)$, and call $Q(t, z)$ a *satisfying polynomial* for $F(t)$, if $Q(t, F(t)) \equiv 0 \in \mathbb{Z}[[t]]$. If $Q(t, z)$ is a satisfying polynomial for $F(t)$ that is chosen such that $\deg_z Q$ is as small as possible, we call $Q(t, z)$ a *minimal polynomial* for $F(t)$.

The reader should note that minimal polynomials in this setting are unique only up to multiplication by elements in $\mathbb{Z}[t]$. Since $\mathbb{Z}[t]$ is not a field, we cannot necessarily take $Q(t, z)$ to be monic in z. Throughout the next two sections, we show how to obtain $Q(t, z)$ using each of two primary methods: Combinatorial grammar, and the theory of free probability. In later chapters, we present some new result on satisfying polynomials. These polynomials are believed to be minimal by experiment, but it is not known whether or not minimality is satisfied.

2.3 Combinatorial Grammar for the Word Problem

The cogrowth generating function can be described by a system of equations derived using combinatorial techniques on the prefixes of words with symbols in the generating set. For a finite free product of finite groups, this system consists of only finitely many equations. We use the concept of a *combinatorial class*, which is explained in Flajolet and Sedgewick [8]. Briefly, a combinatorial class is an ordered pair $\mathcal{C} = (P, l)$, where P is a set of objects, and $l : P \to \mathbb{Z}_{\geq 0}$ associates each object in P to a size. In the case that $P = \{\bigcirc\}$ is a singleton set, we call $\mathcal{C}$ the *neutral class* if $l(\bigcirc) = 0$; an *atom* if $l(\bigcirc) = 1$. We define two combinatorial classes $\mathcal{C} = (P, l)$ and $\mathcal{C}' = (P', l')$ to be combinatorially equivalent if there is a bijection, $\psi : P \to P'$ so that $l' = l \circ \psi$. If l is clearly understood, we use P alone to denote the class $\mathcal{C}$. Furthermore, the class, $\mathcal{C}$ is naturally associated with the generating function,

$$F(t) = \sum_{n \geq 0} |l^{-1}(n)| t^n,$$

where $l^{-1}(n) = \{s \in P : l(s) = n\}$ is the preimage of n with respect to l. If we take our class to be the language, $L(G, S)$, together with word length, then the associated generating function is precisely the cogrowth series.

We also define the Cartesian product of two combinatorial classes: For $\mathcal{A} = (A, l_A)$ and $\mathcal{B} = (B, l_B)$, let $\mathcal{A} \times \mathcal{B} := (A \times B, l_{AB})$, where $l_{AB}(a, b) = l_A(a) + l_B(b)$. If l_A and l_B are clearly understood, then we use $A \times B$ to denote the class, $\mathcal{A} \times \mathcal{B}$.

Let $G_1, \ldots, G_m$ be groups. Let S_i be a given generating set for G_i. Consider the free product $G = G_1 * G_2 * \ldots * G_m$, with the generating set $S = \cup_{i=1}^m S_i$. For each $g \in G$ and $X \subseteq G$, define $Z_{g,X}$ as the combinatorial class of all words in S^*, with size as the word length, that for all $s_1, \ldots, s_n \in S$, with $s = s_1 \cdot \ldots \cdot s_n = g \in G$, and for $i = 1, 2 \ldots, n-1$, it holds that $s_1 \ldots s_i \notin X$. That is, all proper nonempty prefixes of s avoid X. Let $F_{g,X}$ denote the generating function for $Z_{g,X}$. Our goal is to compute $F(t) := F_{1,\emptyset}(t)$. Let ι denote the characteristic function in the sense that, for a property $\mathcal{P}$, we have $\iota(\mathcal{P}) = 1$ if $\mathcal{P}$ is true, and $\iota(\mathcal{P}) = 0$ otherwise. Also, let τ denote an arbitrary atom, and ϵ the empty word, as well as the neutral class. Since all atoms are combinatorially equivalent, we may use τ to denote any atom in general. Lemma 2.7 below shows a system of equalities in the sense of combinatorial bijections. This lemma is stated and proved by Bell and Mishna [4]. We provide a more detailed proof.

Lemma 2.7. *Let $G = G_1 * G_2 * \ldots * G_m$ be a (possibly trivial) free product of m finitely generated groups. Let S_i be a finite generating set for G_i so that $S = \cup_{i=1}^m S_i$ is a generating set for G. For each $1 \leq i \leq m$ and $\{g\} \cup X \subseteq G_i$, using disjoint unions of combinatorial classes, the relations below hold.*

1. $Z_{g,X} = (\iota\,(g \in S_i) \times \tau) \cup \left(\bigcup_{s\in S_i\setminus X} \left(\tau \times Z_{s^{-1}g,s^{-1}X}\right)\right)$, *if* $1 \in X,\ g \neq 1$.
2. $Z_{g,X} = Z_{1,X} \times Z_{g,X\cup\{1\}}$, *if* $1 \notin X,\ g \neq 1$.
3. $Z_{1,X} = \epsilon \cup \left(Z_{1,X} \times \left(Z_{1,X\cup\{1\}} \setminus \epsilon\right)\right)$, *if* $1 \notin X$.
4. $Z_{1,X} = \epsilon \cup \left(\bigcup_{s\in S\setminus S_i} \left(\tau \times Z_{s^{-1},\{s^{-1}\}}\right)\right) \cup \left(\bigcup_{s\in S_i\setminus X} \left(\tau \times Z_{s^{-1},s^{-1}X}\right)\right)$, *if* $1 \in X$.

Proof. We show each relation independently by establishing combinatorial bijections.

(1): If $g \in S_i$, then $g \in Z_{g,X}$. Consider any word $w = w_1 \dots w_n \in Z_{g,X}$ such that $w \neq g$ as words (this is automatic if $g \notin S$). That is, w is not the word consisting of exactly the one character, g, provided that $g \in S$. Note that no proper nonempty prefix of w may evaluate to an element in G_j where $j \neq i$, since otherwise, if such a prefix were to belong to G_j, then some longer prefix must evaluate to $1 \in X \setminus \{g\}$. Write $w = w_1 w'$ with $w' \in Z_{g,X} \cap S^{n-1}$. We have $w_1 \in S_i \setminus X$ and since w has no proper nonempty prefix in X, w' has no proper nonempty prefix in $w_1^{-1}X$, so $w' \in Z_{w_1^{-1}g,w_1^{-1}X}$. On the other hand, if $s \in S_i \setminus X$ and $w' \in Z_{w_1^{-1}g,w_1^{-1}X}$, then $sw' \in Z_{g,X}$.

(2): Observe that

$$Z_{1,X} \times Z_{g,X\cup\{1\}} \subseteq Z_{1,X}^{*} \times Z_{g,X} \simeq Z_{g,X}.$$

Let $w = w_1 \dots w_n \in Z_{g,X}$. Decompose according to the largest prefix equal to 1. Specifically, let $k \in [0,n] \cap \mathbb{Z}$ be the largest possible so that $w_1 \dots w_k = 1 \in G$ and write $w = w_1 \dots w_k w'$. Notice that $k \neq n$ since $\epsilon \neq g \in G \setminus \{1\}$. Also, $w' = (w_1 \cdot \dots \cdot w_k)^{-1} w = 1 \cdot g = g \in G$. The proper prefixes of w' avoid $1X = X$, since those of w avoid X. By our choice of k, the proper nonempty prefixes of w' also avoid 1, and no other choice of k would satisfy this claim.

(3): Notice that $\epsilon \in Z_{1,X\cup\{1\}} \subseteq Z_{1,X}$. Also, concatenation of any number of words in $Z_{1,X}$, is again, in $Z_{1,X}$. Indeed, if $s_1, \dots, s_m \in Z_{1,X}$, then $s = s_1 \dots s_m$ evaluates to 1 in G. This establishes the right to left containment. Conversely, suppose $w = w_1 \dots w_n \in Z_{1,X}$ and $n > 0$. Let $k \in [0,n) \cap \mathbb{Z}$ be the largest possible so that $w_1 \cdot \dots \cdot w_n = 1 \in G$ and write $w = w_1 \dots w_k w'$. By our choice of k, we have that all proper prefixes of w' avoid $X \cup \{1\}$, and so $w' \in Z_{1,X\cup\{1\}}$. However, since $k \neq n$, $w' \neq \epsilon$, so a set bijection is established. Furthermore, no other choices of k satisfies our claim for w', so the decomposition is unique.

(4): It is true that $\epsilon \in Z_{1,X}$. Consider $w = sv$, with $s \in S \setminus X,\ v \in S^*$, and w evaluates to $1 \in G$. We observe 2 cases, noting first that v evaluates to $s^{-1} \in G$.
Case 1: $s \in S_i$. We want to show that $w \in Z_{1,X} \iff v \in Z_{s^{-1},s^{-1}X}$. Since the proper nonempty prefixes of w avoid X if and only if those of v avoid $s^{-1}X$, the result is immediate.
Case 2: $s \notin S_i$. We show that $w \in Z_{1,X} \iff v \in Z_{s^{-1},\{s^{-1}\}}$. The ($\implies$) direction is

clear as proper prefixes of w avoid $1 \in X$. For the converse, if w' is a proper nonempty prefix of w that evaluates to an element in $X \subseteq G_i$, then it has a nonempty prefix that evaluates to $1 \in G$. Without loss of generality, assume $w' = 1 \in G$ and write $w' = sv'$. Then $v' = s^{-1} \in G \setminus \{1\}$, so $v' \neq \epsilon$. This directly contradicts the fact that $v \in Z_{s^{-1},\{s^{-1}\}}$. □

Each of the properties of Theorem 2.7 also has a correspondence with an equation involving the set of generating functions, $F_{g,X}(t)$, as stated in corollary 2.8 below. If A, B, C are combinatorial classes associated with generating functions, $A(t), B(t), C(t)$ respectively, then $C = A \cup B \implies C(t) = A(t) + B(t)$ if the union is disjoint; and $C = A \times B \implies C(t) = A(t)B(t)$. Thus, Lemma 2.7 implies Corollary 2.8.

Corollary 2.8. *Adopting the same notation used in Lemma 2.7, we have the analogous equalities for the set of generating function* $\{F_{g,X}\}$.

1. $F_{g,X}(t) = \iota(g \in S_i)t + \sum_{s \in S_i \setminus X} tF_{s^{-1}g,s^{-1}X}(t)$ *if* $1 \in X$, $g \neq 1$.

2. $F_{g,X}(t) = F_{1,X}(t)F_{g,X\cup\{1\}}(t)$ *if* $1 \notin X$, $g \neq 1$.

3. $F_{1,X}(t) = 1 + F_{1,X}(t)(F_{1,X\cup\{1\}}(t) - 1)$ *if* $1 \notin X$.

4. $F_{1,X}(t) = 1 + \sum_{s \in S \setminus S_i} tF_{s^{-1},\{s^{-1}\}}(t) + \sum_{s \in S_i \setminus X} tF_{s^{-1},s^{-1}X}(t)$ *if* $1 \in X$.

The example below demonstrates an application of Corollary 2.8 with the free product of a cyclic group and a dihedral group.

Example 2.9. Using the notation given in Lemma 2.7, let $m = 2$, $G_1 = \mathbb{Z}_2 = \langle x | x^2 = 1\rangle$, $G_2 = D_3 = \langle r, f | r^3 = f^2 = 1, rf = fr^{-1}\rangle$, with corresponding generating sets $S_1 = \{x\}$, $S_2 = \{r, f\}$. The number of equations given by Corollary 2.8 in this case is $|G_1|2^{|G_1|} + |G_2|2^{|G_2|} = 8 + 6 \cdot 64 = 392$. We give a few of these equations here.

g	X	Corresponding Equation	Property #
1	$\varnothing$	$F_{1,\varnothing}(t) = 1 + F_{1,\varnothing}(t)(F_{1,\{1\}}(t) - 1)$	3
1	$\{1\}$	$F_{1,\{1\}}(t) = 1 + tF_{x,\{x\}}(t) + tF_{r^2,\{r^2\}}(t) + tF_{f,\{f\}}(t)$	4
x	$\{x\}$	$F_{x,\{x\}}(t) = F_{1,\{x\}}(t)F_{x,\{1,x\}}(t)$	2
r	$\{1, f\}$	$F_{r,\{1,f\}}(t) = t + tF_{1,\{r^2,r^2f\}}(t)$	1
r	$\{1, r, f\}$	$F_{r,\{1,r,f\}}(t) = t$	1
rf	$\{1, r\}$	$F_{rf,\{1,r\}}(t) = tF_{r^2,\{f,r^2f\}}(t)$	1
1	$\{1, x\}$	$F_{1,\{1,x\}}(t) = 1 + tF_{r^2,\{r^2\}}(t) + tF_{f,\{f\}}(t)$	4
r	$\{f\}$	$F_{r,\{f\}}(t) = F_{1,\{f\}}(t)F_{r,\{1,f\}}(t)$	2
1	$\{x\}$	$F_{1,\{x\}}(t) = 1 + F_{1,\{x\}}(t)(F_{1,\{1,x\}}(t) - 1)$	4

Table 2.2: Some equations in Example 2.9.

Note that by Lemma 2.7, in order to solve for $Z_{1,\varnothing}$, we only need to consider the combinatorial classes, $Z_{g,X}$ for which g and X are both entirely contained in one of the free factors: For some $i = 1, \ldots, m$, we have $\{g\} \cup X \subseteq G_i$. For $x \in S$, a word with proper prefixes avoiding x to some positive integer exponent also avoid x raised to a higher integer exponent. That is, for each $g \in G$, $x \in S$, and $X \subseteq G$, we have

$$Z_{g,X\cup\{x\}} \subseteq Z_{g,X\cup\{x^2\}} \subseteq Z_{g,X\cup\{x^3\}} \subseteq \ldots.$$

Under certain additional assumptions on the generating set, S, the above chain of inclusions becomes equalities. The following lemma gives the necessary details.

Lemma 2.10. *Let G be a finitely generated group with finite generating set, S. Let $x \in S$ and $X \subseteq G$. Assume that for each integer $k > 0$, every word in S^* evaluating to x^k in G is of the form uxv, where $u, v \in S^*$ and v evaluates to 1 in G. Suppose $0 < j < i$ and $x^i, x^j \in X$. Then for all $g \in G$, we have $Z_{g,X} = Z_{g,X\setminus\{x^i\}}$.*

Proof. Clearly, $Z_{g,X} \subseteq Z_{g,X\setminus\{x^i\}}$. To prove equality, assume, for the sake of contradiction, that $w = w_1 \ldots w_n \in Z_{g,X\setminus\{x^i\}} \setminus Z_{g,X}$. Choose $k > 0$ as small as possible so that $w_1 \cdot \ldots \cdot w_k = x^i$. Then $w_k = x$, so $w' := w_1 \ldots w_{k-1}$ evaluates to x^{i-1} in G. If $i = j + 1$, we see that w' is a proper prefix of w which evaluates to x^j, contradiction. Assume $j - i > 1$ and if $j - i$ was decreased by 1, then any word evaluating to x^i has a proper prefix evaluating to x^j. Immediately, our assumption tells us that w' has a proper prefix evaluating to x^j. Such a prefix is also a proper prefix of w, so we again get a contradiction. □

Observe that if $x \in S$ has finite order of at least three in the group G, then the hypotheses of Lemma 2.10 implies that $x^{-1} \notin S$, in which case S cannot be inverse closed. On the other hand, if x is a generator of some $G_i \cong \mathbb{Z}$, with $S_i = \{x, x^{-1}\}$, then the conditions of Lemma 2.10 are satisfied. As a result, to solve for $F(t)$, it is sufficient to consider $F_{g,X}(t)$ only for (g, X) such that if $\{g\} \cup X \subseteq G_i$, then $\{g\} \cup X \subseteq \{1, x, x^{-1}\}$. We formalize such a result in a theorem.

Theorem 2.11. *Let $G_1, \ldots, G_m$ be finitely generated groups with generating sets $S_1, \ldots, S_m$ respectively. Let $G = G_1 * G_2 * \ldots * G_m$ be the free product of the m groups. Let $C \subseteq [m]$ so that for each $i \in C$, $G_i = \langle x_i \rangle \cong \mathbb{Z}$, and $S_i = \{x_i, x_i^{-1}\}$. Then $F(t)$ depends only on the set of all series $F_{g,X}(t)$ where $\{g\} \cup X \subseteq G_i$ for some $i \in [m]$, so that whenever $i \in C$, we have*

$$\{g\} \cup X \subseteq S_i \cup \{1\}.$$

In other words, all series $F_{g,X}(t)$ not satisfying the above condition are either already known, or have no influence in determining $F(t) := F_{1,\emptyset}(t)$.

Proof. By Lemma 2.7, property 3, $F(t)$ is determined by $F_{1,\{1\}}(t)$, which in turn, is determined, due to property 4, if $F_{s,\{s\}}(t)$ is known for each $s \in S \setminus \{1\}$. The computation of each $F_{s,\{s\}}(t)$ requires, by property 2, only $F_{1,\{s\}}(t)$ and $F_{s,\{1,s\}}(t)$. Any series $F_{g,X}(t)$, for which $\{g\} \cup X \subseteq G_i$ depends only on series of the form $F_{g',X'}(t)$, where $\{g'\} \cup X \subseteq G_k$, and $k \neq i \implies X = \{g'\} \subseteq S_k$. Hence, it is enough to show that if $s \in S_i$ with $i \in C$, then $F_{s,\{s\}}(t)$ depends only on $F_{g,X}(t)$, with either $\{g\} \cup X \nsubseteq G_i$ or $\{g\} \cup X \subseteq S_i \cup \{1\}$. Suppose s and i are as such. Recall that $S_i = \{x_i, x_i^{-1}\}$ for $i \in C$. Lemma 2.7 property 3 shows that $F_{1,\{s\}}(t)$ is determined by $F_{1,\{1,s\}}(t)$, which, by Lemma 2.7 property 4, depends only on $F_{y,\{y\}}(t)$ for $y \in S \setminus S_i$, and $F_{y^{-1},\{y^{-1},y^{-1}s\}}(t)$ for $y \in S_i \setminus \{1, s\} = \{s^{-1}\}$. The latter series is $F_{s,\{s,s^2\}}(t)$, which by Lemma 2.10, is equal to $F_{s,\{s\}}(t)$. Lemma 2.7 property 1 shows that $F_{s,\{1,s\}}(t)$ is determined by $F_{y,\{y\}}(t)$ for $y \in S \setminus S_i$, and $F_{s^2,\{s,s^2\}}(t) = 0$. We have shown that each $F_{s,\{s\}}(t)$ are independent of every $F_{g,X}(t)$ with $\{g\} \cup X \subseteq G_i$ and $(g, X) \notin \{(1, \{s\}), (s, \{1, s\})\}$. Hence, our proof is complete. □

We immediately obtain the following corollary, which imposes a condition when only finitely many equations are needed to describe our grammar.

Corollary 2.12. *Suppose each of the free factors G_i is either the infinite cyclic group or finite. Then $F(t)$ can be determined by a finite system of algebraic equations, provided that each copy of the infinite cyclic group is associated to an inversely closed generating set consisting of two elements.*

We remark that, in addition, it is redundant to consider the infinite cyclic group, $\mathbb{Z}$, as a factor in our free product, as it has the same cogrowth series as $\mathbb{Z}_2 * \mathbb{Z}_2$. To see this, consider $\mathbb{Z} = \langle x \rangle$ and $\mathbb{Z}_2 * \mathbb{Z}_2 = \langle u | u^2 = 1 \rangle * \langle v | v^2 = 1 \rangle$ with generating sets $\{x, x^{-1}\}$ and $\{u, v\}$ respectively. Notice that a word $w = \{u, v\}^*$ is an excursion if and only if w is either the empty word, or w has two consecutive occurrences of the same character such that, when these characters are deleted, the resulting word is again, an excursion. Under this reasoning, we can construct a length preserving bijection $\varphi : \{x, x^{-1}\}^* \to \{u, v\}^*$ as follows: Define $\varphi(\epsilon) = \epsilon$, $\varphi(x) = u$, $\varphi(x^{-1}) = v$; and if $w \in \{x, x^{-1}\}^*$ has length at least 1, then define

$$\varphi(wx) = \begin{cases} \varphi(w)u, & \text{if } w \text{ is an excursion} \\ \varphi(w)u, & \text{if } \varphi(w) \text{ ends with } v \text{ and } w \text{ has more occurrences of } x \text{ than } x^{-1} \\ \varphi(w)u, & \text{if } \varphi(w) \text{ ends with } u \text{ and } w \text{ has less occurrences of } x \text{ than } x^{-1} \\ \varphi(w)v, & \text{ otherwise} \end{cases}$$

and

$$\varphi(wx^{-1}) = \begin{cases} \varphi(w)v, & \text{if } w \text{ is an excursion} \\ \varphi(w)v, & \text{if } \varphi(w) \text{ ends with } v \text{ and } w \text{ has more occurrences of } x \text{ than } x^{-1} \\ \varphi(w)v, & \text{if } \varphi(w) \text{ ends with } u \text{ and } w \text{ has less occurrences of } x \text{ than } x^{-1} \\ \varphi(w)u, & \text{ otherwise} \end{cases}.$$

With this construction, we have that $\phi(w)$ is an excursion if and only if w is an excursion. In the remainder of this thesis, we restrict our consideration to only free products of finite groups. In general, one can also consider including noncylic infinite groups as free factors, but this case will not be studied here.

The system given in Lemma 2.7 and Corollary 2.8 can be used, along with algebraic elimination, to obtain a single polynomial equation that satisfies the cogrowth series. However, the system involved can be quite large, and the elimination process can be inefficient and time consuming. Using the theory of free probability, we can obtain a system that involves far fewer equations and is much more efficient to solve.

2.4 Connections to Free Probability Theory

The theory of free probability is closely connected to the free product of groups. With the help of free probability, we can establish simple and elegant systems of equations that solve the associated algebraic cogrowth series. In this setting, we rely on the result in [14, Theorem 12.7] and the theory of Cauchy transforms. We briefly describe the relevant theory here. We consider the group, $G = G_1 * \ldots * G_m$, as a basis of the associated group algebra $\mathbb{C}[G]$, consisting of finite $\mathbb{C}$-linear combinations of elements in G. The elements in $\mathbb{C}[G]$ are viewed as non-commutative random variables, equipped with the linear *expectation* operator $\phi : \mathbb{C}[G] \to \mathbb{C}$ defined by

$$\phi\left(\left(\sum_{g\in G} \alpha_g g\right)\right) = \alpha_1$$

where each coefficient $\alpha_g \in \mathbb{C}$, and only finitely many of these coefficients are not zero. If S is the generating set of G that we consider, then the sequence,

$$\left\{\phi\left(\left(\sum_{s\in S} s\right)^n\right)\right\}_{n\geq 0},$$

is precisely the cogrowth sequence. To see this, notice that

$$\left(\sum_{s\in S} s\right)^n = \sum_{s_i\in S,\ 1\leq i\leq n} s_1 \cdot s_2 \cdot s_3 \cdot \ldots \cdot s_n \in \mathbb{C}[G]$$

is the sum of the multiset of all group elements corresponding to words in S^* of length n. Hence, the number of summands that evaluate to 1 is the coefficient of t^n in the cogrowth series, $F_{G;S}(t)$.

Let $\alpha = \sum_{g\in G} \alpha_g g$ and $\beta = \sum_{g\in G} \beta_g g$ be elements of $\mathbb{C}[G]$. We define the *Cauchy transform* of α as

$$G_\alpha(t) := \sum_{n\geq 0} \phi(\alpha^n) t^{-n-1}. \tag{2.4}$$

Let $K_\alpha = G_\alpha^{\langle -1\rangle}$ be the compositional inverse of the G_α given in Equation (2.4). If $\alpha_g\beta_g = 0$ for each $g \in G$, then a major result from free probability theory [14, Theorem 12.7] implies

$$K_{\alpha+\beta}(t) = K_\alpha(t) + K_\beta(t) - t^{-1}. \tag{2.5}$$

We now prove a new result below yielding a system of polynomial equations that can be used to solve for the minimal polynomial of a cogrowth series on the free product of cyclic groups. Although the new result assumes finite cyclic factors, similar techniques can be applied to deduce systems of equations for the case of any free product of finitely many finite groups. Here, we restrict ourselves to the case of cyclic factors because their rational generating functions are simple compared to those of other finite groups. Later on, we use this technique with a mixture of dihedral and cyclic factors.

Theorem 2.13 (Cogrowth System for Finite Cyclic Factors). *Let*

$$G := \coprod_{i=1}^{r}\coprod_{j=1}^{m_i} \langle x_{ij} | x_{ij}^{n_i} = 1\rangle = \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2} * \ldots * \mathbb{Z}_{n_r}^{*m_r},$$

where each $n_i \geq 2$ and $m_i \geq 1$. Let the generating set of G be

$$S := \{x_{ij} | i = 1, \ldots, r; j = 1, \ldots, m_i\}.$$

Let $F(t)$ be the cogrowth series of G generated by S. Then the polynomial system in $t, z, z_1, \ldots, z_r$ over $\mathbb{Z}$ given by

$$\begin{aligned} P_i(t, z, z_1, \ldots, z_r) &:= tzz_i^{n_i} - z_i^{n_i-1} - tz = 0,\ \ i = 1, \ldots, r; \\ P_{r+1}(t, z, z_1, \ldots, z_r) &:= z - \left(\sum_{j=1}^{r} m_j tzz_j\right) + \left(\sum_{j=1}^{r} m_j\right) - 1 = 0 \end{aligned} \tag{2.6}$$

solves $F(t)$ in the sense that there are algebraic functions $F_1(t)\ldots, F_r(t)$, all not zero, such that

$$P_i(t, F(t), F_1(t), \ldots, F_r(t)) = 0$$

for $1 \leq i \leq r + 1$.

Proof. We use the sum of generators, apply Cauchy transforms, and employ a few change of variables to establish the desired system. Let $\phi : \mathbb{C}[G] \to \mathbb{C}$ be the expectation operator, and let $s \in \mathbb{C}[G]$ be the sum of the generators:

$$s = \sum_{i=1}^{r} \sum_{j=1}^{m_i} x_{ij}.$$

As before, for $\alpha \in C[G]$, let $G_\alpha(t)$ be its Cauchy transform and $K_\alpha(t)$ be its compositional inverse. For each $i = 1, 2, \ldots r$, and each $j = 1, 2, \ldots, n_i$, it follows that

$$G_{x_{ij}}(t) = \frac{t^{n_i - 1}}{t^{n_i} - 1}$$

and consequently, $K_{x_{ij}}(t)$ is a root of $z^{n_i-1} - tz^{n_i} + t \in (\mathbb{Z}[t])[z]$. By the property of inverse Cauchy transforms stated in Eqn (2.5),

$$\begin{aligned} K_s(t) &= \left(\sum_{i=1}^{r} \sum_{j=1}^{m_i} K_{x_{ij}}(t) \right) - \left(\left(\sum_{i=1}^{r} m_i \right) - 1 \right) t^{-1} \\ &= \left(\sum_{i=1}^{r} m_i K_i(t) \right) - \left(\left(\sum_{i=1}^{r} m_i \right) - 1 \right) t^{-1} \end{aligned}$$

where for each fixed i, $K_i(t)$ denotes any of the equivalent series $K_{x_{ij}}(t)$, with j ranging over $1, 2, \ldots, m_i$. The system of equations,

$$\begin{aligned} z &= \left(\sum_{i=1}^{r} m_i z_i \right) - \left(\left(\sum_{i=1}^{r} m_i \right) - 1 \right) t^{-1} \\ z_i^{n_i-1} - t z_i^{n_i} + t &= 0, \ i = 1, 2, \ldots, r \end{aligned} \tag{2.7}$$

is solved by $z = K_s(t)$, $z_i = K_i(t)$ for each i. Interchanging t and z in (2.7) yields the system

$$\begin{aligned} t &= \left(\sum_{i=1}^{r} m_i z_i \right) - \left(\left(\sum_{i=1}^{r} m_i \right) - 1 \right) z^{-1} \\ z_i^{n_i-1} - z z_i^{n_i} + z &= 0, \ i = 1, 2, \ldots, r \end{aligned} \tag{2.8}$$

which has a solution satisfying $z = G_s(t)$. Since $G_s(t) = t^{-1} F(t^{-1})$, substituting $t^{-1} z$ for z in (2.8) yields

$$\begin{aligned} t &= \left(\sum_{i=1}^{r} m_i z_i \right) - \left(\left(\sum_{i=1}^{r} m_i \right) - 1 \right) t z^{-1} \\ z_i^{n_i-1} - t^{-1} z z_i^{n_i} + t^{-1} z &= 0, \ i = 1, 2, \ldots, r \end{aligned} \tag{2.9}$$

which can be satisfied by $z = F(t^{-1})$. Substituting t^{-1} for t, we obtain

$$\begin{aligned} t^{-1} &= \left(\sum_{i=1}^{r} m_i z_i\right) - \left(\left(\sum_{i=1}^{r} m_i\right) - 1\right) t^{-1} z^{-1} \\ z_i^{n_i - 1} - tzz_i^{n_i} + tz = 0,\ i = 1, 2, \ldots, r & \end{aligned} \tag{2.10}$$

which has a solution satisfying $z = F(t)$. By multiplying the first equation of (2.10) by tz, and rearranging, we obtain (2.6). □

The reader may notice that the theory of free probability is quite powerful in this setting. The system, (2.6), appears to be far more simple to analyze than the ones given in Corollary 2.8. The number of equations we obtain using combinatorial grammar can be exponential order in the number of distinct free factors. Using free probability, this number of equations required has been reduced to linear in the number of distinct free factors. In a later chapter, we apply Theorem 2.13 to obtain degree bounds for the implicit polynomial equation solving the cogrowth series.

2.5 Resultant of Polynomials

Before we analyze implicit equations of cogrowth series, it is useful to recall some preliminary definitions from computer algebra. We take B be an integral domain, for which a quotient field exists. Since a polynomial ring over an integral domain is again, an integral domain, the discussion that follows for univariate polynomials can be naturally extended to multivariate polynomials. For a nonzero univariate polynomial $f \in B[z]$, define its *valuation* with respect to z as

$$\operatorname{val}_z f := \max\{k \in \mathbb{Z}_{\geq 0} : \exists g \in B[z],\ f = z^k g\}.$$

For convenience, we use the convention, $\operatorname{val}_z 0 = \infty$. Note that our definition of valuation is consistent with that of a power series. Consider any $f, g \in B[z], k \in \mathbb{Z}_{\geq 0}$. We use $[z^k]f$ to denote the coefficient of z^k in f, which is an element of B. The notation, $\operatorname{Syl}(f, g, z)$ will be used to denote the *Sylvester matrix* [8, Appendix B] of f and g with respect to z, with coefficients arranged in rows. The determinant of this matrix is called the *resultant* of f and g, and is denoted here as $\operatorname{Res}(f, g, z) := \det \operatorname{Syl}(f, g, z)$. If $f, g \in B[t, z]$ are both nonzero, classic properties of the resultant leads to an upper bound on the degree of $\operatorname{Res}(f, g, z)$ with respect to t. Specifically,

$$\deg_t \operatorname{Res}(f, g, z) \leq (\deg_t f)(deg_z g) + (\deg_t g)(\deg_z f). \tag{2.11}$$

It is possible that $\operatorname{Res}(f,g,z)=0$. Using the convention that $\deg 0 = -\infty$, (2.11) now holds in cases where $fg=0$.

In most circumstances that arise upon investigating our problem of interest, monomial factors in polynomials are of no significance. Hence, it is convenient to remove them whenever needed. For this purpose, we define, for $f \in B[z] \setminus \{0\}$, $\operatorname{trim}_z f$, to be the unique polynomial $h \in B[z]$, so that $f(z) = h(z) z^{\operatorname{val}_z f}$. By construction, $\operatorname{val}_z h = 0$. We call the polynomial, $\operatorname{trim}_z f$, the *trim* of f with respect to z. In addition, we define $\operatorname{trim}_z 0 := 0$. If $f, g \in B[z_1, \ldots, z_n]$ are multivariate, define

$$\operatorname{trim}_B f := \operatorname{trim}_{z_1} \operatorname{trim}_{z_2} \ldots \operatorname{trim}_{z_n} f,$$

and the reduced resultant,

$$\overline{\operatorname{Res}}_B(f,g,z) := \operatorname{trim}_B \operatorname{Res}(f,g,z)$$

where z is any of the z_i for which $(\deg_z f)(\deg_z g) > 0$. It is a fact that, for any $k \in \mathbb{Z}_{>0}$ and $p \in B[z]$, p^k and p have the same roots in the algebraic closure of the quotient field of B. Also, if $\deg_z f = 0$, then $\operatorname{Res}(f,g,z) = f^{\deg_z g}$. Hence, if $\deg_z g > 0$, then we may set $\overline{\operatorname{Res}}_B(f,g,z)$ to $\operatorname{trim}_B f$. A similar discussion follows in the case that $\deg_z g = 0$ but $\deg_z f \neq 0$. If both the degrees are 0, then we can set their reduced resultant to 1, the unity element of B, which is the same as their classic resultant. This discussion leads us to the definition below.

Definition 2.14. Let $f, g \in B[z_1, \ldots, z_n]$, and $z = z_i$ for some $1 \le i \le n$. Then the *reduced resultant* of f and g with respect to z relative to B is given by

$$\overline{\operatorname{Res}}_B(f,g,z) := \begin{cases} \operatorname{trim}_B \operatorname{Res}(f,g,z), & (\deg_z f)(\deg_z g) > 0 \ \vee \ fg \equiv 0 \\ \operatorname{trim}_B f, & \deg_z f = 0, \ \deg_z g > 0 \\ \operatorname{trim}_B g, & \deg_z f > 0, \ \deg_z g = 0 \\ 1, & \deg_z f = \deg_z g = 0 \end{cases} . \tag{2.12}$$

We will see, in later chapters, that using the reduced resultant instead of the ordinary resultant can significantly reduce the degree of the polynomials in our computations.

Finally, for an $n \times n$ matrix $C = (c_{ij})_{i,j=1}^n$, with $c_{ij} \in B[z]$, and $\sigma \in \operatorname{Sym}(n)$, denote

$$C[\sigma] := \prod_{i=1}^n c_{i,\sigma(i)} \in B[z].$$

With this notation and a standard definition of determinant, we have

$$\det C = \sum_{\sigma \in \mathrm{Sym}(n)} \mathrm{sgn}(\sigma) C[\sigma].$$

2.6 Algebraic Elimination

Let $\vec{P}$ be a vector of polynomials. We are interested in solutions of the form $\vec{P} = \vec{0}$, where $\vec{P} = (P_i)_{i=1}^n$, with each $P_i \in B[t, z_1, z_2, \ldots, z_n]$. For our problem of interest, assume that there are algebraic functions $F_i(t) \neq 0,\ i = 1 \ldots n$, so that $\vec{P}(t, F_1(t), \ldots, F_n(t)) \equiv \vec{0}$. The goal of the theory of algebraic elimination is to seek a satisfying bivariate polynomial $P_f(t, z) \in B[t, z]$ for $F_1(t)$. In particular, we want to find P_f so that for any sequence of n nonzero algebraic functions F_i,

$$\vec{P}(t, F_1(t), \ldots, F_n(t)) = \vec{0} \implies P_f(t, F_1(t)) = 0.$$

One way to find P_f via elimination involves the use the resultant to eliminate one variable at a time. This method is valid without the nonzero assumption of our algebraic functions. With this additional assumption, we can instead use the reduced resultant, which in general, will lower the degree of P_f in the variable z that the algorithm outputs. The procedure is stated below.

Algorithm 1 polynomial elimination over an integral domain B

Input: $n \in \mathbb{Z}_{>0}$; $t, z_1, \ldots, z_n$ indeterminate ordered as given; $\vec{P} \in B[t, z_1, \ldots, z_n]^n$.

Assumption: There are algebraic functions $F_1(t), \ldots, F_n(t)$, all nonzero, suct that $\vec{P}(t, F_1(t), \ldots, F_n(t)) = 0$.

Purpose: Find $P_f(t, z) \in B[t, z],\ P_f \not\equiv 0$ so that for any sequence of nonzero algebraic functions, $F_1(t), \ldots, F_n(t)$, it holds that $\vec{P}(t, F_1(t), \ldots, F_n(t)) = 0 \implies P_f(t, F_1(t)) = 0$.

```
$\vec{P}^{(0)} := \vec{P}$.
for $k = 1, 2, \ldots, n-1$ do
    for $i = 1, 2, \ldots, n-k$ do
        $P_i^{(k)} = \overline{\mathrm{Res}}_B(P_i^{(k-1)}, P_{n-k+1}^{(k-1)}, z_{n-k+1}) \in B[t, z_1, \ldots, z_{n-k}]$
    end for
    $\vec{P}^{(k)} := (P_i^{(k)})_{i=1}^{n-k}$
end for
return $P_f(t, z) := P_1^{(n-1)}(t, z) \in B[t, z]$
```

Ideally, we find P_f so that $\deg_z P_f$ is as small as possible. If we run Algorithm 1 with the system of equations (2.6), then the output, P_f, is a satisfying polynomial for the associated cogrowth generating function. The degree, $\deg_z P_f$, provides an upper bound on minimal polynomials of this cogrowth generating function. We make use of such upper bounds in Chapter 3.

2.7 Singularity Analysis

Singularities of an algebraic equation give insight to the rate of exponential growth of the coefficients in its series expansion. In our case, we can gain some insight about the limit behaviour of $|L(G,S) \cap S^n|$. The theory of singularity and asymptotic analysis is discussed extensively in [2, 8, 11]. We provide a brief summary here in this section. In this thesis, we apply this theory to a few examples of groups. Given a nonzero polynomial $f(t) \in B[t]$ with $\alpha = [t^{\deg f}]f(t)$ being the leading coefficient, we define the discriminant of f with respect to t, to be

$$\operatorname{disc}_t f := \alpha^{-1} \operatorname{Res}\left(f, \frac{df}{dt}, t\right).$$

Let $F(t)$ be an algebraic function with a series expansion

$$\sum_{n=0}^{\infty} a_n t^n \in \mathbb{Z}_{\geq 0}[[t]].$$

Suppose that $Q(t,z) \in \mathbb{Z}[t,z] \setminus \{0\}$ satisfies $Q(t,F(t)) = 0$. A singularity is said to be *dominant* if it has the smallest modulus across all singularities. We are often interested in finding the modulus of the dominant singularities of $F(t)$, which can be computed by

$$\rho = \lim_{n\to\infty} \frac{a_n}{a_{n+1}} \geq 0,$$

provided this limit exists. We say that the sequence, $\{a_n\}$, is p-periodic if for some r, we have that

$$\lim_{n\to\infty} \frac{a_{pn+r}}{a_{pn+p+r}}$$

exists. In this case, we have

$$\rho = \min_r \left(\lim_{n\to\infty} \frac{a_{pn+r}}{a_{pn+p+r}}\right)^{1/p}$$

where r ranges over all non-negative integers so that the inner limit exists. The smallest p with the given property is known as the period of $\{a_n\}$. It is known [8, 11] that all singularities of $F(t)$ appear in

$$E := \{w \in \mathbb{C} : ([z^{\deg_z Q}]Q(t,z))(w) = 0\} \cup \{w \in \mathbb{C} : (\operatorname{disc}_z Q)(w) = 0\}$$

The set E, is known as the *exceptional set* of Q. It is the set of roots of the leading coefficient of $Q \in (\mathbb{Z}[t])[z]$, together with the roots of the discriminant of Q with respect to z. Since $F(t) \in \mathbb{Z}_{\geq 0}[[t]]$, the well known Pringsheim's Theorem [12, 8] in complex analysis tell us that ρ is a singularity of $F(t)$. Consequently, $\rho \in E \cap [0, \infty)$. We hence see that ρ can approximated by computing ratios involving a_n for large n. Below defines an outline of how ρ can be computed.

1. Compute the finite set E. If $|E \cap [0, \infty)| = 1$ then ρ is that unique element, and we are done. Otherwise proceed to the next step.

2. Pick a small tolerance parameter $\epsilon > 0$ satisfying

$$2\epsilon < \min_{v \neq w \in E \cap [0,\infty)} |v - w|.$$

3. Obtain an approximation, ρ^*, of ρ, by first generating a_n for large n.

4. Consider the set of elements $w \in E \cap [0, \infty)$, where $|w - \rho^*| < \epsilon$. If this set is empty, go back to the previous steps and generate more terms to get a more precise approximation ρ^*. Otherwise, output ρ to be this unique element, w.

Finally, if the sequence $\{a_n\}$ has period p, then its dominant singularities are precisely $\rho e^{i\frac{2k\pi}{p}}$ where $k = 0, 1, 2, \ldots, p - 1$.

2.8 Iterative Fixed Point Method on Word Grammar

One can usually generate the first few terms in the counting sequence from the combinatorial descriptor [17]. This is useful for verifying any series solution. Initial terms can also be used to guess equations satisfied by a series in some situations. We know a priori that our generating functions are algebraic. If we know the polynomial equation, we can generate a series solution. To do this, an iterative method may be used to generate the initial terms to arbitrary precision.

We first recall some properties of algebraic systems. Consider the complete metric space, $(\mathbb{C}[[t]], d)$, where $d : \mathbb{C}[[t]] \times \mathbb{C}[[t]] \to \mathbb{R}$ is the distance function, such that for $f \neq g \in \mathbb{C}[[t]]$, $d(f, g) := 2^{-\operatorname{val}_t(f-g)}$. Consider an algebraic system of the form $\vec{z} = \vec{P}(t, \vec{z})$ where

$$\vec{z} = (z_1, z_2, \ldots, z_n)^T \text{ and } \vec{P} = (P_1, P_2, \ldots, P_n)^T,$$

with each $P_i \in \mathbb{C}[t, \vec{z}]$. For $\vec{f} = (f_i)_{i=1}^n, \vec{g} = (g_i)_{i=1}^n$ let

$$\vec{d}(\vec{f}, \vec{g}) = (d(f_i, g_i))_{i=1}^n$$

denote the vectors of distances. Also, let $E \subseteq \mathbb{C}[[t]]$ be closed under the topology induced by d such that $\vec{f} \in E^n \implies \vec{P}(t, \vec{f}) \in E^n$. We say that the system, $\vec{z} = \vec{P}(t, \vec{z})$, is a *contraction* in E if there exists some constant $\kappa \in (0, 1)$ such that for each $\vec{f}, \vec{g} \in E^n$, it holds that $\|\vec{d}(\vec{P}(t, \vec{f}), \vec{P}(t, \vec{g}))\| \leq \kappa \|\vec{d}(\vec{f}, \vec{g})\|$, where $\|\cdot\|$ denotes any fixed arbitrary choice of the equivalent norms[3] on $\mathbb{R}^n$. If the system is a contraction in E, then Banach's fixed point theorem implies that the system has exactly one solution in $\vec{z}^* \in E^n$, and that any sequence of the form, $\vec{z}^{(k+1)} := \vec{P}(t, \vec{z}^{(k)}),\ k \geq 0$, as generated by a fixed point iteration, converges to $\vec{z}^*$. Our objective is to analyze convergence properties of the fixed point iterative method that results from the system in Corollary 2.8. For this reason, we now recall the definition of proper algebraic systems and state a commutative version of the definition given in Stanley [19].

Definition 2.15 ([19, 6, 5])**.** The algebraic system, $\vec{z} = \vec{P}(t, \vec{z})$, is said to be *proper* if the following conditions are satisfied:

- The polynomials, P_i, $1 \leq i \leq n$, have no constant terms: $\vec{P}(t, \vec{0}) = \vec{0}$; and
- each P_i has no linear terms except scalar multiples of t: $\forall 1 \leq i, j \leq n, [z_j]P_i(0, \vec{z}) = 0$.

In Proposition 2.17 below, we recall the proof that a proper algebraic system is a contraction on $t\mathbb{C}[[t]]$, the maximal ideal in $\mathbb{C}[[t]]$ consisting of all power series of nonzero valuation. As a result, there must a unique vector of n power series, each with no constant term, that solves a proper algebraic system. Furthermore, the fixed point iteration associated with the system must converge to that solution regardless to the initial vector of power series, provided that all components have no constant term. We first state and prove an inequality involving the valuation of a difference of two products of power series.

Lemma 2.16. *Let $f_1, f_2, \ldots, f_n, g_1, \ldots, g_n \in \mathbb{C}[[t]]$, and $e_1, e_2, \ldots, e_n \in \mathbb{Z}_{\geq 0}$. Then*

$$\operatorname{val}_t \left(\prod_{j=1}^n f_j^{e_j} - \prod_{j=1}^n g_j^{e_j} \right) \geq \sum_{j=1}^n e_j \operatorname{val}_t(f_j - g_j). \tag{2.13}$$

Proof. Without loss of generality, we may assume that each $e_j = 1$. It is sufficient to prove the inequality for $n = 2$, as a straightforward induction on n deduces the general case. The inequality certainly holds if $f_1 f_2 = g_1 g_2$, so assume this is not the case. For $j = 1, 2$, let $\theta_j := \min\{\operatorname{val}_t f_j, \operatorname{val}_t g_j)\}$, so that $f_j = a_j t^{\theta_j} + o(t^{\theta_j})$ and $g_j = b_j t^{\theta_j} + o(t^{\theta_j})$. If $a_1 = b_1$ and

[3] In Flajolet and Sedgewick [8], the supremum norm, $\|\cdot\|_\infty$ is used.

$a_2 = b_2$, then we can replace each f_j, g_j with $f_j - a_j t^{\theta_j}$ and $g_j - b_j t^{\theta_j}$, respectively, which does not change either side of inequality (2.13), and repeat the argument. Thus, suppose $a_j \neq b_j$ for some $j = 1, 2$. In this case,

$$f_1 f_2 - g_1 g_2 = (a_1 a_2 - b_1 b_2) t^{\theta_1 + \theta_2} + o(t^{\theta_1 + \theta_2})$$

has valuation at least $\theta_1 + \theta_2 = \mathrm{val}_t(f_1 - g_1) + \mathrm{val}_t(f_2 - g_2)$. □

We now state and proof the fact that proper algebraic systems are contractions in the closed subset consisting of power series with no constant terms. Although the proof here is very standard, it is not found in many literatures[4], so we give it here for clarity and convenience.

Proposition 2.17. *Let $E = t\mathbb{C}[[t]]$ and let d be the metric equipped on $\mathbb{C}[[t]]$ as before. Then E is closed in the topology induced by d. If $\vec{z} = \vec{P}(t, \vec{z}) \in \mathbb{C}[t, \vec{z}]$ is a proper algebraic system of n polynomial equations, then it is a contraction in E.*

Proof. Consider a sequence of power series $\{f_n\} \subseteq E$ which converges, under d, to some $f \in \mathbb{C}[[t]]$. Then it must hold that $\lim_{n\to\infty} \mathrm{val}_t(f - f_n) = \infty$, which implies that $f(0) = 0$, so $f \in E$. Thus, E is closed. Since our system is proper, no component of $\vec{P}$ has a constant term, so $\vec{P}$ is E^n-invariant in the sense that $\vec{z} \in E^n \implies \vec{P}(t, \vec{z}) \in E^n$. For notational convenience, let us define the index set,

$$\mathcal{I} := \left\{ \alpha = (\alpha_v)_{v \in \{t, z_1, z_2, \ldots, z_n\}} : \alpha_v \in \mathbb{Z}_{\geq 0},\ \sum_v \alpha_v \geq 2,\ \sum_{v \neq t} \alpha_v \geq 1 \right\}.$$

For each $\alpha \in \mathcal{I}$, define $|\alpha|$ to be the sum of all the components of α, and

$$(t, \vec{z})^\alpha := t^{\alpha_t} z_1^{\alpha_{z_1}} \ldots z_n^{\alpha_{z_n}}.$$

For $1 \leq j \leq n$ and $\alpha \in \mathcal{I}$, let

$$c_\alpha^{(j)} := [(t, \vec{z})^\alpha] P_j(t, \vec{z})$$

denote the coefficient of the corresponding monomial. In addition, for $1 \leq j \leq n$, define $\mathcal{I}_j := \{\alpha \in \mathcal{I} : c_\alpha^{(j)} \neq 0\}$, so that $P_j(t, z) = \sum_{\alpha \in \mathcal{I}_j} c_\alpha^{(j)} (t, \vec{z})^\alpha + t f_j(t)$, where $f_j \in \mathbb{C}[t]$. Let $\vec{x}, \vec{y} \in E^n$. We take $\|\cdot\| = \|\cdot\|_\infty$ to be the supremum norm, and deduce, for each j,

[4] For instance, Stanley [19] states this result and gives only a brief idea of the proof.

$$\begin{aligned}\operatorname{val}_t(P_j(t,\vec{x}) - P_j(t,\vec{y})) &= \operatorname{val}_t \sum_{\alpha\in\mathcal{I}_j} c_\alpha^{(j)}((t,\vec{x})^\alpha - (t,\vec{y})^\alpha) \\ &= \operatorname{val}_t \sum_{\alpha\in\mathcal{I}_j} c_\alpha^{(j)} t^{\alpha_t}\left(\prod_{i=1}^n x_i^{\alpha_{z_i}} - \prod_{i=1}^n y_i^{\alpha_{z_i}}\right) \\ &\geq \min_{\alpha\in\mathcal{I}_j}\left[\alpha_t + \operatorname{val}_t\left(\prod_{i=1}^n x_i^{\alpha_{z_i}} - \prod_{i=1}^n y_i^{\alpha_{z_i}}\right)\right] \\ &\geq \min_{\alpha\in\mathcal{I}_j}\left[\alpha_t + \sum_{i=1}^n \alpha_{z_i}\operatorname{val}_t(x_i - y_i)\right]\end{aligned}$$

where the last inequality follows from inequality (2.13) of Lemma 2.16. Observe that, for each $\alpha\in\mathcal{I}$, $\max_{1\leq j\leq n}\alpha_{z_j} = 1 \implies \alpha_t > 0$. Since each of the valuations, $\operatorname{val}_t(x_i - y_i)$, is positive, we deduce that, for $\alpha\in\mathcal{I}$,

$$\alpha_t + \sum_{i=1}^n \alpha_{z_i}\operatorname{val}_t(x_i - y_i) > \operatorname{val}_t(x_k - y_k) \geq \min_{1\leq j\leq n}\operatorname{val}_t(x_j - y_j),$$

where k is chosen so that $\alpha_{z_k} = \max_{1\leq j\leq n}\alpha_{z_j}$. Consequently,

$$\min_{1\leq j\leq n}\operatorname{val}_t(P_j(t,\vec{x}) - P_j(t,\vec{y})) > \min_{1\leq j\leq n}\operatorname{val}_t(x_j - y_j),$$

which implies that

$$\|\vec{d}(\vec{P}(t,\vec{x}),\vec{P}(t,\vec{y}))\| \leq \frac{1}{2}\|\vec{d}(\vec{x},\vec{y})\|,$$

thus showing the contraction property. □

The system of equations described in Corollary 2.8 is expressed in the form, $\vec{z} = \vec{P}(t,\vec{z})$. Recall from Corollary 2.12, that for a free product of finitely many finite group, only finitely many equations in the grammar from Corollary 2.8 is required. We are interested in generating approximate solutions to this system using fixed point iteration. For this reason, Proposition 3.2 is useful to our problem. In particular, we want to generate a sequence of vectors,

$$\left\{\left(F_{g,X}^{(k)}(t)\right)_{g,X}\right\}_{k\geq 0},$$

in the following following way: Set each $F_{g,X}^{(0)}(t) = 0$; and for each $k\geq 0$, compute $F_{g,X}^{(k+1)}(t)$ using the system in Corollary 2.8 after replacing each $F_{g,X}(t)$ with $F_{g,X}^{(k)}(t)$ in the right hand sides, and replacing each $F_{g,X}(t)$ with $F_{g,X}^{(k+1)}(t)$ in the left hand sides. Notice that $F_{g,X}^{(1)}(t) = \iota(g=1)$. The sequence, $(F_{g,X}^{(k)}(t))$, converges to a solution vector $(F_{g,X}^*(t))$ of our algebraic system. This solution vector is unique under the requirement that $F_{g,X}^*(0) = \iota(g=1)$. However, we cannot justify this convergence and uniqueness directly by

Proposition 2.17, since our system is not proper. Instead, we need to make a slight change of variables, $\bar{F}_{g,X}(t) := F_{g,X}(t) - \iota(g = 1)$. Rewriting the system in Corollary 2.8 in terms of $\bar{F}_{g,X}$, we now have a proper algebraic system. We obtain a fixed point iterative method with the new variables: Set each $\bar{F}^{(0)}_{g,X}(t) = 0$; and for each $k \geq 0$, compute $\bar{F}^{(k+1)}_{g,X}(t)$ using our modified version of the system in Corollary 2.8 after replacing each $\bar{F}_{g,X}(t)$ with $\bar{F}^{(k)}_{g,X}(t)$ in the right hand sides, and replacing each $\bar{F}_{g,X}(t)$ with $\bar{F}^{(k+1)}_{g,X}(t)$ in the left hand sides. The properness of our new algebraic system implies that our new system is a contraction in the space of power series with no constant terms, by Proposition 2.17. Hence, by the fixed point theorem, the system has a unique solution vector, $(\bar{F}^*_{g,X}(t))$, with $\bar{F}^*_{g,X}(0) = 0$; and the fixed point iterates converge to this solution. Formally, under the metric, d,

$$\lim_{k\to\infty} \bar{F}^{(k)}_{g,X}(t) = \bar{F}^*_{g,X}(t).$$

However, it is not difficult to verify that $\bar{F}^{(k)}_{g,X}(t) + \iota(g = 1) = F^{(k+1)}_{g,X}(t)$, which immediately implies that

$$\lim_{k\to\infty} F^{(k)}_{g,X}(t) = F^*_{g,X}(t),$$

justifying the convergence of the iterates based on our original variables. An implementation of this algorithm, with a minor truncation speedup, is provided in Appendix A.

It is noteworthy to mention that the change of variable trick discussed above can be generalized to any algebraic system $\vec{z} = \vec{P}(t, \vec{z})$, that is a constant shift of a proper system in the sense that that modified system, $\vec{z} = \vec{P}(t, \vec{z}) - \vec{P}(0, \vec{0})$, is proper. Although the discussion above guarantees convergence of the grammar, it provides no evidence of how many iterations are needed to approximate the cogrowth generating function to a prescribed accuracy. Hence, after a given number of iterations, k, we would like to know how many of the first terms of $F^{(k)}_{1,\emptyset}(t)$ matches with that of the true cogrowth generating function, $F^*_{1,\emptyset}(t)$. In general we do not know $F^*_{1,\emptyset}(t)$ precisely. However, we can use a satisfying polynomial to perform this test of accuracy. This is the topic of the next section.

2.9 Verification of Coefficients

After we compute our satisfying polynomial for the associated cogrowth generating function, we often want to verify the correctness of this polynomial in case errors are made during computation. During any given iteration of a iterative method described in the previous section, we are interested in knowing which of these terms matches with the precise, unknown, series expansion of $F(t)$. Algebraic elimination can be used to compute a single satisfying polynomial for $F(t)$. We discuss below, a method that can be used to test the number of lowest order terms of the series approximation that agrees with the series expansion of $F(t)$.

Assume we have a polynomial $P(t,z) \in \mathbb{C}[t,z]$, with $d = \deg_z P$. Let $p_i(t) := [z^i]P$. Let $F(t) = \sum_{n\geq 0} f_n t^n$ be the generating function for $\{f_n\} \subseteq \mathbb{C}$. For $m \in \mathbb{Z}_{\geq 0}$, write $F(t) = O(t^m)$ to denote that the valuation of $F(t)$ is at least m. Suppose $P(t, F(t)) \equiv 0$. Similarly, let $G(t)$ be the series for $\{g_n\}$, with $F(t) - G(t) = O(t^m)$. We see that

$$\begin{aligned} P(t, G(t)) &= P(t, G(t)) - P(t, F(t)) \\ &= (G(t) - F(t)) \sum_{i=1}^{d} p_i(t)\psi_i(t) \\ &= O(t^m), \end{aligned}$$

where $\psi_i(t) = \sum_{j=0}^{i-1} F^j(t) G^{i-1-j}(t)$. Note that $\psi_i(0) = \sum_{j=0}^{i-1} f_0^j g_0^{i-1-j}$. Furthermore, if $\sum_{i=1}^{d} p_i(0)\psi_i(0) \neq 0$, then

$$P(t, G(t)) = O(t^m) \iff F(t) - G(t) = O(t^m). \tag{2.14}$$

Taking $m \to \infty$ gives us $P(t, G(t)) = 0 \iff F(t) = G(t)$. Intuitively, this shows that the sequence $\{f_n\}$ that we desire, is uniquely determined under certain not too tight restrictions. For the purpose of analysing cogrowth sequences, we are primarily interested in the case where $f_0 = g_0 = 1$, and so $\psi_i(0) = i$. We have established the result below.

Proposition 2.18. *Let $\{f_n\}, \{g_n\} \subseteq \mathbb{C}$ be sequences with generating function $F(t), G(t)$ respectively. Let $P(t,z) = p_d(t)z^d + \ldots + p_1(t)z + p_0(t) \in \mathbb{C}[t,z]$. Assume that $f_0 = g_0 = 1$ and*

$$\sum_{i=1}^{d} i p_i(0) \neq 0. \tag{2.15}$$

Then for each $m \in \mathbb{Z}_{\geq 0}$, the following are equivalent:

1. *$F(t) - G(t) = O(t^m)$;*
2. *$P(t, F(t)) - P(t, G(t)) = O(t^m)$.*

Proposition 2.18 is useful in the following way: We want to generate the unknown sequence $\{f_n\}$ so that $F(t)$ is a root of $P(t, \cdot)$. We know that this sequence satisfies some combinatorial system. We run an iterative algorithm that generates $\{g_n\}$ as an approximation to $\{f_n\}$. We wish to test the accuracy of this approximation. If the hypothesis of this theorem holds true, and computing the series expansion of $P(t, G(t))$ gives the expression $a_m t^m + a_{m+1} t^{m+1} + \ldots$, with $a_m \neq 0$. Then we can conclude that the first m terms of the approximation are correct, and the $m+1$-th term is incorrect. Usually, $G(t)$ is a polynomial, so such a series expansion is not difficult to compute. Notice that the hypothesis of Proposition 2.18 is independent of $G(t)$ apart from g_0, so any sequence $\{g_n\}$ can be tested for accuracy in this way, provided that $g_0 = 1$. We now give an example:

Example 2.19 ($\mathbb{Z}_2^2 * \mathbb{Z}_3$)**.** Consider the case where

$$G := \mathbb{Z}_2^2 * \mathbb{Z}_3 = \langle x_1 | x_1^2 = 1 \rangle * \langle x_2 | x_2^2 = 1 \rangle * \langle y | y^3 = 1 \rangle$$

with the inverse closed generating set $S = \{x_1, x_2, y, y^{-1}\}$. Using the `solve` and `Minpoly` commands in the Maple programming language, we deduce that a satisfying polynomial for the cogrowth generation function $F(t) := F_{G;S}(t)$ is

$$Q(t,z) := 2\,t - 2 - (t-1)^2\, z + \left(8\,t^3 - 12\,t^2 - 2\,t + 2\right) z^2 + (t-1)\,(3\,t+1)\,(4\,t-1)\, z^3.$$

Applying our iterative algorithm described in Section 2.8, we obtain

$$\begin{aligned}
&F_{1,\emptyset}^{(0)}(t) = 0;\\
&F_{1,\emptyset}^{(k)}(t) = 1,\ \ k = 1,2,3;\\
&F_{1,\emptyset}^{(4)}(t) = 1 + 4t^2;\\
&\qquad\quad \vdots\\
&F_{1,\emptyset}^{(9)}(t) = 1 + 4\,t^2 + 2\,t^3 + 28\,t^4 + 30\,t^5 + 200\,t^6 + 266\,t^7 + \ldots + 2239488\,t^{29} + 373248\,t^{30}.
\end{aligned}$$

However, we make the assertion that $F_{1,\emptyset}^{(9)}(t)$ is accurate only up to the degree 5 term: $[t^k]F_{1,\emptyset}^{(9)}(t) = [t^k]F_{1,\emptyset}^{*}(t)$ for $k = 0,1,2,3,4,5$; but $[t^6]F_{1,\emptyset}^{(9)}(t) \neq [t^6]F_{1,\emptyset}^{*}(t)$. We check this assertion by noting that $Q(t, F_{1,\emptyset}^{(9)}(t)) = -204t^6 + O(t^7)$, is a series of valuation 6, so Proposition 2.18 implies our assertion. The few 14 terms of the cogrowth sequence of G with respect to S is precisely

$$1, 0, 4, 2, 28, 30, 234, 378, 2172, 4538, 21674, 53614, 227922, 631046, 2491374.$$

These 14 terms can be identified after 24 iterations of our fixed point algorithm. ⋄

Notice that Example 2.19 involves an inversely closed generating set. Nevertheless, in Chapter 3, we discuss general free products of cyclic groups with respect to minimal generating sets.

2.10 Finite Groups and Representation Theory

Finite groups have rational cogrowth generating functions, for which the degree of the numerator and denominator can be effectively bounded by the degrees of their irreducible representations. These bounds can be shown using the Cayley-Hamilton Theorem. We first state and prove this result, and then demonstrate the result on the cyclic and dihedral groups.

Lemma 2.20 (Bell, U. of Waterloo [3])**.** *Let H be a finite group with degrees of irreducible representations given by $n_1, \ldots, n_d$, with T as a generating set. Let $\alpha := \sum_{s \in T} s \in \mathbb{C}[H]$, and $A(t) := \sum_{n \geq 0} \phi(\alpha^n) t^n$. Then $A(t)$ is the power series expansion of a rational function $P(t)/Q(t)$ where $P, Q \in \mathbb{Z}[t]$ are polynomials with $Q(0) = 1$ and*

$$(\deg P) + 1, \deg Q \leq n_1 + \cdots + n_d \leq |H|.$$

In particular, if $\deg Q = |H|$ or $\deg P = |H| - 1$, then H is abelian.

Proof. We make use of facts from representation theory and construct a map from our group ring into a direct product of matrix rings. Let $M_k(F)$ denote the ring of $k \times k$ matrices over a given field F. Let $\bar{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$. We have, as a consequence of Wedderburn's Theorem [7, Section 18.2, Theorem 10], an isomorphism

$$\Psi : \overline{\mathbb{Q}}[H] \to M_{n_1}(\overline{\mathbb{Q}}) \times \cdots \times M_{n_d}(\overline{\mathbb{Q}}).$$

Then $\Psi(\alpha)$ is a d-tuple of matrices $(Y_1, \ldots, Y_d)$ where each $Y_i \in M_{n_i}(\overline{\mathbb{Q}})$. Observe that Ψ induces a $\overline{\mathbb{Q}}$-algebra isomorphism between the power series rings $\overline{\mathbb{Q}}[H][[t]]$ and

$$\left(M_{n_1}(\overline{\mathbb{Q}}) \times \cdots \times M_{n_d}(\overline{\mathbb{Q}})\right)[[t]]$$

that sends the series, $\sum_{n \geq 0} \alpha^n t^n$ to

$$\sum_{n \geq 0} (Y_1^n, \ldots, Y_d^n) t^n. \tag{2.16}$$

By the Cayley-Hamilton theorem, the series, (2.16), has coefficients which satisfy a linear recurrence of order at most $n_1 + \cdots + n_d$. Thus, $\sum_{n \geq 0} \alpha^n t^n$ is the Maclaurin series expansion in t of $P(t)/Q(t)$ with $P, Q \in \overline{\mathbb{Q}}[t]$ coprime, $Q(0) \neq 0$, $\deg(Q) \leq \sum n_i$, and $\deg(P) \leq \sum n_i - 1$. By rescaling, we may assume that $Q(0) = 1$. Since $A(t)$ has integer coefficients, P/Q must be invariant under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ and so since $Q(0) = 1$, we see that P and Q have rational coefficients. Now notice that $Q(t)A(t) = P(t)$. We can show[5] that the roots of $Q(t^{-1})$ must be algebraic integers and so $Q(t)$ is an integer polynomial and we can then have P is an integer polynomial, since $P = AQ$ and A and Q have integer coefficients.

Finally, standard representation theory implies that $|H| = \sum_{i=1}^{d} n_i^2$. Hence, if $\deg Q = |H|$ or $\deg P = |H| - 1$, then $n_1 = n_1^2 = 1$ for each $1 \leq i \leq n$, which is an equivalent condition [7] for H being abelian. □

[5] This property can be shown using the series generated by the adjacency matrix of the related Cayley graph, We leave the reader to fill in the details. See [8].

Notice that if $G = \mathbb{Z}_n$ is a finite cyclic group with a generating set S, then Lemma 2.20 implies that the cogrowth generating function, $F_{G;S}(t)$, is the series expansion of a rational function $p(t)/q(t)$, where $p, q \in \mathbb{Z}[t]$, with $\deg p \leq n - 1$ and $\deg q \leq n$. However, as seen in Example 2.1, $F_{G;S}(t) = \frac{1}{1-t^n}$. Thus, in the case, our denominator achieves the bound in Lemma 2.20 with equality, but our numerator is constant. We now exhibit the example of dihedral groups.

Example 2.21 (Degree bounds for finite dihedral groups)**.** Consider the dihedral group $G = D_m$, with the generating set $S = r, f$, as described in Section 2.1. In this case, the sum, r, of the degrees of the inequivalent irreducible representations of G is $m + 2$ if m is even; and $m + 1$ if m is odd. Lemma 2.20 tells us that $F_{G;S}(t) = p(t)/q(t)$, where $\deg p \leq r - 1$, and $\deg q \leq r$. However, Corollary 2.4 deduces much tighter restrictions: $\deg p = \deg q \leq \frac{r}{2}$.

Although Corollary 2.4 provides tighter bounds than Lemma 2.20, Corollary 2.4 only applies to a specific class of finite groups and generating sets, whereas Lemma 2.20 applies to any arbitrary finite group and generating set. Nevertheless, the reader should note that the bounds given in Lemma 2.20 are not necessarily tighter, and that specific cases may deduce far tighter bounds.

To end this chapter, we briefly elaborate on the case where G is a free product of finitely many finite groups. Notice that such groups are finitely generated. Unlike for finite groups, the associated cogrowth generating function for G is not necessarily rational, and explicit forms are often difficult to obtain. Instead, we work with their minimal polynomials. The primary goal of the next two chapters is to deduce degree bounds on the minimal polynomials for cogrowth generating functions of these free products.

Chapter 3

New Bounds on Free Products of Cyclic Groups

Minimal polynomials of the cogrowth sequence gives insight to complexity of the cogrowth generating function. These minimal polynomials are difficult to compute in general, as it is difficult to verify minimality. Thus, we instead, seek upper bounds on degrees and coefficients of these minimal polynomials. The satisfying polynomials discussed in this chapter may not be minimal, although most of them are believed[1] to be minimal. Instead, we use such polynomials to obtain upper bounds for the degrees of their minimal polynomials. In this chapter, we study the case where our group is a free product of finite cyclic groups with respect to minimal generating set. We adopt the notation used in Theorem 2.13 in this thesis. In particular, we take, as before,

$$G := \coprod_{i=1}^{r} \coprod_{j=1}^{m_i} \langle x_{ij} | x_{ij}^{n_i} = 1 \rangle = \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2} * \ldots * \mathbb{Z}_{n_r}^{*m_r},$$

where r is the number of distinct cyclic groups appearing in the free product; and we take our generating set to be $S = \{x_{ij} : 1 \leq i \leq r, 1 \leq j \leq n_i\}$.

We also adopt notation for Theorem 2.13 and Algorithm 1. Let $\vec{P}$ and P_i for $1 = 1, 2, \ldots, r+1$, be as given in Theorem 2.13. Let $\vec{P}^{(k)}$and $P_i^{(k)}$ for $1 = 1, 2, \ldots, r+1$ and $k = 0, 1, \ldots r$, be as given in Algorithm 1. We write $\overline{\text{Res}}$ as $\overline{\text{Res}}_{\mathbb{Z}}$ for short.

The case, $r = 1$, where the free factors are identical, has been solved by Bell and Mishna [4, Example 4.1]. An explicit form of a satisfying polynomial is known in this case. We first revisit this example below as a starting point.

[1] These polynomials are computed using the `eliminate` function in the Maple programming language.

σ	$\operatorname{sgn}\sigma$	$M[\sigma]$
(1)	1	$tz(z+m-1)^n$
$(1\ 2)$	-1	$mtz(z+m-1)^{n-1}$
$(1\ n{+}1\ n\ n{-}1\ \ldots\ 2)$	$(-1)^n$	$(-1)^{n+1}m^nt^{n+1}z^{n+1}$

Table 3.1: The permutations in Example 3.1 where $M[\sigma] \neq 0$.

Example 3.1. Let $G = \mathbb{Z}_n^{*m} = *_{j=1}^m \langle x_j | x_j^n = 1\rangle$ with $m, n \geq 2$ and generating set $S = \{x_1, x_2, \ldots, x_m\}$, for which

$$P_1^{(0)} = P_1 = tzz_1^n - z_1^{n-1} - tz$$

and

$$P_2^{(0)} = P_2 = z - mtzz_1 + m - 1.$$

Consider the Sylvester matrix, $M := \operatorname{Syl}(P_1, P_2, z_1) = (M_{ij})_{i,j=1}^{n+1}$, where the entries are given by

$$M_{ij} = \begin{cases} tz, & i = j = 1 \\ -1, & i = 1, j = 2 \\ -tz, & i = 1, j = n+1 \\ -mtz, & j = i-1 \\ z+m-1, & i = j > 1 \\ 0, & \text{otherwise.} \end{cases} \tag{3.1}$$

For each $\sigma \in \operatorname{Sym}(n+1)$, we have that $M[\sigma] \neq 0$ if and only if

$$\sigma \in \{(1), (1\ 2), (1\ n+1\ n\ n-1 \ldots\ 2)\},$$

as expressed in standard disjoint cycle notation. Table 3.1 summarizes the values of $M[\sigma]$ for these three values of σ. Using the permutation formula for determinant, we deduce that $\det M = tz\left((z-1)(z+m-1)^{n-1} - m^nt^nz^n\right)$, so $[tz](\det M) = -m+1 \neq 0$. Consequently,

$$P_1^{(1)}(t, z) = (tz)^{-1} \det M = (z-1)(z+m-1)^{n-1} - m^nt^nz^n \tag{3.2}$$

is a satisfying polynomial for the cogrowth generating function, $F_{G;S}(t)$. This result is consistent with the result obtained in Bell and Mishna [4]. ⋄

For the remainder of this chapter, we primarily focus on the case of two distinct cyclic factors, for which the general satisfying polynomial is not determined explicitly, but tight

$\sigma(1)$	σ	$\operatorname{sgn}\sigma$	$M[\sigma]$
1	Id	1	$tz(z - m_1tzz_1 + m_1 + m_2 - 1)^{n_2}$
2	$(1\ 2)$	-1	$m_2tz(z - m_1tzz_1 + m_1 + m_2 - 1)^{n_2-1}$
$n_2 + 1$	$(1\ n_2{+}1\ n_2\ n_2{-}1\ \dots\ 2)$	$(-1)^{n_2}$	$(-1)^{n_2+1}m_2^{n_2}t^{n_2+1}z^{n_2+1}$

Table 3.2: The permutations where $M[\sigma] \neq 0$

upper bounds on their degrees are known. For cases of three or more distinct factors, we develop degree bounds using classic properties of resultant.

3.1 Case of Two Distinct Cyclic Factors

We now derive bounds for case where $r = 2$, that is $G := \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2}$. The computation is this case is significantly more difficult than the $r = 1$ case presented in Example 3.1. The reason for this increase in difficulty is that we require an additional iteration, and after each iteration, the complexity of the resultants increase. However, the first step can be carried out in a manner similar to that in the case of identical free factors.

In this case, the three polynomials given in (2.6) in Theorem 2.13 are

$$\begin{aligned} P_1 &= tzz_1^{n_1} - z_1^{n_1-1} - tz \\ P_2 &= tzz_1^{n_1} - z_1^{n_1-1} - tz \\ P_3 &= z - m_1tzz_1 - m_2tzz_2 + m_1 + m_2 - 1. \end{aligned}$$

Let $M = \mathrm{Syl}(P_2, P_3, z_2) = (M_{ij})$, which is an $(n_2 + 1) \times (n_2 + 1)$ matrix. The entries of M are given by

$$M_{ij} = \begin{cases} tz, & i = j = 1 \\ -1, & i = 1, j = 2 \\ -tz, & i = 1, j = n_2 + 1 \\ -m_2tz, & j = i - 1 \\ z - m_1tzz_1 + m_1 + m_2 - 1, & i = j > 1 \\ 0, & \text{otherwise.} \end{cases} \tag{3.3}$$

Similar to the observation in Example 3.1, for $\sigma \in \mathrm{Sym}(n_2 + 1)$, we have that $M[\sigma] \neq 0$ if and only if

$$\sigma \in \{(1), (1\ 2), (1\ n_2 + 1\ n_2\ n_2 - 1 \dots\ 2)\}.$$

Table 3.2 indicates the value of $M[\sigma]$ in each of the 3 possible cases.

By a straightforward computation, and by definition of resultant,

$\operatorname{Res}(P_2, P_3, z_2) = \det M = tz[(z-m_1tzz_1+m_1-1)(z-m_1tzz_1+m_1+m_2-1)^{n_2-1}-(m_2tz)^{n_2}]$.

Expanding this resultant, we deduce that $[z^1]\operatorname{Res}(P_2, P_3, z_2) = (m_1-1)(m_1+m_2-1)^{n_2-1}t$. Since $m_1, m_2 \geq 1$, this coefficient is 0 if and only if $m_1 = 1$, in which case we have $[z^2]\operatorname{Res}(P_2, P_3, z_2) = m_2^{n_2}t(1-tz_1) \neq 0$. We therefore conclude that

$$\operatorname{val}\operatorname{Res}(P_2, P_3, z_2) = 1 + \iota(m_1 = 1) \tag{3.4}$$

where ι denotes the characteristic function that was defined in Section 2.3. Recall from Algorithm 1 that $P_2^{(1)} = \overline{\operatorname{Res}}(P_2, P_3, z_2)$. Thus,

$$P_2^{(1)} = \begin{cases} (z-m_1tzz_1+m_1-1)(z-m_1tzz_1+m-1)^{n_2-1}-(m_2tz)^{n_2}, & m_1 > 1 \\ (1-tz_1)(z-tzz_1+m_2)^{n_2-1}-m_2^{n_2}t^{n_2}z^{n_2-1}, & m_1 = 1 \end{cases} \tag{3.5}$$

where $m = m_1 + m_2$.

Let us first assume $m_1 = 1$. After the first iteration of Algorithm 1, we have eliminated z_2, so the system has been reduced to two equations given by $P_i^{(1)} = 0$ for $i = 1, 2$; where

$$\begin{aligned} P_1^{(1)} &= tzz_1^{n_1} - z_1^{n_1-1} - tz \\ P_2^{(1)} &= (1-tz_1)(z-tzz_1+m_2)^{n_2-1} - m_2^{n_2}t^{n_2}z^{n_2-1} \end{aligned} \tag{3.6}$$

are polynomials in z, z_1, with coefficients in $\mathbb{Z}[t]$. The degree of these polynomials are as follows:

$$\deg_z P_1^{(1)} = 1,\ \deg_z P_2^{(1)} = n_2 - 1,$$
$$\deg_z P_2^{(1)} = n_1,\ \deg_z P_2^{(1)} = n_2.$$

Using Equation (2.11), we obtain the inequality

$$\deg_z \operatorname{Res}(P_1^{(1)}, P_2^{(1)}, z_1) \leq n_2 + n_1(n_2-1). \tag{3.7}$$

For notional convenience, let $\gamma_k(t,z) := [z_1^k]P_2^{(1)}$ so that $P_2^{(1)} = \sum_{k=0}^{n_2}\gamma_k(t,z)z_1^k$. Then Eqn 3.6 implies

$$\gamma_0(t,0) = m_2^{n_2-1},\ \gamma_{n_2} = (-1)^{n_2-1}t^{n_2}z^{n_2-1}. \tag{3.8}$$

Furthermore, for $1 \leq k \leq n_2 - 1$, Eqn (3.6) implies

$$\gamma_k = \binom{n_2-1}{k}(-tz)^k(z+m_2)^{n_2-1-k} + t\binom{n_2-1}{k-1}(-tz)^{k-1}(z+m_2)^{n_2-1-k}, \tag{3.9}$$

with its lowest degree term with respect to z as $(-1)^{k-1}t^k z^{k-1}\binom{n_2-1}{k-1}m_2^{n_2-k}$. Thus, Equations (3.8) and (3.9) together imply that $\operatorname{val}_z \gamma_k = \max\{0, k-1\}$ for $k \leq n_2$.

Now assume $m_1 > 1$. With an argument similar to the $m_1 = 1$ case above, we get

$$\deg_z P_1^{(1)} = 1,\ \deg_z P_1^{(2)} = n_2,$$
$$\deg_z P_2^{(1)} = n_1,\ \deg_z P_2^{(2)} = n_2.$$

As a result,

$$\deg_z \operatorname{Res}(P_1^{(1)}, P_2^{(1)}, z_1) \leq n_2(n_1+1) - n_2 + 1 = n_1 n_2 + 1. \tag{3.10}$$

The resultant in Equation (3.10) is a satisfying polynomial for the corresponding cogrowth sequence and it has positive valuation with respect to z. Hence, we can adopt a stronger bound for the corresponding reduced resultant, $P_1^{(2)}$, the satisfying polynomial obtained in the final iteration of Algorithm 1. We give the specifics in the proposition below regarding this valuation.

Proposition 3.2. *Using the standard order in $\bar{\mathbb{R}} := \mathbb{R} \cup \{\pm\infty\}$, for any $m_1, m_2 \geq 1$,*

$$\min_{\sigma \in \operatorname{Sym}(n_1+n_2)} \operatorname{val}_z \operatorname{Syl}(P_1^{(1)}, P_2^{(1)}, z_1)[\sigma] = n_2 - 1. \tag{3.11}$$

Proof. Let $M = \operatorname{Syl}(P_1^{(1)}, P_2^{(1)}, z_1)$. Let M_{ij} denote its ij-th entry indexed from 1. It is sufficient to consider only the permutations σ for which $M[\sigma] \neq 0$. As before, write $P_2^{(1)} = \sum_{k=0}^{n_2} \gamma_k(t,z) z_1^k$. If none of the $M_{i\sigma(i)}$ are -1, then we have that $M[\sigma]$ is a multiple of $(tz)^{n_2}$, so $\operatorname{val}_z M[\sigma] \geq n_2$. Otherwise, let i^* be the smallest index so that $M_{i^*\sigma(i^*)} = -1$. Then $i^* \leq n_2$, $\sigma(i^*) = i^* + 1$ and for $i < i^*$, $M_{i\sigma(i)} \in \{\pm tz\}$. Also, there is some index $\bar{i} \leq i^*$ such that $\sigma^{-1}(\bar{i}) > i^*$. Thus, $M_{\sigma^{-1}(\bar{i}),\bar{i}} = \gamma_k$ for some $k > n_2 - \bar{i}$. We have that

$$\operatorname{val}_z M[\sigma] \geq \operatorname{val}_z((tz)^{i^*-1}\gamma_k(t,z)) \geq (i^*-1) + (n_2 - \bar{i}) \geq n_2 - 1.$$

Finally, if $\sigma(i) = i+1$ for each $i \neq n_2 + 1$, then we have that

$$M[\sigma] = (-1)^{n_2}\gamma_{n_2}\gamma_0^{n_1-1}$$

so $\operatorname{val}_z M[\sigma] = n_2 - 1$ and the result follows. □

Our discussion throughout this section proves the theorem below.

Theorem 3.3. *Let $F(t)$ be the cogrowth generating function for*

$$G = \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2} = \coprod_{i=1}^{2}\coprod_{j=1}^{m_i} \langle x_{ij} | x_{ij}^{n_i} = 1 \rangle$$

	$m_2 = 1$	$m_2 > 1$
$m_1 = 1$	$1 + n_1 n_2 - \max\{n_1, n_2\}$	$1 + n_1(n_2 - 1)$
$m_1 > 1$	$1 + n_2(n_1 - 1)$	$1 + n_1 n_2$

Table 3.3: Upper Bounds for $\deg_z Q$ for $r = 2$ based on the values of m_1, m_2.

with respect to the minimal generating set $S = \{x_{1j} : 1 \leq j \leq m_1\} \cup \{x_{2j} : 1 \leq j \leq m_2\}$*. Then there is a satisfying polynomial* $Q \in \mathbb{Z}[t, z] \setminus \{0\}$ *for the cogrowth series* $F_{G;S}(t)$ *such that, under the appropriate conditions of* m_1, m_2*, it holds that* $\deg_z Q$ *is at most the upper bound given in Table 3.3.*

The upper bounds in Theorem 3.3 are not necessarily tight. Computations suggest that these bounds can be further improved. Conjectures 3.4 and 3.5 are the improvements.

Conjecture 3.4. *The valuation of the resultants of the polynomials yielded after the first iteration satisfy the inequality*

$$\operatorname{val}_z \operatorname{Res}(P_1^{(1)}, P_2^{(1)}, z_1) \geq n_2.$$

That is, if we take the products, $\operatorname{sgn}(\sigma) \operatorname{Syl}(P_1^{(1)}, P_2^{(1)}, z_1)[\sigma]$ *with valuation* $n_2 - 1$*, and add up their lowest order terms, they all cancel out to zero.*

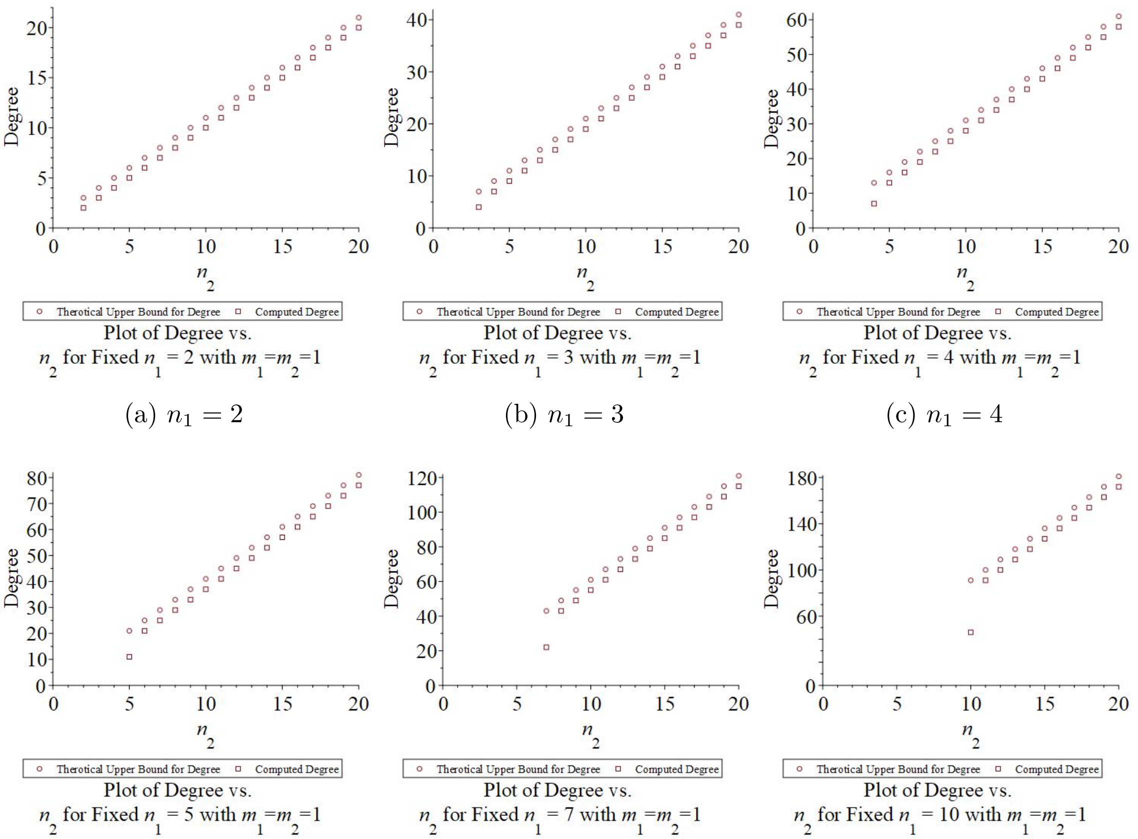
Notice that if Conjecture 3.4 is correct, then all the entries in Table 3.3 can be decreased precisely by one. Further improvements may be possible in the case where $m_1 = m_2 = 1$, which we specify in a second conjecture below.

Conjecture 3.5. *Let* $G = \mathbb{Z}_{n_1} * \mathbb{Z}_{n_2} = \langle x_1 | x_1^{n_1} = 1\rangle * \langle x_2 | x_2^{n_2} = 1\rangle$ *with the minimal generating set* $S = \{x_1, x_2\}$*. Then the cogrowth series,* $F_{G;S}(t)$*, has a minimal polynomial,* $Q(t, z) \in \mathbb{Z}[t, z]$*, with degree (in* z*) satisfying the inequality,*

$$\deg_z Q \leq 1 + n_1 n_2 - \max\{n_1, n_2\} - \min\{n_1, n_2\} + 1 = 2 + n_1 n_2 - n_1 - n_2.$$

Notice that Conjecture 3.5 is true if $n_1 = n_2$, since in this case, Example 3.1 already yields n_1 as an upper bound. We now present some tables and plots to back up our conjectures.

In Figures 3.1 and 3.2, it is evident that our theoretical bound and the degree of the actual satisfying polynomials differ by a constant when $n_1 < n_2$. By symmetry, this principle is true for $n_1 \neq n_2$. If $m_1 = m_2 = 1$, this constant appears to increase with the value of n_1. If $m_1, m_2 > 1$, this constant appears to be independent with n_1. In Table B.1 below, the computed degrees, excluding the case $n_1 = n_2$, satisfy Conjecture 3.5 with equality. In Table B.2, the computed degrees for $n_1 \neq n_2$ are each exactly one less than the corresponding



(a) $n_1 = 2$

(b) $n_1 = 3$

(c) $n_1 = 4$

(d) $n_1 = 5$

(e) $n_1 = 7$

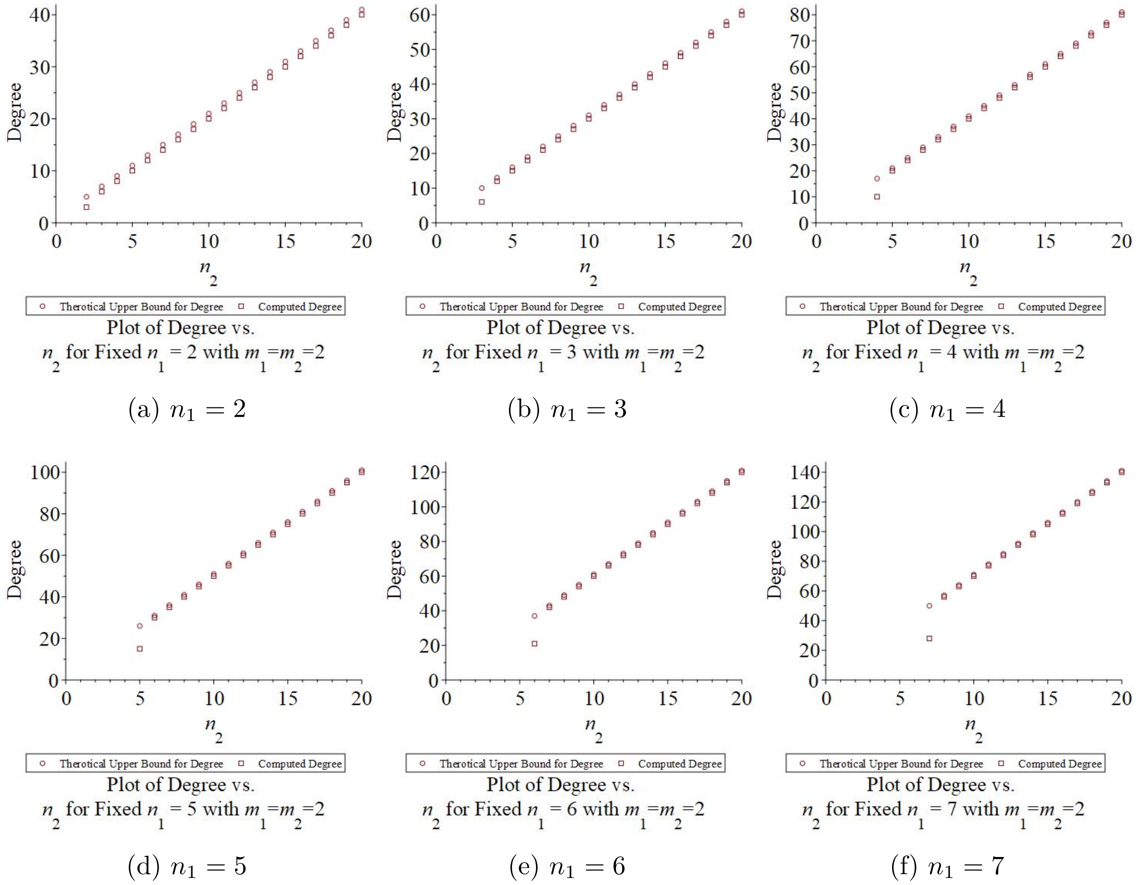
(f) $n_1 = 10$

Figure 3.1: Plots of actual degrees and upper bounds vs. $n_2 = n_1, n_1 + 1, \ldots, 20$ for various fixed n_1, in the case $m_1 = m_2 = 1$.

theoretical upper bounds obtained based on Table 3.3. Hence, these computations support Conjecture 3.4.

Two tables, Table B.1 and Table B.2, provide in Appendix B, provide the computed degrees and the theoretical upper bounds for various n_1, n_2. We remark that the values shown in the two tables of computed degrees does not necessarily match with the degree of $P_1^{(2)}$, computed from Algorithm 1. However, $\deg_z P_1^{(2)}$ is necessarily at least as large as the corresponding degree value shown in the table. This is evident in the case that $n_1 = n_2$, for which the variables z_1, z_2 are identical in our initial system of equations, with $P_1 = P_2$. By classic properties of resultants [8], the polynomial, $P_1^{(2)}$, must have a factor that is a perfect square of a polynomial in $\mathbb{Z}[t, z]$ that is not a monomial. To help the reader visualize this property, we give an example below.

[2] In order to save computation time and memory, the experiment in Maple was done by setting $m_1 = m_2 = 2$ rather than keeping them symbolic.



(a) $n_1 = 2$ (b) $n_1 = 3$ (c) $n_1 = 4$

(d) $n_1 = 5$ (e) $n_1 = 6$ (f) $n_1 = 7$

Figure 3.2: Plots of actual degrees and upper bounds vs. $n_2 = n_1, n_1 + 1, \ldots, 20$ for various fixed n_1, in the case[2] $m_1, m_2 > 1$.

Example 3.6 ($n_1 = n_2 = 3$)**.** Consider the case of $G = \mathbb{Z}_3 * \mathbb{Z}_3$. If we run algorithm 1 with $r = 2$ and $m_1 = m_2 = 2$, we obtain

$$P_1^{(2)} = (8t^3z^3 - z^3 - z^2 + z + 1)(t^3z + z + 1)^2,$$

a satisfying polynomial for the cogrowth generating function, with degree 5 in z. Using a built-in algebraic elimination function in the Maple programming language starting with the system in Theorem 2.13 and $r = 2$, we obtain the satisfying polynomial,

$$Q := (8t^3z^3 - z^3 - z^2 + z + 1)(t^3z + z + 1),$$

which is of degree 4, as displayed in the cell of Table B.1 with a cyan background. We can make a further improvement: Set $r = 1$ and following Example 3.1 with $m = 1$. Equation (3.2) gives us

$$P_1^{(1)} = -(8t^3z^3 - z^3 - z^2 + z + 1),$$

a satisfying polynomial of degree 3.

We further remark that the computed degrees given in the two tables above are not minimal for $n_1 = n_2$, since the degree values exceed the bound obtained in Example 3.1.

If $n_1 \neq n_2$, then the above computation appear to suggest that $P_1^{(2)}$ achieves the computed degree. However, we have not proven whether or not this statement is true in general.

3.2 Free Products of at Least Three Distinct Factors

In this section, we discuss the case where our group, G, have at least 3 distinct cyclic factors. The steps carried out in previous sections apply similarly here during the first two iterations of Algorithm 1. As mentioned in the beginning of this chapter, we continue to adopt the notation for polynomials and vectors of polynomials as given in Theorem 2.13 and Algorithm 1. We make an important observation that after any given iteration, only the last polynomial changes, and the other polynomials remain the same as before. Specifically, during the k-th iteration, we eliminate the variable, z_{r+1-k}. As a result, we have, for $i = 1, 2, \ldots r-k$, that

$$P_i^{(k)} = P_i^{(k-1)} = P_i^{(k-2)} = \ldots = P_i^{(1)} = P_i^{(0)}.$$

This chain of equalities hold if we view these polynomials with respect to the natural inclusion of polynomial rings:

$$\mathbb{Z}[t, z, z_1, \ldots, z_{r-k}] \subseteq \mathbb{Z}[t, z, z_1, \ldots, z_{r-k+1}] \subseteq \ldots \subseteq \mathbb{Z}[t, z, z_1, \ldots, z_{r-1}] \subseteq \mathbb{Z}[t, z, z_1, z_2, \ldots, z_r].$$

Such a observation holds since we defined our reduced resultant piecewise according to (2.12) in Definition 2.14. If we instead defined $\overline{\text{Res}}$ naively only to avoid extra monomial factors, then Algorithm 1 would introduce redundant exponents after each iteration, unnecessarily adding to our degree count. The last polynomial that appears in the system after the k-th iteration is $P_{r+1-k}^{(k)}$, which is different from $P_{r+1-k}^{(k-1)}$ that appears in the previous iteration. Also, if $k < r$ so that we are not at the final iteration, then the degree of $P_{r+1-k}^{(k)}$, with respect to any variable depends on k and $n_r, n_{r-1}, \ldots, n_{r+1-k}$ in the same way regardless of the value of r. We now formalize this last property in a proposition.

Proposition 3.7. *Let $k \in \mathbb{Z}_{\geq 0}$. Then for integers $r > k$, $0 < j \leq r-k$, and $d \geq 0$, there is a unique function*[3] *$f_{k;v;d;j} : \mathbb{Z}_{\geq 2}^k \to \mathbb{Z}_{\geq 0}$ such that*

$$\deg_v \left([z_j^d] P_{r-k+1}^{(k)} \right) = f_{k;v;d;j}(n_r, n_{r-1}, \ldots, n_{r-k+1}) \tag{3.12}$$

in the sense that this degree is independent of $n_1, \ldots, n_{r-k}$. Furthermore, the function, $f_{k;v;d;j}$, is independent of r.

[3] We use the convention that $\mathbb{Z}_{\geq 2}^0 = \{()\}$ is the singleton set consisting of the empty sequence.

Proof. We proceed with induction on k. If $k = 0$, we obtain the original polynomial P_{r+1} and the claim is true since the degrees given in (3.12) are either 0 or 1. Suppose $k > 0$ and the claim is true with $k - 1$ in place of k. Let $i = r - k + 1$ and consider the resultant, $R_k := \operatorname{Res}(P_i^{(k-1)}, P_{i+1}^{(k-1)}, z_i)$. It can be verified that $R_k = \eta_k(m_1 z_1 + m_2 z_2 + \ldots + m_{i-1} z_{i-1})$ for some $\eta_k(s) \in (\mathbb{Z}[t, z])[s]$. Observe that $P_i^{(k-1)} = P_i$ depends only on n_i, z_i, t, z, and in particular, is independent of r. By the induction hypothesis, for every $d \in \mathbb{Z}_{\geq 0}$, the polynomial, $[z_i^d]P_{i+1}^{(k-1)}$, has degrees with respect to every variable that are independent of r. Although R_k is not completely determined by $n_r, n_{r-1}, \ldots, n_i$ without knowledge of r, the polynomial, $\eta_k(s)$, is completely determined without knowledge of r. Assume $v \in \{t, z\}$. For each $0 < j < i$, and $d \geq 0$, the polynomial, $[z_j^d]R_k$ is a $\mathbb{Z}[z_1, z_2, \ldots, z_{j-1}, z_{j+1}, \ldots, z_{i-1}]$-linear combination of the coefficients of $\eta_k(s)$. Thus, $\deg_v[z_j^d]R_k$ can be expressed as a function of $n_r, n_{r-1}, \ldots, n_i$ without explicit knowledge of r. We now consider the case of $v \notin \{t, z\}$. Without loss of generality, we can assume $v = z_1$ and $j = 2$. It is evident that $\deg_v[z_j^d]R_k = \deg_v[z_2^d]\eta_k(m_1 z_1 + m_2 z_2)$ can be expressed in terms of a polynomial independent of r. We have shown that all the degree, $\deg_v[z_j^d]R_k$, can be expressed as a function of $n_r, n_{r-1}, \ldots, n_i$ without explicit knowledge of r. In remains to show that the same is true for all the valuations of $[z_j^d]R_k$. The ring, $\mathbb{Z}[t, z, z_1, z_2, \ldots, z_{i-1}]$, can be interpreted as a $\mathbb{Z}[t, z]$-module, for which the set,

$$\left\{ \left(\sum_{j \in A} m_j z_j \right)^d : d \in \mathbb{Z}_{\geq 0} \right\},$$

for any nonempty subset $A \subseteq \{1, 2, \ldots, i-1\}$, forms a basis for a $\mathbb{Z}[t, z]$-submodule. If $v = z_1$ and $j = 2$, then $\operatorname{val}_v[z_2^d]R_k = \operatorname{val}_v[z_2^d]\eta_k(m_1 z_1 + m_2 z_2)$ is completely determined without knowing r. If $v \in \{t, z\}$, then $\operatorname{val}_v R_k = \operatorname{val}_v \eta_k$ is independent of r. Hence, the claim in the proposition is now shown for our choice of k, completing our induction step. □

An immediate consequence of Proposition 3.7 is that a similar statement holds upon dropping the coefficient of z_j^d of (3.12). Since $v \neq z_j$, we can write

$$\deg_v \left(P_{r-k+1}^{(k)} \right) = f_{k;v}(n_r, n_{r-1}, \ldots, n_{r-k+1})$$

where $f_{k;v} := \max_{d \geq 0} f_{k;v;d;j}$. To help the reader make sense of the statement in Proposition 3.7, we provide a brief example: Suppose $r = 7, k = 3$, and $\deg_v P_5^{(3)} = n_7^3 + n_6^3 + n_5^3$. In this hypothetical scenario, Proposition 3.7 implies that increasing r to 1000 gives us that $\deg_v P_{998}^{(3)} = n_{1000}^3 + n_{999}^3 + n_{998}^3$. That is, if we shift all the subscripts by the same index and keep all else the same, we preserve the validity of the equation.

The reader must be cautious here and observe that Proposition 3.7 applies only up to the second to last iteration of Algorithm 1. Indeed, after the final iteration, the only remaining variables are t and z, so it is senseless to extract those coefficients. However, if we skip the coefficient extraction, then a analogous statement can be formulated even after the final iteration. We give this formulation in the corollary below.

Corollary 3.8. *For each $r \geq 2$, consider the polynomial $P_1^{(r)}$ as generated by Algorithm 1 during the final iteration. Then for each variable $v \in \{t, z\}$, and for each $d \in \mathbb{Z}_{\geq 0}$, we have that*

$$\deg_v \left(P_1^{(r)}\right) = f_{(v,d);r}(n_r, n_{r-1}, \ldots, n_1) \tag{3.13}$$

for a unique function $f_{(v,d);r} : \mathbb{Z}_{\geq 2}^r \to \mathbb{Z}_{\geq 0}$. Furthermore, adopting the notation in Proposition 3.7, it follows that for $2 \leq k < r$ and $0 < j \leq r - k$, we have the following inequality:

$$f_{(v,d);k} \leq \max_{d \geq 0} f_{k;v;d;j}. \tag{3.14}$$

Proof. For each $r \geq 2$, define $R_r^* := \mathrm{Res}(P_1^{(r-1)}, P_2^{(r-1)}, z_1)$ according to the last iteration of Algorithm 1 given r distinct factors. Now, we fix r, and define, for $2 \leq k < r$, the resultant, R_k, as in the proof of Proposition 3.7. Notice that $R_k^* = \eta_k^*(0)$ and

$$R_k = \eta_k(m_1 z_1 + m_2 z_2 + \ldots + m_{r-k} z_{r-k}),$$

where $\eta_k^*(s), \eta_k(s) \in (\mathbb{Z}[t, z])[s]$ are nearly identical except of the fact that, in order to construct η_k^*, we need to take the expression for η_k, and substitute the parameters, $n_r, n_{r-1}, \ldots,$ n_{r-k+1}, with $n_k, n_{k-1}, \ldots, n_1$ respectively. We have seen from the proof of Proposition 3.7, that

$$\deg_v R_k = \max_{d \geq 0} \deg_v [z_j^d] R_k$$

and [4]

$$\mathrm{val}_v R_k = \min_{d \geq 0} \mathrm{val}_v [z_j^d] R_k$$

can both be computed from the coefficients of η_k as a function of $n_r, n_{r-1}, \ldots, n_{r-k+1}$ independent of r. In addition, by the argument made in the proof of Proposition 3.7 regarding submodule bases, we have

$$\deg_v R_k = \max_{d \geq 0} \deg_v([s^d]\eta_k) \text{ and } \mathrm{val}_v R_k = \min_{d \geq 0} \mathrm{val}_v([s^d]\eta_k). \tag{3.15}$$

Since $R_k^* = \eta_k^*(0)$, it follows that

$$\deg_v R_k^* = \deg_v([s^0]\eta_k^*) \text{ and } \mathrm{val}_v R_k^* = \mathrm{val}_v([s^0]\eta_k^*). \tag{3.16}$$

[4] Recall that we are using the convention: $\mathrm{val}_v\, 0 = +\infty$.

Consequently, by construction of η_k and η_k^*, the inequality, (3.14), follows immediately from equations (3.15) and (3.16). □

We also obtain degree bounds for the last polynomial obtained in the first and second iterations.

Corollary 3.9. *For $r \geq 1$, $\deg_t P_r^{(1)} = \deg_z P_r^{(1)} = n_r$.*
For $r \geq 2$, it holds that $\deg_z P_{r-1}^{(2)} \leq 1 + n_{r-1}n_r$.

Proof. A direct computation shows that $P_r^{(1)} = \gamma^{n_r} - m_r\gamma^{n_r-1} - (m_r tz)^{n_r}$, where

$$\gamma(t, z, z_1, z_2, \dots, z_{r-1}) = z - tz\sum_{j=1}^{r-1} m_j z_j + \sum_{j=1}^{r} m_j - 1.$$

The bound on $P_{r-1}^{(2)}$ is verified for $r = 2$ in Theorem 3.3. By Proposition 3.7 and Corollary 3.8, this bound must hold for any arbitrary $r \geq 2$. □

In order to establish upper bounds on the degree of minimal polynomials, we would like to use the symmetry of our system form Theorem 2.13 to our advantage. It is evident that, for any upper bound expressed in terms $n_1, n_2, \dots, n_r$, permuting these parameters in our expressions gives us another upper bound. For our convenience, we recall the definition of a symmetric function, and then define symmetric closures.

Definition 3.10. Let $D \subseteq \mathbb{Z}^m$ be a set and let $f : D \to \mathbb{R}$ be a real-valued[5] function. The set, D, is considered to be *symmetric* if each $(k_1, k_2, \dots, k_m) \in D$ and $\sigma \in \mathrm{Sym}(m)$, we have $(\sigma(k_1), \sigma(k_2), \dots, \sigma(k_m)) \in D$.
For a symmetric set D,

- the function, f, is considered to be *symmetric* if

  $$f(k_1, k_2, \dots, k_m) = f(\sigma(k_1), \sigma(k_2), \dots, \sigma(k_m))$$

  for each $\sigma \in \mathrm{Sym}(m)$; and

- we define the *minimum symmetric closure*, $\mathrm{minCl}(f)$, of f (which may or may not be symmetric), to be the map

  $$(k_1, k_2, \dots, k_m) \in D \mapsto \min_{\sigma \in \mathrm{Sym}(m)} f(\sigma(k_1), \sigma(k_2), \dots, \sigma(k_m)).$$

[5] In our setting, we only need to consider functions that map to non-negative integers, but we use $\mathbb{R}$ here as a generalization.

Similarly, the *maximum symmetric closure*, maxCl(f), of f is defined as

$$(k_1, k_2, \dots, k_m) \in D \mapsto \max_{\sigma \in \mathrm{Sym}(m)} f(\sigma(k_1), \sigma(k_2), \dots, \sigma(k_m)).$$

◇

Notice that minCl(f) and maxCl(f) are symmetric functions; and f is symmetric $\iff$ $f = \mathrm{minCl}(f) \iff f = \mathrm{maxCl}(f)$. In the previous section, we have obtained, from Table 3.3 of Theorem 3.3, symmetric upper bounds for the degrees of minimal polynomials. In the case where $r \geq 3$, Algorithm 1 requires at least three iterations before terminating with the satisfying polynomial. In this case, the resultant computations gets increasingly complicated after each iteration, making tight degree bounds difficult to establish. However, we can compute loose upper bounds using a classic property of resultants given in Equation (2.11). We give an example below with $r = 3$.

Example 3.11 ($r = 3$ case)**.** Consider the case where $G = \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2} * \mathbb{Z}_{n_3}^{*m_3}$ with our usual minimal generating set. Using the notation of polynomials given in Algorithm 1, we get, after the second iteration, that $P_1^{(2)} = P_1$, and $P_2^{(2)}$ is a polynomial with the properties: $\deg_z P_2^{(2)} \leq 1 + n_2 n_3$ by Theorem 3.3, and

$$\deg_{z_1} P_2^{(2)} \leq (\deg_{z_1} P_1^{(1)})(\deg_{z_2} P_2^{(1)}) + (\deg_{z_2} P_1^{(1)})(\deg_{z_1} P_2^{(1)}) = n_2 n_3$$

by the inequality in (2.11). After the third and final iteration, we obtain our satisfying polynomial, $P_f := P_1^{(3)}$ with

$$\deg_z P_f \leq (\deg_z P_1^{(2)})(\deg_{z_1} P_2^{(2)}) + (\deg_{z_1} P_1^{(2)})(\deg_z P_2^{(2)}) = n_1 + n_2 n_3(1 + n_1),$$

giving us an upper bound for a minimal polynomial of the associated cogrowth series that is not symmetric in n_1, n_2, n_3. Thus, a valid symmetric upper bound is

$$\mathrm{minCl}((n_1, n_2, n_3) \mapsto n_1 + n_2 n_3(1 + n_1)).$$

Since $n_1, n_2, n_3 \geq 2$, it can be shown, using straightforward algebra, that the minCl expression above can be simplified to

$$\max\{n_1, n_2, n_3\} + n_1 n_2 n_3 \left(1 + \frac{1}{\max\{n_1, n_2, n_3\}}\right).$$

◇

We can similarly obtain a naive upper bound with any number of distinct cyclic factors by repeatedly applying Equation (2.11). We now state and prove a major theorem below. By computing the upper bounds in each iteration of Algorithm 1, it is evident that Proposition

3.7 and Corollary 3.8 both apply. However, using these two results, we are able to give a more concise proof.

Theorem 3.12. *For $r \geq 3$, consider the group,*

$$G := \coprod_{i=1}^{r} \coprod_{j=1}^{m_i} \langle x_{ij} | x_{ij}^{n_i} = 1 \rangle = \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2} * \ldots * \mathbb{Z}_{n_r}^{*m_r},$$

with the generating set, $S := \{x_{ij} : 1 \leq i \leq r, 1 \leq j \leq n_i\}$, where each $n_i \geq 2$ and each $m_i \geq 1$. Let $P_i^{(k)}$, for $0 \leq k \leq r$ and $1 \leq i \leq r-k+1$, denote the polynomial generated after k iterations of Algorithm 1 with input as the system of equations, (2.6), given in Theorem 2.13. Then we have

$$\deg_z P_1^{(r)} \leq (n_1 n_2 \ldots n_r) \left(1 + \frac{1}{n_{r-1} n_r} + \sum_{k=1}^{r-2} \frac{1}{n_k} \right) < (n_1 n_2 \ldots n_r) \left(1 + \sum_{k=1}^{r} \frac{1}{n_k} \right), \quad (3.17)$$

and for $0 \leq k < r$, $1 \leq j \leq r-k$: $\deg_{z_j} P_{r-k+1}^{(k)} \leq n_{r-k+1} \ldots n_{r-1} n_r$.

Proof. We apply induction on r. If $r = 3$, the theorem is already deduced in Example 3.11. Let $r_0 > 3$ be a fixed integer and suppose the result is true for $r = r_0 - 1$. We show that the result holds for $r = r_0$. Suppose $0 \leq k < r$, $1 \leq j \leq r-k$. If $k = 0$, then $\deg_{z_j} P_{r-k+1}^{(k)} = 1$, so assume $k > 0$. Observe that

$$\begin{aligned} \deg_{z_j} P_{r-k+1}^{(k)} &\leq \deg_{z_j} P_{r-k+1}^{(k-1)} \deg_{z_{r-k+1}} P_{r-k+2}^{(k-1)} + \deg_{z_j} P_{r-k+2}^{(k-1)} \deg_{z_{r-k+1}} P_{r-k+1}^{(k-1)} \\ &\leq 0 \cdot (n_{r-k+2} \ldots n_{r-1} n_r) + (n_{r-k+2} \ldots n_{r-1} n_r) \cdot n_{r-k+1} \\ &= n_{r-k+1} \ldots n_{r-1} n_r, \end{aligned}$$

where the first inequality follows from Eqn 2.11, and the second inequality follows from the induction hypothesis and Corollary 3.8. Again, by the induction hypothesis and Corollary 3.8, it holds that $\deg_z P_2^{(r-1)} \leq (n_2 n_3 \ldots n_r) \left(1 + \frac{1}{n_{r-1} n_r} + \sum_{k=2}^{r-2} \frac{1}{n_k} \right)$. Hence,

$$\begin{aligned} \deg_z P_1^{(r)} &\leq \deg_z P_1^{(r-1)} \deg_{z_1} P_2^{(r-1)} + \deg_{z_1} P_1^{(r-1)} \deg_z P_2^{(r-1)} \\ &\leq 1 \cdot (n_2 n_3 \ldots n_r) + n_1 \cdot \deg_z P_2^{(r-1)} \\ &\leq (n_1 n_2 \ldots n_r) \left(1 + \frac{1}{n_{r-1} n_r} + \sum_{k=1}^{r-2} \frac{1}{n_k} \right), \end{aligned}$$

establishing the first inequality in (3.17). The second equality follows for the fact that $n_r, n_{r-1} \geq 2$. □

An interesting observation is that, if we fix the orders of all the distinct cyclic factors except one of them, then the degree bound given in Eqn (3.17) suggests that the degree of our minimal polynomial is bounded linearly by the one varying factor. Specifically, let

$\Delta(n_1, n_2, \ldots, n_r)$ denote the degree in z of any minimal polynomial, $Q(t,z) \in \mathbb{Z}[t,z]$, for our cogrowth series, $F_{G;S}(t)$, of which $Q(t, F_{G;S}(t)) = 0$. Then for each $i = 1, 2, \ldots, r$, we deduce that

$$\Delta(n_1, n_2, \ldots, n_r) \leq \beta_0(n_1, n_2, \ldots, n_{i-1}, n_{i+1}, \ldots, n_r) + n_i\beta_1(n_1, n_2, \ldots, n_{i-1}, n_{i+1}, \ldots, n_r)$$

for some functions $\beta_0, \beta_1 : \mathbb{Z}_{\geq 2}^{r-1} \to \mathbb{Z}_{\geq 0}$. Theorem 3.12 tells us that β_0, β_1 can be chosen independently from i. To help us visualize this linear relationship, we provide a plot in Figure 3.3. The plotted upper bounds are calculated based the minimum symmetric closure of the bound given by the first inequality in (3.17). The computed degrees in the plot provide further evidence that the relationship between the minimal degree and the order of the varying cyclic factor is linearly bounded. By observing the computed degrees, we may further conjecture that this relationship is precisely linear. However, we are unable to prove such a conjecture since we do not know whether or not the computed degree is truly minimal.

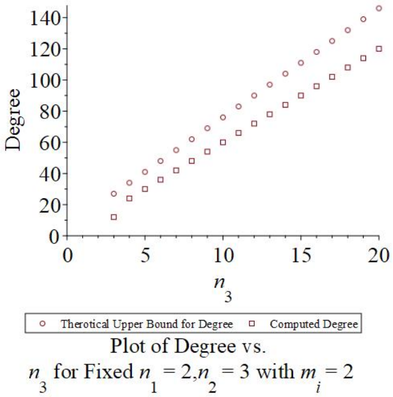


Figure 3.3: Plots of Actual Degrees and Upper Bounds vs. $n_3 = 3, 4, \ldots, 20$ for fixed $n_1 = 2, n_2 = 3$ with m_1, m_2, m_3 as parameters.

We conclude this section by comparing Theorem 3.12 to a theorem regarding irreducible representations of general finite groups.

Theorem 3.13 (Bell [3])**.** *Let $G_1, \ldots, G_r$ be finite groups with generating sets $S_1, S_2, \ldots, S_r$ respectively. Let Δ_i denote the sum of the degrees of the irreducible representations of G_i for $i = 1, \ldots, r$. Then the cogrowth series $F(t)$ of $\coprod_{i=1}^{s} G_i^{*m_i}$ with respect to the generating set $S := \cup_{i=1}^{r} S_i$, is algebraic and satisfies $Q(t, F(t)) = 0$, where $Q(t,z) \in \mathbb{Z}[t,z]$ with $\deg_t(Q)$ and $\deg_X(Q)$ both at most*

$$\left(\prod_{i=1}^{s} \Delta_i\right)\left(1 + \sum_{i=1}^{s} \frac{1}{\Delta_i}\right).$$

In the case of free product of cyclic groups, Theorem 3.13 is implied by the second inequality of (3.17). In our setting, we take G to be a free product of cyclic groups with orders

$n_1, n_2, \ldots, n_r$. Hence, to satisfy the hypothesis of Theorem 3.13, if we let each $G_i = \mathbb{Z}_{n_i}$ and each $S_i \subseteq G_i$ a generating set consisting of one element, then standard results from representation theory [7] tells us that each $\Delta_i = n_i$. Consequently, Theorem 3.12 deduces this special case of Theorem 3.13. Theorem 3.13 applies to any free product of finitely many finite groups, each equipped with arbitrary, and thus, is far more powerful than Theorem 3.12. However, the first inequality in (3.17) of Theorem 3.12 provides a non-symmetric upper bound, that is an improvement compared to that of Theorem 3.13. This improved bound is significantly tighter on examples where n_r and n_{r-1} are large.

Chapter 4

Free Products of Cyclic and Dihedral Groups

In this chapter, we discuss the free product of finite cyclic groups and finite dihedral groups. We perform singularity analysis on specific examples, and then obtain degree bounds on the case where the free factors are identical dihedral groups.

4.1 An Example with One Cyclic and One Dihedral Factor

In order to motivate our problem, we start with the example below regarding the free product of a cyclic factor and a dihedral factor.

Example 4.1 ($\mathbb{Z}_2 * D_3$)**.** Consider the free product

$$G = \mathbb{Z}_2 * D_3 = \langle x | x^2 = 1 \rangle * \langle r, f | r^3 = 1, f^2 = 1, rf = fr^{-1} \rangle$$

with the minimal generating set $S = \{x, r, f\}$. Figure 4.1 below gives the Cayley graph, $\chi(G, S)$, for this example. The black edges represent a walk in the direction of x. Amongst the blue edges, the directed ones correspond to the rotation $r \in D_3 \cap S$, and undirected ones corresponds to the flip, $f \in D_3 \cap S$.

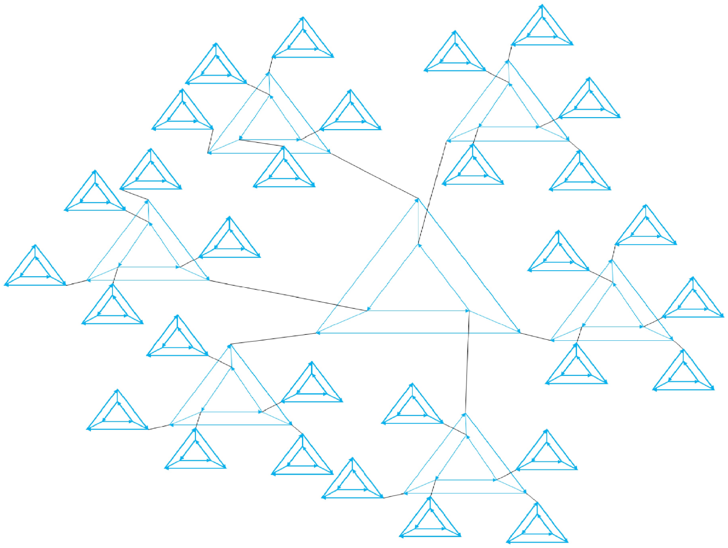


Figure 4.1: Cayley graph of $\mathbb{Z}_2 * D_3$ with generating set $S = \{x, r, f\}$.

Applying the free probability method to prove Theorem 2.13, we deduce that $z = F(t) := F_{G;S}(t)$ is a solution to the system

$$\begin{aligned} -tzz_1 - tzz_2 + z + 1 &= 0 \\ tz{z_1}^2 - tz - z_1 &= 0 \\ (tzz_2 - 1)\left({z_2}^2 - z_2 - 2\right) - 1 &= 0. \end{aligned} \tag{4.1}$$

Using the algebraic elimination procedure described in Algorithm 1, we deduce that a satisfying polynomial for $F(t)$ is defined by $Q(t, z)$:

$$Q(t,z) := \begin{bmatrix} (3t-1)(2t+1)(t+1)(t-1)^2 \\ (t-1)(t+1)(t^3-3t^2-t+1) \\ (t-1)(2t-1)(t+1) \\ -t^2-t+1 \end{bmatrix}^T \begin{bmatrix} z^3 \\ z^2 \\ z \\ 1 \end{bmatrix} \in \mathbb{Z}[t,z].$$

We perform singularity analysis on both the implicit and explicit solutions, following the technique described in Section 2.7. The explicit solution of the cogrowth series, $F(t)$, as computed using the `solve` and `eliminate` commands in the Maple programming language, is given by

$$
\begin{aligned}
F(t) = {} & \frac{\sqrt[3]{H_2\,(t)}}{6\ (3\,t-1)\,(2\,t+1)\,\sqrt[3]{t+1}\,(t-1)} \\
& + \frac{2\,\sqrt[3]{t+1}\,(t^6-6\,t^5-29\,t^4+56\,t^3-8\,t^2-14\,t+4)}{3\,\sqrt[3]{H_2\,(t)}\,(t-1)\,(3\,t-1)\,(2\,t+1)} \\
& - \frac{t^3-3\,t^2-t+1}{3\,(t-1)\,(3\,t-1)\,(2\,t+1)}
\end{aligned}
\tag{4.2}
$$

where

$$H_1(t) = \sqrt{-3\frac{(4t^4-48t^3+20t^2+13t-5)(t^3+3t^2+2t-4)^2}{t-1}}$$

and

$$
\begin{aligned}
H_2(t) = {} & 12t(t-1)(3t-1)(2t+1)H_1(t) - 8t^7(t^3-8t^2-39t-288) \\
& + 1140t^6 - 6348t^5 + 788t^4 + 2588t^3 - 504t^2 - 272t + 64.
\end{aligned}
$$

The *possible* singularities of $F(t)$ are computed by setting each expression that appears in (4.2) either as a denominator, or underneath a square root. This process may yield some values that are not singularities since cancellations may occur upon simplifying the given expression for $F(t)$. Upon implementing the procedure described above in Maple, we obtain the set of possible singularities,

$$
\begin{aligned}
P := \{ & -4.18554, -1, -0.5, \frac{1}{3}, 0.36392, 0.49578, 0.796321903, 1, \\
& -1.89816 - 1.19167i, -1.89816 + 1.19167i, \\
& -0.5054897169, 0.3497985349, 0.612422133, 11.54326905\} \subseteq \mathbb{C}.
\end{aligned}
$$

The set, P, suggests that the dominant singularity of $F(t)$ is $\frac{1}{3}$. However, we will see shortly that this is not the case.

We now perform singularity analysis on the implicit satisfying polynomial, $Q(t, z)$. To do this, we first compute the exceptional set, the union of the roots the leading coefficient of Q in z, and the discriminant of Q with respect to z. In this case, we computed the exceptional set to be

$$E := \{-1, -0.506, -0.5, 0, 0.3333, 0.3498, 0.6124, 0.7963, 1, 11.543, -1.898 - 1.192i, -1.898 + 1.192i\}.$$

It is a known fact [12, 8, 2] that the set, E, contains the dominant singularities of the cogrowth series, $F(t)$. The modulus of a dominant singularity of $F(t)$ satisfy the equation

$$\rho = \lim_{n\to\infty} \frac{[t^n]F(t)}{[t^{n+1}]F(t)} \tag{4.3}$$

provided the given limit exists, as stated in Section 2.7.
We use Maple to generate the coefficients $[t^n]F(t)$ for large n and concluded the approximation $\rho \approx 0.3497985381 \in E$. $\diamond$

Although Example 4.1 above demonstrates properties of asymptotic singularities, the main objective of this thesis is not to analyze singularities, but to discuss algebraic and enumerative properties of cogrowth generating functions.

4.2 Free Product of Identical Finite Dihedral Groups

We now consider the case where $G = D_n^{*m}$ is the free product of $m \geq 2$ identical copies of the group D_n. Unlike the cyclic case in Example 3.1, obtaining the satisfying polynomial explicitly in the case of identical dihedral groups is more difficult, since rational generating functions for dihedral groups are more complex than the geometric series for cyclic groups. However the results in Corollary 2.4 yield upper bounds on degrees of the satisfying polynomial. We formalize this result below, using the definition,

$$d_n := \begin{cases} \frac{n+1}{2}, & n \text{ is odd} \\ 2\lceil \frac{n}{4} \rceil, & n \text{ is even} \end{cases}$$

as stated in Equation (2.2) of Corollary 2.4.

Proposition 4.2. *Let $G = D_n^{*m} = \coprod_{i=1}^{m} \langle r_i, f_i | r_i^n = 1, f_i^2 = 1, r_i f_i = f_i r_i^{-1} \rangle$ with the generating set, $S = \{r_1, f_1, r_2, f_2, \ldots, r_m, f_m\}$. Then the cogrowth series, $F(t) := F_{G;S}(t)$, has a satisfying polynomial $P(t,z) \in \mathbb{Z}[t,z]$ with $\deg_t P \leq d_n$ and $\deg_z P \leq d_n + 1$.*

Proof. We know from Corollary 2.4 that $F(t)$ is the Taylor series of $\frac{p(t)}{q(t)}$ for some $p, q \in \mathbb{Z}[t]$ with $p(0) = q(0) = 1$ and $\deg p = \deg q \leq d_n$. Let $s = \sum_{x \in S} x \in \mathbb{C}[G]$, and let $G_s(t)$ denote its Cauchy transform. It follows that

$$G_s(t) = t^{-1}F(t^{-1}) = \frac{\bar{p}(t)}{\bar{q}(t)},$$

where $\bar{p}(t) := t^{\deg q} p(t^{-1}) \in \mathbb{Z}[t, t^{-1}]$ and $\bar{q}(t) := t^{(\deg q)+1} q(t^{-1}) \in \mathbb{Z}[t, t^{-1}]$.
Hence, $\bar{p}, \bar{q} \in \mathbb{Z}[t]$ with $\deg \bar{p} = \deg q = \deg \bar{q} - 1$. The compositional inverses, $K(t), \bar{K}(t)$, of the Cauchy transforms of s and $r_i + f_i$, respectively, for any $i = 1, \ldots, n$, satisfy the following relations:

$$\bar{p}(\bar{K}(t)) = t\bar{q}(\bar{K}(t)); \;\; K(t) = m\bar{K}(t) - (m-1)t^{-1}.$$

In particular, the polynomial system,

$$\begin{aligned} z &= mz_1 - (m-1)t^{-1} \\ \bar{p}(z_1) &= t\bar{q}(z_1) \end{aligned} \tag{4.4}$$

has a solution with $z = K(t)$. Upon performing elementary algebraic manipulations on Eqn (4.4), we get that the system,

$$\begin{aligned} z &= mtzz_1 - (m-1) \\ \bar{p}(z_1) &= tz\bar{q}(z_1) \end{aligned} \tag{4.5}$$

has a solution with $z = F(t)$. The first equation in (4.5) yields $z_1 = \frac{z+m-1}{mtz}$. After performing a substitution and clearing denominators, we deduce that a satisfying polynomial for $F(t)$ is

$$Q(t,z) := \sum_{k=0}^{(\deg q)+1} (z+m-1)^k (mtz)^{(\deg q)+1-k} \left(([t^k]\bar{p}) - tz([t^k]\bar{q})\right) \in \mathbb{Z}[t,z]. \tag{4.6}$$

Note that $\bar{q}(0) = 0$ and $[t^1]\bar{q} \neq 0$, which implies that $\deg_z Q = (\deg q) + 2$ and $\deg_t Q = (\deg q) + 1$. Since $[t^{(\deg q)+1}]\bar{p} = 0$, we have $\operatorname{val}_z Q \geq 1$ and $\operatorname{val}_t Q \geq 1$. Hence, taking

$$\begin{aligned} P(t,z) &:= (tz)^{-1} Q(t,z) \\ &= \left(\sum_{k=0}^{\deg q} m(z+m-1)^k (mtz)^{(\deg q)-k} \left(([t^k]\bar{p}) - tz([t^k]\bar{q})\right) \right) - (z+m-1)^{(\deg q)+1} \\ &\in \mathbb{Z}[t,z] \end{aligned} \tag{4.7}$$

gives us the desired bound. □

If follows from Equation (4.7) that $P(0,0) = (m-1)^{\deg q} \neq 0$, where $q \in \mathbb{Z}[t]$ is the denominator of the relevant cogrowth generating function selected according to Corollary 2.4. Consequently, P has zero valuation in both t and z, so in fact, $P = \operatorname{trim}_{\mathbb{Z}} Q$. Table 4.1 documents some properties of the satisfying polynomials computed in the proof of Proposition 4.2 for some specific values of n, the number of vertices in each dihedral factor. The number of free factors, m, is held as a general parameter.

The data provided in Table 4.1 is consistent with the statement of Proposition 4.2, and the given degree bounds are satisfied with equality in these examples.

We make a few observations on the properties of the satisfying polynomial, $P(t,z)$, based on Table 4.1. Notice that the leading coefficient of $P(t,z)$ with respect to z has maximal

n	d_n	Degree in z	Degree in t	Leading coefficient in z[a]	Constant term in z
3	2	3	2	$(mt+1)(2mt-1)$	$(m-1)^2$
4	2	3	2	$(2mt-1)(2mt+1)$	$(m-1)^2$
5	3	4	3	$-(2mt-1)(m^2t^2-mt-1)$	$(m-1)^3$
6	4	5	4	$-(2mt-1)(2mt+1)(mt-1)(mt+1)$	$(m-1)^4$
7	4	5	4	$-(2mt-1)(m^3t^3+2m^2t^2-mt-1)$	$(m-1)^4$
8	4	5	4	$-(2mt-1)(2mt+1)(2m^2t^2-1)$	$(m-1)^4$
9	5	6	5	$(2mt-1)(mt+1)(m^3t^3-3m^2t^2+1)$	$(m-1)^5$
10	6	7	6	$(2mt-1)(2mt+1)O((mt)^4)$	$(m-1)^6$
11	6	7	6	$(2mt-1)O((mt)^5)$	$(m-1)^6$
12	6	7	6	$(3m^2t^2{-}1)(2mt{-}1)(2mt{+}1)(mt-1)(mt+1)$	$(m-1)^6$
13	7	8	7	$-(2mt-1)O((mt)^6)$	$(m-1)^7$
14	8	9	8	$-(2mt-1)(2mt+1)O((mt)^6)$	$(m-1)^8$
15	8	9	8	$-(mt+1)(2mt-1)(m^2t^2-mt-1)O((mt)^4)$	$(m-1)^8$
16	8	9	8	$-(2mt-1)(2mt+1)(2m^2t^2-1)O((mt)^4)$	$(m-1)^8$
17	9	10	9	$(2mt-1)O((mt)^8)$	$(m-1)^9$
18	10	11	10	$(2mt-1)(2mt+1)(mt-1)(mt+1)O((mt)^6)$	$(m-1)^{10}$
19	10	11	10	$(2mt-1)O((mt)^9)$	$(m-1)^{10}$
20	10	11	10	$(2mt-1)(2mt+1)(5m^4t^4-5m^2t^2+1)O((mt)^4)$	$(m-1)^{10}$
30	16	17	16	$-(mt-1)(mt+1)(2mt-1)(2mt+1)O((mt)^{12})$	$(m-1)^{16}$

[a] The notation, $O((mt)^d)$, represents a polynomial in $\mathbb{Z}[mt]$ of degree d with positive leading coefficient.

Table 4.1: Properties of satisfying polynomials $P(t,z)$ over $\mathbb{Z}$ for the cogrowth series of $G = D_n^{*m} = \coprod_{i=1}^m \langle r_i, f_i | r_i^n = 1, f_i^2 = 1, r_i f_i = f_i r_i^{-1}\rangle$ generated by $S = \{r_1, f_1, r_2, f_2, \ldots, r_m, f_m\}$.

degree and depends solely on mt. That is, $[z^{\deg_z P}]P(t,z)$ is a polynomial[1] in $\mathbb{Z}[mt]$ of degree $\deg_t P(t,z)$. The linear factor, $2mt+1$, appears in all the leading coefficients. The factor, $mt+1$, appears whenever n is a multiple of 3. Finally, even though only the leading coefficient is shown in Table 4.1, we suspect that $P(t,z) = P(-t,z)$ whenever n is even[2]. We now summarize our observations as a conjecture.

Conjecture 4.3. *Let $G = D_n^{*m} = \coprod_{i=1}^m \langle r_i, f_i | r_i^n - 1, f_i^2 - 1, r_i f_i - f_i r_i^{-1}\rangle$ with the generating set, $S = \{r_1, f_1, r_2, f_2, \ldots, r_m, f_m\}$. Then the cogrowth series, $F(t) := F_{G;S}(t)$, has a satisfying polynomial $P(t,z) \in \mathbb{Z}[t,z]$ as defined in Equation (4.7). Let $L(t) := [z^{\deg_z P}]P(t,z)$ be the leading coefficient of P with respect to z. Then the following properties hold:*

1. *The polynomial, $L(t) \in \mathbb{Z}[t]$, belongs to $\mathbb{Z}[mt]$;*

2. $\deg L = \deg_t P$*;*

3. $2mt - 1 | L(t)$*;*

[1] Warning: $[z^d]P(t,z)$ is a polynomial in t, and is, in general, not the same as $[t^0 z^d]P(t,z)$.

[2] This property was verified using Maple for $n \in \{4, 6, 8, \ldots, 20\} \cup \{30, 36, 40\}$.

4. *if n is even, then $P(t,z) = P(-t,z)$; and*

5. *if $3|n$, then $mt+1|L(t)$.*

Throughout this thesis, we have focused on groups of the form

$$G = \mathbb{Z}_{n_1}^{*r_1} * \mathbb{Z}_{n_2}^{*r_2} * \ldots * \mathbb{Z}_{n_k}^{*r_k} * D_{m_1}^{*s_1} * D_{m_2}^{*s_2} * \ldots * D_{m_l}^{*s_l}$$

with each $n_j \geq 2$, $m_j \geq 3$, $r_i \geq 1$, $s_i \geq 1$, and $k + l > 0$. The case where $l = 0$ was discussed in the previous chapter. Section 4.2 discussed the case where $k = 0, l = 1$, for which G is the product of identical dihedral groups. More such cases can be analyzed as possible future work. Based on the results we obtained, we conjecture that, in the general case, a possible degree bound for G with a minimal generating set, in z, is

$$\deg_z P \leq (n_1 n_2 \ldots n_k d_{m_1} d_{m_2} \ldots d_{m_l}) \left(1 + \sum_{i=1}^{k} n_i^{-1} + \sum_{j=1}^{l} d_{m_j}^{-1}\right).$$

where d_n is defined, as before, in Proposition 4.2 at the beginning of this section.

Chapter 5

Conclusion

We have made effective, a known fact, that finite free products of finite groups have algebraic cogrowth generating functions. That is, they satisfy polynomial equations in two variables with integer coefficients. This fact was established using two different methods: constructing combinatorial grammar using formal language theory; and using the theory of free probability. We first construct a system of polynomial equations over the integers, then use a standard elimination technique in computer algebra to reduce the system down to one equation, yielding the desired satisfying polynomial.

The system we generate using grammar involves a number of equations that is exponential to the sum of the order of the free factors. The process of variable elimination can be reasonably carried out computationally but can be difficult to analyze in theory. Using free probability, we get that the number of equations involved is linear to the number of free factors. In both scenarios, identical free factors can be considered together. Thus, the formulation of our algebraic system can be reduced so that the number of variables and equations involved depends only on the number of distinct free factors.

As observed throughout this thesis, the difficulty the of computational analysis involved increases significantly as the number of distinct free factors increases by one. The case of identical cyclic factors yielded an simple explicit satisfying polynomial. For the case of two distinct cyclic factors, it was not easy to compute an explicit satisfying polynomial, but we did, however, establish upper bounds on their degrees, which are quadratic in the two cyclic orders. We also noticed that the usage of dihedral factors produced more complications, compared to using only cyclic factors. Unlike in the cyclic case, we were unable to produce explicit formulas for the satisfying polynomials for cases involving dihedral factors, using only integer coefficients.

Notice that we only considered cyclic and finite dihedral free factors in this thesis. Since the infinite cyclic group, $\mathbb{Z}$, has the same cogrowth sequence as a free product of two copies of $\mathbb{Z}_2$, we observed that it is sufficient to consider only finite cyclic factors. In general, one can also consider other types of groups as free factors, such as symmetric groups, general Abelian groups, special linear groups, etc.

Finally, we remark that Section 5 of Bell and Mishna [4] mentions a theorem stating that if our group is finitely generated and the generating set is inverse closed, then radius of convergence of the cogrowth series lies in $\left(0, \frac{1}{2\sqrt{2}}\right) \cup \{\frac{1}{2}, 1\}$. Since the majority of cases used in this thesis involves minimal generating sets, it may be of interest to develop a similar result of the minimal case.

Bibliography

[1] A. V. Anisimov. Group languages. *Kibernetika*, 4:18–24, 1971.

[2] Cyril Banderier and Michael Drmota. Formulae and asymptotics for coefficients of algebraic functions. *Combinatorics, Probability and Computing*, 24, 2015.

[3] Jason Bell. Personal Contact, March 2021.

[4] Jason Bell and Marni Mishna. On the complexity of the cogrowth sequence. *arXiv*, 1805.08118v1, 2018.

[5] Mireille Bousquet-Melou. Rational and algebraic series in combinatorial enumeration, 2008.

[6] Robert Brignall, Sophie Huczynska, and Vincent Vatter. Simple permutations and algebraic generating functions. *Journal of Combinatorial Theory Series A*, 115:423–441, 2007.

[7] David S. Dummit and Richard M. Foote. *Abstract Algebra.* John Wiley & Sons Inc., 2004.

[8] Philippe Flajolet and Robert Sedgewick. *Analytic Combinatorics.* Cambridge University Press, 2009.

[9] Werner Kuich and Arto Salomaa, editors. *Semirings, Automata, Languages.* Springer-Verlag, Berlin, Heidelberg, 1985.

[10] Harry R. Lewis and Christos H. Papadimitriou. *Elements of the Theory of Computation.* Prentice-Hall, Inc., 1998.

[11] Stephen Melczer. *Analytic Combinatorics in Several Variables: Effective Asymptotics and Lattice Path Enumeration.* PhD thesis, University of Waterloo, 2017.

[12] Marni Mishna. *Analytic Combinatorics A Multidimensional Approach.* CRC Press, 2020.

[13] David E. Muller and Paul E. Schupp. Groups, the theory of ends, and context-free languages. *Journal of Computer and System Sciences*, 26, 1982.

[14] Alexandru Nica and Roland Speicher. *Lectures on the Combinatorics of Free Probability.* Cambridge University Press, 2006.

[15] P. S. Novikov. On the algorithmic unsolvability of the word problem in group theory. *Trudy Mat. Inst. Steklov.*, 44:3–143, 1955.

[16] Igor Pak. Complexity problems in enumerative combinatorics. *arXiv*, 1803.06636, 2018.

[17] Carine Pivoteau, Bruno Salvy, and Michele Soria. Algorithms for combinatorial structures: Well-founded systems and newton iterations. *Journal of Combinatorial Theory*, 119, 2012.

[18] Gregory Quenell. Combinatorics of free product graphs. *Contemp. Math*, pages 257–281, 1994.

[19] Richard P. Stanley. *Enumerative Combinatorics*, volume 2. Cambridge University Press, 1999.

Appendix A

Maple Code

```
# user defined helper files
read "maple_helper/listutils.mpl";
read "maple_helper/stringutils.mpl";
read "maple_helper/polytools.mpl";
read "maple_helper/singularity_analysis.mpl";

# Maple standard packages
with(FileTools);
with(StringTools);
with(cominat);
with(gfun);
gfun:-version; # load 3.76



# functions

get_approx_inverse_exp_seqs :=
proc(aseq,p,r,num_apprs,ratio_method)
    # ratio_method should be 'single' or 'double'
    # for analyzing cogrowth sequence, we only need r=0
    # aseq should be passed as a list
    local nth_ratio, N, nmax;
    nth_ratio := n -> evalf(ifelse(ratio_method = 'single',
     (aseq[r + p*n + 1]/aseq[r + p*(n + 1) + 1])^(1/p),
    (aseq[r + 2*p*n + 1]*aseq[r + p*(n + 1) + 1]/(\
      aseq[r + p*n + 1]*aseq[r + 2*p*(n + 1) + 1]))^(1/p)));
    N := nops(aseq); nmax := floor(ifelse(ratio_method = 'single'
       ,
     (N - r - 1)/p - 1, 1/2*(N - r - 1)/p - 1));
    return map(nth_ratio, [seq(nmax + 1 - num_apprs .. nmax)]);
```

```
end proc


# reduce the complexity of code output by Maple's built in 'latex
    ' function
simple_latex := proc(aexpr)
     local tmp;
     tmp := latex(aexpr, output = string);
     # string subtitution
     return Subs(["\\left" = "", "\\right" = "", "\\," = ""], tmp)
         ;
end proc


# Use dynamic programming to implement a procedure
## getting the cogrowth series of a finite dihedral group
_Dm_memo_table := table([]);
Dm_cogrowth_series := proc(m, tt := 't')
     local j, F, N, cs, i, D, c;
     global _Dm_memo_table;
     if not assigned(_Dm_memo_table[m, tt]) then
          # formula for Dm
          F := 1/2 + 1/2*add(1/(1-2*cos(2*Pi*j/m)*tt), j = 0..m-1)/
              m;
          F := simplify(F);

          # express it as a ratio of integer polynomials
          N := expand(numer(F));
          cs := coeffs(N, tt, 'tv'); cs := map(simplify, [cs]);
          cs := map(a -> convert(round(a), integer), map(evalf, cs)
              );
          N := add(cs[i]*tv[i], i = 1..nops(cs)); D := collect(
              denom(F), tt);
          cs := coeffs(D, tt, 'tv');
          cs := map(simplify, [cs]);
          cs := map(a -> convert(round(a), integer), map(evalf, cs)
              );
          D := add(cs[i]*tv[i], i = 1 .. nops(cs)); c := subs(t =
              0, N);
          N := expand(N/c); D := expand(D/c); F := N/D;

          # memoization technique
          _Dm_memo_table[m, tt] := F;
     end if;
     return _Dm_memo_table[m, tt];
end proc;
```

```
# cogrowth system for the cyclic case
## derived from free probability
cogrowth_system := proc(n, m, r)
    local varlist, i, syst, x;
    varlist := [t, z, seq(x[i], i = 1 .. r)];
    syst := [seq(t*z*x[i]^n[i] - x[i]^(n[i] - 1) - t*z, i = 1 ..
       r)];
    syst := [seq(syst), z + add(-t*z*x[i]*m[i] + m[i], i = 1 .. r
       ) - 1];
    return varlist, syst;
end proc

# Do we want our generating set to be inverse closed, or minimal?
inv_closed := true


get_input_file := proc()
    local dirloc;
    description
        "gets the name of the file to read containing the FD
           variables and system of equations",
        "the file to read contains 2 items",
        "syst: system of eqns, varlist: list of variable names
           used in the system",
        "the first variable, varlist[1], gives the cogrowth
           sequence";
    dirloc := "maple_data_files/";
    return sprintf("%sZ2_m1__Z3_m2__Z5_m3__%s-dat.maple", dirloc,
        ifelse(inv_closed, "ic", ""));
end proc


# Ftcoeffs: the guessed cogrowth sequence
# Q: a satisfying polynomial
# prints a message checking if all the terms match
check_cogrowth_seq := proc(Ftcoeffs, Q)
    local N, P, i, odr;
    N := nops(Ftcoeffs); P := add(Ftcoeffs[i + 1]*t^i, i = 0 .. N
        - 1);
    print(sort(rem(P, t^16, t), t, ascending));
    odr := get_series_order(series(expand(subs(z = P, Q)), t = 0,
        1));
    printf("computed order, %d, is %sequal to the number of terms
        found\n", odr,
        ifelse(odr = N, "", "not "));
    printf("Hence, the terms found are %saccurate\n", ifelse(odr
       = N, "", "not "));
end proc

# Fixed-point iterative algorithm:
# Speedup #1: truncate the iterates down to the degree of
   accuracy of the cogrowth approximation
FP_iter_deg_trunc := proc(Kmax, trunc_tol, syst, varlist, Q,
   cg_seq_file, verbose)
local ifverb, printv, printfv, indexed_syst,
    cur, v, Fiter, Fterms, Ftcoeffs, k,
     has_mismatch, dacc, mpft;
     description "";
    ifverb := proc(write, verbose)
        return proc() if verbose then write(_passed); end if; end
            proc;
    end proc;
    printv := ifverb(print, verbose);
    printfv := ifverb(printf, verbose);
    unassign('j');
    indexed_syst := map(X -> lhs(X)[j + 1] = eval(subs(seq(v = v[
       j], v = varlist), rhs(X))), syst);
    cur[0] := [seq(v[0] = 0, v = varlist)]; Fiter[0] := table(cur
       [0])[v0[0]];
    Fterms := terms(Fiter[0]); printfv("_________\n");
    Ftcoeffs := load_cogrowth_seq(cg_seq_file);
    if Ftcoeffs = 'FAIL' then Ftcoeffs := 1; end if;
    for k from 0 to Kmax - 1 do
        printfv("Iteration %d - ", k + 1);
        cur[k + 1] := expand(subs(cur[k], subs(j = k,
           indexed_syst)));
        Fiter[k + 1] := table(cur[k + 1])[v0[k + 1]];
        Fiter[k + 1] := sort(collect(Fiter[k + 1], t), t,
           ascending);
        Fterms := terms(Fiter[k + 1]); has_mismatch := false;
        for dacc from 0 to nops([Ftcoeffs]) - 1 do
            if not ([Ftcoeffs][dacc + 1] = coeff(Fiter[k + 1], t,
                dacc)) then
            dacc := dacc - 1; has_mismatch := true;
            break; end if;
        end do;
        if not has_mismatch then
        printfv("subbing into minimal polynomial Q(t,z):
           computing");
        mpft := series(expand(subs(z = Fiter[k + 1], Q)), t = 0,
           10);
        dacc := get_series_order(mpft, t) - 1; end if;
        printfv("Number of excursions accurate up to length %d\n"
           , dacc);
        while nops([Ftcoeffs]) <= dacc do
            Ftcoeffs := Ftcoeffs, coeff(Fiter[k + 1], t, nops([
               Ftcoeffs]));
        end do;
        cur[k + 1] := map(eqn -> lhs(eqn) = rem(rhs(eqn), t^(dacc
            + 21 + trunc_tol), t), cur[k + 1]);
        Fiter[k + 1] := table(cur[k + 1])[v0[k + 1]];
        printfv("_________\n");
    end do;
    return Ftcoeffs;
end proc
```

Appendix B

Tables of Computed and Theoretical Degrees

Computed Degrees ($m_1 = m_2 = 1$)														
n_2 n_1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3	3	4 [a]	7	9	11	13	15	17	19	21	23	25	27	29
4	4	7	7	13	16	19	22	25	28	31	34	37	40	43
5	5	9	13	11	21	25	29	33	37	41	45	49	53	57
6	6	11	16	21	16	31	36	41	46	51	56	61	66	71
7	7	13	19	25	31	22	43	49	55	61	67	73	79	85
8	8	15	22	29	36	43	29	57	64	71	78	85	92	99
9	9	17	25	33	41	49	57	37	73	81	89	97	105	113
10	10	19	28	37	46	55	64	73	46	91	100	109	118	127
11	11	21	31	41	51	61	71	81	91	56	111	121	131	141
12	12	23	34	45	56	67	78	89	100	111	67	133	144	155
13	13	25	37	49	61	73	85	97	109	121	133	79	157	169
14	14	27	40	53	66	79	92	105	118	131	144	157	92	183
15	15	29	43	57	71	85	99	113	127	141	155	169	183	106

Theoretical Upper Bounds for Degrees ($m_1 = m_2 = 1$)														
n_2 n_1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	4	7	9	11	13	15	17	19	21	23	25	27	29	31
4	5	9	13	16	19	22	25	28	31	34	37	40	43	46
5	6	11	16	21	25	29	33	37	41	45	49	53	57	61
6	7	13	19	25	31	36	41	46	51	56	61	66	71	76
7	8	15	22	29	36	43	49	55	61	67	73	79	85	91
8	9	17	25	33	41	49	57	64	71	78	85	92	99	106
9	10	19	28	37	46	55	64	73	81	89	97	105	113	121
10	11	21	31	41	51	61	71	81	91	100	109	118	127	136
11	12	23	34	45	56	67	78	89	100	111	121	131	141	151
12	13	25	37	49	61	73	85	97	109	121	133	144	155	166
13	14	27	40	53	66	79	92	105	118	131	144	157	169	181
14	15	29	43	57	71	85	99	113	127	141	155	169	183	196
15	16	31	46	61	76	91	106	121	136	151	166	181	196	211

Table B.1: Actual computed degrees and the theoretical upper bounds from Theorem 3.3 for $n_1, n_2 = 2, 3, \ldots, 15$: $m_1 = m_2 = 1$.

[a] This cell is coloured with a cyan background for ease of reference in Example 3.6.

Computed Degrees[a] ($m_1, m_2 > 1$)

n_2 n_1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	3	6	8	10	12	14	16	18	20	22	24	26	28	30
3	6	6	12	15	18	21	24	27	30	33	36	39	42	45
4	8	12	10	20	24	28	32	36	40	44	48	52	56	60
5	10	15	20	15	30	35	40	45	50	55	60	65	70	75
6	12	18	24	30	21	42	48	54	60	66	72	78	84	90
7	14	21	28	35	42	28	56	63	70	77	84	91	98	105
8	16	24	32	40	48	56	36	72	80	88	96	104	112	120
9	18	27	36	45	54	63	72	45	90	99	108	117	126	135
10	20	30	40	50	60	70	80	90	55	110	120	130	140	150
11	22	33	44	55	66	77	88	99	110	66	132	143	?	?
12	24	36	48	60	72	84	96	108	120	132	78	?	?	?
13	26	39	52	65	78	91	104	117	130	143	?	?	?	?
14	28	42	56	70	84	98	112	126	140	?	?	?	?	?
15	30	45	60	75	90	105	120	135	150	?	?	?	?	?

[a] The cells with the "?" represent values that are not computed due to taking too long.

Theoretical Upper Bounds for Degrees ($m_1, m_2 > 1$)

n_2 n_1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	5	7	9	11	13	15	17	19	21	23	25	27	29	31
3	7	10	13	16	19	22	25	28	31	34	37	40	43	46
4	9	13	17	21	25	29	33	37	41	45	49	53	57	61
5	11	16	21	26	31	36	41	46	51	56	61	66	71	76
6	13	19	25	31	37	43	49	55	61	67	73	79	85	91
7	15	22	29	36	43	50	57	64	71	78	85	92	99	106
8	17	25	33	41	49	57	65	73	81	89	97	105	113	121
9	19	28	37	46	55	64	73	82	91	100	109	118	127	136
10	21	31	41	51	61	71	81	91	101	111	121	131	141	151
11	23	34	45	56	67	78	89	100	111	122	133	144	155	166
12	25	37	49	61	73	85	97	109	121	133	145	157	169	181
13	27	40	53	66	79	92	105	118	131	144	157	170	183	196
14	29	43	57	71	85	99	113	127	141	155	169	183	197	211
15	31	46	61	76	91	106	121	136	151	166	181	196	211	226

Table B.2: Actual computed degrees and the theoretical upper bounds from Theorem 3.3 for $n_1, n_2 = 2, 3, \ldots, 15$: $m_1, m_2 > 1$.