Enumerative Properties of Cogrowth Series on Free Products of Finite Groups

ACA 2021 Session on Algorithmic Combinatorics

Haggai Liu
Joint work with Marni Mishna and Jason Bell

Simon Fraser University
Department of Mathematics

July 24, 2021

Introduction

Word Problem

Given a group G with a finite generating set, S, determine if a given product of elements in S is the group identity.

Introduction

Word Problem

Given a group G with a finite generating set, S, determine if a given product of elements in S is the group identity.

Language of the Word Problem

$$L(G, S) := \{ \underbrace{s_1 s_2 \dots s_n}_{\text{symbol concatenation}} : n \geq 0, \ s_i \in S, \ \underbrace{s_1 \cdot s_2 \cdot \dots \cdot s_n}_{\text{group product}} = 1 \in G \}$$

Cogrowth Sequence and Series

Language of the Word Problem

$$L(G,S) := \{s_1 s_2 \dots s_n : n \geq 0,\ s_i \in S,\ s_1 \cdot s_2 \cdot \dots \cdot s_n = 1 \in G\}$$

Cogrowth Sequence and Series

Language of the Word Problem

$L(G,S) := \{s_1 s_2 \ldots s_n : n \geq 0,\ s_i \in S,\ s_1 \cdot s_2 \cdot \ldots \cdot s_n = 1 \in G\}$

- G: group generated by a finite set $S \subseteq G \setminus \{1\}$
- *cogrowth sequence* of G with respect to S:
$$\{|L(G,S) \cap S^n|\}_{n \geq 0}$$
- cogrowth series (GFs):
$F(t) \equiv F_{G;S}(t) := \sum_{n \geq 0} |L(G,S) \cap S^n|\, t^n \in \mathbb{Z}_{\geq 0}[[t]]$

Setup and Motivation

$$L(G,S) := \{s_1 s_2 \dots s_n : n \geq 0,\ s_i \in S,\ s_1 \cdot \ldots \cdot s_n = 1 \in G\}$$

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

Setup and Motivation

$$L(G,S) := \{s_1 s_2 \dots s_n : n \geq 0,\ s_i \in S,\ s_1 \cdot \dots \cdot s_n = 1 \in G\}$$

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

- Continue the study of Bell and Mishna (2018), on free products of (finitely many) finite groups
- $G = G_1 * G_2 * \dots * G_d$; G_i cyclic or dihedral

Result of Muller and Schupp

Free products of finite groups have **algebraic** GFs

- ie. $Q(t, F(t)) = 0$ for some $Q(t,z) \in \mathbb{Z}[t,z] \setminus \{0\}$
- Call Q a **satisfying polynomial** of $F(t)$
- $\deg_z Q$ is minimum $\implies$ Q is a **minimal polynomial** of $F(t)$

Setup and Motivation

$$L(G,S) := \{s_1 s_2 \ldots s_n : n \geq 0,\ s_i \in S,\ s_1 \cdot \ldots \cdot s_n = 1 \in G\}$$

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

Result of Muller and Schupp

Free products of finite groups have **algebraic** GFs

- ie. $Q(t, F(t)) = 0$ for some $Q(t,z) \in \mathbb{Z}[t,z] \setminus \{0\}$
- Call Q a **satisfying polynomial** of $F(t)$
- $\deg_z Q$ is minimum $\implies$ Q is a **minimal polynomial** of $F(t)$

Main Objective

Obtain degree bounds on minimal polynomials.

Excursions on Cayley Graphs

We can visualize the problem using Cayley graphs.

- Cayley Graph of G with respect to S: $\chi(G,S) = (V,E)$
  - $V = G$, $E = \{(g, gs) : g \in G,\ s \in S\}$ (ie. directed)
  - Arcs show multiplication by elements of S
  - Walks show products on elements of S
- *Excursions* of $\chi(G,S)$:
  - Excursions are walks that start and end at $1 \in G$
  - $L(G,S) \leftrightarrow$ excursions on $\chi(G,S)$

The cogrowth sequence counts excursions on $\chi(G,S)$

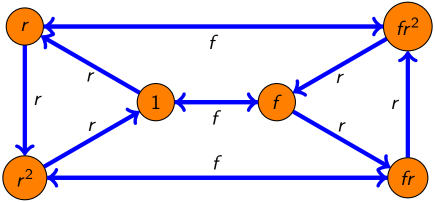
Examples: Finite Cyclic and Dihedral Groups

$G := \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \langle x | x^n = 1 \rangle$; $S := \{x\}$

- $L(G, S) = \{\epsilon, x^n, x^{2n}, x^{3n}, \ldots\}$
- Cogrowth GF: $F_{G;S}(t) = \frac{1}{1-t^n}$
- $\chi(G, S)$ is the directed cycle on n vertices

$G := D_n = \langle r, f | r^n = 1, f^2 = 1, rf = fr^{-1} \rangle$; $S := \{r, f\}$

- $L(D_3, S) = \{ff, rrr, rfrf, frfr, rrfrrf, rfrrfr, frrfrr\}^*$
- $\chi(D_3, S)$: See below



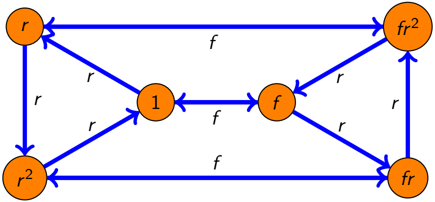
Examples: Finite Cyclic and Dihedral Groups

$G := \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \langle x | x^n = 1 \rangle$; $S := \{x\}$

- $L(G, S) = \{\epsilon, x^n, x^{2n}, x^{3n}, \ldots\}$
- Cogrowth GF: $F_{G;S}(t) = \frac{1}{1-t^n}$
- $\chi(G, S)$ is the directed cycle on n vertices

$G := D_n = \langle r, f | r^n = 1, f^2 = 1, rf = fr^{-1} \rangle$; $S := \{r, f\}$

- $L(D_3, S) = \{ff, rrr, rfrf, frfr, rrfrrf, rfrrfr, frrfrr\}^*$
- Cogrowth GF: $F_n(t) := F_{D_n;S}(t) = ?$
- $\chi(D_3, S)$: See below



Cogrowth GF for D_n

Proposition 1

For each $n \geq 3$,

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

Corollary 2

$F_n(t) = \dfrac{p(t)}{q(t)}$, *with* $p, q \in \mathbb{Z}[t]$, $p(0) = q(0) = 1$, *and* $\deg p = \deg q \leq d_n$, *where*

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

Initial Bound on Finite Groups using Representation Theory

Lemma 3 (Bell, L., Mishna 2021+)

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.

Initial Bound on Finite Groups using Representation Theory

Proof.

- Consider an isomorphism $\Psi : \overline{\mathbb{Q}}[H] \to M_{n_1}(\overline{\mathbb{Q}}) \times \cdots \times M_{n_d}(\overline{\mathbb{Q}})$.
- Ψ induces a $\overline{\mathbb{Q}}$-algebra isomorphism between the power series rings $\overline{\mathbb{Q}}[H][[t]]$ and $\left(M_{n_1}(\overline{\mathbb{Q}}) \times \cdots \times M_{n_d}(\overline{\mathbb{Q}})\right)[[t]]$ sending $\sum_{n\geq 0} \alpha^n t^n \mapsto \sum_{n\geq 0}(Y_1^n, \ldots, Y_d^n)t^n$ where $\Psi(\alpha) = (Y_1, \ldots, Y_d)$.
- By Cayley Hamilton, this image satisfy a linear recurrence of order at most $n_1 + \cdots + n_d$.
- Thus, $A(t) := \sum \alpha^n t^n = p(t)/q(t)$ with $p, q \in \overline{\mathbb{Q}}[t]$ coprime, and $q(0) = 1$.
- Since $A(t) \in \mathbb{Z}[[t]]$, p/q must be invariant under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
- The roots of $q(t^{-1})$ are algebraic integers, so $p, q \in \mathbb{Z}[t]$.

$\square$

Initial Bound on Finite Groups using Representation Theory

Example ($G = \mathbb{Z}_n = \langle x | x^n = 1 \rangle; S = \{x\}$)

Lemma 3 implies that $F_{G;S}(t) \equiv \frac{1}{1-t^n} = \frac{p(t)}{q(t)}$, where $p, q \in \mathbb{Z}[t]$, with $\deg p \leq n-1$ and $\deg q \leq n$.

Here, $\deg p = 0$ and $\deg q = n$.

Example ($G = D_n \equiv \langle r, f | r^n{=}1, f^2{=}1, rf = fr^{-1} \rangle; S := \{r, f\}$)

- Sum, $N := n_1 + n_2 + \ldots + n_d$ is $n+2$ if n is even; $n+1$ if n is odd
- Lemma 3 $\implies$ $F_{G;S}(t) = p(t)/q(t)$, $\deg p \leq N-1$, $\deg q \leq N$.
- Corollary 2 $\implies$ $\deg p = \deg q \leq \frac{N}{2}$.

Free Products of Finite Groups

Definition

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 $K^{*m} := \underbrace{K * K * \ldots * K}_{m \text{ factors}}$.

Example

$\mathbb{Z}_2^{*3} \equiv \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2 \equiv \langle x, y, z | x^2 = 1, y^2 = 1, z^2 = 1 \rangle$ $(xy \neq yx)$

Important

The cogrowth GF of G depends on the cogrowth GF of each G_i in a nontrivial way

Free Products of Finite Groups

Definition

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 $K^{*m} := \underbrace{K * K * \ldots * K}_{m \text{ factors}}$.

Example

$\mathbb{Z}_2^{*3} \equiv \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2 \equiv \langle x, y, z | x^2 = 1, y^2 = 1, z^2 = 1 \rangle \ (xy \neq yx)$

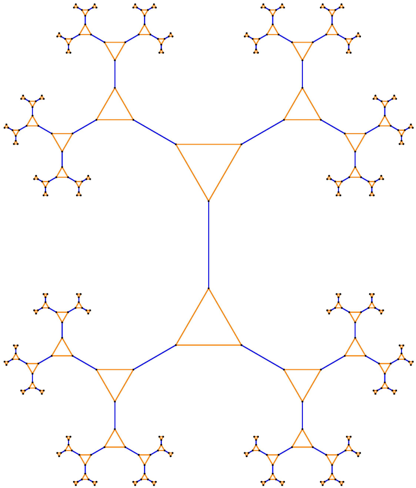
Important

The cogrowth GF of G depends on the cogrowth GF of each G_i in a nontrivial way

- We focus on the case where each G_i is finite
- Generating set: $S = \cup_{i=1}^{m} S_i$; S_i a generating set for G_i

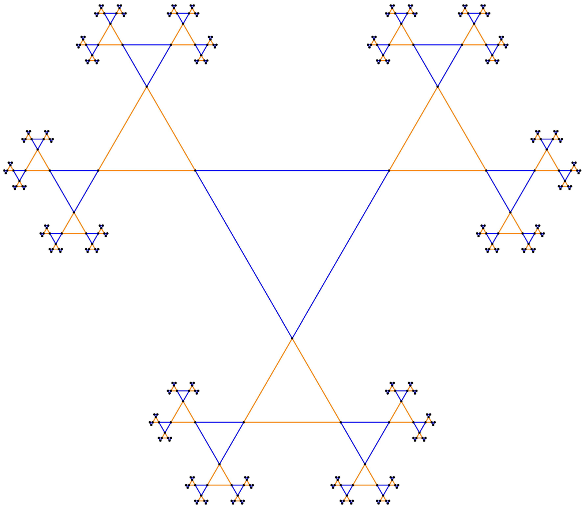
Visualization of Cayley Graphs

$$\mathbb{Z}_2 * \mathbb{Z}_3 \equiv \langle x | x^2 = 1 \rangle * \langle y | y^3 = 1 \rangle$$



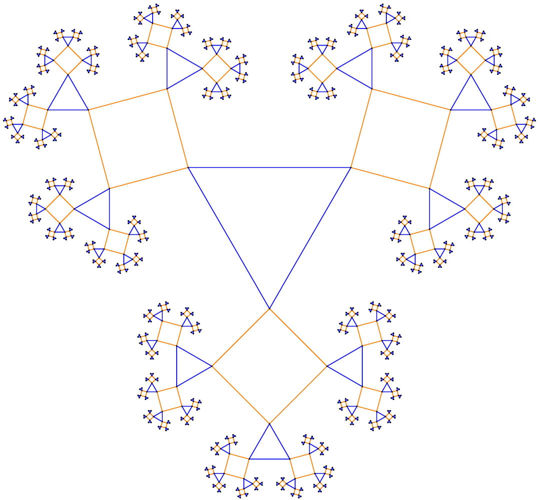
Visualization of Cayley Graphs

$$\mathbb{Z}_3 * \mathbb{Z}_3 \equiv \langle x | x^3 = 1 \rangle * \langle y | y^3 = 1 \rangle$$



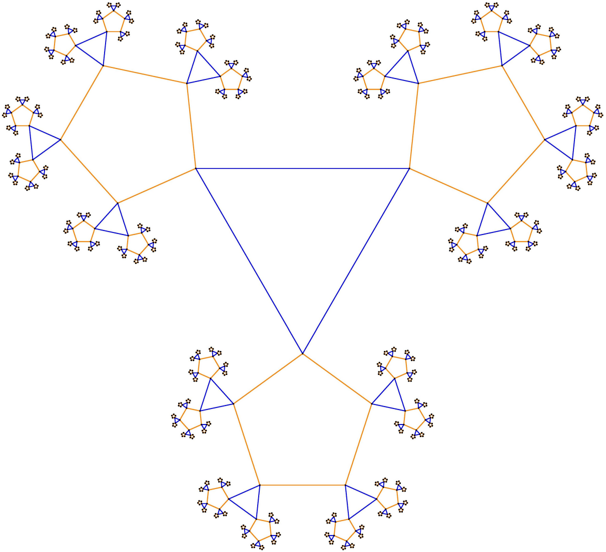
Visualization of Cayley Graphs

$$\mathbb{Z}_3 * \mathbb{Z}_4 \equiv \langle x | x^3 = 1 \rangle * \langle y | y^4 = 1 \rangle$$



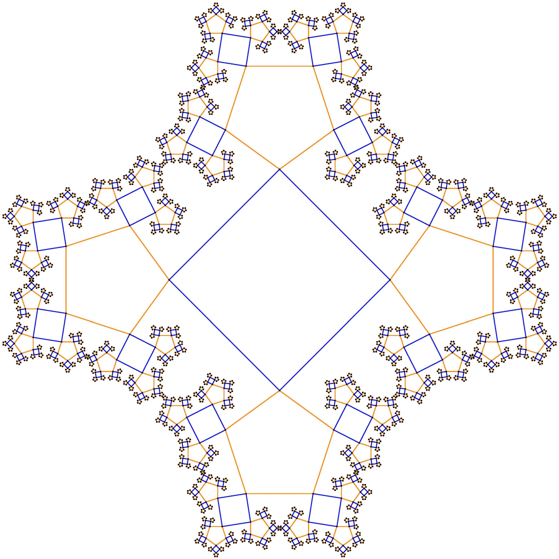
Visualization of Cayley Graphs

$$\mathbb{Z}_3 * \mathbb{Z}_5 \equiv \langle x | x^3 = 1 \rangle * \langle y | y^5 = 1 \rangle$$



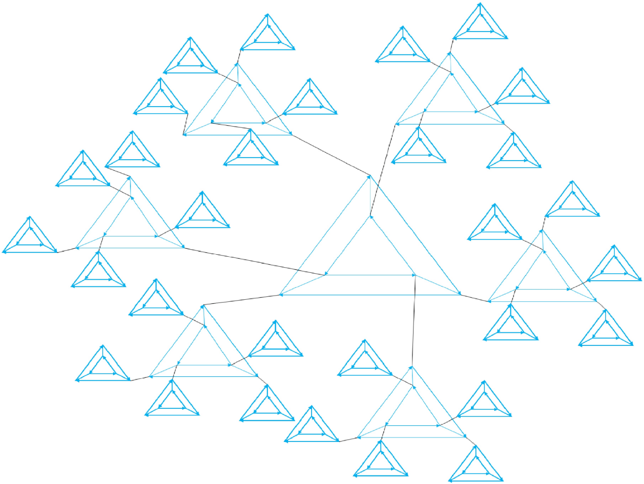
Visualization of Cayley Graphs

$$\mathbb{Z}_4 * \mathbb{Z}_5 \equiv \langle x | x^4 = 1 \rangle * \langle y | y^5 = 1 \rangle$$



Visualization of Cayley Graphs

$\mathbb{Z}_2 * D_3 \ (S = \{x, r, f\})$



System using Combinatorial Grammar

- $g \in G$, $X \subseteq G$, τ: an atom, ι: characteristic function.
- $Z_{g,X}$: (combinatorial class of) words in S^* evaluating to g, with proper nonempty prefixes avoiding X

System using Combinatorial Grammar

- $g \in G$, $X \subseteq G$, τ: an atom, ι: characteristic function.
- $Z_{g,X}$: (combinatorial class of) words in S^* evaluating to g, with proper nonempty prefixes avoiding X

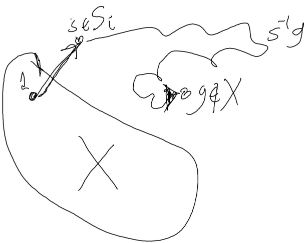
Lemma 4 (Bell and Mishna)

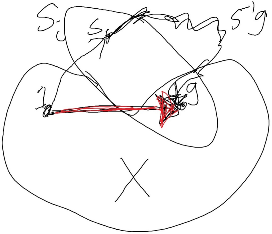
Let $G = G_1 * G_2 * \ldots * G_m$ be a (possibly trivial) free product of m finitely generated groups. Let S_i be a finite generating set for G_i so that $S = \cup_{i=1}^m S_i$ is a generating set for G. For each $1 \leq i \leq m$ and $\{g\} \cup X \subseteq G_i$, using disjoint unions of combinatorial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

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

System using Combinatorial Grammar

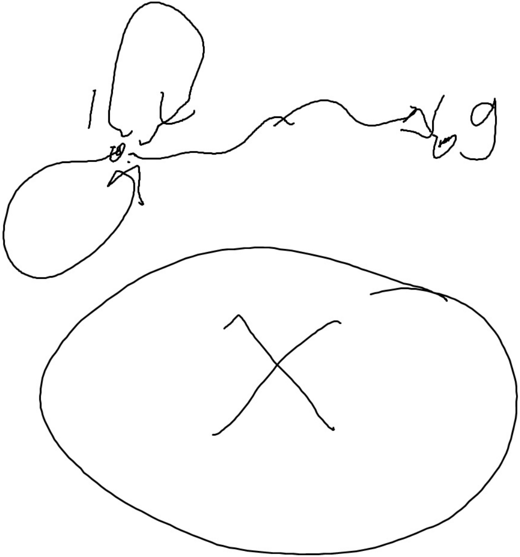
1. $Z_{g,X} = \left(\iota\left(g \in S_i \cap X\right)\tau\right) \cup \left(\bigcup_{s \in S_i \setminus X} \left(\tau \times Z_{s^{-1}g, s^{-1}X}\right)\right)$, if $1 \in X$, $g \neq 1$.





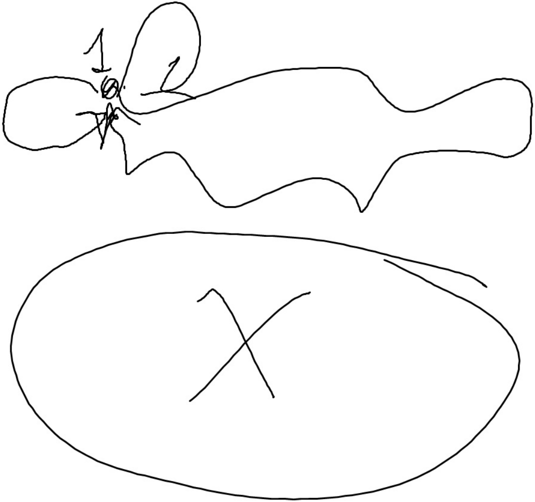
System using Combinatorial Grammar

2. $Z_{g,X} = Z_{1,X} \times Z_{g,X \cup \{1\}}$, if $1 \notin X$, $g \neq 1$.



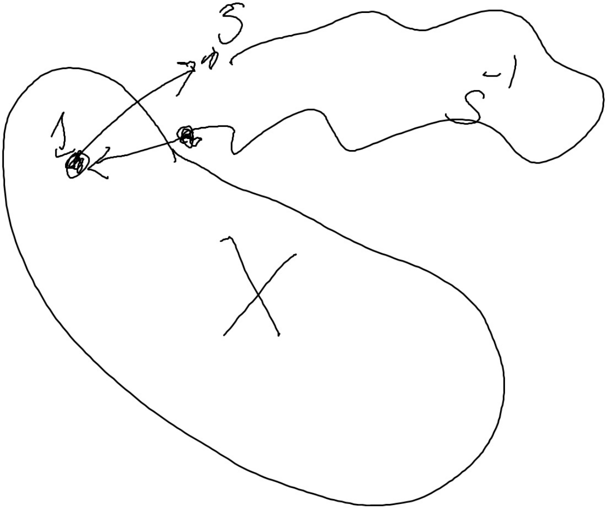
System using Combinatorial Grammar

3. $Z_{1,X} = \epsilon \cup \left(Z_{1,X} \times \left(Z_{1,X\cup\{1\}} \setminus \epsilon\right)\right)$, if $1 \notin X$.



System using Combinatorial Grammar

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



Combinatorial Grammar to GF

- $F_{g,X}$: GF for $Z_{g,X}$

Corollary 5 (Bell and Mishna)

Adopting the same notation used in Lemma 4, we have the analogous equalities for the set of generating functions $\{F_{g,X}\}$.

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

Consequences and Obstructions

- Each G_i is finite $\implies$ the combinatorial grammar contains only finitely many equations.
- We can eliminate variables on the grammar to obtain a satisfying polynomial.
- Obstructions:
  - The size of the initial system can be large (exponential in $|G_i|$)
  - Elimination process is time consuming, even for a computer

Consequences and Obstructions

- Each G_i is finite $\implies$ the combinatorial grammar contains only finitely many equations.
- We can eliminate variables on the grammar to obtain a satisfying polynomial.
- Obstructions:
  - The size of the initial system can be large (exponential in $|G_i|$)
  - Elimination process is time consuming, even for a computer
- Solution: Use free probability theory and obtain a system of size linear in $|G_i|$

Free Probability: A Brief Introduction

- $G = G_1 * \ldots * G_m$; $S = \cup_{i=1}^m S_i$ as before
- Group algebra $\mathbb{C}[G]$: non-commutative random variables
- linear **expectation** operator $\phi : \mathbb{C}[G] \to \mathbb{C}$,

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

- $\left\{\phi\left(\left(\sum_{s \in S} s\right)^n\right)\right\}_{n \geq 0}$: cogrowth sequence
- *Cauchy transform* of $\alpha \in \mathbb{C}[G]$: $G_\alpha(t) := \sum_{n \geq 0} \phi(\alpha^i) t^{-n-1}$
- Inverse Cauchy transform of α: $K_\alpha = G_\alpha^{\langle -1 \rangle}$.
- **Important Fact**: For $\alpha = \sum \alpha_g g$, $\beta = \sum \beta_g g$, if $\alpha_g \beta_g = 0$ for each $g \in G$, then $K_{\alpha+\beta}(t) = K_\alpha(t) + K_\beta(t) - t^{-1}$.

Resultants of Polynomials

Strategy: Use resultants to eliminate variables

Resultants of Polynomials

Strategy: Use resultants to eliminate variables

Upper Bound on Resultants

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

Resultants of Polynomials

Strategy: Use resultants to eliminate variables

Upper Bound on Resultants

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

Reduced Resultant

$$\overline{\operatorname{Res}}(f, g, z) := \begin{cases} \operatorname{trim} \operatorname{Res}(f, g, z), & (\deg_z f)(\deg_z g) > 0 \\ \operatorname{trim} f, & \deg_z f = 0,\ \deg_z g > 0 \\ \operatorname{trim} g, & \deg_z f > 0,\ \deg_z g = 0 \\ 1, & \deg_z f = \deg_z g = 0 \end{cases}$$

where $\operatorname{trim} f = f \cdot \prod_v v^{-\operatorname{val}_v f}$.

Resultants of Polynomials

Strategy: Use resultants to eliminate variables

Upper Bound on Resultants

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

Reduced Resultant

$$\overline{\operatorname{Res}}(f, g, z) := \begin{cases} \operatorname{trim} \operatorname{Res}(f, g, z), & (\deg_z f)(\deg_z g) > 0 \\ \operatorname{trim} f, & \deg_z f = 0,\ \deg_z g > 0 \\ \operatorname{trim} g, & \deg_z f > 0,\ \deg_z g = 0 \\ 1, & \deg_z f = \deg_z g = 0 \end{cases}$$

where $\operatorname{trim} f = f \cdot \prod_v v^{-\operatorname{val}_v f}$.

Purpose of $\overline{\operatorname{Res}}$

To remove monomial factors and redundant exponents in order to decrease the degrees of the polynomials.

Algorithm for Algebraic Elimination

Algorithm 1 polynomial elimination over an integral domain B

Input: $n \in \mathbb{Z}_{>0}$; $t, z_1, \ldots, z_n$ indeterminate; $\vec{P} \in B[t, z_1, \ldots, z_n]^n$.
Assumption: There are algebraic functions $F_1(t), \ldots, F_n(t)$, all nonzero, such 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
        $P_i^{(k)} := \overline{\mathrm{Res}}_B(P_i^{(k-1)}, P_{n-k+1}^{(k-1)}, z_{n-k+1})$
    end for
    $\vec{P}^{(k)} := (P_i^{(k)})_{i=1}^{n-k}$
end for
return $P_f(t,z) := P_1^{(n-1)}(t,z) \in B[t,z]$
```

A First Bound on Free Products of Finite Groups

Theorem 6 (Bell, L., Mishna 2021+)

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 $\coprod_{i=1}^r G_i^{*m_i}$ 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 $\deg_z(Q)$ both at most

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

- Theorem 6 $\implies$ second inequality of Eqn (4) in Theorem 9
- Theorem 6 is applicable to any finite groups with any generating sets

Free Products of Cyclic Groups

- $G := \coprod_{i=1}^{r} \coprod_{j=1}^{m_i} \langle x_{ij} | x_{ij}^{n_i} = 1 \rangle = \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2} * \ldots * \mathbb{Z}_{n_r}^{*m_r}$
- $S = \{x_{ij} : 1 \leq i \leq r, 1 \leq j \leq m_i\}$
- r: number of <u>distinct</u> cyclic factors

Free Products of Cyclic Groups

- $G := \coprod_{i=1}^{r} \coprod_{j=1}^{m_i} \langle x_{ij} | x_{ij}^{n_i} = 1 \rangle = \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2} * \ldots * \mathbb{Z}_{n_r}^{*m_r}$
- $S = \{x_{ij} : 1 \leq i \leq r, 1 \leq j \leq m_i\}$
- r: number of distinct cyclic factors
- Using free probability, we obtain a system of equations for $z = F_{G;S}(t)$.

Free Products of Cyclic Groups

Theorem 7 (Liu)

For $n_i \geq 2$ and $m_i \geq 1$, let

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

and $S := \{x_{ij} | i = 1, \ldots, r; j = 1, \ldots, m_i\}$. Let $F(t) := F_{G;S}(t)$ be the cogrowth GF. Then the system,

$$P_i(t, z, z_1, \ldots, z_r) := tzz_i^{n_i} - z_i^{n_i - 1} - tz = 0, \;\; i = 1, \ldots, r;$$
$$P_{r+1}(t, z, z_1, \ldots, z_r) := z - (\sum_{j=1}^{r} m_j tzz_j) + (\sum_{j=1}^{r} m_j) - 1 = 0 \quad (3)$$

solves $F(t)$: There are algebraic functions $F_j(t) \not\equiv 0$, such that $P_i(t, F(t), F_1(t), \ldots, F_r(t)) = 0$ for $1 \leq i \leq r+1$.

Case of Identical Cyclic Factors($r = 1$): $G = \mathbb{Z}_n^{*m}$

Solved by Bell and Mishna using combinatorial grammar.

$$\boldsymbol{Q(t,z) = (z-1)(z+m-1)^{n-1} - m^n t^n z^n}$$

From Free Probability,

- $P_1^{(0)} = P_1(t,z,z_1) = tzz_1^{n_1} - z_1^{n_1-1} - tz$;
- $P_2^{(0)}(t,z,z_1) = P_2(t,z,z_1) = z - mtzz_1 + m - 1$;
- $P_1^{(1)}(t,z) = (z-1)(z+m-1)^{n-1} - m^n t^n z^n \boldsymbol{= Q(t,z)}$.

Case of Identical Cyclic Factors($r = 1$): $G = \mathbb{Z}_n^{*m}$

Solved by Bell and Mishna using combinatorial grammar.

$$\boldsymbol{Q(t,z) = (z-1)(z+m-1)^{n-1} - m^n t^n z^n}$$

From Free Probability,

- $P_1^{(0)} = P_1(t,z,z_1) = tzz_1^{n_1} - z_1^{n_1-1} - tz$;
- $P_2^{(0)}(t,z,z_1) = P_2(t,z,z_1) = z - mtzz_1 + m - 1$;
- $P_1^{(1)}(t,z) = (z-1)(z+m-1)^{n-1} - m^n t^n z^n \boldsymbol{= Q(t,z)}$.

Key Observation

The degree of satisfying polynomial is independent of m.
We can generalize this result to an arbitrary number of distinct free factors.

Case of Two Distinct Factors ($r = 2$)

- $G := \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2}$
- System of polynomials:

$$
\begin{aligned}
P_1 &= tzz_1^{n_1} - z_1^{n_1-1} - tz \\
P_2 &= tzz_2^{n_2} - z_2^{n_2-1} - tz \\
P_3 &= z - m_1 tzz_1 - m_2 tzz_2 + m_1 + m_2 - 1.
\end{aligned}
$$

- After one iteration of Algorithm 1: $P_1^{(1)} = P_1$;
$$P_2^{(1)} = \begin{cases} (z - m_1 tzz_1 + m_1 - 1)(z - m_1 tzz_1 + m - 1)^{n_2-1} - (m_2 tz)^{n_2}, & m_1 > 1 \\ (1 - tz_1)(z - tzz_1 + m_2)^{n_2-1} - m_2^{n_2} t^{n_2} z^{n_2-1}, & m_1 = 1 \end{cases}$$

Case of Two Distinct Factors ($r = 2$)

- $G := \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2}$
- System of polynomials:

$$
\begin{aligned}
P_1 &= tzz_1^{n_1} - z_1^{n_1-1} - tz \\
P_2 &= tzz_2^{n_2} - z_2^{n_2-1} - tz \\
P_3 &= z - m_1 tzz_1 - m_2 tzz_2 + m_1 + m_2 - 1.
\end{aligned}
$$

- After one iteration of Algorithm 1: $P_1^{(1)} = P_1$;

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

- Upper bound on resultants: $\deg_z \mathrm{Res}(P_1^{(1)}, P_2^{(1)}, z_1) \leq n_2 + n_1(n_2 - 1)$

Degree Bound Theorem for $r = 2$

Theorem 8 (Liu)

Let

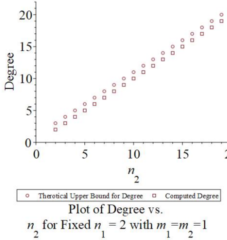
$$G = \mathbb{Z}_{n_1}^{*m_1} * \mathbb{Z}_{n_2}^{*m_2} = \coprod_{i=1}^{2} \coprod_{j=1}^{m_i} \langle x_{ij} | x_{ij}^{n_i} = 1 \rangle$$

be generated by $S = \{x_{ij} : i = 1, 2;\ 1 \leq j \leq m_i\}$. *Then there is a satisfying polynomial* $Q \in \mathbb{Z}[t, z] \setminus \{0\}$ *for the cogrowth series* $F_{G;S}(t)$ *such that* $\deg_z Q$ *satisfy the upper bounds given in the table below.*

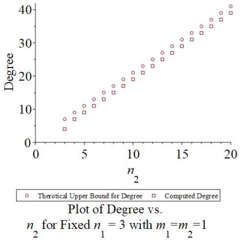
	$m_2 = 1$	$m_2 > 1$
$m_1 = 1$	$1 + n_1 n_2 - \max\{n_1, n_2\}$	$1 + n_1(n_2 - 1)$
$m_1 > 1$	$1 + n_2(n_1 - 1)$	$1 + n_1 n_2$

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

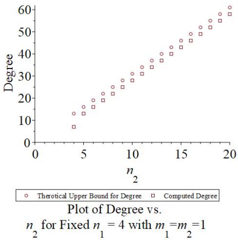
Plots for $r = 2$: Computed Degrees vs. Upper Bounds



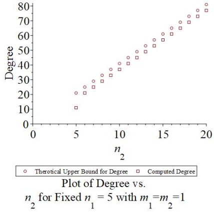
(a) $n_1 = 2$



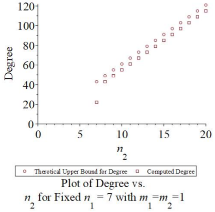
(b) $n_1 = 3$



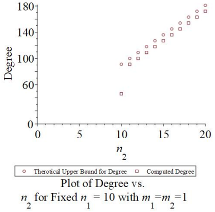
(c) $n_1 = 4$



(d) $n_1 = 5$



(e) $n_1 = 7$



(f) $n_1 = 10$

Plots of actual degrees and upper bounds vs. $n_2 = n_1, \ldots, 20$ for various fixed n_1; $m_1 = m_2 = 1$.

Conjectures for $r = 2$

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

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

- Entries in our table of upper bounds can be decreased precisely by one.
- If $m_1 = m_2 = 1$, then

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

Arbitrary Number of Distinct Cyclic Factors

Theorem 9 (Liu)

Fix $r \geq 3$. As before, consider the group,

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

generated by $S := \{x_{ij}\}$, $n_i \geq 2$; $m_i \geq 1$. Running Algorithm 1 with input as the system (3), given in Theorem 7, we deduce

$$\begin{aligned} \deg_z P_1^{(r)} &\leq (n_1 n_2 \ldots n_r) \left(1 + \frac{1}{n_{r-1} n_r} + \sum_{k=1}^{r-2} \frac{1}{n_k} \right) \\ &< (n_1 n_2 \ldots n_r) \left(1 + \sum_{k=1}^{r} \frac{1}{n_k} \right), \end{aligned} \quad (4)$$

and for $0 \leq k < r$, $1 \leq j \leq r - k$,

$$\deg_{z_j} P_{r-k+1}^{(k)} \leq n_{r-k+1} \ldots n_{r-1} n_r .$$

Identical Dihedral Factors

- $G = D_n^{*m} \equiv \coprod_{i=1}^{m} \langle r_i, f_i | r_i^n = 1, f_i^2 = 1, r_i f_i = f_i r_i^{-1} \rangle$
- $S = \{r_1, f_1, r_2, f_2, \ldots, r_m, f_m\}$
- Obtaining $Q(t, z)$ explicitly in this case is difficult, since GFs for dihedral groups are not geometric series

Identical Dihedral Factors

Recall! (from Prop. 1)

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

Proposition 10

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 $\deg_z P \leq d_n + 1$.

Table of Degrees and Leading Coefficients: D_n^{*m}

n	d_n	$deg_z P$	$\deg_t P$	Leading coefficient in z	$P(t,0)$
3	2	3	2	$(mt+1)(2mt-1)$	$(m-1)^2$
4	2	3	2	$(4m^2t^2-1)$	$(m-1)^2$
5	3	4	3	$-(2mt-1)(m^2t^2-mt-1)$	$(m-1)^3$
6	4	5	4	$-(4m^2t^2-1)(m^2t^2-1)$	$(m-1)^4$
7	4	5	4	$-(2mt-1)(m^3t^3+2m^2t^2-mt-1)$	$(m-1)^4$
8	4	5	4	$-(4m^2t^2-1)(2m^2t^2-1)$	$(m-1)^4$
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	$(3m^2t^2-1)(4m^2t^2-1)(m^2t^2-1)$	$(m-1)^6$

Properties of satisfying polynomials $P(t,z)$ over $\mathbb{Z}$ for the cogrowth GF of $G = D_n^{*m}$; $S = \{r_1, f_1, r_2, f_2, \ldots, r_m, f_m\}$.

Properties of the Satisfying Polynomial: D_n^{*m}

Theorem 11 (Liu)

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 GF, $F(t) := F_{G;S}(t)$, has a satisfying polynomial $P(t,z) \in \mathbb{Z}[t,z]$, with leading coefficient $L(t) := [z^{\deg_z P}]P(t,z)$ and $P(t,0) \in \mathbb{Z}[m] \setminus \{0\}$, such that 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. $2mt - 1 | L(t)$;
4. *if n is even, then $P(t,z) = P(-t,z)$; and*
5. $3 | n$ *if and only if* $mt + 1 | L(t)$.

Proof of Theorem 11

- We can deduce

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

  where $\bar{p}(t) := t^{\deg q} p(t^{-1})$ and $\bar{q}(t) := t^{(\deg q)+1} q(t^{-1})$.
- $P(t,0) = (m-1)^{\deg q}$.
- Property 1: $L(t) = q(mt)$.
- Property 2: $\deg L = \deg q = d_n \geq \deg_t P$ since $\bar{q}(0) = 0$.
- Property 3: $2t-1 | q(t)$ by Proposition 1.
- Property 4: $\deg q = d_n$ is even
  - $[t^k]\bar{q} = 0$ if k is even; $[t^k]\bar{p} = 0$ if k is odd;
  - decompose the summation expression for P into odd and even indices.
- Property 5: For $A \subseteq [0,1]$ finite, $f(t) = \prod_{c \in A}(1 - 2\cos(c\pi)t)$, it holds that

$$1 + t | f(t) \iff f(-1) = 0 \iff \frac{2}{3} \in A.$$

Summary: Free Product of Cyclic and Dihedral Groups

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

The dihedral factors are each generated by a rotation and a flip.

$l = 0$ (all cyclic)	$k = 1$	Bell-Mishna
	$k = 2$	Theorem 8
	$k \geq 3$	Theorem 9
$k = 0$ (all dihedral)	$l = 1, s_1 = 1$	Proposition 1
	$l = 1, s_1 > 1$	Proposition 10; Theorem 11
	$l \geq 2$	Difficult: Not yet known
$l > 0, k > 0$	?	

Identical Finite Factors

Proposition 10 generalizes to any finite group

Identical Finite Factors

Proposition 10 generalizes to any finite group

Theorem 12 (Liu)

Suppose H is finite with generating set $T \subseteq H$. Let $G := H^{*m} \simeq H_1 * H_2 * \ldots * H_m$ with each $H_i \simeq H$ via an isomorphism $\phi_i : H \to H_i$. Consider $S := \cup_{i=1}^{m} \phi_i(T)$ which generates G. Write the cogrowth GF $F_{H;T}(t) = \frac{p(t)}{q(t)}$ with $p(0)q(0) \neq 0$. Let $M := \max\{\deg p + \delta_p, \deg q + \delta_q\}$, $\delta_p := \max\{0, \deg q - 1 - \deg p\}$, $\delta_q := \max\{0, \deg p + 1 - \deg q\}$. Then $F(t) := F_{G;S}(t)$ satisfies $P(t,z) \in \mathbb{Z}[t,z] \setminus \{0\}$ such that

1. $\deg_t P \leq M + 1$ *and* $\deg_z P \leq M + 1$;
2. *if* $\delta_q > 0$, *then* $\deg_t P \leq M$;
3. *if* $\deg p + \delta_p < \deg q + \delta_q$, *then* $\deg_t P \leq M$ *and* $\deg_z P \leq M$;
4. *if* $\delta_q > 0$ *and* $\deg p + \delta_p < \deg q + \delta_q$, *then* $\deg_t P \leq M - 1$.

General Approach to Finding Satisfying Polynomials

Given a group G and a generating set S, to construct $P(t, z)$,

- Find bounds on $\deg_t P \leq d_t$ and $\deg_z P \leq d_z$.
- Generate sufficiently many first few terms of the cogrowth GF $F_{G;S}(t)$.
- Solve a linear system for the $(d_t + 1)(d_z + 1)$ undetermined coefficients that defines $P(t, z)$.

Conclusion

- Free products of finitely many finite groups have algebraic cogrowth GFs.
- Free probability provides a useful tool for bounding degrees of satisfying polynomials.
- Degrees of minimal polynomials do not (in general) depend on the number of identical free factors.

Conclusion

- Free products of finitely many finite groups have algebraic cogrowth GFs.
- Free probability provides a useful tool for bounding degrees of satisfying polynomials.
- Degrees of minimal polynomials do not (in general) depend on the number of identical free factors.

Possible Next Steps

- Involve other classes of finite groups.
- Experiment with other generating sets.
- Bound degrees using ideal elimination and Gröbner bases.
- Obtain results on radii of convergence of the cogrowth GFs.

Thank you for listening!
Questions?

References

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

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

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

[4] Haggai Liu. On the cogrowth series of free products of finite groups. Master's thesis, Simon Fraser University, 2021.

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

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