UNIVERSITY OF CALIFORNIA
Los Angeles

Computational Complexity in Combinatorics and Algebra

A dissertation submitted in partial satisfaction
of the requirements for the degree
Doctor of Philosophy in Mathematics

by

David Soukup

2024

ABSTRACT OF THE DISSERTATION

Computational Complexity in Combinatorics and Algebra

by

David Soukup
Doctor of Philosophy in Mathematics
University of California, Los Angeles, 2024
Professor Igor Pak, Chair

We present a series of results on the theme of using computational complexity to analyze combinatorial objects with algebraic significance.

Chapter 1 concerns the cogrowth sequence of nilpotent groups. We prove that congruences of such sequences are undecidable in general. We then show that related problems in analytic combinatorics are uncomputable as well. This is done by constructing matrices of size $\leq 10^{86}$ which create a *universal Turing machine*.

In Chapter 2 we present negative results to versions of questions posed by Sergey Fomin on quiver mutation equivalence. We do this by embedding versions of classic computationally difficult problems into quivers. Finally, we give a quick characterization of mutation classes of quivers with two mutable vertices as a contrast.

Chapters 3 and 4 are centered around the use of involutions to count posets. We give tight bounds for the number of posets of height 2 with an odd number of linear extensions, shedding new light on a conjecture of Chan and Pak. Then, we give a combinatorial interpretation (and corresponding positivity result) of area generating functions of partitions evaluated at -1.

The dissertation of David Soukup is approved.

Tim Austin

Artem Chernikov

Pavel Galashin

Igor Pak, Committee Chair

University of California, Los Angeles

2024

Past and Future of the Dog License

Прошедшее и будущее собачьего налога

Vergangenheit und Zukunft der Hundessteuer

[Che87]

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

Obviously, this dissertation would never have been finished without the generous mentorship and guidance of my advisor, Igor Pak. He was a wonderful teacher of reading, writing, speaking on, and *doing* math.

I would also like to thank my family for their love and support over the years.

I am also grateful for the support of the greater UCLA mathematical community, including Aaron Anderson, Mohit Bansil, Raymond Chu, Pavel Galashin, Nikita Gladkov, James Leng, Greta Panova, Daniel Raban, J.R., the members of Frobenius Monk and Poincare Disk, and many others.

Several chapters of this dissertation have appeared in other places:

Chapter 1 is a version of [PS1], which is joint with Igor Pak.

Chapter 2 is a version of [Sou1].

Chapter 3 is a version of [Sou2].

I am also grateful for the support of UCLA's Dissertation Year Fellowship for 2023-2024.

VITA

2014	B.S. with Honors (Mathematics), University of Rochester, Rochester, New York.
2018-2023	Teaching Assistant, Mathematics Dept., UCLA
2019	M.A. in Mathematics, UCLA, Los Angeles, California.
2022	C. Phil. in Mathematics, UCLA, Los Angeles, California.

PUBLICATIONS

Complexity of sign imbalance, parity of linear extensions, and height 2 posets, preprint (2023).

Complexity of Ice Quiver Mutation Equivalence, accepted, *Annals of Combinatorics*.

(with Igor Pak) Algebraic and arithmetic properties of the cogrowth sequence of nilpotent groups, preprint (2022).

Embeddings of weighted graphs in Erdos-type settings, *Mosc. J. Comb. Number Theory* **8**(2), 2019.

(With Mike Desgrottes, Steven Senger, and Renjun Zhu) A general framework for studying finite rainbow configurations, *Springer Proc. Math. Stat.* **297**, 2020.

Part I

Cogrowth

CHAPTER 1

Algebraic and arithmetic properties of the cogrowth sequence of nilpotent groups

1.1 Introduction

On a fundamental level, the *growth* and *cogrowth sequences* are used to extract global properties of finitely generated groups from a local information. Although many problems remain unresolved, the *asymptotic approach* to both sequences has led to a number of spectacular advances (see below).

The *algebraic approach* to growth and cogrowth sequences is usually stated in terms of their generating functions (GF). Do they satisfy an algebraic equation? What about a differential-algebraic equation? Given that both sequences are sensitive with respect to the change in the generating sets, one might not think there is much to this problem, and yet there is a plethora of positive results and some notable negative results in this direction (see below).

In this paper we present an arithmetic approach to the cogrowth sequences of nilpotent groups as a means to obtain negative results for their algebraic properties. We first state the main results and historical remarks. We postpone the applications until Section 1.3.

1.1.1 Main results

Let G be a fixed finitely generated group, and let $\mathcal{S} = \mathcal{S}^{-1}$ be a symmetric generating set $\langle \mathcal{S} \rangle = G$. Denote by

$$\operatorname{cog}_{\mathcal{S}}(n) := \big|\big\{(s_1, \ldots, s_n) \in \mathcal{S}^n \,:\, s_1 \cdots s_n = 1\big\}\big|.$$

the number of products of generators equal to one. The sequence $\{\operatorname{cog}_{\mathcal{S}}(n)\}$ is called the *cogrowth sequence*. It can be viewed as the number of closed walks of length n in the *Cayley graph* $\Gamma(G, \mathcal{S})$. The *unitriangular group* $\mathrm{UT}(m, \mathbb{Z})$ is the (nilpotent) group of $m \times m$ upper triangular matrices with 1's on the diagonal.

Theorem 1.1.1 (Main theorem)**.** *There exist integers $m \geq 3$, $a \geq 1$, and a prime p, such that the following problem is undecidable: Given symmetric generating sets $\mathcal{S}, \mathcal{T}$ in $\mathrm{UT}(m, \mathbb{Z})$, determine whether*

$$\forall n \in \mathbb{N} \;:\; \operatorname{cog}_{\mathcal{S}}(n) \equiv \operatorname{cog}_{\mathcal{T}}(n) \mod p^a.$$

Moreover, the result holds for $p = 2$, $a = 40$, and some $m \leq 9.6 \cdot 10^{85}$.

This is a rare undecidable problem for the relatively tame class of nilpotent groups. The proof uses a technical yet explicit embedding of general Diophantine equations into the cogrowth. Solvability of Diophantine equations is famously undecidable by the negative solution of *Hilbert's 10th problem* (the Matiyasevich, Robinson, Davis and Putnam theorem), see e.g. [Mat1].

Our main theorem should be compared with the following result:

Theorem 1.1.2. *Let $a \geq 1$ be an integer, let p be a prime, and let G be a finitely generated abelian group. The following problem is decidable: Given finite symmetric generating sets $\mathcal{S}, \mathcal{T}$ in G, determine whether*

$$\forall n \in \mathbb{N} \;:\; \operatorname{cog}_{\mathcal{S}}(n) \equiv \operatorname{cog}_{\mathcal{T}}(n) \mod p^a.$$

This result is derived from a remarkable theorem of Adamczewski and Bell [AB], which in turn extends a series of results by Furstenberg [Fur], Deligne [Del], Denef and Lipshitz [DL], on diagonals of rational functions modulo prime powers. Our own motivation for the main theorem comes from the opposite direction, and can be stated as follows.

The *cogrowth series* for the group $G = \langle \mathcal{S} \rangle$ is defined as

$$\operatorname{Cog}_{\mathcal{S}}(t) \ := \ 1 \ + \ \sum_{n=1}^{\infty} \operatorname{cog}_{\mathcal{S}}(n) t^n.$$

Let

$$B(x_1, \ldots, x_k) \ = \sum_{(n_1,\ldots,n_k) \in \mathbb{N}^k} b(n_1, \ldots, n_k)\, x_1^{n_1} \cdots x_1^{n_k} \ \in \ \mathbb{Z}[[x_1, \ldots, x_k]]$$

be a multivariate generating function. The *diagonal* of B is defined as $\sum_{n \geq 0} b(n, \ldots, n) t^n$.

Theorem 1.1.3. *For a fixed sufficiently large integer $m \geq 0$, the following problem is not computable: Given a symmetric generating set $\mathcal{S}$ of the unitriangular group $\mathrm{UT}(m, \mathbb{Z})$, write the cogrowth series $\operatorname{Cog}_{\mathcal{S}}(t)$ as a diagonal of a rational function P/Q, for some polynomials $P, Q \in \mathbb{Z}[x_1, \ldots, x_k]$, and $k \geq 1$. Moreover, the result holds for some $m \leq 9.6 \cdot 10^{85}$.*

In other words, either some cogrowth series are not diagonal, or all of them are diagonals, but the proof of that result would be ineffective to make the diagonals uncomputable. Let us mention a quick motivation for this problem (see more on this below).

Kontsevich's question, for the case of nilpotent groups (see below), asks whether the cogrowth series $\operatorname{Cog}_{\mathcal{S}}(t)$ is always *D-finite*, i.e. a solution of an ODE with polynomial coefficients. Christol's Conjecture 1.3.1 (see below), reduces the problem to whether $\operatorname{Cog}_{\mathcal{S}}(t)$ is always a diagonal of a rational function. Until Theorem 1.1.3, no progress has been made in this direction.

Remark 1.1.4. *Let us further discuss our Theorem 1.1.3 in context of Kontsevich's question. First, it is possible and even likely, that already for the* Heisenberg group $\mathrm{UT}(3, \mathbb{Z})$ *with four standard generators, the cogrowth series is not a diagonal (and non-D-finite), see §1.6.3. It*

is also possible and even likely, that for all $m \geq 3$, *and* all *symmetric generating sets* $\mathcal{S}$ *of* $\mathrm{UT}(m, \mathbb{Z})$, *the cogrowth series is not a diagonal. Theorem 1.1.3 gives no contradiction with that.*

On the other hand, it is possible that for some $\mathcal{S}$ *the cogrowth series is a diagonal. It is also possible that* for all $\mathcal{S}$ *the cogrowth series is a diagonal. What Theorem 1.1.3 shows is that there is no* constructive proof *that the cogrowth series is always a diagonal.*

1.1.2 Historical background

Here we give a very brief overview of the vast literature on the subject.

(1) The growth of groups goes back to the works of Schwarz (1955) and Milnor (1968), and is now a staple of Geometric Group Theory [Har2]. Notably, all nonamenable groups have exponential growth, but not vice versa. *Gromov's theorem* proves that the growth is polynomial if and only if the group is virtually nilpotent. We refer to [Har1, Ch. VI,VII] for an extensive introduction, and to [Mann] for a detailed treatment.

In probabilistic context, the cogrowth was first introduced by Pólya [Pól], to study transience and recurrence of random walks in $\mathbb{Z}^d$, via asymptotic estimates on the *return probability* $\mathrm{cog}_{\mathcal{S}}(n)/|\mathcal{S}|^n$, and later by Kesten [Kes] in connection with *amenability*. In Group Theory, the study of cogrowth was initiated by Grigorchuk [Gri] and extended by Cohen [Coh] and others. We refer to [Woe] for a comprehensive presentation of both group theoretic and probabilistic results.

(2) The generating function (GF) approach became popular after the *Golod–Shafarevich theorem* on the growth of algebras [Ufn, §3.5]. In a remarkable development, the *growth series* (the GF for the growth sequence) is shown to be rational for every generating set of many classes of groups, including virtually abelian [Ben] and hyperbolic [Can].

For other classes of groups, growth series can be more complicated. Notably, there are

wreath products of abelian groups for which growth series are algebraic but not rational [Par]. For the fundamental group of a 3-dimensional $\mathrm{PSL}(2,\mathbb{R})$-manifold, which is a $\mathbb{Z}$-extension of a hyperbolic group, the growth series is rational for one generating set and non-algebraic for another [Sha]. It is known (see e.g. [GP3]) that the growth series is non-algebraic (in fact, non-D-finite), for all groups of intermediate growth. See [GH, §4] for further examples and many references.

For nilpotent groups, the growth series is especially interesting. In a breakthrough paper [Sto], Stoll gave an example of a *higher Heisenberg group* $H_5 \subset \mathrm{UT}(4,\mathbb{Z})$ and two generating sets so that one growth series is rational while another is non-algebraic. Curiously, for the (usual) Heisenberg group $H_3 = \mathrm{UT}(3,\mathbb{Z})$, the growth series is always rational [DS].

(3) After Pólya's work, *lattice walks* on $\mathbb{Z}^d$ have been intensely studied for various generating sets $\mathcal{S}$ (called *steps*). The corresponding return probabilities are always diagonals of rational functions, but this stops being true when geometric constraints are added. These walks continue to be intensely studied in Enumerative and Asymptotic Combinatorics, see e.g. [Bou, Mis].

For free groups F_k, the cogrowth series are always algebraic. This was shown independently in [Hai] in a combinatorial context, and in [Aom, FTS] in a probabilistic context. The cogrowth series is algebraic for many free products of groups [BM, Kuk2], and D-finite for Baumslag–Solitar groups $\mathrm{BS}(N,N)$ [ERRW].

In recent years, the interest to the problem came from Kontsevich's question whether the cogrowth series is always D-finite on linear groups, see [Sta2]. By the *Tits alternative* and the *Milnor–Wolf theorem*, Kontsevich's question is reduced to three cases: virtually nilpotent groups, virtually solvable groups of exponential growth, and groups containing free group F_2 as a subgroup. Our state of knowledge is very different in these three cases.

For solvable groups the question was resolved in the negative in [GP3] by the following argument. Let G be a solvable group of exponential growth and bounded Prüfer rank. It

was proved by Pittet and Saloff-Coste in [PS2], that for every symmetric generating set $\mathcal{S}$, the cogrowth satisfies

$$|\mathcal{S}|^n e^{-\alpha n^{1/3}} \le \operatorname{cog}_{\mathcal{S}}(n) \le |\mathcal{S}|^n e^{-\beta n^{1/3}}.$$

The *Birkhoff–Trjitzinsky theorem*[1] then implies that the cogrowth series not D-finite [GP3]. An easy example of such group is $\mathbb{Z} \ltimes \mathbb{Z}^2 \subset \mathrm{SL}(3,\mathbb{Z})$, see e.g. [Woe, §15.B]. In response to a solution in [GP3], Katzarkov, Kontsevich and Stanley independently asked if the cogrowth series is always D-algebraic.[2] This strengthening of Kontsevich's question remains unresolved.

In fact, the bounded Prüfer rank assumption above is not necessary for the conclusion. Recently, Bell and Mishna used an analytic argument [BM] to show that, for all amenable groups of superpolynomial growth, the cogrowth series is non-D-finite, resolving the conjecture in [GP3] and completing this case of Kontsevich's question.

For nilpotent groups, the subject of this paper, the *Bass–Guivarc'h formula* computes the polynomial degree $d(G)$ of the growth sequence. Several notable probabilistic results can be combined to give the following asymptotics

$$C_1 |\mathcal{S}|^n n^{-d(G)/2} \le \operatorname{cog}_{\mathcal{S}}(n) \le C_2 |\mathcal{S}|^n n^{-d(G)/2},$$

see [Woe, §3.B,§15.B] and references therein. Now *Jungen's theorem* [Jun], implies that the cogrowth series is not algebraic for even $d(G)$. For odd $d(G) \ge 5$, only a weaker result is known, that the cogrowth series is not $\mathbb{R}_+$-algebraic; this follows from [BD, Thm 3]. At this point the analytic arguments lose their power as there are numerous examples of D-finite and even algebraic GFs with the same asymptotics as the cogrowth sequences, see e.g. [BD, FS].

(4) *Hilbert's 10th problem* was resolved by Matiyasevich (1970) building on the earlier work by Davis, Putnam and Robinson (1949–1969). Solvability of Diophantine equations over

[1] There are gaps in the proof of this result and it remains an open problem in full generality, see a discussion in [FS, §VIII.7] and [Odl, §9.2]. For integral sequences which grow at most exponentially, the gaps were filled in a series of paper, see [GP3, §5.1].

[2] Personal communication, 2015.

various rings is now fundamental in both Logic and Number Theory, and applied throughout mathematical sciences, from Group Theory to Integral Programming. We refer to [Mat1] for a thorough treatment, to [Poo1] for a short note introduction to recent developments, and to [MF] for an introductory textbook.

(5) The study of classes of GFs was initially motivated by applications in Number Theory and Analysis, but came to prominence in connection to Formal Languages Theory. The GF for the number of accepted paths by a *Finite State Automaton* is always rational (see e.g. [Sta1, §4.7]), and algebraic for a *Pushdown Automaton* (see references in [BD]).

The class of diagonals of rational functions coincides with the class of GFs for (balanced) *binomial sums*, see [BLS, Gar]. This class received much attention after the work of Wilf and Zeilberger on binomial identities [WZ, Zei], which made heavy use of the fact that they are D-finite (*holonomic* in their terminology).

Finding an explicit presentation of a GF as a diagonal of a rational function is of great interest in Computer Algebra due to its many applications, see e.g. [BLS, Mel]. These range from congruences of combinatorial sequences, see [AB, RY], to asymptotic analysis, see [BMPS, MS]. We should note that there can be more than one way a function can be presented as diagonal, see e.g. [RY]. On the other hand, for many series finding its presentation as a diagonal is a challenging open problem, see §1.6.6. Our Theorem 1.1.3 proving uncomputability of such presentation is the first negative result in this direction.

Proving that a series is not D-finite (not D-algebraic) is a major challenge, of interest both in Enumerative Combinatorics [Pak] and Differential Algebra [ADH]. Outside of analytic arguments, an Automata Theory approach was developed in [GP2], which proves non-D-finiteness for GFs of various permutation classes. In the context of cogrowth series, [GP3] uses this approach to prove non-D-finiteness in the (less interesting) case of *non-symmetric* generating sets of nonamenable groups.

(6) The undecidability approach to algebraic properties of cogrowth series appears to be new.

It is also surprising, since both the word, the conjugacy and even the isomorphism problems are decidable for finite nilpotent groups [GS] (see also discussion in [Sap, §3.2]). On the other hand, the solvability of a *system of equations* is undecidable for $H_3 = \mathrm{UT}(3, \mathbb{Z})$ [DLS, GMO], as well group membership in the product of cyclic subgroups of $\mathrm{UT}(m, \mathbb{Z})$ [Loh]. The proofs of these results are similarly based on Hilbert's 10th problem, cf. §1.6.3.

1.1.3 Paper structure

After a few notation in Section 1.2, we start with a technology of generating functions in Section 1.3. There, we give quick proofs of Theorem 1.1.2 from the Adamczewski–Bell theorem (Theorem 1.3.3), and of Theorem 1.1.3 from the Main Theorem 1.1.1. There, we also formulate Theorem 1.3.5 on a possible non-D-algebraic cogrowth series for $\mathrm{UT}(m, \mathbb{Z})$. We then prove Main Theorem 1.1.1 in a lengthy Section 1.4. The proof of Theorem 1.3.5 is given in Section 1.5. We conclude with final remarks and open problems in Section 1.6.

1.2 Notation

We use the convention that **bold** letters represent multi-indices, e.g. $\boldsymbol{x} = (x_1, \ldots, x_k) \in \mathbb{Z}^k$. We use $|\boldsymbol{x}| := |x_1| + \ldots + |x_k|$ to denote the ℓ^1 norm of $\boldsymbol{x}$.

For vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^k$, denote

$$\binom{\boldsymbol{a}}{\boldsymbol{b}} := \binom{a_1}{b_1} \cdots \binom{a_k}{b_k}. \tag{1.1}$$

The unipotent group $\mathrm{UT}(m, \mathbb{Z})$ is the group of all $m \times m$ upper-triangular integer matrices

with ones on the diagonal:

$$\begin{bmatrix} 1 & \mathbb{Z} & \mathbb{Z} & \cdots & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} & \cdots & \mathbb{Z} & \mathbb{Z} \\ 0 & 0 & 1 & \cdots & \mathbb{Z} & \mathbb{Z} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \mathbb{Z} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

Since we will be working with many families of indexed matrices, we will adopt the convention that $[A]_{ij}$ refers to the (i,j)-th entry of matrix A. Let I_n be the $n \times n$ identity matrix, and $E_{i,j}$ be the matrix that is 1 in the (i,j)-th coordinate and 0 otherwise.

When working with matrices, we write XY to denote the product of matrices X and Y. We use $X \circ Y$ to denote the word with matrices as letters. Lastly, we use $\oplus$ for the operation of making a block-diagonal matrix out of smaller matrices:

$$X \oplus Y := \begin{bmatrix} X & 0 \\ 0 & Y \end{bmatrix}.$$

We use $X \oplus^k Y$ to mean that Y is added k times: $X \oplus Y \oplus \cdots \oplus Y$. Finally, a word $(s_1 \cdots s_n)$ in the generators $s_i \in \mathcal{S}$, is called a *cogrowth word*, if the product $s_1 \cdots s_n = 1$.

1.3 Cogrowth series

1.3.1 Classes of generating functions

Let $\{a_n\}$ be an integer sequence, and let

$$A(t) := \sum_{n=0}^{\infty} a_n t^n \in \mathbb{Z}[[t]]$$

be the corresponding *generating function* (GF). We write $a_n = [t^n]A$ to denote the coefficient of the GF. For a multivariate GF $B \in \mathbb{Z}[[x_1, \ldots, x_k]]$, the *diagonal* of B is defined as

$$\operatorname{diag} B \,:=\, \sum_{n=0}^{\infty} \big(\big[x_1^n \cdots x_k^n\big]\, B\big) t^n \,\in\, \mathbb{Z}[[t]],$$

the GF for diagonal coefficients of B.

For $A \in \mathbb{Z}[[t]]$, we define the following five main classes of GFs, see e.g. [Sta1, Ch. 6]:

Rational:	$A(t) = P(t)/Q(t)$, for some $P, Q \in \mathbb{Z}[t]$,
Algebraic:	$c_0 A^k + c_1 A^{k-1} + \ldots + c_k = 0$, for some $k \in \mathbb{N}$, $c_i \in \mathbb{Z}[t]$,
Diagonal:	$A(t) = \operatorname{diag} P/Q$, for some $P, Q \in \mathbb{Z}[x_1, \ldots, x_k]$, $k \geq 1$,
D-finite:	$c_0 A + c_1 A' + \ldots + c_k A^{(k)}$, for some $k \in \mathbb{N}$, $c_i \in \mathbb{Z}[t]$,
D-algebraic:	$Q\big(t, A, A, \ldots, A^{(k)}\big) = 0$, for some $k \in \mathbb{N}$, $Q \in \mathbb{Z}[t, x_0, x_1, \ldots, x_k]$.

It is well known and easy to see that

$$\textit{Rational} \,\subsetneq\, \textit{Algebraic} \,\subsetneq\, \textit{Diagonal} \,\subsetneq\, \textit{D-finite} \,\subsetneq\, \textit{D-algebraic}$$

It is known that the cogrowth series $\operatorname{Cog}_{\mathcal{S}}(t) \in \textit{Rational}$ if and only if G is finite [Kuk1]. For example, for $G = \mathbb{Z}$ and $\mathcal{S} = \{\pm 1\}$, we have:

$$\operatorname{Cog}_{\mathcal{S}}(t) \,=\, \sum_{n=0}^{\infty} \tbinom{2n}{n} t^{2n} \,=\, \operatorname{diag} \frac{1}{1-x-y} \,=\, \frac{1}{\sqrt{1-4t^2}} \,\in\, \textit{Algebraic}\,.$$

For $G = \mathbb{Z}^2$ and $\mathcal{S} = \{(\pm 1, 0), (0, \pm 1)\}$, the cogrowth series $\operatorname{Cog}_{\mathcal{S}}(t) = \sum_{n \geq 0} \binom{2n}{n}^2 t^{2n}$ is diagonal but not algebraic.[3] Diagonal GFs have coefficients which grow at most exponentially, so $\sum_{n \geq 0} n! t^n$ is D-finite but not a diagonal. *Christol's Conjecture* claims that this is the only restriction:

[3] This was observed by Furstenberg [Fur] via Schneider's theorem on transcendental numbers. As noted in [Mel, p. 137], this is also immediate from $\binom{2n}{n}^2 \sim \frac{1}{\pi n} 16^n$. Jungen's theorem can be used to show that the cogrowth series is non-algebraic *for all* generating sets of $\mathbb{Z}^2$.

Conjecture 1.3.1 (Christol [Chr1]). *Let* $A(t) = \sum_{n\geq 0} a_n t^n \in \mathbb{Z}[[t]]$. *Let* $|a_n| < c^n$ *for all* $n \in \mathbb{N}$ *and some* $c > 0$, *and let* $A \in$ *D-finite. Then* $A \in$ *Diagonal.*

Note that *Euler's partition function*

$$P(t) \,:=\, 1 + \sum_{n=1}^{\infty} p(n) t^n \,=\, \prod_{i=1}^{\infty} \frac{1}{1-t^i} \;\in\; \textit{D-algebraic},$$

see [MC]. See also an explicit algebraic differential equation in [Pak, §2.5]. Since $p(n) = e^{O(\sqrt{n})}$, it follows that $P(t) \notin$ *D-finite*. In particular, Christol's Conjecture does not extend to D-algebraic GFs.

1.3.2 Proofs of Theorems 1.1.2 and 1.1.3

We start with the following two results.

Theorem 1.3.2 (Kuksov [Kuk2, §5.1]). *Let* G *be a finitely generated abelian group with a finite symmetric generating set* $\mathcal{S}$. *Then the cogrowth series* $\operatorname{Cog}_{\mathcal{S}}(t) \in$ *Diagonal.*

For $G = \mathbb{Z}^d$, this result is folklore, see e.g. [Mis, §3.1.4]. Note that Kuksov's formulation is different, but equivalent to ours.

Theorem 1.3.3 (Adamczewski–Bell [AB, Thm. 9.1(i)]). *Let* $C(t) = \sum_{n\geq 0} c_n t^n \in$ *Diagonal, let* p *be a prime, and let* $a \geq 1$, $b \geq 0$ *be integers. The following problem is decidable:*

$$\exists n \in \mathbb{N} \;:\; c_n \equiv b \mod p^a.$$

Theorems 1.1.2 and 1.1.3 now follows easily by a combination of these results and the Main Theorem 1.1.1.

Proof of Theorem 1.1.2. Note that the proof of Theorem 1.3.2 in [Kuk2, §5.1] is completely constructive, giving $\operatorname{Cog}_{\mathcal{S}} = \operatorname{diag} P_1/Q_1$ and $\operatorname{Cog}_{\mathcal{T}} = \operatorname{diag} P_2/Q_2$ for some explicit polynomials $P_1, P_2, Q_1, Q_2 \in \mathbb{Z}[x_1, \ldots, x_2]$. Let $C(t) = \sum_{n\geq 0} c_n t^n := \operatorname{diag}\big(P_1/Q_1 - P_2/Q_2\big)$. Apply

Theorem 1.3.3 to $C(t)$ with all possible $1 \le b < p^a$, to check if there is a solution for $b \not\equiv 0 \mod p^a$. If not, then we have $c_n \equiv 0 \mod p^a$ for all $n \in \mathbb{N}$, as desired. □

Proof of Theorem 1.1.3. Let $p = 2$, $a = 40$, and let $G = \mathrm{UT}(m, \mathbb{Z})$ be as in Theorem 1.1.1. Suppose every cogrowth series $\mathrm{Cog}_{\mathcal{S}}(t)$ is a diagonal of polynomials which are computable (given $\mathcal{S}$). Then the same holds for the difference: $\mathrm{Cog}_{\mathcal{S}}(t) - \mathrm{Cog}_{\mathcal{T}}(t) = \mathrm{diag}P/Q$, for every two symmetric generating sets $\mathcal{S}$ and $\mathcal{T}$ of G, and some computable multivariate polynomials P, Q. By Theorem 1.3.3, the congruence

$$\forall n \in \mathbb{N} \ : \ \mathrm{cog}_{\mathcal{S}}(n) \equiv \mathrm{cog}_{\mathcal{T}}(n) \mod 2^{40}$$

is decidable, a contradiction with Theorem 1.1.1. □

1.3.3 Non-D-algebraic cogrowth series

Ideally, one would want to give a construction of a non-D-algebraic cogrowth series of a unitriangular group. As an application of our tools we give such a construction assuming there is a Diophantine equation with certain properties.

Denote $\boldsymbol{x} = (x_1, \ldots, x_k)$, and let $f \in \mathbb{Z}[x_1, \ldots, x_k]$. Consider a Diophantine equation $f(\boldsymbol{x}) = 0$. Denote by $\mathcal{R}(f) := \{\boldsymbol{x} \in \mathbb{Z}^k \ : \ f(\boldsymbol{x}) = 0\}$ be the *set of roots*.

We say that f is *sparse* if all roots $\boldsymbol{x} \in \mathcal{R}(f)$ have distinct ℓ^1 norm: $|\boldsymbol{x}| \neq |\boldsymbol{y}|$ for all $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{R}(f)$. In this case we can assume that the roots of f are ordered according to the norm: $\mathcal{R}(f) = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots\}$, where $|\boldsymbol{r}_1| < |\boldsymbol{r}_2| < \ldots$ For a sparse f, we use $\rho_i := |\boldsymbol{r}_i|$.

Finally, for $z \in \mathbb{Z}$, let $\mathrm{bin}(z)$ denote the number of 1's in the binary expansion of $|z|$.

Conjecture 1.3.4. *There exists $k \in \mathbb{N}$ and a sparse $f \in \mathbb{Z}[x_1, \ldots, x_k]$ which satisfies:*

(1) *ρ_i is even for all $i \ge 1$,*

(2) $\rho_{i+1}/\rho_i \to \infty$ *as* $i \to \infty$,

(3) *for every integers* $a, b \geq 1$, *there exists* $i \geq 1$, *s.t.* $\rho_i/2 \equiv a \mod 2^b$,

(4) *for every integers* $a, b, h \geq 1$, *there exists some* $N = N(a, b, h) \geq 1$, *s.t. for all* $i > N$ *we have:*

$$\min\left\{ y \,:\, \mathrm{bin}(c\rho_i - y) \leq a \right\} \,\geq\, b\rho_{i-1} \quad \text{for all} \quad 1 \leq c \leq h.$$

Theorem 1.3.5. *Suppose Conjecture 1.3.4 holds. Then there exists an integer* $m \geq 1$ *and a symmetric generating set* $\mathcal{S}$ *of* $\mathrm{UT}(m, \mathbb{Z})$, *s.t. the cogrowth series* $\mathrm{Cog}_{\mathcal{S}}(t)$ *is not D-algebraic.*

We prove Theorem 1.3.5 in Section 1.5. The proof is based on the following result of independent interest. It also explains the nature of assumptions in the conjecture.

Lemma 1.3.6. *Let* $\{\lambda_n\} \in \mathbb{N}^\infty$ *be an integer sequence s.t.* $\lambda_0 = 1$. *Suppose there exists an increasing integer sequence* $\{n_1 < n_2 < \ldots\}$ *with the following properties:*

(1) λ_{n_i} *is odd for every* $i \in \mathbb{N}$,

(2) $n_{i+1}/n_i \to \infty$ *as* $i \to \infty$,

(3) *for every integers* $a, b \geq 1$, *there exists* $i \geq 1$, *s.t.* $n_i \equiv a \mod 2^b$,

(4) *for every* $C, D \geq 1$, *there exists* $N = N(C, D) > 0$, *s.t. for every* $i_1, \ldots, i_D > N$, *if*

$$n_{i_1} + \cdots + n_{i_D} - C \leq b_1 + \cdots + b_D \leq n_{i_1} + \cdots + n_{i_D}$$

for some nonnegative integers $b_1, \ldots, b_D$, *then either:*

- λ_{b_j} *is even for at least one* j.
- $\{b_1, \ldots, b_D\}$ *and* $\{n_1, \ldots, n_D\}$ *are equal up to rearrangement.*

Then the sequence $\{\lambda_n\}$ *is not D-algebraic.*

For example, the sequence $\{n_i = i! + i\}$ satisfies properties (2) and (3) above. Therefore, every integer sequence $\{\lambda_n\}$, where all λ_n are odd if and only if $n = i! + i$ for some i, is not D-algebraic.

More generally, every integer sequence $\{\lambda_n\}$, where λ_n is odd whenever $n = i! + i$, and even when n is not between $i! + i$ and $i! + 2i$ for some i, is also not D-algebraic. This is because we can take $n_i := i! + i$ and property (4) will still hold.

Remark 1.3.7. *If the sequence $\{n_1, n_2, \dots\}$ covers every index where a_n is odd, then condition* (4) *follows from condition* (3)*. This is because we could let N be large enough such that $n_i > Dn_{i-1}$ for all $i > N$. This case was previously considered by Garrabrant and the first author.*[4]

1.4 Proof of Theorem 1.1.1

The key idea in this proof will be to encode the existence of roots of an arbitrary Diophantine equation f into statements about cogrowth in $\mathrm{UT}(m, \mathbb{Z})$. We proceed as follows. In Lemma 1.4.1 we show that words of a particular structure can compute the value of f at integers. Then, in Lemmas 1.4.3 and 1.4.4 we extend our matrices so that this computation is true for a broader class of words.

Next, Lemmas 1.4.8 and 1.4.12 allows us to turn the question of Theorem 1.1.1 into a statement about the existence of integer roots of an arbitrary Diophantine equation. An explicit solution of Hilbert's 10th problem completes the proof.

1.4.1 Polynomials via matrix products

We start with the following key lemma.

[4] *Scott Garrabrant and Igor Pak, unpublished notes (2015).*

Lemma 1.4.1. *Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$ and let $D := \deg f$. Then there exists matrices $P, Q, A_1, \ldots, A_k \in \mathrm{UT}(m, \mathbb{Z})$ for some $m \leq (D+1)\binom{D+k}{k} + 2$, such that*

$$PAQA^{-1}P^{-1}AQ^{-1}A^{-1} \;=\; I_m \,+\, f(x_1, \ldots, x_k)\, E_{1m}$$

for all

$$A = A_1^{x_1} A_2^{x_2} \cdots A_k^{x_k} \qquad \textit{and} \qquad (x_1, \ldots, x_k) \in \mathbb{N}^k.$$

Proof. Denote $\boldsymbol{x} = (x_1, \ldots, x_k)$ and recall the multi-index notation (1.1). Write $f(\boldsymbol{x})$ in the binomial basis $\{\binom{\boldsymbol{x}}{\boldsymbol{d}} : \boldsymbol{d} \in \mathbb{N}^k\}$ as follows:

$$f(\boldsymbol{x}) \;=\; \sum_{|\boldsymbol{d}| \leq \mathrm{D}} b_{\boldsymbol{d}} \binom{\boldsymbol{x}}{\boldsymbol{d}} \qquad \text{for some} \qquad b_{\boldsymbol{d}} \in \mathbb{Z}, \;\; \boldsymbol{d} \in \mathbb{N}^k. \tag{1.2}$$

Let $p, q \geq 1$. Denote by J_q the $q \times q$ Jordan block with 1's on and above the diagonal. We have:

$$J_q \;=\; \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \qquad \text{and} \qquad \big(J_q\big)^p \;=\; \begin{bmatrix} 1 & \binom{p}{1} & \binom{p}{2} & \cdots & \binom{p}{q-2} & \binom{p}{q-1} \\ 0 & 1 & \binom{p}{1} & \cdots & \binom{p}{q-3} & \binom{p}{q-2} \\ 0 & 0 & 1 & \cdots & \binom{p}{q-3} & \binom{p}{q-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \binom{p}{1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}. \tag{1.3}$$

Now, for each $\boldsymbol{d} = (d_1, \ldots, d_k)$ in the sum in (1.2), define matrices $B_{\boldsymbol{d},i} \in \mathrm{UT}(|\boldsymbol{d}|+1, \mathbb{Z})$ as follows:

$$\begin{cases} B_{\boldsymbol{d},1} \;:=\; J_{d_1+1} \oplus I_{d_2 + \ldots + d_k} \\ B_{\boldsymbol{d},2} \;:=\; I_{d_1} \oplus J_{d_2+1} \oplus I_{d_3 + \ldots + d_k} \\ \qquad\quad \vdots \\ B_{\boldsymbol{d},k} \;:=\; I_{d_1 + \ldots + d_{k-1}} \oplus J_{d_k+1} \end{cases} \tag{1.4}$$

For example, if $\boldsymbol{d} = (2, 3, 0, 1)$ then

$$B_{\boldsymbol{d},1} = \begin{bmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} & 0 & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & 0 & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad B_{\boldsymbol{d},2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 0 \\ 0 & 0 & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & 0 \\ 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & 0 \\ 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$B_{\boldsymbol{d},3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad B_{\boldsymbol{d},4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} \\ 0 & 0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{1} \end{bmatrix}$$

Note that each of the $B_{\boldsymbol{d},i}$ contains one nontrivial Jordan block, highlighted in red above. In the case where $d_i = 0$, the Jordan block has size one. The block is located between indices $(d_1 + \ldots + d_{i-1} + 1)$ and $(d_1 + \ldots + d_i + 1)$. That means that the nontrivial block overlaps the nontrivial blocks of $B_{\boldsymbol{d},i-1}$ and $B_{\boldsymbol{d},i+1}$ in exactly one place.

Let $B_{\boldsymbol{d}} = B_{\boldsymbol{d},1}^{x_1} \cdots B_{\boldsymbol{d},k}^{x_k}$. Then the top-right entry of B is given by

$$\left[B_{\boldsymbol{d}}\right]_{1,|\boldsymbol{d}|+1} = \sum_{(j_1,\ldots,j_{k+1}) \,:\, j_1=1,\, j_{k+1}=|\boldsymbol{d}|+1} \left[B_{\boldsymbol{d},1}^{x_1}\right]_{j_1,j_2} \left[B_{\boldsymbol{d},2}^{x_2}\right]_{j_2,j_3} \cdots \left[B_{\boldsymbol{d},k}^{x_k}\right]_{j_k,j_{k+1}}. \tag{1.5}$$

We investigate which of the terms in the sum (1.5) survive. Since all the $B_{\boldsymbol{d},i}$ are upper triangular we can only have a nonzero term if $j_1 \leq j_2 \leq \cdots \leq j_{k+1}$. By the block structure of the $B_{\boldsymbol{d},i}$, the only way to have a nonzero term where $j_i < j_{i+1}$ is if j_i and j_{i+1} satisfy

$$d_1 + \ldots + d_{i-1} + 1 \;\leq\; j_i \;<\; j_{i+1} \;\leq\; d_1 + \ldots + d_i + 1.$$

Therefore, there is only one nonzero term in the sum (1.5), given by $j_i = d_1 + \ldots + d_{i-1} + 1$, for all i. This term is the product of the top-right entries of all the nontrivial Jordan blocks in $B_{\boldsymbol{d},1}$ to $B_{\boldsymbol{d},k}$. By (1.3), this gives

$$[B_{\boldsymbol{d}}]_{1,|\boldsymbol{d}|+1} \;=\; \left[J^{x_1}_{d_1+1}\right]_{1,d_1+1} \cdots \left[J^{x_k}_{d_k+1}\right]_{1,d_k+1} \;=\; \tbinom{x_1}{d_1+1-1} \cdots \tbinom{x_k}{d_k+1-1} \;=\; \tbinom{\boldsymbol{x}}{\boldsymbol{d}}. \tag{1.6}$$

Now we need to arrange these parts to create f. For each i, define

$$A_i \;:=\; I_1 \oplus \left[\bigoplus_{|\boldsymbol{d}|\le \mathrm{D}} B_{\boldsymbol{d},i}\right] \oplus I_1\,.$$

Let m be the size of A_i. For each $|\boldsymbol{d}| \le \mathrm{D}$, let $(\alpha_{\boldsymbol{d}}, \beta_{\boldsymbol{d}})$ be the coordinates of the top-right entry of the block in A_i coming from $B_{\boldsymbol{d},i}$. Then we can define

$$P \;:=\; I_m \;+\; \sum_{|\boldsymbol{d}|\le \mathrm{D}} E_{1,\alpha_{\boldsymbol{d}}} \quad \text{and} \quad Q \;:=\; I_m \;+\; \sum_{|\boldsymbol{d}|\le \mathrm{D}} b_{\boldsymbol{d}}\, E_{\beta_{\boldsymbol{d}},m}\,,$$

where the $b_{\boldsymbol{d}}$ are the coefficients defined in (1.2). The top-right corner of PAQ is

$$[PAQ]_{1,m} \;=\; \sum_{1\le j_1,j_2\le m} [P]_{1j_1}\,[A]_{j_1j_2}\,[Q]_{j_2m} \;=\; \sum_{\boldsymbol{d}_1,\boldsymbol{d}_2} [A]_{\alpha_{\boldsymbol{d}_1}\beta_{\boldsymbol{d}_2}}\, b_{\boldsymbol{d}_2}\,.$$

But since the A_i's were defined as block matrices, the only way for $[A]_{\alpha_{\boldsymbol{d}_1},\beta_{\boldsymbol{d}_2}}$ to be nonzero is if $\boldsymbol{d}_1 = \boldsymbol{d}_2$. Thus, using (1.6) this becomes

$$[PAQ]_{1,m} \;=\; \sum_{\boldsymbol{d}} [A]_{\alpha_{\boldsymbol{d}},\beta_{\boldsymbol{d}}}\, b_{\boldsymbol{d}} \;=\; \sum_{\boldsymbol{d}} [B_{\boldsymbol{d}}]_{1,|\boldsymbol{d}|+1}\, b_{\boldsymbol{d}} \;=\; \sum_{\boldsymbol{d}} b_{\boldsymbol{d}} \binom{\boldsymbol{x}}{\boldsymbol{d}} \;=\; f(\boldsymbol{x}). \tag{1.7}$$

Now that we have a $f(\boldsymbol{x})$ in the top-right corner, we need to make all the entries between this corner and the diagonal zero. Let $M = PAQA^{-1}$. Then we investigate its entries $[M]_{ij}$. Recall that

$$[M]_{ij} \;=\; \sum_{i\le m_1\le m_2\le m_3\le j} [P]_{i,m_1}\,[A]_{m_1,m_2}\,[Q]_{m_2,m_3}\,[A^{-1}]_{m_3,j}$$

and that the only above-diagonal nonzero entries of P are on the top row, of Q are in the right column, and of A are in neither the top row or right column.

We have the following cases:

- If $i = j$, then $[M]_{i,j} = 1$ because $M \in \mathrm{UT}(m, \mathbb{Z})$.
- If $i > j$, then $[M]_{i,j} = 0$, analogously.
- If $1 < i < j < m$, then we are above the diagonal of but not along the top or right edge of the matrix. Here the only terms in (1.4.1), such that $[P]_{i,m_1} \neq 0$ will be those where $m_1 = i$. Likewise we must have $m_2 = m_3$, since $m_3 < m$. Thus, we can ignore P and Q in the product, and conclude $[M]_{ij} = [AA^{-1}]_{ij} = 0$.
- If $1 = i < j < m$, then we are on the top row of the matrix but not in the corner. Again we can ignore Q because $m_3 < m$. So $[M]_{i,j} = [PAA^{-1}]_{ij} = [P]_{ij}$.
- If $1 = i < j = m$, then we are in the top-right corner of the matrix. Here A^{-1} cannot contribute to the sum, since $[A^{-1}]_{m_3,m}$ is nonzero only when $m_3 = m$. Thus, $[M]_{1,m} = [PAQ]_{1,m} = f(\boldsymbol{x})$ by (1.7).

To summarize, M is of the form

$$M = \begin{bmatrix} 1 & [P]_{1,2} & [P]_{1,3} & [P]_{1,4} & \cdots & [P]_{1,m-1} & f(\boldsymbol{x}) \\ 0 & 1 & 0 & 0 & \cdots & 0 & \xi_1(\boldsymbol{x}) \\ 0 & 0 & 1 & 0 & \cdots & 0 & \xi_2(\boldsymbol{x}) \\ 0 & 0 & 0 & 1 & \cdots & 0 & \xi_3(\boldsymbol{x}) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \tag{1.8}$$

where the $\xi_i(\boldsymbol{x})$ denote some polynomials.

Note that P is nonzero only in the first row and zero in the top-right corner. Thus, the

same holds for P^{-1}. Therefore, we can right-multiply (1.8) by P^{-1} to get

$$MP^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & f(\boldsymbol{x}) \\ 0 & 1 & 0 & 0 & \cdots & \xi_1(\boldsymbol{x}) \\ 0 & 0 & 1 & 0 & \cdots & \xi_2(\boldsymbol{x}) \\ 0 & 0 & 0 & 1 & \cdots & \xi_3(\boldsymbol{x}) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}. \tag{1.9}$$

Similarly, $P^{-1}M$ must be equal to M except possibly in the first row. But $P^{-1}M = AQA^{-1}$ is the product of three matrices whose first rows are trivial. Thus, $P^{-1}M$ must also be trivial in the first row. We conclude:

$$P^{-1}M = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & \xi_1(\boldsymbol{x}) \\ 0 & 0 & 1 & 0 & \cdots & \xi_2(\boldsymbol{x}) \\ 0 & 0 & 0 & 1 & \cdots & \xi_3(\boldsymbol{x}) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}. \tag{1.10}$$

Combining (1.9) and (1.10), we get

$$\begin{aligned} PAQA^{-1}P^{-1}AQ^{-1}A^{-1} &= \left(PAQA^{-1}P^{-1}\right)\left(AQ^{-1}A^{-1}\right)^{-1} \\ &= MP^{-1}\left(P^{-1}M\right)^{-1} = I_m + f(\boldsymbol{x}), \end{aligned}$$

as desired.

We now consider the size of m. There are exactly $\binom{\mathrm{D}+k}{k}$ possible multi-indices $\boldsymbol{d}$ with $|\boldsymbol{d}| \leq \mathrm{D}$. Each of these contributes at most $(\mathrm{D}+1)$ to the size of A_i, and we get an additional 1 from each I_1. This gives $m \leq (\mathrm{D}+1)\binom{\mathrm{D}+k}{k} + 2$. □

Corollary 1.4.2. *A word of the form*

$$PW_1QW_2P^{-1}W_3Q^{-1}W_4 \qquad \textit{where} \qquad W_1 = W_2^{-1} = W_3 = W_4^{-1} = A_1^{x_1}\cdots A_k^{x_k}$$

is a cogrowth word if and only if $\boldsymbol{x} = (x_1, \ldots, x_k)$ *is a root of* f.

1.4.2 Larger families of words

We now have the tools to evaluate Diophantine equations, but in order to be able to eliminate extraneous words, we will need to extend the matrices defined in Lemma 1.4.1 to new matrices. Therefore the next lemmas will reduce the problem to Corollary 1.4.2. Note that we will continue referring to the new matrices as A_i, P, and Q in order to connect their roles to those in Lemma 1.4.1.

First, we extend our matrices so that the four words W_1, W_2, W_3, W_4 do in fact need to be inverses as in the statement of Lemma 1.4.1.

Lemma 1.4.3. *Suppose $f \in \mathbb{Z}[x_1, \dots, x_k]$ has degree $D := \deg f$. Then there exists matrices P, Q, $A_1, \dots, A_k \in \mathrm{UT}(m, \mathbb{Z})$ for some $m \leq 4(D+1)\binom{D+k}{k} + 8$, such that the conclusion of Corollary 1.4.2 holds, and such that every word of the form*

$$PW_1QW_2P^{-1}W_3Q^{-1}W_4 \qquad \text{where} \quad W_i \in \langle A_1^{\pm 1}, \dots, A_k^{\pm k} \rangle$$

is a cogrowth word only if $W_1 = W_2^{-1} = W_3 = W_4^{-1}$.

Proof. Let $P', Q', A_1', \dots, A_k'$ be the matrices produced by Lemma 1.4.1. Define

$$P := \begin{bmatrix} P' & 0 & 0 & 0 \\ 0 & I_m & 0 & I_m \\ 0 & 0 & I_m & 0 \\ 0 & 0 & 0 & I_m \end{bmatrix}, \qquad Q := \begin{bmatrix} Q' & 0 & 0 & 0 \\ 0 & I_m & 0 & 0 \\ 0 & 0 & I_m & I_m \\ 0 & 0 & 0 & I_m \end{bmatrix}, \qquad A_i := \begin{bmatrix} A_i' & 0 & 0 & 0 \\ 0 & I_m & 0 & 0 \\ 0 & 0 & I_m & 0 \\ 0 & 0 & 0 & A_i' \end{bmatrix}.$$

If $W_1 = A_{i_1}^{\pm 1} \cdots A_{i_s}^{\pm 1}$, then define

$$W_1' := (A_{i_1}')^{\pm 1} \cdots (A_{i_s}')^{\pm 1}$$

and analogously for W_2', W_3', W_4'. A computation then shows

$$PW_1QW_2P^{-1}W_3Q^{-1}W_4 = \begin{bmatrix} V & 0 & 0 & 0 \\ 0 & I_m & 0 & W_3'W_4'(I_m - W_2'W_1') \\ 0 & 0 & I_m & W_4'(I_m - W_2'W_3') \\ 0 & 0 & 0 & W_1'W_2'W_3'W_4' \end{bmatrix}$$

where $V = P'W_1'Q'W_2'(P')^{-1}W_3'(Q')^{-1}W_4'$. The construction in Lemma 1.4.1 shows that Corollary 1.4.2 holds.

Moreover, for this matrix to be the identity, we must have

$$W_3'W_4'(I_m - W_2'W_1') = W_4'(I_m - W_2'W_3') = 0 \quad \text{and} \quad W_1'W_2'W_3'W_4' = I_m\,,$$

which implies $W_1' = (W_2')^{-1} = W_3' = (W_4')^{-1}$. This gives $W_1 = W_2^{-1} = W_3 = W_4^{-1}$ as required. □

We now know that the W_i need to evaluate to the same matrix, but Lemma 1.4.1 is only able to speak about subwords. So we must extend our matrices again, this time so that the only possible cogrowth words are equivalent to subwords.

We do this by noticing that if we flip the Jordan block construction from Lemma 1.4.1 so the blocks go from bottom-right to top-left instead, then instead of evaluating monomials the above-Jordan-block terms will be zero. That allows us to prove the following:

Lemma 1.4.4. *Let $f \in \mathbb{Z}[x_1, \dots, x_k]$ with $D = \deg f \geq 2$. Then there exists matrices $P, Q, A_1, \dots, A_k \in \mathrm{UT}(m, \mathbb{Z})$ for some*

$$m \leq 4(D+1)\tbinom{D+k}{k} + 8 + \tfrac{1}{2}\tbinom{D+k}{k}(D+1)^3,$$

such that the conclusion of Corollary 1.4.2 holds, and such that every word of the form

$$PW_1QW_2P^{-1}W_3Q^{-1}W_4 \tag{1.11}$$

where $W_i \in \langle A_1^{\pm 1}, \dots, A_k^{\pm k}\rangle$, is a cogrowth word only if $W_1 = W_2^{-1} = W_3 = W_4^{-1} = A_1^{x_1} \cdots A_k^{x_k}$ for some integers $x_1, \dots, x_k$.

Proof. Let $P', Q', A_1', \dots, A_k'$ be the matrices produced by Lemma 1.4.1. We consider the structure of matrices in $\langle (A_1')^{\pm 1}, \dots, (A_k')^{\pm}\rangle$ more deeply. Each consists of a collection of blocks defined as $B_{\boldsymbol{d},i}$ in (1.5). Fix any particular $B_{\boldsymbol{d}}$. By construction, it is of size $|\boldsymbol{d}| + 1$.

For any matrix $X \in \mathrm{UT}(L, \mathbb{Z})$, let $\varphi(X)$ be the matrix obtained by reflecting X along the main antidiagonal. Then $\Phi : X \mapsto \varphi(X)^{-1}$ is an automorphism of $\mathrm{UT}(L, \mathbb{Z})$. Now, $B_{\boldsymbol{d},1}, \ldots, B_{\boldsymbol{d},k}$ have their nontrivial blocks arranged from top left to bottom right; so $\Phi(B_{\boldsymbol{d},1}), \ldots, \Phi(B_{\boldsymbol{d},k})$ have their nontrivial blocks arranged from bottom right to top left.

For example, if

$$B_{\boldsymbol{d},1} = \begin{bmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad B_{\boldsymbol{d},2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ 0 & 0 & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}$$

then

$$\Phi(B_{\boldsymbol{d},1}) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & \mathbf{-1} & \mathbf{1} \\ 0 & 0 & 0 & \mathbf{0} & \mathbf{1} & \mathbf{-1} \\ 0 & 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} \qquad \Phi(B_{\boldsymbol{d},2}) = \begin{bmatrix} \mathbf{1} & \mathbf{-1} & \mathbf{1} & \mathbf{-1} & 0 & 0 \\ \mathbf{0} & \mathbf{1} & \mathbf{-1} & \mathbf{1} & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{-1} & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Sublemma 1.4.5. *A matrix $W \in \langle B_{\boldsymbol{d},1}^{\pm 1}, \ldots, B_{\boldsymbol{d},k}^{\pm 1} \rangle$ is equal to $B_{\boldsymbol{d},1}^{x_1} \cdots B_{\boldsymbol{d},k}^{x_k}$ for some integers $x_1, \ldots, x_k$ if and only if $\Phi(W)$ is zero outside of the nontrivial Jordan blocks of $\Phi(B_{\boldsymbol{d},1}), \ldots, \Phi(B_{\boldsymbol{d},k})$.*

Proof. The forward direction is immediate: because the nontrivial Jordan blocks of the $\Phi(B_{\boldsymbol{d},i})$ are in bottom right to top left order, the matrix

$$\Phi\left(B_{\boldsymbol{d},1}^{x_1} \cdots B_{\boldsymbol{d},k}^{x_k}\right) = \Phi(B_{\boldsymbol{d},1})^{x_1} \cdots \Phi(B_{\boldsymbol{d},k})^{x_k}$$

will not have any nonzero entries outside the nontrivial Jordan blocks of the matrices $\Phi(B_{\boldsymbol{d},i})$.

Conversely, suppose $\Phi(W)$ is zero outside of the nontrivial Jordan blocks of $\Phi(B_{\boldsymbol{d},i})$. Since W is in the subgroup generated by the $B_{\boldsymbol{d},i}$, we can write

$$W = B_{\boldsymbol{d},j_1}^{\varepsilon_1} \cdots B_{\boldsymbol{d},j_m}^{\varepsilon_m} \tag{1.12}$$

for some integer m, indices $1 \leq j_m \leq k$, and exponents $\varepsilon_m = \pm 1$. Let $y_1, \ldots, y_k$ be the net number of $B_{\boldsymbol{d},1}, \ldots, B_{\boldsymbol{d},k}$ in expression (1.12). In other words, we have:

$$y_i = \sum_{s \,:\, j_s = i} \varepsilon_s \,.$$

By assumption, $\Phi(W)$ agrees with $\Phi(B_{\boldsymbol{d},1})^{y_1} \cdots \Phi(B_{\boldsymbol{d},k})^{y_k}$ outside of the nontrivial Jordan blocks. Fix some index α, β within the nontrivial Jordan block of $B_{\boldsymbol{d},\gamma}$. Then (1.12) implies that

$$\Phi(W) = \Phi(B_{\boldsymbol{d},j_1})^{\varepsilon_1} \cdots \Phi(B_{\boldsymbol{d},j_m})^{\varepsilon_m} \,.$$

Note that the only terms that can contribute to the α, β index are those where $j_s = \gamma$. This means

$$[\Phi(W)]_{\alpha,\beta} = [\Phi(B_{\boldsymbol{d},\gamma})^{y_\gamma}]_{\alpha,\beta} = [\Phi(B_{\boldsymbol{d},1})^{y_1} \cdots \Phi(B_{\boldsymbol{d},k})^{y_k}]_{\alpha,\beta}$$

Since this holds for any α, β we get

$$\Phi(W) = \Phi(B_{\boldsymbol{d},1})^{y_1} \cdots \Phi(B_{\boldsymbol{d},k})^{y_k} = \Phi(B_{\boldsymbol{d},1}^{y_1} \cdots B_{\boldsymbol{d},k}^{y_k}) \,.$$

The result follows since Φ is a bijection. □

The next sublemma will allow us to force particular entries in $\Phi(W)$ to be zero.

Sublemma 1.4.6. *Let $V \in \mathrm{UT}(q, \mathbb{Z})$ and let $1 < a \leq b < q$. Then*

$$\big(I_q + E_{1,a}\big)V\big(I_q + E_{b,L}\big)V^{-1}\big(I_q + E_{1,a}\big)^{-1}V\big(I_q + E_{b,q}\big)^{-1}V^{-1} = I_q + [V]_{a,b}E_{1,q} \,.$$

Proof. The left-hand side is equal to

$$(I_q + E_{1,a})V(I_q + E_{b,q})V^{-1}(I_q - E_{1,a})V(I_q - E_{b,q})V^{-1}$$

Expanding this and using the fact that V and V^{-1} are upper triangular gives $I_q + E_{1,a} V E_{b,q} V^{-1}$. This equals the right-hand side. $\square$

To finish the proof of Lemma 1.4.3, we construct our matrices as follows. Let the matrices $P'', Q'', A_1'', \ldots, A_k''$ be the matrices obtained in Lemma 1.4.3. For every $B_{\boldsymbol{d}}$ in the construction of A_i', and every (α, β) above the nontrivial Jordan blocks of $\Phi(B_{\boldsymbol{d},i})$, let

$$\begin{aligned} P &:= P'' \oplus \left(I_{|\boldsymbol{d}|+3} + E_{1,\alpha+1}\right) \\ Q &:= Q'' \oplus \left(I_{|\boldsymbol{d}|+3} + E_{\beta+1,|\boldsymbol{d}|+3}\right) \\ A_i &:= A_i'' \oplus I_1 \oplus \Phi(B_{\boldsymbol{d},i}) \oplus I_1 \end{aligned}$$

for all $1 \le i \le k$. There are at most $\binom{\mathrm{D}+k}{k}$ of the $B_{\boldsymbol{d}}$'s, and for each of them we append at most $\frac{1}{2}(\mathrm{D}+1)^2$ new matrices of size at most $\mathrm{D}+1$. Therefore these new matrices have size

$$m \le 4(\mathrm{D}+1)\binom{\mathrm{D}+k}{k} + 8 + \frac{1}{2}\binom{\mathrm{D}+k}{k}(\mathrm{D}+1)^3,$$

as desired.

Suppose a word of the form (1.11) is cogrowth. Then by Lemma 1.4.3 we have $W_1 = W_2^{-1} = W_3 = W_4^{-1}$. Therefore, by construction and Sublemma 1.4.6 all of the entries of $\Phi(W_1)$ outside of the nontrivial Jordan blocks are zero. Then, Sublemma 1.4.5 implies that $W_1 = A_1^{y_1} \cdots A_k^{y_k}$ for the y_i defined in Sublemma 1.4.5. This completes the proof of Lemma 1.4.3. $\square$

Corollary 1.4.7. *For a fixed root $\boldsymbol{x} = (x_1, \ldots, x_k)$ of f, the word*

$$V = A_1^{x_1} \circ \cdots \circ A_k^{x_k}$$

is the unique shortest word that evaluates to $A_1^{x_1} \cdots A_k^{x_k}$.

Proof. We only need to prove the case $k \ge 2$. Suppose to the contrary, there is some other word V' which also evaluates to $A_1^{x_1} \cdots A_k^{x_k}$. Since the net number of A_i's in V' needs to be x_i, it must be that V' is some nontrivial permutation of V.

This means there exists some $j_1 < j_2$, such that an $A_{j_2}^{\pm 1}$ appears before an $A_{j_1}^{\pm 1}$ in the word W_i. But then the above-diagonal entry in the block corresponding to $\binom{j_1}{1}\binom{j_2}{1}$ will be nonzero, so this cannot be a cogrowth word. □

1.4.3 The construction

We are now ready to construct our generating sets $\mathcal{S}$ and $\mathcal{T}$ as in Theorem 1.1.1. For a fixed polynomial $f \in \mathbb{Z}[x]$, let P', Q', A'_1, …, $A'_k \in \mathrm{UT}(m, \mathbb{Z})$ be the matrices given by Lemma 1.4.4. Construct new matrices $A_i := A'_i \oplus I_3$, for $1 \le i \le k$, and let

$$P := P' \oplus \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad Q := Q' \oplus \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad R := I_m \oplus \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Denote by $\mathcal{E}_m = \{I_m \pm E_{i,i+1} : 1 \le i < m\}$ the standard generating set of $\mathrm{UT}(m, \mathbb{Z})$. Fix be a positive integer u to be determined later. Let

$$\begin{aligned} \mathcal{S} &:= \{A_1^{\pm 1}, A_2^{\pm 1}, \ldots, A_k^{\pm 1}\} \cup u \cdot \{P^{\pm 1}, Q^{\pm 1}\} \cup u^{10} \cdot \mathcal{E}_{m+3}, \text{ and} \\ \mathcal{T} &:= \mathcal{S} \cup u^5 \cdot \{R^{\pm 1}\}, \end{aligned} \tag{1.13}$$

where by $n \cdot X$ we denote n copies of the set X.

Our next lemma will exploit the modular condition in Theorem 1.1.1 to eliminate any word that does not fit the pattern of Lemma 1.4.4.

Lemma 1.4.8. *Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$, and define $\mathcal{S}$ and $\mathcal{T}$ as in (1.13). Let c_n be the number of cogrowth words of length n of the form*

$$PV_1QV_2P^{-1}V_3Q^{-1}V_4, \quad \textit{where } V_i \textit{ are words in } \langle A_1^{\pm 1}, \ldots, A_k^{\pm k} \rangle.$$

Then:

$$\mathrm{cog}_{\mathcal{T}}(n) - \mathrm{cog}_{\mathcal{S}}(n) \equiv 2n(n-1)c_{n-1}u^9 \mod u^{10}.$$

Proof. First, note that we can ignore all words that contain any of the standard generators. By construction, such words will appear a multiple of u^{10} times.

Second, note that the left-hand side counts the number of cogrowth words that are in $\langle \mathcal{T} \rangle$ but not in $\langle \mathcal{S} \rangle$. This corresponds to words with at least one $R^{\pm 1}$. However, words with two or more $R^{\pm 1}$ will be eliminated by the modulo condition.

Next, there is a bijection between words containing one R and those containing one R^{-1} given by reversing the order of the word and inverting all the elements. So let us look only at words that contain just an R. This gives a factor of 2 on the right hand side.

In order to cancel out the -1 in R we can only use copies of $P^{\pm 1}$ and $Q^{\pm 1}$. But every word with an R and at least five of these will also be eliminated since the total weight would be divisible by u^{10}. So the only possible words that remain have some cyclic permutation of $PQP^{-1}Q^{-1}$, which gives the factor of u^9.

Because any cyclic permutation of a cogrowth word is still cogrowth, we can take the unique word that starts with P. This gives a factor of n on the right hand side.

Finally, note that R commutes with P, Q, and all the A_i. Since our word has exactly one R, we can just ignore it in counting words by looking at words of length $(n-1)$. This gives us one more factor of $(n-1)$ on the right-hand side. The result counts exactly c_{n-1}. □

The following two corollaries relate this lemma to whether or not the polynomial f has integer roots.

Corollary 1.4.9. *Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$ be a polynomial with no integer roots, Then*

$$\operatorname{cog}_{\mathcal{T}}(n) - \operatorname{cog}_{\mathcal{S}}(n) \equiv 0 \mod u^{10}.$$

In a different direction, we have:

Corollary 1.4.10. *Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$ be a polynomial with an integer root $\boldsymbol{x} \in \mathbb{Z}^k$. Suppose that $|\boldsymbol{x}|$ is even, and $|\boldsymbol{x}|$ is minimal among all integer roots of f. Let $u = 16$ and*

let $\mathcal{S}, \mathcal{T}$ be defined by (1.13). Then:

$$\operatorname{cog}_{\mathcal{T}}(4|\boldsymbol{x}|+5) \;-\; \operatorname{cog}_{\mathcal{S}}(4|\boldsymbol{x}|+5) \;\not\equiv\; 0 \mod u^{10}.$$

Proof. By Lemma 1.4.8, we have:

$$\operatorname{cog}_{\mathcal{T}}\big(4|\boldsymbol{x}|+5\big) \;-\; \operatorname{cog}_{\mathcal{S}}\big(4|\boldsymbol{x}|+5\big) \;\equiv\; 2\big(4|\boldsymbol{x}|+5\big)\big(4|\boldsymbol{x}|+4\big)\,c_{4|\boldsymbol{x}|+4}\,16^9 \mod 16^{10}.$$

Since $|\boldsymbol{x}|$ is minimal, the only way to have a cogrowth word in $c_{4|\boldsymbol{x}|+4}$ is to let $V_i = A_1^{x_1} \circ \cdots \circ A_k^{x_k}$ by Lemma 1.4.4 and Corollary 1.4.7. So $c_{4|\boldsymbol{x}|+4} = 1$. Because $|\boldsymbol{x}|$ is even, the right hand side has only at most $1 + 0 + 2 + 36 = 39$ factors of 2. That means that it not not zero modulo 16^{10}, as desired. □

Remark 1.4.11. *Unfortunately, not every polynomial has a root satisfying the conditions of Corollary 1.4.10. For example, the polynomial $f(x_1, x_2) = x_1^2 - 13x_2^2 - 1$ has four solutions with minimal ℓ^1-norm, namely $(\pm 649, \pm 180)$. This would imply that $c_{3317} = 4$, introducing an extra factor of 2 to the right-hand side and making the two sides congruent.*

To avoid the issue in the remark above, we introduce an auxiliary variable which will separate out the ℓ^1 norms of all integer roots.

Lemma 1.4.12. *There exists a map $\Phi : \mathbb{Z}[x_1, \ldots, x_k] \to \mathbb{Z}[y_1, \ldots, y_{k+1}]$, such that for all $\widetilde{g} = \Phi(g)$ we have:*

- *polynomials g and $\widetilde{g}$ have the same (possibly infinite) number of integer roots,*
- *$\boldsymbol{x} \in \mathbb{Z}^{k+1}$ is an integer root of $\widetilde{g} \;\Rightarrow\; |\boldsymbol{x}|$ is even,*
- *$\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^{k+1}$ are integer roots of $\widetilde{g} \;\Rightarrow\; |\boldsymbol{x}| \neq |\boldsymbol{y}|$,*
- $\deg \widetilde{g} \leq \max\{2 \deg g, 4k + 12\}$.

Proof. Let $v = v(\boldsymbol{y}) := 4(y_1^2 + y_2^2 + \cdots + y_k^2 + 1)$, and let

$$\widetilde{g}(y_1, \ldots, y_{k+1}) \;=\; \Phi(g) \;:=\; g(y_1, \ldots, y_k)^2 \,+\, \left(-y_{k+1} \,+\, v^{k+3} \,+\, \sum_{i=1}^{k} y_i v^{i+1} \,+\, \sum_{i=1}^{k} y_i\right)^2 .$$

Note that condition (1.4.12) is clearly satisfied.

In order for $\widetilde{g}$ to have a root, we must have $g(y_1, \ldots, y_k) = 0$ and

$$y_{k+1} \;=\; v^{k+3} + \sum_{i=1}^{k} y_i v^{i+1} + \sum_{i=1}^{k} y_i \,.$$

This implies (1.4.12).

Next, suppose $\boldsymbol{r} = \{y_1, \ldots, y_{k+1}\}$ is an integer root of $\widetilde{g}$. Because v is even, we have:

$$|\boldsymbol{r}| \;\equiv\; |y_1| + \ldots + |y_k| + 0 + y_1 + \ldots + y_k \;\equiv\; 0 \mod 2,$$

which proves (1.4.12).

On the other hand, observe that

$$\begin{aligned} \big||\boldsymbol{r}| \,-\, v^{k+3}\big| \;&\leq\; \sum_{i=1}^{k} |y_i| \,+\, \left|\sum_{i=1}^{k} y_i v^{i+1} \,+\, \sum_{i=1}^{k} y_i\right| \;\leq\; \sum_{i=1}^{k} |y_i| \left(2 + v^{i+1}\right) \\ &\leq\; (2 + v^{k+1}) \sum_{i=1}^{k} |y_i| \;\leq\; (2 + v^{k+1}) \frac{v}{4} \;\leq\; v^{k+3} - (v-1)^{k+3} \,. \end{aligned}$$

This implies that if $\widetilde{g}(\boldsymbol{x}) = \widetilde{g}(\boldsymbol{y})$, then $v(\boldsymbol{x}) = v(\boldsymbol{y})$.

Now suppose that $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^{k+1}$ are roots of $\widetilde{g}$ such that $|\boldsymbol{x}| = |\boldsymbol{y}|$. From above, $v(\boldsymbol{x}) = v(\boldsymbol{y})$. Write $Y := |\boldsymbol{y}| - v(\boldsymbol{y})^{k+3}$ as a polynomial in $y_1, \ldots, y_k$ and observe that y_i's are uniquely determined by the integrality. For example, y_1 is the closest integer to Y/v^{k+1}, etc. The same argument for $\boldsymbol{x}$ shows that $\boldsymbol{x} = \boldsymbol{y}$, which implies (1.4.12). This finishes the proof of the lemma. □

We can now complete the proof of Theorem 1.1.1. Suppose an algorithm exists that determines whether or not, for arbitrary generating sets $\mathcal{S}$ and $\mathcal{T}$, we have

$$\exists n \geq 0 \;:\; \operatorname{cog}_{\mathcal{S}}(n) \;\not\equiv\; \operatorname{cog}_{\mathcal{T}}(n) \mod p^a. \tag{1.14}$$

Then we could use this algorithm to determine whether or not a Diophantine equation $g(x_1, \ldots, x_k)$ has an integer root as follows. First construct $\widetilde{g}$ as in Lemma 1.4.12. Then construct $\mathcal{S}$ and $\mathcal{T}$ with $f = \widetilde{g}$ and $u = 16$ as in Lemma 1.4.4. By Corollaries 1.4.9 and 1.4.10, polynomial $\widetilde{g}$, and thus f, has a root if and only if (1.14) holds with $p = 2$ and $a = 40$, so $p^a = u^{10}$.

Finally, Jones [Jon] shows that Diophantine problems over $\mathbb{N}$ are undecidable for polynomials of degree at most 96 in 21 variables. By a standard reduction (see e.g. [Gas, Thm 3.3]), the Diophantine problem over $\mathbb{Z}$ is undecidable for $\deg g = 192$ and $k = 63$. Then $\mathrm{D} = \deg \widetilde{g} = 384$, which by Lemma 1.4.4 gives the desired bound $m \leq 9.6 \cdot 10^{85}$. This completes the proof of Theorem 1.1.1. □

Remark 1.4.13. *In fact, Jones [Jon] (see also [Gas]), gives several pairs (degree, number of variables) which give rise to a minimal Diophantine equation. Of these, we chose the one which gives the smallest bound on n.*

1.5 Non-D-algebraic series

The previous sections gave us information about the parity of cogrowth sequences. We first prove Lemma 1.3.6 where the parity information is enough to conclude that a sequence is not D-algebraic. We then deduce Theorem 1.3.5.

1.5.1 Proof of Lemma 1.3.6

Let $\Lambda(t) = \sum \lambda_n t^n$, and suppose that Λ satisfies an algebraic differential equation. Then by definition there exist positive integers C and D together with a finite family of polynomials $\{\Pi_{c,d}\}_{0 \leq c \leq C, 0 \leq d \leq D}$, not all zero, such that for all n

$$\sum_{c,d} \sum_{i_1 + \cdots + i_d = n - c} \Pi_{c,d}(i_1, \ldots, i_d)\, \lambda_{i_1} \cdots \lambda_{i_d} = 0.$$

Note that this sum has repeated terms, so e.g. $\lambda_3\lambda_7$ and $\lambda_7\lambda_3$ are counted separately. We recast this as a sum over partitions:

$$\sum_{c,d} \sum_{\nu \vdash (n-c)\,:\,|\nu|=d} \Gamma_{\nu,n}\, \lambda_1 \cdots \lambda_d \;=\; 0 \qquad \text{for all } n, \tag{1.15}$$

where $\Gamma_{\nu,n}$ are sums of the corresponding $\Pi_{c,d}$.

Denote by $v_2(x)$ the largest power of 2 dividing x. Take some μ such that $v_2(\Gamma_\mu, n)$ is minimized. This is always possible because not all Γ_ν are zero, since the ADE is trivial otherwise. If there are ties, then we pick the one where c is minimal.

Let $V = v_2(\Gamma_\mu, n)$, and let $\ell = \ell(\mu)$. By the assumption of our lemma, there exist distinct indices $n_{\alpha_1}, \ldots, n_{\alpha_\ell}$, such that $n_{\alpha_i} \equiv \mu_i$ modulo 2^{V+1}. Furthermore, we can assume that all of these indices are greater than $N(C, D)$ as defined in condition (4).

We claim that this contradicts (1.15). Indeed, consider the equality modulo 2^{V+1}. Letting $\nu = \{n_{\alpha_1}, \ldots, n_{\alpha_\ell}\}$, by the assumption we get that $V = v_2(\Gamma_\nu, n)$. Since all $\lambda_{n_{\alpha_i}}$ are odd, this particular term will have $v_2 = V$.

Any term with lower c will have $v_2(\Gamma, n) > V$, so we can ignore those terms in (1.15). On the other hand, any other term besides ν will have $v_2(\Gamma, n) \geq V$, and by condition (4) at least one of the λ_i is even, meaning such terms will also have $v_2(\Gamma, n) > V$.

Thus the left-hand side of (1.15) has exactly one term which is not congruent to zero modulo 2^{V+1}, a contradiction. Hence our sequence cannot be D-algebraic. □

1.5.2 Proof of Theorem 1.3.5

Suppose we have a polynomial f satisfying the conditions prescribed in Conjecture 1.3.4. Construct $A_1, \ldots, A_k$ and P, Q, R as in the proof of Theorem 1.1.1. Suppose for the sake of contradiction that $\mathrm{cog}_{\mathcal{S}}(n)$ and $\mathrm{cog}_{\mathcal{T}}(n)$ are both D-algebraic.

Now, let $\mathcal{W}$ be the set of cogrowth words of the form

$$PW_1QW_2P^{-1}W_3Q^{-1}W_4,$$

where W_i are words in $\{A_1^{\pm 1}, \ldots, A_k^{\pm 1}\}$. Define ω_n to be the number of words in $\mathcal{W}$ of length n.

Lemma 1.4.4 shows that the evaluations of W_1 and W_3 are the same, and are equal to the inverse of the evaluations of W_2 and W_4. Also, there must be a root $\boldsymbol{x} = (x_1, \ldots, x_k)$ of f, such that the net number of A_i's in W_1 is equal to x_i, for all $i \in [k]$. The same must be true (up to minus sign) for W_2, W_3, W_4.

We now proceed to make one more modification of our matrices. We expand P and Q by adding k copies of a 5×5 matrix $I_5 + E_{13}$ and $I_5 + E_{23} + E_{45}$, respectively:

$$P \leftarrow P \oplus^k \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad \text{and} \qquad Q \leftarrow Q \oplus^k \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Then, for each j, create two versions of A_j. One will be $A \oplus I_{5k}$, called the *neutral version*. The other will be

$$A_j \oplus I_{5(j-1)} \oplus \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \oplus I_{5(k-j)},$$

called the *positively charged version*. Symmetrically, there will also be a *neutral* and *negatively charged version* of A_i^{-1}.

We have added a $5k \times 5k$ sub-block to each of the matrices in our generating set. Call this sub-block the *new parts* of the matrix. Also let the *net charge* of a word be the number of positively charged A_i's minus the number of negatively charged A_i's.

Let $\mathcal{W}'$ be the set of cogrowth words of the form

$$PW_1QW_2P^{-1}W_3Q^{-1}W_4,$$

where W_i are words in $\{A_1^{\pm 1}, \ldots, A_k^{\pm 1}\}$ together with their charged versions.

Lemma 1.5.1. *A word in $\mathcal{W}'$ will be cogrowth if and only if it corresponds to a word in $\mathcal{W}$ in which W_1 through W_4 all have net charges of 0.*

Proof. Suppose that the words W_1 through W_4 have charges c_1 through c_4. Then the new part of W_i is

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & c_i & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

This means that the new part of the whole word can be computed to be

$$\begin{bmatrix} 1 & 0 & 0 & c_1 + c_2 & c_1 - c_2 - c_3 \\ 0 & 1 & 0 & c_2 + c_3 & -c_2 - c_3 \\ 0 & 0 & 1 & c_1 + c_2 + c_3 + c_4 & -c_2 - c_3 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

This gives a cogrowth word if and only if $c_1 = c_2 = c_3 = c_4 = 0$, as desired. □

Denote by γ_n be the number of charged words which are cogrowth words, so we have $\gamma_n \geq \omega_n$. One can think of this as giving a weight to each of the words in $\mathcal{W}$ counting how many ways we can assign charges so that each of the W_i has net charge zero. Since we can always neutrally charge all the A_i's every word has weight at least 1. If this word is the minimal word for some root, then that is the only choice; otherwise there will be many.

Let us assign charges to the A_i's in W_1. Without loss of generality we can assume that $x_i \geq 0$. Since there are $v + x_i$ instances of A_i and v instances of A_i^{-1}, there are

$$\sum_{u=0}^{v} \binom{v + x_i}{u} \binom{v}{u} = \binom{2v + x_i}{v}$$

ways of doing this. We charge u each of the positive and negative ones. It can be shown (see e.g. in [Sta1, Exc. 1.6]), that $\binom{2v+x_i}{v}$ is odd only if there exists some positive integer d such that

$$2^d - x_i \leq v \leq 2^d. \tag{1.16}$$

This implies that for a fixed x_i, there will be an even number of ways of assigning charge for a set of v's having density 1. In particular, for there to be an odd weight on a word, we need (1.16) to hold for all W's and x's. That implies

$$|n - 4 - e| \leq 4|\boldsymbol{x}|, \tag{1.17}$$

where e is the sum of at most $4k$ powers of 2. Note that we also have $n - 4 \geq 4|\boldsymbol{x}| + 4$.

Define the sequence

$$\lambda_n = \frac{1}{2^{39}}\big(\operatorname{cog}_{\mathcal{T}}(8n+5) - \operatorname{cog}_{\mathcal{S}}(8n+5)\big).$$

Then by Lemma 1.4.8, $\{\lambda_n\}$ is a sequence of integers which is congruent to γ_{2n} modulo 2. By assumption, the GF for $\{\lambda_n\}$ is D-algebraic. We claim that this contradicts Lemma 1.3.6.

Indeed, let $n_i = |\rho_i|/2$. Conditions (1), (2) and (3) of Lemma 1.3.6 follow from the assumptions of Theorem 1.3.5 and Corollary 1.4.10. Therefore $\{\lambda_n\}$ cannot be D-algebraic. And condition (4) of Lemma 1.3.6 follows from the above computation plus assumption (4) of Conjecture 1.3.4. As subsequences of D-algebraic sequences along arithmetic progressions are also D-algebraic, we can conclude that at least one of $\operatorname{cog}_{\mathcal{S}}$ and $\operatorname{cog}_{\mathcal{T}}$ is not D-algebraic. □

1.6 Final remarks and open problems

1.6.1 Grappling with undecidability

To further understand the meaning of our Main Theorem 1.1.1, we state the following corollary:

Corollary 1.6.1. *For some integer $m \leq 9.6 \cdot 10^{85}$, there are symmetric generating sets $\mathcal{S}$ and $\mathcal{T}$ of the unitriangular group $\mathrm{UT}(m, \mathbb{Z})$, such that the following problem is independent of ZFC* [5] *:*

$$\forall n \in \mathbb{N} \ : \ \mathrm{cog}_{\mathcal{S}}(n) \equiv \mathrm{cog}_{\mathcal{T}}(n) \mod 2^{40}.$$

The corollary follows from a standard diagonalization argument (see e.g. [Poo2, p. 212]). Here is another corollary which is even easier, but perhaps more suggestive.

For a matrix $M = (m_{ij})$, denote $\phi(M) := \sum_{ij} |m_{ij}|$ the total sum of absolute values of the entries. Similarly, denote by $\phi(\mathcal{S}) := \sum_{M \in \mathcal{S}} \phi(M)$ the *size of* $\mathcal{S}$. The following corollary follows from basic results on computability:

Corollary 1.6.2. *For some integer $m \leq 9.6 \cdot 10^{85}$, there are symmetric generating set $\mathcal{S}$ and $\mathcal{T}$ of the unitriangular group $\mathrm{UT}(m, \mathbb{Z})$, such that*

$$\exists n \in \mathbb{N} \ : \ \mathrm{cog}_{\mathcal{S}}(n) \not\equiv \mathrm{cog}_{\mathcal{T}}(n) \mod 2^{40},$$

but the first time the inequality holds is for $n > \mathrm{Tow}(\mathrm{Tow}(\mathrm{Tow}(\phi)))$, [6] *where $\phi := \phi(\mathcal{S}) + \phi(\mathcal{T})$.*

Here $\mathrm{Tow}(k)$ is the tower of 2's of length k. While a single tower is unusual but does occur for natural combinatorial problems, see e.g. [Gow, HNP], the iterated towers get us close to the edge of human imagination.

In the context of cogrowth sequences, we can only think of [Moo] which proves a single tower lower bound on the size of the Følner sets for the Thompson's group F. This does not refute the conjecture that F is nonamenable (cf. [Sap, §5.4]), but suggests that the proof would be rather involved. We refer to a curious numerical investigation of the cogrowth sequence [PG] (see also [HHR]), strongly suggesting nonamenability.

[5] *We chose ZFC to make the statement more accessible. The proof naturally extends to any system of axioms.*

[6] *We stopped at three towers for clarity. We could just as well have written* $\mathrm{Tow}(\phi)$ *of towers, for example.*

1.6.2 Unitriangular group

Jennings famously proved in [Jen] (see also [GW]), that every torsion-free nilpotent group is a subgroup of the unitriangular group $\mathrm{UT}(m, \mathbb{Z})$ for some m. This explains why we chose to work with the unitriangular group towards Kontsevich's question for nilpotent groups. In fact, this can be stated formally: if the analogue of Theorem 1.1.1 holds for *some* nilpotent group and its families of generating sets, then the "using multiple copies of extra generators" trick used in §1.4.3 one can still obtain the first part of Theorem 1.1.1.

1.6.3 Heisenberg group

For the Heisenberg group $H_3 = \mathrm{UT}(3, \mathbb{Z})$ with natural generators, the first 71 terms were computed by Pantone, see [OEIS, A307468]. His analysis suggests that there are no lower order algebraic differential equation (ADE) for the cogrowth series. We conjecture that this cogrowth series is not D-algebraic. Thus, in particular, it is non-D-finite and not a diagonal.

Continuing the discussion of Stoll's example in §1.1.2, there is a deeper reason why H_3 has simpler structure than the higher Heisenberg group $H_5 \subset \mathrm{UT}(4, \mathbb{Z})$, see [NY]. In fact, from metric geometry point of view, group H_5 is the "most distorted" relative to the abelian group, see [Naor]. Additionally, every equation is decidable in H_3 [DLS, §2.2], and there are relatively few distinct words [GL]. Thus, if one is looking for a conceptual proof of non-D-finiteness in a smaller example, perhaps H_5 or $\mathrm{UT}(4, \mathbb{Z})$ is a better place to start than H_3.

1.6.4 Dependence on the generators

A deep problem for cogrowth series is whether their properties depend on the generating set. For D-finiteness we have a partial answer: they do not for free groups and amenable groups of superpolynomial growth (see §1.1.2). We conjecture that they do not for virtually nilpotent group as well. We are at loss what happens to general nonamenable groups, but

that's where we would look for counterexamples.

1.6.5 Abelian groups

Kuksov's Theorem 1.3.2 holds for general abelian groups. We found an alternative proof using binomial sums, which implies a stronger statement: that the cogrowth series is always a diagonal of an $\mathbb{N}$-rational function, see [GP1]. It would be interesting to extend Theorem 1.3.2 to other tame classes of group. We conjecture that the cogrowth series for a virtually abelian group is always a diagonal of a rational function. Thus, in particular, it is D-finite.

1.6.6 Christol's conjecture

There is a healthy debate in the literature about the validity of Christol's Conjecture 1.3.1. A large number of potential counterexamples were suggested by Christol himself and his coauthors [B+, Chr2]. A few of these were recently refuted, i.e. shown to be diagonals of rational functions [AKM, BY]. It would be most exciting if there is an uncomputability result analogous to Theorem 1.1.3 in this setting.

1.6.7 Explicit construction

The construction of generating sets in Corollary 1.6.1 can be made explicit if one uses an explicit construction of a Diophantine equation whose solution is independent of ZFC. This equation, in principle, can be obtained from an explicit construction of a Turing machine whose halting is independent of ZFC, see [YA] and follow the approach in [CM]. We would be curious to see the resulting numerical bounds on the size of the resulting generating sets.

Part II

Quivers

CHAPTER 2

Complexity of quiver mutation equivalence

2.1 Introduction

Quivers and their mutations (defined in Section 2.2) were introduced by Fomin and Zelevinsky in [FZ1] and [FZ2] in the context of cluster algebras. They are widely used in algebraic combinatorics (see [Kel10] for a survey). However, many combinatorial questions about these objects remain unresolved.

The question of whether a given quiver Q is equivalent to only finitely many other quivers was addressed in [FST], where a list of such quivers is given. Also, Fomin and Neville show in [FN] that there are long cycles in the graph of quivers. Recently, Fomin asked in [Fom22] for algorithmic solutions to the following questions:

1. Given quivers Q_1 and Q_2, determine whether Q_1 and Q_2 are mutation equivalent.

2. Given a quiver Q and a nonnegative integer k, determine whether there exists a quiver $Q_0 \in [Q]$ such that Q_0 has two vertices with exactly k arrows between them.

However, Fomin also proposed that these problems may be computationally difficult or even undecidable:

"We don't have any algorithm that would detect if two quivers are mutation equivalent or not ... of course it would be absurd if this were algorithmically undecidable - there must be an algorithm - well, who knows? Maybe not."

–Sergei Fomin, [Fom22], May 16, 2022

Formally, Fomin's problem asks whether these questions are decidable for general quivers. We approach the problem from both ends. First, we present a couple of NP-hardness results about the second of Fomin's questions. Past results such as [BFZ] have shown that certain determinants are preserved by quiver mutation. Since determinants can be computed in polynomial time, however, these results show that it is unlikely that a determinantal formula can capture everything that is going on in a quiver. Next, we will show that quivers with only two mutable vertices can only have a very limited set of equivalent quivers, and derive asymptotics of the quivers in such mutation classes.

2.1.1 Hardness results

We begin by stating our main results. Both concern complexity of questionsrelated to quiver mutation equivalence, specifically Fomin's second question.

Theorem 2.1.1 (NP-hardness)**.** *Let Q be a quiver, and let $k > 1$ be an integer. The following problem is NP-hard: Determine whether there exists a quiver Q_0 which is mutation equivalent to Q such that Q_0 contains two vertices with exactly k arrows between them.*

In the context of quivers, it is natural to be interested in strong NP-hardness. In ordinary NP-hardness, the inputs to the problem are assumed to be in binary. Specifically, when there are k arrows between two vertices in a quiver, this is assumed to take $log_2 k$ bits of input. However, the arrows in a quiver may each carry algebraic information and thus have independent meaning. When inputs to a decision problem are given in unary instead of binary, then the corresponding notion is strong NP-hardness. Problems such as Knapsack or Subset Sum do not meet this stronger criterion. See [GJ] for background on this topic.

Let an arrow in a quiver be *icebound* if it goes between two frozen vertices.

Theorem 2.1.2 (Strong NP-hardness)**.** *Let Q be a quiver. The following problem is strongly NP-hard: Determine whether there exists a sequence of mutations which takes Q to a quiver with no icebound arrows.*

See Section 2.4.3 for implications of these results.

2.1.1.1 Non-hardness result

Let us limit the number of vertices at which we are allowed to mutate the quiver. In this case, the set of mutation-equivalent quivers becomes quite limited. If there is only one mutable vertex, then, since mutation is an involution, there can only be two quivers in a mutation class.

Our theorem describes the mutation classes of quivers with exactly two mutable vertices. Again,since mutations are involutions, the only way to get new quivers is to alternate mutating at the two vertices.

Theorem 2.1.3. *Let Q be a quiver with exactly two mutable vertices called C and D. Define α to be the number of arrows between C and D. Then:*

If $\alpha = 0$, we have $\big|[Q]\big| \leq 4$.

If $\alpha = 1$, we have $\big|[Q]\big| \leq 10$.

If $\alpha = 2$, then in any nontrivial case the number of arrows in $(\mu_D\mu_C)^n(Q)$ grows linearly.

If $\alpha \geq 3$, then in any nontrivial case the number of arrows in $(\mu_D\mu_C)^n(Q)$ grows exponentially.

Furthermore, if $\alpha \geq 2$, let $\delta_{I,J}(n)$ be the number of arrows between I and J in $(\mu_D\mu_C)^n(Q)$. For any vertex $A \neq C, D$ we have:

$$\lim_{n\to\infty} \frac{\delta_{A,C}(n)}{\delta_{A,D}(n)} = \frac{1}{2}\left(\alpha + \sqrt{\alpha^2 - 4}\right)$$

See 2.4.6 for possible extensions of this result.

2.1.2 Structure of the chapter

We will proceed as follows. In Section 2.2 we begin with notation,definitions, and examples. Next we prove our theorem in Section 2.3. We conclude with final remarks in Section 2.4.

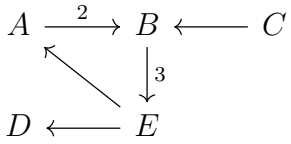
2.2 Notation, definitions, and examples

2.2.1 Basic definitions

For positive integers n, define $[n]$ to be the set $\{1, 2, \ldots, n\}$. Also, let $\mathbb{N}$ be the set $\{0, 1, 2, \ldots\}$.

2.2.2 Quivers

A *quiver* is a directed multigraph with no loops or 2-cycles, the edges of which are called *arrows*. We will indicate multiple arrows between vertices by labeling edges with numbers. For example,the following graph is a quiver on five vertices with eight arrows:



2.2.3 Quiver mutation

In a quiver, we assign a subset of the vertices to be *mutable*; the remaining vertices are *frozen*. While Fomin and Zelevinsky's original definition ignored any arrows between frozen vertices, we will follow [Pre20] and allow them. To each mutable vertex in the quiver we associate anoperation called *mutation*. For a vertex X, mutation at X, denoted by μ_X, proceeds in the following three steps:

1. for every two step path $Y \to X \to Z$, add an arrow from Y to Z,
2. reverse the direction of every arrow incident to X.

3. remove 2-cycles one by one.

For example, applying the mutation μ_B will turn the quiver on the left into the quiver on the right and vice versa in the picture below:

It is easily seen that every mutation is an involution. That is, $\mu_X(\mu_X(Q)) = Q$ for every quiver Q with vertex X. It is also easy to see that mutations at nonadjacent vertices commute. Two quivers aresaid to be *mutation equivalent* if one can be obtained from the other by a finite sequence of mutations.Mutation equivalence is an equivalence relation, so we can define the mutation class of a quiver Q, denoted $[Q]$, to be the equivalence class of Q under this relation.

2.3 Proofs

2.3.1 Proof of Theorem 2.1.1

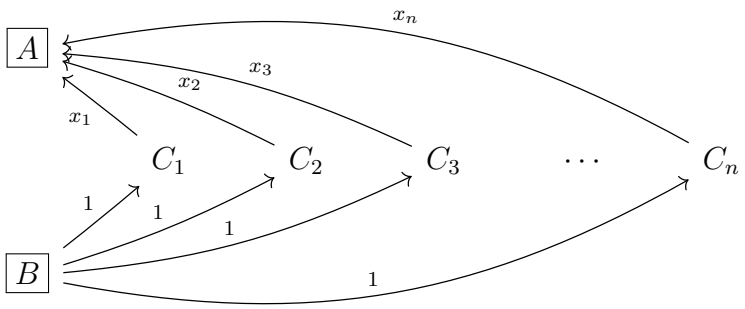
We reduce the problem to Subset Sum, which is defined as follows:

Subset Sum

Input: $X \subset \mathbb{N}$ a finite set, and $k \in \mathbb{N}$.

Decide: $\exists A \subseteq X$ such that $\sum_{a \in A} a = k$?

This problem is is known to be NP-hard (see e.g. [GJ, §A3.2]). Let $X = \{x_1, \ldots, x_n\}$ be a set of positive integers, and let $k > 1$ be another integer. Let Q be the following quiver:



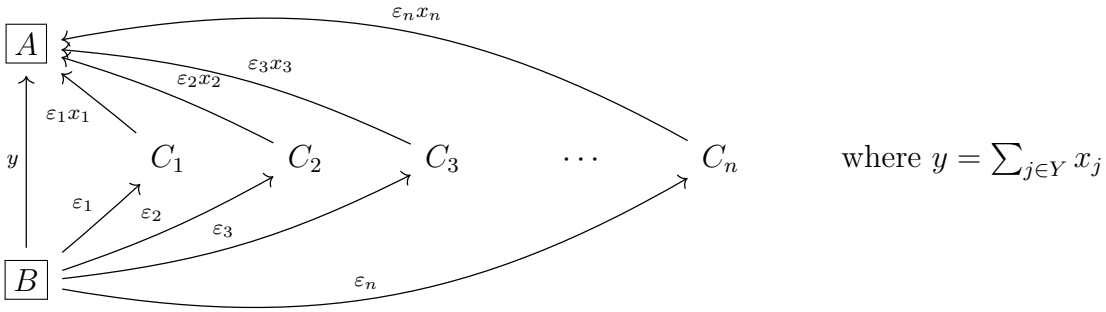
For each $i \in [n]$, let μ_i be μ_{C_i}. Suppose we apply the sequence of mutations $\mu := \mu_{i_1} \cdots \mu_{i_k}$. Define $Y \subseteq [n]$ by

$$Y = \{j \in [n] : \mu_{C_j} \text{is used an odd number of times}\}$$

Then, for each $j \in [n]$ let

$$\varepsilon_j = \begin{cases} 1 & \text{if } j \notin Y \\ -1 & \text{if } j \in Y \end{cases}$$

An easy induction shows that $\mu(Q)$ is given by



That means that if $k \notin \{0, 1\} \cup X$, the only way for $\mu(Q)$ to contain an arrow with weight k is for k to be the weight of the arrow between B and A. That means that k is present in some quiver equivalent to Q if and only if k is a subset-sum of X. The result follows from NP-hardness of Subset Sum. □

2.3.2 Proof of theorem 2.1.2

We use the following formulation of the 3-PARTITION problem:

3-PARTITION

Input: $n \geq 3$ and $X \subseteq \binom{[n]}{3}$.

Decide: $\exists \mathcal{A} \subseteq \mathcal{X}$ such that every $i \in [n]$ is contained in exactly one $A \in \mathcal{A}$?

That is, given a positive integer n and a subset $X \subseteq \binom{[n]}{3}$, does there exist a partition of $[n]$ into elements of X? This is strongly NP-hard (see e.g. [GJ, §A3.1]). Without loss of generality, we may assume that each element of $[n]$ is in at least one of the elements of X. Given n and X, we construct a quiver with vertices:

$$\underbrace{A_1, \ldots, A_n, C}_{\text{frozen}}, \{B_X\}_{X \in \mathcal{X}}$$

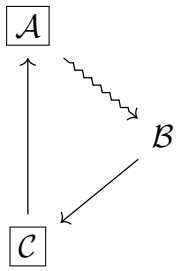
Take the following edges:

One edge from Ai to B_X whenever $i \in X$.

One edge from B_X to C for each X.

One edge from C to A_i for each i.

The resulting quiver has this shape:



Here $\mathcal{A}$ and $\mathcal{B}$ represent the sets of vertices of the form A_i and B_X, respectively. There is only one vertex labeled C. The solid arrows represent one arrow between every pair of

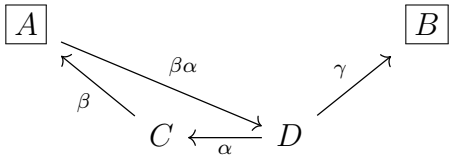
vertices from the respective sets. The squiggly arrow between A and B represents arrows between an A_i and a B_X if and only if $i \in X$. If a partition $P \subset X$ od $[n]$ exists, we can apply the mutations $\mu_{B_P} : P \in \mathcal{P}$, which will eliminate all icebound edges. More generally, note that all mutations commute. Moreover, they are all involutions. So we need only consider the effect of using mutations at most once. In that case, we eliminate the icebound edges if and only if the mutations we use correspond to a partition of $[n]$. We have therefore reduced the problem to 3-PARTITION. Because 3-PARTITION is strong NP-hard, the result follows.

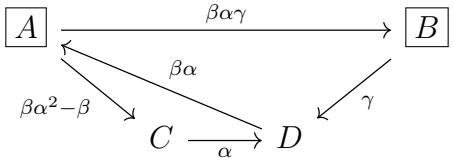
2.3.3 Proof of theorem 2.1.3

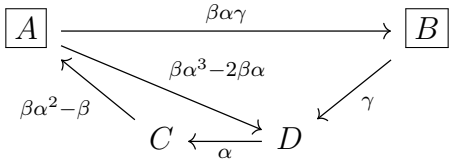
First, we note that it suffices to prove the case where Q has exactly four vertices. This is because, for any subset $Q' \subset V(Q)$ of size 4 containing both C and D, the action of μ_C and μ_D commutes with restriction to Q'.

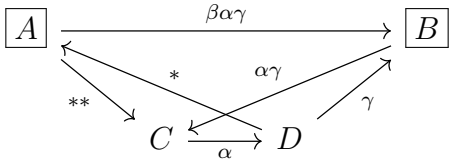
Let the other two vertices in Q' be A and B. It also suffices to consider the case where A and B start with no arrows between them. If C and D haveno arrows between them to start, then the statement is trivial. If C and D have one arrow between them, then it is an easy computation to check that $(\mu_D \mu_C)^{10}(Q) = Q$.

So assume there are $\alpha \geq 2$ arrows from C to D. One possible case consists of arrows from A to C and from D to B Then we can write down the first few quivers that we get:



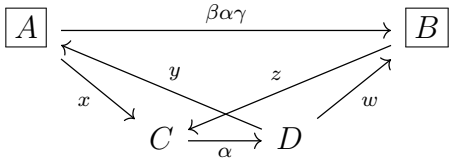


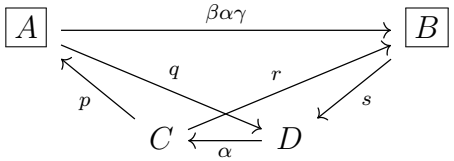




where $* = \beta\alpha^3 - 2\beta\alpha$ and $** = \beta\alpha^4 - 2\beta\alpha^2 - \beta\alpha^3 + \beta$.

Note that these are both positive since $\alpha \geq 2$.Consider the quivers $Q_1(x, y, z, w)$ and $Q_2(p, q, r, s)$ defined below:





We claim that all future quivers will be of one of these two forms and thus $\beta\alpha\gamma$ is the only thing that appears on top. We can compute that

$$\mu_C\left(Q_1(x,y,z,w)\right) = Q_2(x, \alpha x - y, z, \alpha z - w)$$

so long as $\alpha x > y$ and $\alpha z > w$. Next we apply μ_D to find

$$\begin{aligned}\mu_D\left(\mu_C\left(Q_1(x,y,z,w)\right)\right) &= Q_1\left(\alpha(\alpha x - y) - x, \alpha x - y, \alpha(\alpha z - w) - z, \alpha z - w\right) \\ &:= Q_1(x', y', z', w'),\end{aligned}$$

this time assuming $\alpha(\alpha x - y) > x$ and $\alpha(\alpha z - w) > w$. This is a stronger condition than the previous. Note that our conditions are equivalent to $\frac{\alpha}{\alpha^2-1} < \min\left(\frac{x}{y}, \frac{z}{w}\right)$ which is satisfied by our original picture. However, we have computed

$$\frac{x'}{y'} = \frac{\alpha(\alpha x - y) - x}{\alpha x - y} = \alpha - \frac{x/y}{\alpha(x/y) - 1}$$

So the problem reduces to iteratively applying the function

$$f(t) = \alpha - \frac{t}{\alpha t - 1}$$

and it is easy to see that this converges to a limit of

$$\frac{x}{y} = t = \frac{1}{2}\left(\alpha + \sqrt{\alpha^2 - 4}\right)$$

A similar picture holds for the other three starting positions. □

2.4 Final remarks

2.4.1 Undecidability

The paper [FN] does show the existence of small quivers which are nonetheless polynomially far apart with respect to mutation. Of course, undecidability is far stronger. Suppose, for example, that it is undecidable whether or not two quivers are mutation equivalent. Then, there would exist quivers Q_1 and Q_2 with a_1 and a_2 arrows, respectively, such that the shortest sequence of mutations taking one to the other has length

$$\ell \geq \text{Tow}(\text{Tow}(\text{TowTow}(\text{Tow}(a_1 + a_2 + 47))))$$

where $\text{Tow}(k)$ is a tower of 2s of length k. Put fancifully, this means there is no limit as to how far into the sky one has to go in order to show that two quivers are mutation equivalent. Note that Theorem 2.1.3 shows that more than two mutable vertices are needed for this to happen.

2.4.2 Knots and Plabic Graphs

Deep connections exist between quiver mutation equivalence and knot theory including via plabic graphs (see e.g., [BS], [GL], [FPST], or [STWZ]). For knots and links, upper bounds exist for the number of Reidemeister moves needed to show equivalence. Here is the best known bound due to [CL]. Suppose D_1 and D_2 are diagrams of the same link or knot. Let their crossing numbers be c_1 and c_2, respectively. Then there exists a sequence of Reidemeister moves taking D_1 to D_2 of length at most

$$\text{Tow}(C)^{(c_1+c_2)} \qquad \text{where } C = \left(10^{10^6}\right)^{(c_1+c_2)}$$

Again, $\text{Tow}(k)$ is a tower of 2s of length k. It may well be the case that such a bound exists for mutation equivalence of quivers as well.

2.4.3 Quiver Invariants

Fix a quiver Q and some $k \in \mathbb{N}$. Fomin's question in the introduction asks for an algorithm to determine whether there exists a quiver $Q' \in [Q]$ such that two vertices in Q' have exactly k arrows between them. One hope is that determinantal invariants would be able to answer these questions. Our results suggest that one should investigate the quivers used in the construction of Theorems 2.1.1 and 2.1.2.

2.4.4 Mutable and Immutable Vertices

Frozen vertices and arrows between them are essential for the proofs of Theorems 2.1.1 and 2.1.2. It would be interesting to see whether the number of frozen vertices can be reduced.

2.4.5 Other Properties of Quivers

There are many other questions about quivers for which an algorithmic test would be of interest. For instance, one could ask whether a quiver is mutation acyclic, that is, mutation equivalent to an acylic quiver. Much work remains to be done in this area.

2.4.6 Quiver gadgets

Embedding difficult problems into quiver mutation equivalence requires the construction of quivers whose mutations can be controlled. Many questions even about simple quivers remain unanswered. In particular, one method would be to embed *Hilbert's tenth problem* or the *post-correspondence problem* into quivers (see e.g., [PS1]). We are still far away from this.

To illustrate, we give a natural possible generalization of Theorem 2.1.3. Let Q be a quiver of the following form: $\boxed{A} \xrightarrow{x_0} C_1 \xrightarrow{x_1} \ldots \xrightarrow{x_{k-1}} C_k \xrightarrow{x_k} \boxed{B}$ Then we conjecture that for all Q' which is mutation equivalent to Q, the number of arrows between A and B is

always 0 or $x_0x_1 \cdots x_k$. The cases $k = 0$ and $k = 1$ are trivial, and the case $k = 2$ is proven in Theorem 2.1.3. However, the general case is open.

Part III

Posets and parity

CHAPTER 3

Complexity of sign imbalance, parity of linear extensions, and height 2 posets

3.1 Introduction

Let P be a poset on n elements, and fix some labeling of P with labels $\{1, \ldots, n\}$. Then the sign imbalance (defined in section 3.2.1) is a natural statistic counting the difference between the number of odd and even linear extensions of P.

Sign imbalance was introduced by Ruskey in [Rus88] in the context of Gray codes. Define a graph $G(P)$ with vertices corresponding to linear extensions of P and connect pairs of vertices which differ by a transposition. Then it is an easy observation that if $G(P)$ has a Hamiltonian path, then the sign imbalance of P must be at most 1. Furthermore, $G(P)$ is always connected (see §3.5.2). The converse was conjectured by Ruskey in [Rus88]. It remains open. Only a small class of special cases have been shown; see [Rus03, §5] for a reference or [Müt23, §5.5] for a more recent overview. Further information can be found in [Sta05] or [Knu11]. Sign imbalance has also been applied to real algebraic geometry [SS06] (see §3.5.2).

Few general results exist for computing the sign imbalance of arbitrary posets. If P is a poset where every nonminimal element is greater than at least two other elements, then P is sign-balanced; switching the labels 1 and 2 provides a bijection between odd and even permutations [Rus88]. Suppose that P is a poset on n elements and that for every maximal chain C, the length of C is congruent to n modulo 2. Stanley observed in [Sta05] that the

promotion operator provides a sign-reversing involution and soPmust be sign-balanced.

Ruskey conjectured that a product of chain posets $C_m \times C_n$ with $m, n > 1$ is sign-balanced if and only if $m \equiv n$ modulo 2 and showed the case where m, n are both even [Rus92]. This conjecture was proven by White [Whi01], who gave a formula for the case $m \not\equiv n$. Some other results for specific posets exist (e.g. [Ber18]).

We note that sign imbalance naturally correspond to counting domino tableaux (see Lemma 3.3.1). For posets arising from Young diagrams, these are the special case of rim hook tableaux where all rim hooks have size 2 with labels that must be increasing along rows and columns.

One problem is to compute the sign imbalance of a poset:

SIGN IMBALANCE

Input: A poset P.

Output: The sign imbalance $si(P)$.

Stachowiak gives a complexity result (cf. 3.5.3):

Theorem 3.1.1 (Theorem 1 of [Sta97a])**.** SIGN IMBALANCE *is #P-hard. This holds even if we consider only posets with height 2.*

The proof gives a parsimonious reduction from the sign imbalance of height 2 posets to counting linear extensions. This corresponds to one direction of Lemma 1.4.1. Since counting linear extensions was shown to be #P-hard by Brightwell and Winkler [BW91], this shows that SIGN IMBALANCE is #P-hard.

By a theorem of Dittmer and Pak [DP20], counting linear extensions is still #P-hard even in the restricted case of height 2 posets. We prove a complementary result: determining whether a height 2 poset has at least a given sign imbalance is decidable in polynomial time.

H2SB

Input: A poset P of height 2 and an integer k.

Decide: Is the sign imbalance of P at least k?

Theorem 3.1.2. H2SB *is in* P. *In the specific case* $k = 1$ *we obtain that determining whether a height 2 poset is sign balanced is in* P.

Note that the polynomial bound above implicitly depends on k.

Recently, Kravitz and Sah showed in [KS21] an upper bound of $O(\log a \log\log a)$ for the minimal number of elements in a poset with a linear extensions. Lemma 1.4.1 then allows us to obtain the following corollary:

Corollary 3.1.3. *For every positive integer* a, *there exists a height 2 poset* P *with* $O(\log a \log\log a)$ *elements such that* $si(P) = a$.

We contrast Corollary 3.1.3 with the following conjecture of Chan and Pak:

Conjecture 3.1.4 (Conjecture 5.17 in [CP23])**.** *For every sufficiently large integer* m *there exists a height 2 poset* P *such that* $LE(P) = m$.

Note that without the "height 2" condition, Conjecture 3.1.4 would be trivial, as $C_{m-1} + C_1$ has m linear extensions. Furthermore, since a height 2 poset on n elements must have at least $(n/2)!^2$ linear extensions, a positive resolution of Conjecture 3.1.4 would imply a logarithmic bound similar to that of Conjecture 3.1.3 or [KS21].

We note that the number of linear extensions of height 2 posets is not equally distributed among odd and even numbers. Let $f(n)$ be the number of height 2 posets on n elements which have an *odd* number of linear extensions.

Given a poset $P = (X, \prec)$, we define

$$re(P) := \#\{i, j \in X : i \prec j\}$$

$$cr(P) := \#\{i, j \in X : i \text{ covers } j\}$$

Equivalently, $re(P)$ is the number of edges in the comparability graph and $cr(P)$ is the number of edges in the Hasse diagram of P. Also, for any positive integer k we let $\mathcal{O}_k$ be the set of posets on k elements with an odd number of linear extensions.

Theorem 3.1.5. *For every $n \geq 1$ we have*

$$f(2n+1) = f(2n) = \sum_{P \in \mathcal{O}_n} 2^{re(P)-cr(P)}$$

and

$$2^{\binom{n-1}{2}} \leq f(2n) \leq 2^{\binom{n}{2}}$$

See §3.5.4 for an example when $n = 3$. Note that the bounds for f imply that nearly all posets of height 2 have an even number of linear extensions. A similar result holds for all primes:

Theorem 3.1.6. *Let q be prime. Let $f_q(m)$ be the number of height 2 posets P with m vertices such that $q \nmid e(P)$. Then*

$$f_q(m) \leq 2^{\frac{q-1}{4q}m^2+O(m)}$$

For comparison, note that there are $2^{\frac{1}{4}m^2+O(m)}$ total height 2 posets on m vertices. In the case $q = 2$, Theorems 3.1.5 and 3.1.6 agree on an asymptotic $2^{\frac{1}{8}m^2+O(m)}$.

3.2 Definitions and Examples

We use the notation $[n] := \{1, 2, ..., n\}$. Also, C_n and A_n will denote chain posets and antichain posets on n elements, respectively. A lower order ideal of a poset $P = (X, \prec)$ is a subset $Y \subset X$ such that $y \in Y, x \prec y \Rightarrow x \in Y$.

3.2.1 Posets and linear extensions

We will assume familiarity with basic notions of posets (see e.g. [Sta97b, §3] or surveys [BW00, Tro95]). Suppose P is a poset $(X, \prec)$, where X has n elements. Then a *linear*

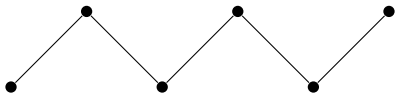


Figure 3.2.1: A poset with 61 linear extensions

extension of P is a bijection $\ell : X \to [n]$ such that $\ell(x1) < \ell(x2)$ whenever $x1 \prec x2$. We describe the linear extension as assigning the labels in $[n]$ to the elements of P . We denote the number of linear extensions of P by $e(P)$ and the set of linear extensions by $LE(P)$.

Fix an arbitrary bijection $f : X \to n$. Then every linear extension corresponds to either an odd or an even permutation. We define the sign imbalance as

$$si(P) := \left| \sum_{\ell \in LE(P)} \operatorname{sgn}(\ell) \right| \tag{3.1}$$

It is easy to show that $si(P)$ is independent of the choice of f. Thus we will suppress the dependence on f. A poset P for which $si(P) = 0$ is called *sign-balanced*. For example, the poset in Figure 3.2.1 has $e(P) = 61$ and $si(P) = 1$.

We note that $e(P) \equiv si(P) \bmod 2$ for all posets P. Furthemore, we denote by $P \oplus Q$ the ordinal sum (linear sum) of the posets and by $P + Q$ the disjoint union (parallel sum). Also, a poset is *disconnected* if its Hasse diagram is disconnected.

3.2.2 Domino tableaux and quotients

Given a poset $P = (X, \prec)$ with n elements, a *domino tableau* M is a set partition of X such that:

1. Every part is a chain of length 2 except for possibly one chain of length 1.

2. If there is a chain of length 1, then it is a maximal element.

Figure 3.2.2: A pair of posets illustrating domino tableaux

3. There exists an ordering $X_1, \ldots, X_k$ of the parts of M such that for all $1 \leq j \leq k$, the set $Xi \cup \cdots \cup Xj$ is a lower order ideal.

Condition (1) is equivalent to saying that M is a perfect matching in the Hasse diagram plus possibly one extra vertex. We say that a linear extension ℓ of P is *adapted* to M when i and $i+1$ are assigned to same part of X for all odd $i < n$. (If n is odd, then the label n will be assigned to the singleton vertex). Condition (3) implies that there is a linear extension $f \in LE(P)$ adapted to M . This can be constructed by assigning 1 and 2 to X_1, then 3 and 4 to X_2, and so on. We denote by $DT(P)$ the set of all domino tableaux of P.

For example, consider the pair of posets in Figure 3.2.2. The left poset has a highlighted domino tableau with an adapted linear extension. The right poset does not admit a domino tableau even though the Hasse diagram does have a perfect matching. Indeed, suppose we match a with d and b with e. We cannot put (a, d) before (b, e) because $b \prec d$. And we cannot put (b, e) before (a, d) because $a \prec e$.

It is not hard to show that any two linear extensions adapted to the same domino tableau must have the same sign. Therefore, we define the sign of a domino tableau to be the sign of the linear extensions which are adapted to it.

Given a poset P with a domino tableau M, we can construct the quotient poset P/M as follows. The vertices of P/M are the elements of M. The comparisons of P/M are generated by relations of the form

$$X_1 \preceq X_2 \text{ in } P/M \iff x_1 \preceq x_2 \text{ in } P \text{ for some } x_1 \in X_1, x_2 \in X_2$$

Condition (3) implies that this defines a valid poset structure for P/M . As an example, the left poset in the diagram above has P/M isomorphic to $C_2 + C_1$.

3.3 Lemmas

The following lemma is based on a standard involution (see for instance [Rus92, Lem. 3], [Sta97a, Thm. 1], [Whi01, §5], and [Sta05, Corr. 4.2].

Lemma 3.3.1. *Let P be a poset. Then*

$$si(P) = \left| \sum_{M \in DT(P)} \operatorname{sgn}(M) e(P/M) \right| \tag{3.2}$$

Proof. We construct an involution Φ on $LE(P)$ where $P = (X, \prec)$. Suppose P has n vertices and consider a linear extension ℓ of P. Define the set S to be the set of all odd integers $i \in [n-1]$ such that ℓ assigns i and $i+1$ to incomparable elements of P.

If S is the empty set, then we let $\Phi(\ell) = \ell$. Otherwise, let j be the smallest element of S. Then construct $\Phi(\ell)$ by switching the labels j and $j+1$. By assumption, this is still a valid linear extension. Moreover, it has opposite sign to ℓ. Therefore the terms corresponding to ℓ and $\Phi(\ell)$ will cancel out in the sum (3.1).

We give an example of Φ in 3.3. Since 3 is the smallest odd number not comparable to its successor, it gets switched with 4.

We are left only with fixed points of Φ. Suppose ℓ is a fixed point. Then ℓ is adapted to a unique domino tableau M formed by partitioning X into $\{\ell^{-1}(1), \ell^{-1}(2)\}, \{\ell^{-1}(3), \ell^{-1}(4)\}, \ldots$. This tableau will by definition have $\operatorname{sgn}(M) = \operatorname{sgn}(\ell)$. We can define a linear extension ℓ' on

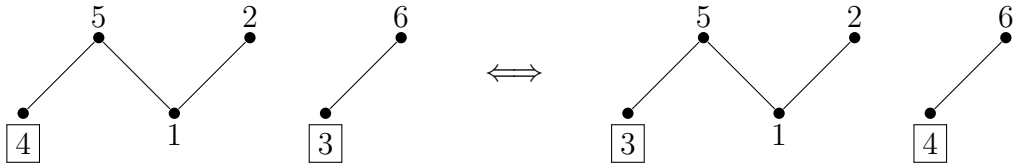


Figure 3.3.1: The involution Φ.

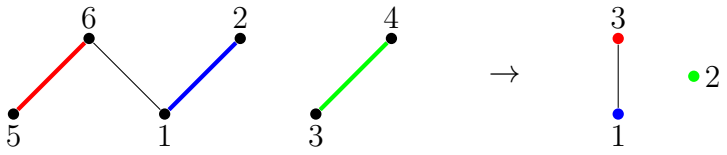


Figure 3.3.2: The quotienting operation.

P/M by assigning the label i to the subset containing $2i-1$. This is illustrated in Figure 3.3.

This constitutes a bijection between linear extensions of P which are adapted to M and $LE(P/M)$. Since every linear extension adapted to a domino tableau is also a fixed point of Φ, we obtain the formula (3.2). □

We give an example of Lemma 3.3.1. Consider the poset P at the top of Figure 3.3. It has two perfect matchings Y_1, Y_2, Y_3, Y_4 and Z_1, Z_2, Z_3, Z_4, both of which are domino tableaux, illustrated in at the bottom of the figure.

The two quotient posets (let us call them Y and Z) are not isomorphic. The red quotient Y has $e(P/M) = 4$, and the blue quotient Z has $e(P/M) = 2$. Since the two tableaux have opposite signs, we get $si(P) = |4-2| = 2$.

If P has very few domino tableaux, then we can reduce the problem of finding the sign imbalance of P to smaller posets:

Corollary 3.3.2. *If P is a poset that does not admit a domino tableau, then P is sign-balanced. If P is a poset with a unique domino tableau M, then $si(P) = e(P/M)$.*

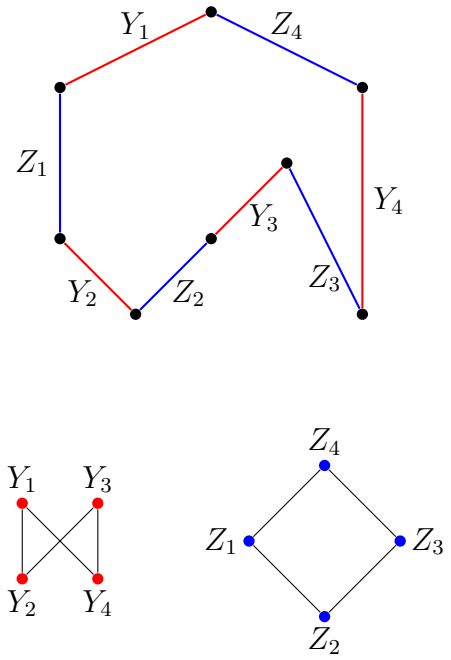


Figure 3.3.3: An example of Lemma 3.3.1

Our goal is to flip Lemma 3.3.1 by building a poset where we control $e(P/M)$. To that end, we will define an operation on posets.

Let $P = (X, \prec)$ be a poset. Call R *good* if it is a subset of X^2 with the following properties:

1. $(x, x) \in R$ for all $x \in X$,
2. $(x, y) \in R$ for all $x, y \in X$ such that y covers x in P,
3. If $(x, y) \in R$ then $x \preceq y$ in P.

In other words, R consists of the diagonal of X, all covering relations of P, and some subset of the non-covering relations of P. Then we define the poset $A(P, R)$ as follows. The vertices consist of pairs of the form (x, i) for $x \in X, i \in \{0, 1\}$. And our relations are given

by

$$(x, i) \prec (y, j) \text{ if } i = 0, j = 1, \text{ and } (x, y) \in R.$$

We claim that this allows us to control the sign imbalance of height 2 posets. We note that the first part of this lemma was proved (in the case where R is maximal) by Stachowiak in [Sta97a], who used it to show that counting the sign imbalance of a poset is #P-hard. See §3.5.4 for examples of this construction.

Lemma 3.3.3 (Main lemma)**.** *Let P be a poset. Then for any good R defined as above, $A(P, R)$ is a poset with height 2 and*

$$si(A(P, R)) = e(P).$$

Conversely, suppose Q is a poset with height 2 that is not sign-balanced. Then if Q has even number of vertices, there exists a poset P and a good set R such that

$$Q = A(P, R)$$

And if Q has an odd number of vertices, then there exists a poset P and a good set R such that

$$Q = A(P, R) + C_1.$$

Proof. For the first part, note that by construction the Hasse diagram of $A(P, R)$ has only one perfect matching, namely $M = \{((x, 0), (x, 1)) : x \in X\}$. This is also a domino tableau. Since R contains all the covering relations of P, we know $A(P, R)/M = P$. The result follows from Corollary 3.3.2.

For the other direction, suppose Q is a poset with height 2 which is not sign-balanced. By Corollary 3.3.2, Q must have at least one domino tableau M. Suppose that Q has an even number of vertices. We claim that the Hasse diagram of Q must in fact have only one perfect matching. Suppose for contradiction that it had another perfect matching N. Then $M \cup N$ must contain at least one cycle of length > 2. As Q was assumed to have height

2, this cycle can only correspond to a subposet of Q which is isomorphic to a crown poset. That is, we have elements $x_1, \ldots, x_{2k}$ in Q such that

$$x_1 \prec_M x_2 \succ_N x_3 \prec_M x_4 \succ_N \cdots x_1 \prec_M x_{2k} \succ_N x_1$$

But this contradicts M being a domino tableau, since we now have a loop in Q/M. Therefore M is the unique perfect matching. By construction, every pair of M has a bottom element and a top element.

Now let $P = Q/M$, and define $R \subset M^2$ by

$$(M_1, M_2) \in R \iff x \prec y \text{ for some } x \in M_1, y \in M_2,$$

It is easy to see that $Q = A(P, R)$.

Suppose now that Q has an odd number of vertices. If Q has no isolated vertices, then without loss of generality it has more minimal than maximal elements. But then Q cannot have a domino tableau. So Q must be sign-balanced. (Note that flipping a poset vertically does not affect whether it is sign-balanced). If it has two or more isolated vertices, it also cannot have a domino tableau. So for Q to not be sign-balanced, it must have exactly one isolated vertex v. This vertex must be the singleton in the domino tableau, which means $Q - v$ is a height 2 poset which is not sign-balanced. Now we just apply the previous case. □

3.4 Proofs

3.4.1 Proof of Theorem 3.1.5

First, suppose P is a height 2 poset with an odd number of linear extensions and $2n + 1$ vertices. Clearly P cannot be sign-balanced. Therefore Lemma 3.3.3 implies that P consists of an isolated vertex and a subposet of $2n$ vertices which also has an odd number of linear extensions. This implies that $f(n + 1) = f(2n)$. Therefore, we will assume that our posets

have an even number of vertices.

Consider the map A from Lemma 3.3.3. It is easy to see that A is injective. Take the chain poset C_n; this clearly has an odd number of linear extensions. Then there are exactly $2^{\binom{n-1}{2}}$ possible good sets R. Thus the set

$$\{A(C_n, R) : R \text{ good}\}$$

establishes our lower bound.

For the upper bound, consider the poset Π_n with vertex set $[n] \times \{0, 1\}$ and relations

$$(a_1, b_1) \prec (a_2, b_2) \text{ if } a_1 \leq a_2 \text{ and } b_1 \leq b_2$$

Let $\mathcal{D}$ be the set of subposets of Π_n such that $(a, 0) \prec (a, 1)$ for all $a \in [n]$. It is clear that the image of A is equal to D and that $|D| = 2^{\binom{n}{2}}$. Since any poset with an odd number of linear extensions is not sign-balanced, the lower bound follows. (Note that some posets in the image of A have an even number of linear extensions, so we do not have equality here). □

3.4.2 Proof of Theorem 3.1.6

Note that it suffices to consider the case where q is prime. We prove a somewhat broader version of 3.3.3. The proof essentially follows that of 3.1.5. Let P be a height 2 poset on m elements such that $q \nmid e(P)$. Fix ℓ to be a linear extension of P. Consider the subposets $P_1, P_2, \ldots, P_{\lfloor m/q \rfloor}$ defined by

$$\begin{aligned} P_1 &:= \text{ the induced subposet on elements labeled } 1, 2, \ldots, q \\ P_2 &:= \text{ the induced subposet on elements labeled } q+1, q+2, \ldots, 2q \\ &\cdots \end{aligned}$$

Note that there may be up to $q-1$ elements which are not contained in a subposet. Call ℓ *adapted* if none of these subposets are disconnected. (In the case $q = 2$, this means that ℓ is adapted to a domino tableau in the sense of Lemma 3.3.3).

Lemma 3.4.1. *If $q \nmid e(P)$ then P has a linear extension which is adapted.*

Proof. We show that the number of linear extensions which are not adapted is a multiple of q. The following is an equivalence relation on linear extensions which are not adapted.

Given a linear extension ℓ which is not adapted, let i be minimal such that P_i is disconnected. Let $\ell \equiv \ell'$ if ℓ and ℓ' are equal when restricted to P P_i. It is easy to see that this is an equivalence relation, and the size of an equivalence class is $e(P_i)$.

P_i is disconnected and has q elements. Therefore there exist nonempty posets Q_1, Q_2 such that $P_i = Q_1 + Q_2$. But since

$$e(Pi) = \binom{q}{|Q_1|} e(Qi)e(Q2)$$

we have $q|e(Pi)$. This follows because q is prime. That means that the set of linear extensions which are not adapted has been partitioned into equivalence classes of sets each of which has size a multiple of q. □

So we can fix an adapted linear extension ℓ and corresponding subposets $P_1, P_2, \ldots, P_{\lfloor m/q \rfloor}$ By construction, the edges from P_i to P_j where $i < j$ can only be between a bottom vertex of P_i and a top vertex of P_j. The notion of bottom and top vertex are well-defined because P_i and P_j are connected. Each subposet can have only at most $q-1$ elements on the top or bottom. A simple perturbation argument shows that the greatest number of external edges is possible when the first half of the subposets are of the form $A_{q-1} \oplus A_1$ and the second half are of the form $A_1 \oplus A_{q-1}$. (For simplicity we will assume $\lfloor m/q \rfloor$ is even; extending to the case where $\lfloor m/q \rfloor$is odd is trivial.) In this case there are at most

$$\left(\frac{1}{2}\left\lfloor\frac{m}{q}\right\rfloor\right)^2 \cdot (q-1)^2 + \left(\frac{1}{2}\left\lfloor\frac{m}{q}\right\rfloor\right)^2 \cdot (q-1) + O(m)$$

possible external edges. (The first term counts edges which go between the first and second halves, and the second counts edges which remain within one half or the other). Let c_q be the number of connected height 2 posets with q elements. Then we can construct P as follows: first, we pick each of the $\lfloor m/q \rfloor$ subposets. Then we add external edges between the subposets; the above discussion gives a bound on the number of ways to do this. Lastly, each of the $m - \lfloor m/q \rfloor$ remaining vertices can be greater than or incomparable to all the previous vertices. This gives an upper bound of

$$c_q^{\lfloor m/q \rfloor} 2^{\left(\frac{1}{2}\left\lfloor \frac{m}{q} \right\rfloor\right)^2 \cdot (q)(q-1)+O(m)} \cdot 2^{(m-\lfloor m/q \rfloor)} = 2^{\frac{q-1}{4q}m^2+O(m)}$$

possible posets, as required. This completes the proof of Theorem 3.1.6.

3.5 Final remarks

3.5.1 Completeness of the number of linear extensions of height 2 posets

Our results do not contradict Conjecture 3.1.4, but can be used to construct numbers which are not the number of linear extensions of any height 2 poset. We begin by giving a loose bound on the possible odd numbers of linear extensions of a height 2 poset:

Proposition 3.5.1. *Let P be a height 2 poset on $2n$ vertices with an odd number of linear extensions. Then*

$$(n!)^2 \leq e(P) \leq (n!)(2n-1)!!$$

Proof. By Lemma 3.3.3, any such poset must satisfy

$$\bigcup_{i=1}^{n} C_2 \subseteq P \subseteq A_n \oplus A_n$$

□

Letting $n = 9$ we see that any height 2 poset on ≤ 18 elements for which $e(P)$ is odd has at most $9! \cdot 17!! = 125046361440004$ linear extensions. But letting $n = 10$ we see that

any height 2 poset on 20 vertices for which $e(P)$ is odd has at least $10!^2 = 13168189440000$ linear extensions. Also by Lemma 3.3.3, any height 2 poset P on 19 elements with an odd number of linear extensions has an isolated vertex, and so $19 \mid e(P)$. Combining these facts we obtain that there is no height 2 poset with $10!^2 - 1 = 13168189439999$ linear extensions. See the footnote of §6.4 in [CP23].

3.5.2 Geometric definition of Ruskey's conjecture

Given a poset P with elements labeled by $[n]$, the *order polytope* $O(P)$ is the subset of $[0,1]^n$ given by

$$x_i \leq x_j \text{ whenever } i \prec j \text{ in } P$$

Its *canonical triangulation* is given by cutting $O(P)$ with the hyperplanes of the form $x_i = x_j$ for $i, j \in [n]$. Note that each simplex corresponds to a linear extension of P . Since this is a triangulation obtained by cutting with hyperplanes, it must be bipartite. [SS06] observed that the two parts correspond exactly to the odd and ever permutations in the definition of sign imbalance, and so a poset is sign-balanced if and only if both parts are the same size.

We note that this provides an immediate proof that the graph $G(P)$ is connected. Any two face-adjacent simplicies in the canonical triangulation of $O(P)$ correspond to linear extensions which differ by an adjacent transposition. Since triangulations must be face-connected, $G(P)$ is connected.

Soprunova and Sottile [SS06] considered toric varieties associated to order polytopes. In this case, sign imbalance provides a lower bound for the number of real solutions of a Wronski polynomial system.

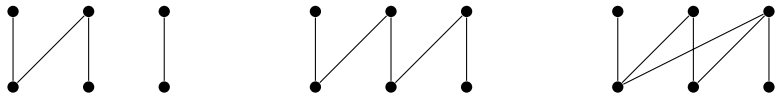


Figure 3.5.1: All height 2 posets on 6 vertices with an odd number of linear extensions.

3.5.3 GapP and #P

It is easy to see that sign imbalance is the absolute difference between two #P functions, one counting even linear extensions and the other counting odd linear extensions. However, this does not imply (as claimed in [Sta97a]) that sign imbalance is in #P. The closure of #P under subtraction is called GapP and was defined independently in [FFK94] and [Gup95] building on [OH93]. Therefore, the following conjecture remains open:

Conjecture 3.5.2. Sign Imbalance *is not in #P.*

Many natural combinatorial differences are not in #P; see [IP22] for a survey.

3.5.4 An example of Theorem 3.1.5

Consider the case $n = 3$. There are two posets on 3 elements with an odd number of linear extensions, namely $C_2 + C_1$ and C_3. The former poset has $re(C_2 + C_1) = cr(C_2 + C_2) = 1$, and the latter has $re(C_3) = 2$ and $cr(C_3) = 1$. So there are $2^{1-1} + 2^{2-1} = 3$ height 2 posets on 6 elements with an odd number of linear extension, illustrated in Figure 3.5.4

These posets were obtained by applying the map A in Lemma 3.3.3. The left poset has $P = C_1 + C_2$, and the other two have $P = C_3$ for different choices of R. They have 75, 61, and 57 linear extensions respectively.

3.5.5 Euler numbers and posets for which many primes do not divide $e(P)$.

The Euler numbers E_n [OEIS, A000111] count the number of linear extensions of a zizag poset Z_n and have exponential generating function $\sec x + \tan x$. Using these, we can construct

posets whose number of linear extensions avoids divisibility by many primes. Theorem 3.1.6 shows that for all q the number of posets with $q \nmid e(P)$ is small. Here we give an example of an infinite set of posets which satisfy many such conditions.

Proposition 3.5.3. *Let Q be a finite set of primes. Then there exists an infinite sequence of posets $P_1, P_2, \ldots,$ such that*

$$e(P_i) \equiv 1 \mod q \text{ for all } q \in Q, i \geq 1$$

Proof. We show that for any prime q and integer $n > q$,

$$E_n \equiv E_q E_{n-(q-1)} \mod q \tag{3.3}$$

Indeed, consider the set of $\ell \in LE(Z_n)$ such that $1, 2, \ldots, q$ are not in a contiguous block. For each of these linear extensions, we can permute the labels $1, 2, \ldots, q$ in some number of ways that is divisible by q. (This is essentially the same as the proof of Lemma 3.4.1). So, mod q, we can ignore these. But if $1, \ldots, q$ are in a contiguous block, then we can collapse the entire block into a single element; this leaves $Z_{n-(q-1)}$. This shows 3.3.

Since $E_q \equiv \pm 1 \mod q$ [OEIS, A000111] and $E_1 = 1$ we need only pick n such that $n \equiv 1 \mod (q-1)$ for all $q \in Q$. □

As a side note, we show that $3 \nmid E_n$ for all $n \geq 1$. Indeed, one can verify that $3 \nmid En$ for all $1 \leq n \leq 3$, and by 3.3 the result follows. Similarly, computer calculations show that $p \nmid E_n$ for all n for

$$p = 3, 7, 11, 23, 83, 107, 163, 167, 179, 191, 199, 211, 227, 239, 367, 383, 443, 479, 487, 503, 599, \ldots$$

It is not clear if there are infinitely many such primes.

CHAPTER 4

Area generating functions

4.1 Introduction

Let λ be an integer partition[1]. Then we can define the *area generating function* $f_\lambda(q)$ as:

$$f_\lambda(q) = \sum_{\mu \subseteq \lambda} q^{|\mu|}$$

Note that this generalizes other well-known q-series. Specifically, when λ is a partition corresponding to an a-by-b rectangle, then $f_\lambda(q) = \binom{a+b}{a}_q$. And when λ is the staircase partition $(n\ n-1\ \ldots\ 2\ 1)$, then $f_\lambda(q) = C_{n+1}(q)$, where C a *q-Catalan number* in the sense of Carlitz and Riordan [CR64].

In this chapter we analyze area generating functions of partitions. We give a combinatorial interpretation of $f_\lambda(-1)$ in Section 4.4. We also give a simple criterion to determine when $f_\lambda(-1)$ is zero. Lastly, we use our results to show a weak form of Ruskey's conjecture.

Clearly, partitions contained in λ are equivalent to up-right walks in the Young diagram of λ. We will use these notions interchangeably.

[1]Throughtout this chapter, the unqualified term *partition* will refer to integer partitions.

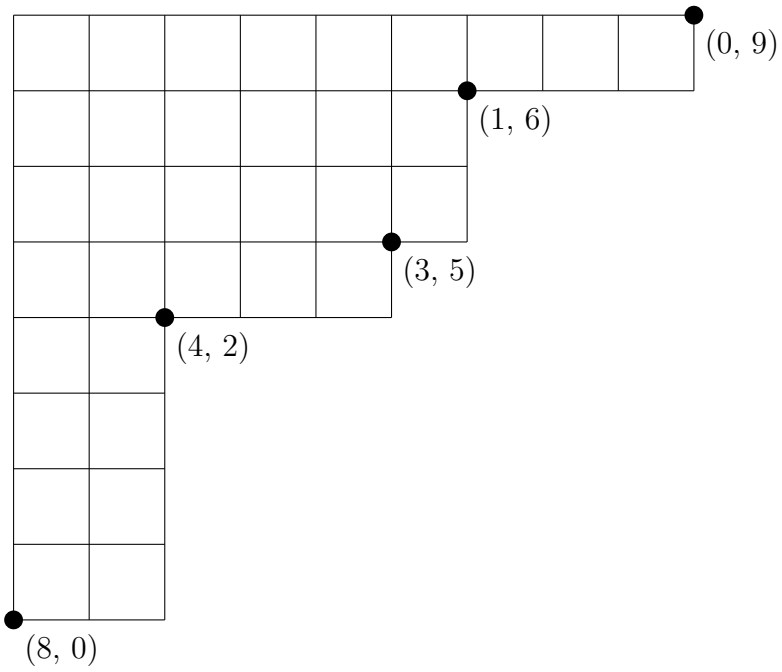


Figure 4.2.1: Interior corners of a partition

4.2 Definitions

4.2.1 Partitions and generating functions

We assume familiarity with the basic notions of Young diagrams and partitions. Let $\lambda = (\lambda_1, \ldots \lambda_k)$ be a partition with $\lambda_1 \geq \cdots \geq \lambda_k$. Then an *interior corner* of λ is a pair of integers (i, j) such that $\lambda_{i+1} = j$ and $\lambda_i > j$, where we adopt the convention that $\lambda_0 = \infty$ and $\lambda_{k+1} = 0$. See Figure 4.2.1 for an example of a partition and its five interior corners. Note that by convention the empty partition has a unique interior corner at $(0, 0)$.

Next, we define properties of polynomials. Let $f(x) = a_0 + a_1 x + \cdots + a_k x^k \in \mathbb{N}[x]$ be a polynomial. Then f is *unimodal* if for some integer $\ell \leq k$ we have

$$a_0 \leq a_1 \leq \cdots \leq a_{\ell-1} \leq a_\ell \geq a_{\ell+1} \geq \cdots \geq a_{k-1} \geq a_k.$$

We say f is *sign-balanced* if $f(-1) = 0$. And we define f to be *2-decomposable* if

$$\frac{f(x)}{x+1} \in \mathbb{N}[x]$$

where $\mathbb{N} = \{0, 1, 2, \dots\}$. We extend each of these definitions to ordered finite lists of integers.

Trivially, every 2-decomposable polynomial is also sign-balanced, but the converse is not true ($1 + x^3$ is a counterexample). It is easily seen that every unimodal sign-balanced polynomial is also 2-decomposable.

We note that partition generating functions are not always unimodal. Stanton [Sta87] discovered the example $\mu = (8\ 8\ 4\ 4)$, which has area generating function

$$\begin{aligned} f_\mu(q) = 1 + q + 2q^2 + 3q^3 + 5q^4 + 6q^5 + 9q^6 + 11q^7 + 15q^8 + \\ + 17q^9 + 21q^{10} + 23q^{11} + 27q^{12} + 28q^{13} + \boxed{31q^{14} + 30q^{15} + 31q^{16}} + \\ + 27q^{17} + 24q^{18} + 18q^{19} + 14q^{20} + 8q^{21} + 5q^{22} + 2q^{23} + q^{24} \end{aligned}$$

where the boxed section indicates the place at which unimodality fails. In fact, μ and its conjugate μ' are the smallest examples of partitions with nonunimodal area generating functions. We note that unimodality does hold for rectangular partitions; this is a classic and nontrivial result first proved by Sylvester [Syl78]. Later proofs and extensions were given by O'Hara [OHa90], Proctor [Pro82], and Pak and Panova [PP].

For each partition λ we construct a poset $P(\lambda) = (X, \prec)$ as follows. The elements of X are given by partitions $\mu \subseteq \lambda$, ordered by containment. Then it is clear that $P(\lambda)$ is a graded poset and that f_λ is its rank generating function. Let $G(\lambda)$ be the Hasse diagram of $P(\lambda)$. Ruskey's conjecture [Rus88] implies that if f_λ is sign-balanced, then $G(\lambda)$ has a Hamiltonian path. We will prove a weaker version of this in Theorem 4.3.4.

4.2.2 Modified Young diagrams and tiled walks

In order to simplify the statements of our theorems, we modify Young diagrams as follows. Let $\lambda = (\lambda_1, \dots, \lambda_k)$ be a partition with Young diagram Y. Then, if λ_1 is odd we add a

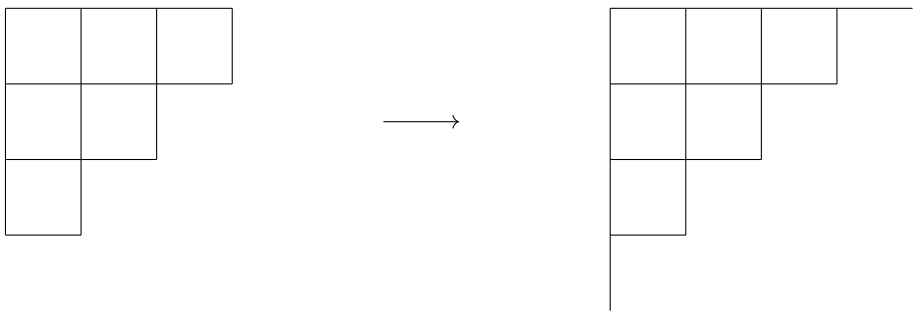


Figure 4.2.2: Modification of a Young diagram

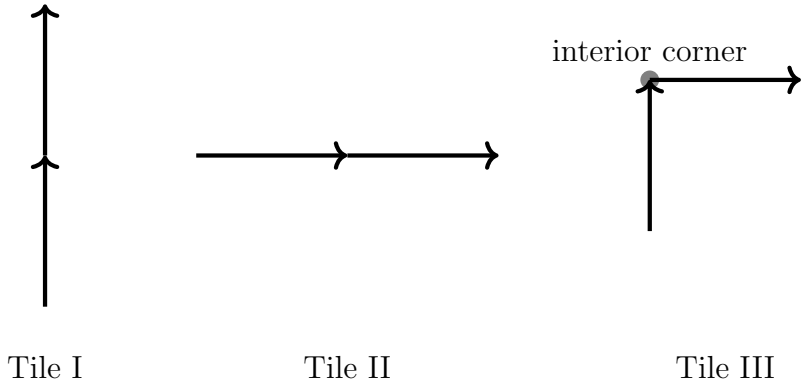


Figure 4.2.3: The three allowable tiles in a tiled walk

single horizontal segment to the top right of Y. And, if k is odd we add a single vertical segment to the bottom left of Y. This is illustrated in Figure 4.2.2.

Consider a partition λ with a modified Young diagram Y. An *up-right walk* through λ is a walk from the bottom left corner of Y to the top right corner of Y which only moves up and right. An up-right walk in Y is *tiled* if it can be partitioned into the three tiles illustrated in Figure 4.2.2. Note that Tile III requires the indicated point to be an interior corner of Y. Every modified Young diagram has at least one tiled walk consisting of a number of Tile Is followed by a number of Tile IIs.

Suppose $T_k, T_{k+1}, \ldots, T_\ell$ are sequence of consecutive tiles in a walk W in a modified Young diagram Y such that $\ell > k$. We call such an interval *flippable* if either of the two

following conditions holds:

1. T_k and T_ℓ are both instances of Tile III, and there are no other instances of Tile III between T_k and T_ℓ.

2. T_k is an instance of Tile I and T_ℓ is an instance of Tile II such that the middle points of both tiles are interior corners of Y. Furthermore, W does not touch the border of Y between tiles T_k and T_ℓ.

An up-right walk in a modified Young diagram is *bad* if it does not contain a flippable interval. And an up-right walk is *good* if it is not bad. Note that a walk that uses Tile III at least twice must be good. See Observation 4.4.1

4.3 Results

Our main result is a combinatorial interpretation for $f_\lambda(-1)$, proved by a sign-reversing partial involution on the up-right walks in W.

Theorem 4.3.1. *Let λ be a partition. Then $f_\lambda(-1)$ is equal to the number of bad walks in the modified Young diagram of λ.*

We note the following immediate corollary which is not inherently obvious.

Corollary 4.3.2. *Let λ be a partition. Then $f_\lambda(-1) \geq 0$.*

Our result also allows us to give the following simple criterion for whether f_λ is sign-balanced.

Theorem 4.3.3. *Let λ be a partition. Then $f_\lambda(-1) = 0$ (that is, f_λ is sign-balanced) if and only if every interior corner of λ has at least one odd coordinate.*

In fact, by modifying the involution we obtain a weak form of Ruskey's conjecture in this special case.

Theorem 4.3.4. *Let λ be a partition with $f_\lambda(-1) = 0$ (that is, f_λ is sign-balanced). Then $G(\lambda)$ has a perfect matching.*

Again we get an immediate corollary:

Theorem 4.3.5. *Let λ be a partition with $f_\lambda(-1) = 0$ (that is, f_λ is sign-balanced). Then f_λ is 2-defomposable.*

4.4 Positivity

4.4.1 Proof of Theorem 4.3.1

First, we point out that we need only consider tiled walks. Indeed, suppose a walk W is not tiled. Then there exists some even positive integer i such that steps $i-1$ and i are different (either up then right or right then up). If so, then we can simply flip the order of these two steps, changing the area above the path by 1. This is a sign-reversing operation similar to the operation in 3.3.1. (Note that we need to exclude cases where this would lead to us escaping the partition; this corresponds to Tile III).

Fix a partition λ. Let $\mathcal{W}_Y$ be the set of all up-right tiled walks through the modified Young diagram Y of λ. Next, let $\mathcal{G}_Y \subseteq \mathcal{W}_Y$ be the set of good up-right walks in Y. Our goal will be to provide a sign-reversing involution on $\mathcal{G}_Y$.

If W is a walk, then let $n_3(W)$ be the number of instances of tile III in W. We begin with the following easy observation:

Observation 4.4.1. *$n_3(W)$ is always even.*

This follows from the fact that a modified Young diagram has an even number of up and right steps to take. Given a walk W we denote by $|W|$ the area above and to the left of it, which corresponds to the size of the corresponding partition. Our next lemma relates the parity of W with the types of tiles it contains.

Lemma 4.4.1. *For any walk W, we have $(-1)^{|W|} = (-1)^{n_3(W)/2}$.*

Note that this is well-defined by Observation 4.4.1.

Proof. We proceed by induction on $n_3(W)$. If the walk W contains no instances of Tile III, then the corresponding partition has only even parts; thus $|W|$ is clearly even.

So we may assume $n_3(W) \geq 2$. Let T and U be the last two tiles of type III in W. Then the area above W can be split into seven regions plus an extra unit square as in Figure 4.4.1.

But regions A_3 and A_6 both have even area by the base case of our induction. Regions A_1, A_2, A_4, and A_5 are rectangles with at least one even dimension, so they all have even area as well. And A_7 is the area above a walk with two fewer instances of Tile III, so by the inductive hypothesis

$$(-1)^{|W|} = (-1) \cdot (-1)^{(n_3(W)-2)/2}$$

as required.

□

Now we can define our involution Φ. Fix a good walk W. Let $T_k, \ldots, T_\ell$ be the lexicographically smallest flippable interval in W. Then, if T_k and T_ℓ are Tile I and Tile II respectively, we replace them both with Tile III, 'pushing' the portion of the walk between them up and left. Likewise, if they are both Tile III, we replace them with Tile I and Tile II respectively, 'pushing' the portion of the walk between them down and left.

It is easy to see that the conditions on flippable intervals ensure that Φ is a valid function from $\mathcal{G}_Y$ to $\mathcal{G}_Y$. Since Φ changes the number of Tile IIIs in a walk by 2, Lemma 4.4.1 ensures that Φ is sign-reversing. It is also straightforward to show that Φ is an involution. Therefore all good walks cancel out in the computation of $f_\lambda(-1)$.

Lastly, we note that all bad walks have no instances of Tile III. If a walk has at least one Tile III, then by Observation 4.4.1 it must have at least two. Therefore, the interval of the

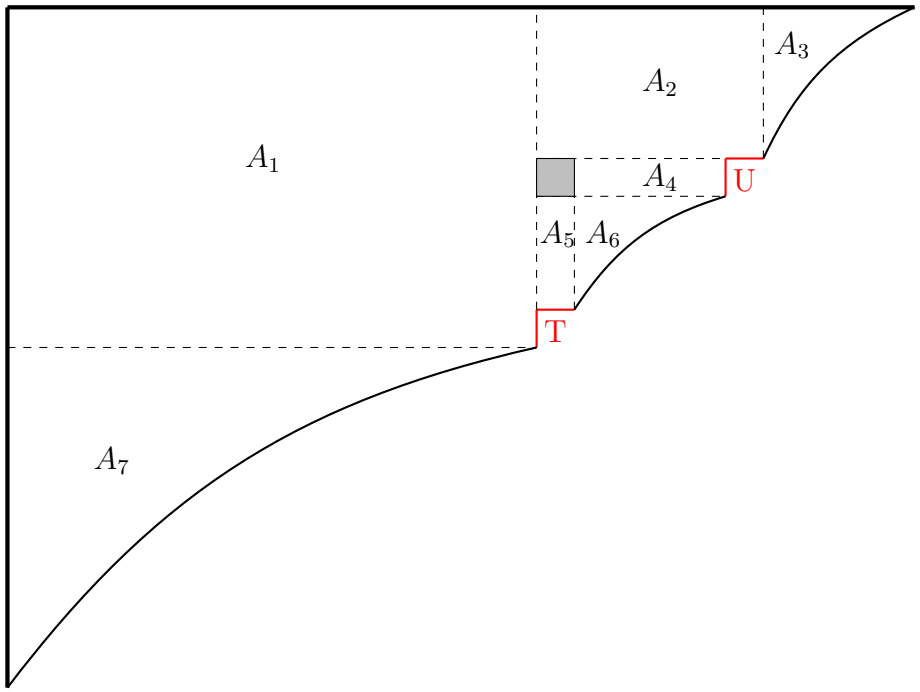


Figure 4.4.1: The inductive step of the proof of Lemma 4.4.1

Figure 4.4.2: The flipping operation

walk between the last two copies of Tile III (inclusive) would have to be a flippable interval. By 4.4.1 this means that all bad walks have a positive sign.

Therefore $f_\lambda(-1)$ is equal to the number of bad walks and we are done. □

4.4.2 Proof of Theorem 4.3.3

This follows from our characterization of bad walks in the proof of Theorem 4.3.1. A bad walk can only have tiles of Types I and II.

Suppose a partition λ has at least one odd coordinate in every interior corner. Then, by definition, λ has an odd number of parts and the largest part has odd size. So in constructing the modified Young diagram Y we must have added both an extra vertical and an extra horizontal segment.

Fix an up-right walk W in $\mathcal{W}_Y$. By parity, if W touches an interior corner of Y then it can only be in the middle of the tile. However, the added segments mean that W must begin with a Tile I (with an interior corner in the middle) and end with a Tile II (with an interior corner in the middle).

If this is not a flippable walk, then W must touch the border of Y at least once in between these. However, that must mean that it touches an interior corner. Depending on whether this is at a Type I or a Type II tile, we have a smaller version of the problem either after or before this interior corner. A simple induction concludes the proof.

For the other direction, suppose there is an interior corner with both coordinates even. Then it is easy to construct a walk of Tiles I and II that touches the border of Y exactly at this corner (and perhaps at the very beginning and end). Such a walk cannot have a flippable interval.

4.5 2-decomposability

4.5.1 Proof of Theorem 4.3.4

. Fix a parition λ with no bad walks. Again, let $\mathcal{W}_Y$ be the set of all up-right walks and $G(\lambda)$ the corresponding graph. The operation at the beginning of the proof of Theorem 4.3.1 produces a matching M on all *non-tiled* walks. Let Φ be the main involution of Theorem 4.3.1.

Let W be a tiled walk. Since W is good, it has a lexicographically smallest flippable interval I. Without loss of generality, the first tile in this interval is of type III (so we flip up to get $\Phi(W)$). Now, it is possible that W and $\Phi(W)$ are adjacent in $G(\lambda)$, in which case we add that edge to M. This happens if $|\Phi(W)| - |W| = 1$.

Otherwise, we will construct a path from W to $\Phi(W)$ in $G(\lambda)$ such that every other edge belongs to M. Using this, we can extend M by the Hungarian method to cover all of $G(\lambda)$.

Define I to begin and end at the interior corners of λ. A step in $G(\lambda)$ corresponds to pushing the walk up by one square. Our process will proceed as follows: first, go right to left along I, pushing the walk up by one every time it is possible. (This will happen at every horizontal edge). Then, go right to left, pushing up each time it is possible. (This will happen at every vertical step). It is easy to see that every other step is along M and that no two of these paths will intersect. Therefore, there is a perfect matching in $G(\lambda)$.

4.6 Examples

We illustrate Theorem 4.3.1 with an evaluation of $f_\lambda(-1)$ for some classic examples of partition families.

Example 4.6.1. *The q-binomial coefficient is an area generating function for a rectangular*

partition. If λ is an a by b rectangle we get

$$f_\lambda(-1) = \left[\binom{a}{b}_q\right]_{q=-1} = \begin{cases} 0 & \text{if } a, b \text{ odd} \\ \binom{(a+b-1)/2}{(a-1)/2} & \text{if } a \text{ odd}, b \text{ even.} \\ \binom{(a+b-1)/2}{a/2} & \text{if } a \text{ even}, b \text{ odd.} \\ \binom{(a+b)/2}{a/2} & \text{if } a, b \text{ even} \end{cases}$$

Proof. By Theorem 4.3.1 we need only consider tiled walks with only tiles I and II.

If a and b are both odd, then the modified Young diagram has both extra vertical and horizontal segments. Any walk would have to use Tile I to start and Tile II to end and thus could not touch the border in between. Thus such walks are automatically good.

Conversely, if one of a or b is even then all such walks are bad; there is no way to construct a flippable interval. So we are counting all walks with even runs. □

We can also compute the case of the q-Catalan numbers as follows:

Example 4.6.2. *The q-Catalan number is an area generating function for a staircase partition. If λ is the partition $(n-1\ n-2\ \cdots 1)$ for some $n \geq 1$ then we get*

$$f_\lambda(-1) = C_n(-1) = \begin{cases} 0 & \text{if } n \text{ even} \\ c_{(n-1)/2} & \text{if } n \text{ odd} \end{cases}$$

where c_k is the kth Catalan number.

Proof. If n is even then Theorem 4.3.3 ensures that $f_\lambda(-1) = 0$. But if n is odd then it is easy to see that every path consisting of only Tiles I and II is bad. These paths correspond exactly to up-right walks in a smaller staircase partition. □

[AKM] Youssef Abdelaziz, Christoph Koutschan and Jean-Marie Maillard, On Christol's conjecture, *J. Phys. A* **53** (2020), no. 20, 205201, 16 pp.

[AB] Boris Adamczewski and Jason B. Bell, Diagonalization and rationalization of algebraic Laurent series, *Ann. Sci. Éc. Norm. Supér.* **46** (2013), 963–1004.

[Aom] Kazuhiko Aomoto, Spectral theory on a free group and algebraic curves, *J. Fac. Sci. Univ. Tokyo, Sect. IA Math.* **31** (1984), 297–318.

[ADH] Matthias Aschenbrenner, Lou van den Dries and Joris van der Hoeven, *Asymptotic differential algebra and model theory of transseries*, Princeton Univ. Press, Princeton, NJ, 2017, 849 pp.

[ABBS] Ibrahim Assem, Martin Blais, Thomas Brüstle, and Audrey Samson, Mutation classes of skew-symmetric 3×3-matrices, *Comm. Algebra* **36** (2008), no. 4, pp. 1209-1220.

[BD] Cyril Banderier and Michael Drmota, Formulae and asymptotics for coefficients of algebraic functions, *Combin. Probab. Comput.* **24** (2015), 1–53.

[BMPS] Yuliy Baryshnikov, Stephen Melczer, Robin Pemantle and Armin Straub, Diagonal asymptotics for symmetric rational functions via ACSV, in *LIPIcs. Leibniz Int. Proc. Inform.* **110**, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2018, Art. No. 12, 15 pp.

[BS] Véronique Bazier-Matte and Ralf Schiffler, Knot theory and cluster algebras. *Advances in Mathematics* **408** (2022), part B

[BBH] Andre Beineke, Thomas Brüstle, and Lutz Hille, Cluster-Cyclic Quivers with Three Vertices and the Markov Equation, *Algebras and Representation Theory* **14** (2011), no.1 pp. 97-112.

[BM] Jason Bell and Marni Mishna, On the complexity of the cogrowth sequence, *J. Comb. Algebra* **4** (2020), 73–85.

[Ben] Max Benson, Growth series of finite extensions of $\mathbb{Z}^n$ are rational, *Invent. Math.* **73** (1983), 251–269.

[BFZ] Arkady Berenstein, Sergey Fomin and Andrei Zelevinsky, Cluster algebras III: Upper bounds and double Bruhat cells, *Duke Math. J.* **126** (2005), no. 1, pp. 1-52.

[Ber18] George Bergman, Some results on counting linearizations of posets, preprint (2018), 20 pp. `arxiv:1802:01712`.

[B+] Alin Bostan, Salah Boukraa, Gilles Christol, Saoud Hassani and Jean-Marie Maillard, Ising n-fold integrals as diagonals of rational functions and integrality of series expansions, *J. Phys. A* **46** (2013), no. 18, 185202, 44 pp.

[BLS] Alin Bostan, Pierre Lairez and Bruno Salvy, Multiple binomial sums. *J. Symbolic Comput.* **80** (2017), 351–386.

[BY] Alin Bostan and Sergey Yurkevich, On a class of hypergeometric diagonals, *Proc. AMS* **150** (2022), 1071–1087.

[Bou] Mireille Bousquet-Mélou, Rational and algebraic series in combinatorial enumeration, in *Proc. ICM*, Vol. III, EMS, Zürich, 2006, 789–826.

[BW00] Graham Brightwell and Douglas B. West, Partially ordered sets, Ch. 11 in Handbook of discrete and combinatorial mathematics, CRC Press, Boca Raton, FL, 2000, 717–752.

[BW91] Graham Brightwell and Peter Winkler, Counting linear extensions, *Order* **8** (1991), pp. 225-242.

[Can] James W. Cannon, The combinatorial structure of cocompact discrete hyperbolic groups, *Geom. Dedicata* **16** (1984), 123–148.

[CM] Merlin Carl and Boris Z. Moroz, On a Diophantine representation of the predicate of provability, *J. Math. Sci.* **199** (2014), 36–52.

[CR64] L. Carlitz and J. Riordan, Two element lattice permutation numbers and their q-generalization, *Duke Math. J.* **31** (1964), 371-388.

[CP23] Swee Hong Chan and Igor Pak, Computational complexity of counting coincidences, preprint (2023), 23 pp. `arxiv:2308.10214`

[Che87] Anton Chekov, From the Diary of a Violent Tempered Man / Из записок вспыльчивого человека (in Russian), *Budlinik* No. 26, 27 (1887).

[Chr1] Gilles Christol, Globally bounded solutions of differential equations, in *Lecture Notes in Math.* **1434**, Springer, Berlin, 1990, 45–64.

[Chr2] Gilles Christol, Fonctions Hypergéométriques et diagonales de fractions rationnelles (in French), talk slides in *Journées Holonomes* (Feb. 14, 2014); available at tinyurl.com/3xuj8xcd

[Coh] Joel M. Cohen, Cogrowth and amenability of discrete groups, *J. Funct. Anal.* **48** (1982), 301–309.

[CL] Alexander Coward and Marc Lackenby, An upper bound on Reidemeister moves, *Amer. J. Math.* **136** (2014), no. 4, pp. 1023-1066.

[Del] Pierre Deligne, Intégration sur un cycle évanescent (in French), *Invent. Math.* **76** (1984), 129–143.

[DL] Jan Denef and Leonard Lipshitz, Algebraic power series and diagonals, *J. Number Theory* **26** (1987), 46–67.

[DP20] Sam Dittmer and Igor Pak, Counting linear extensions of restricted posets, *Electronic Journal of Combinatorics* **27** (2020), pp. 1-13.

[DLS] Moon Duchin, Hao Liang and Michael Shapiro, Equations in nilpotent groups, *Proc. AMS* **143** (2015), 4723–4731.

[DS] Moon Duchin and Michael Shapiro, The Heisenberg group is pan-rational, *Adv. Math.* **346** (2019), 219–263.

[ERRW] Murray Elder, Andrew Rechnitzer, Esaias J. Janse van Rensburg and Thomas Wong, The cogrowth series for $BS(N, N)$ is D-finite, *Internat. J. Algebra Comput.* **24** (2014), 171–187.

[FST] Anna Felikson, Michael Shapiro, and Pavel Tumarkin. Skew-symmetric cluster algebras of finite mutation type. *J. Eur. Math. Soc.* **14** (2008), no. 4, pp. 1135- 1180.

[FFK94] Stephen Fenner, Lance Fortnow, and Stuart Kurtz, Gap-definable counting classes, *Journal of Computer and System Sciences* **48** (1994), pp. 116-148

[FTS] Alessandro Figà-Talamanca and Tim Steger, Harmonic analysis for anisotropic random walks on homogeneous trees, *Mem. AMS* **110** (1994), no. 531, 68 pp.

[FS] Philippe Flajolet and Robert Sedgewick, *Analytic combinatorics*, Cambridge Univ. Press, Cambridge, 2009, 810 pp.

[Fom22] Sergey Fomin, Quiver mutations, talk at *Open Problems in Algebraic Combinatorics*, Minneapolis (2022), slides available at https://www.samuelfhopkins.com/OPAC/files/slides/fomin.pdf, video at https://youtu.be/ watch?v=bIRnb0OFvlM, approx. 66 min.

[FN] Sergey Fomin and Scott Neville. Long mutation cycles, preprint (2023), 41 pp. `arxiv:2304.11505`

[FPST] Sergey Fomin, Pavlo Pylyavskyy, Eugenii Shustin, and Dylan Thurston. Morsifications and mutations. *J. Lond. Math. Soc.* **105** (2022), no. 4, pp. 2478-2554.

[FWZ] Sergey Fomin, Lauren Williams, and Andrei Zelevinsky. Introduction to Cluster Algebras. Chapters 1-3, `arxiv:1608.05735`. Chapters 4-5, `arxiv:1707.07190`. Chapter 6, `arxiv:2008.09189`. Chapter 7, `arxiv:2106.02160`.

[FZ1] Sergey Fomin and Andrei Zelevinsky. Cluster algebras. I. Foundations. *J. Amer. Math. Soc.* **15** (2002), no. 2, pp. 51-89.

[FZ2] Sergey Fomin and Andrei Zelevinsky. Cluster algebras. II. Finite type classification. *Invent. Math.* **154** (2003), no. 1, pp. 63-121.

[Fur] Harry Furstenberg, Algebraic functions over finite fields, *J. Algebra* **7** (1967), 271–277.

[GL] Pavel Galashin and Thomas Lam. Plabic links, quivers, and skein relations, preprint (2022), `arxiv:2208.01175`, 44 pp.

[GJ] Michael Garey and David Johnson, "Strong" NP-completeness results: motivation, examples, and implications, *J. ACM* **25** (1978), pp. 499-508.

[GJ2] Michael Garey and David Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman and Company, San Francisco, CA, 1979, 338 pp.

[Gar] Stavros Garoufalidis, G-functions and multisum versus holonomic sequences, *Adv. Math.* **220** (2009), 1945–1955.

[GP1] Scott Garrabrant and Igor Pak, Counting with irrational tiles, preprint (2014), 29 pp.; arXiv:1407.8222.

[GP2] Scott Garrabrant and Igor Pak, Pattern avoidance is not P-recursive, preprint (2015), 18 pages; `arXiv:1505.06508`; Permutation patterns are hard to count, in *Proc. 27th SODA*, ACM, New York, 2016, 923–936.

[GP3] Scott Garrabrant and Igor Pak, Words in linear groups, random walks, automata and P-recursiveness, *J. Comb. Algebra* **1** (2017), 127–144.

[GMO] Albert Garreta, Alexei Miasnikov and Denis Ovchinnikov, Diophantine problems in solvable groups, *Bull. Math. Sci.* **10** (2020), no. 1, 2050005, 27 pp.

[Gas] William Gasarch, Hilbert's tenth problem: refinements and variants, *ACM SIGACT News* **52** (2021), no. 2, 36–44.

[Gow] W. Timothy Gowers, Lower bounds of tower type for Szemerédi's uniformity lemma, *Geom. Funct. Anal.* **7** (1997), 322–337.

[GL] Be'eri Greenfeld and Hagai Lavner, Growth of unbounded subsets in nilpotent groups, random mapping statistics and geometry of group laws, *Int. Math. Research Not.*, published online Feb. 5, 2022.

[Gre] Driss Gretete, Random walk on a discrete Heisenberg group, *Rend. Circ. Mat. Palermo* **60** (2011), 329–335.

[Gri] Rostislav I. Grigorchuk, Symmetrical random walks on discrete groups, in *Multi-component random systems*, Dekker, New York, 1980, 285–325.

[GH] Rostislav I. Grigorchuk and Pierre de la Harpe, On problems related to growth, entropy, and spectrum in group theory, *J. Dynam. Control Systems* **3** (1997), 51–89.

[GS] Fritz Grunewald and Daniel Segal, Some general algorithms. II. Nilpotent groups, *Annals of Math.* **112** (1980), 585–617.

[GW] Funda Gul and Armin Weiß, On the dimension of matrix embeddings of torsion-free nilpotent groups, *J. Algebra* **477** (2017), 516–539.

[Gup95] Sanjay Gupta, Closure properties and witness reduction. *Journal of Computer and System Sciences* **50** (1995),pp. 412-432

[HHR] Søren Haagerup, Uffe Haagerup and Maria Ramirez-Solano, A computational approach to the Thompson group F, *Internat. J. Algebra Comput.* **25** (2015), 381–432.

[Hai] Mark Haiman, Noncommutative rational power series and algebraic generating functions, *European J. Combin.* **14** (1993), 335–339.

[Har1] Pierre de la Harpe, *Topics in geometric group theory*, Univ. of Chicago Press, Chicago, IL, 2000, 310 pp.

[Har2] Pierre de la Harpe, On the prehistory of growth of groups, preprint (2021), 15 pp.; arXiv:2106.02499.

[HNP] Philipp Hieronymi, Danny Nguyen and Igor Pak, Presburger arithmetic with algebraic scalar multiplications, *Log. Methods Comput. Sci.* **17** (2021), no. 3, Paper No. 4, 34 pp.

[IP22] Christian Ikenmeyer and Igor Pak, What is in #Pand what is not?, extended abstract in *Proceedings of the 63rd FOCS* (2022), pp. 860-871, full version arxiv:2204.13149.

[Jen] Stephen A. Jennings, The group ring of a class of infinite nilpotent groups, *Canadian J. Math.* **7** (1955), 169–187.

[Jon] James P. Jones, Universal Diophantine equation, *J. Symbolic Logic* **47** (1982), 549–571.

[Jun] Reinwald Jungen, Sur les séries de Taylor n'ayant que des singularités algébrico-logarithmiques sur leur cercle de convergence (in French), *Comment. Math. Helv.* **3** (1931), 266–306.

[Kel10] Bernhard Keller. Cluster algebras, quiver representations and triangulated categories. In T. Holm, P. Jørgensen, & R. Rouquier (Eds.), Triangulated Categories. Cambridge University Press, Cambridge. (2010)

[Kes] Harry Kesten, Symmetric random walks on groups, *Trans. AMS* **92** (1959), 336–354.

[Knu11] Donald Knuth, *The Art of Computer Programming, Vol. 4A: Combinatorial Algorithms, Part 1*. Addison-Wesley, Reading MA, 2011, 883 pp.

[KS21] Noah Kravitz and Ashwin Sah, Linear extensions of numbers of n-element posets, *Order* **38** (2021), pp. 49-66.

[Kuk1] Dmitri G. Kuksov, On rationality of the cogrowth series, *Proc. AMS* **126** (1998), 2845–2847.

[Kuk2] Dmitri G. Kuksov, *Cogrowth of groups*, Ph.D. thesis, Brigham Young University, 1998, 86 pp.

[Loh] Markus Lohrey, Rational subsets of unitriangular groups, *Internat. J. Algebra Comput.* **25** (2015), 113–121.

[Mann] Avinoam Mann, *How groups grow*, Cambridge Univ. Press, Cambridge, UK, 2012, 199 pp.

[Mat1] Yuri V. Matiyasevich, *Hilbert's tenth problem* (in Russian), Nauka, Moscow, 1993, 224 pp.; English translation by MIT Press, Cambridge, MA, 1993, 264 pp.

[Mat2] Yuri V. Matiyasevich, What can and cannot be done with Diophantine problems, *Proc. Steklov Inst. Math.* **275** (2011), 118–132.

[Mel] Stephen Melczer, *Algorithmic and symbolic combinatorics—an invitation to analytic combinatorics in several variables*, Springer, Cham, 2021, 418 pp.

[MS] Stephen Melczer and Bruno Salvy, Effective coefficient asymptotics of multivariate rational functions via semi-numerical algorithms for polynomial systems, *J. Symbolic Comput.* **103** (2021), 234–279.

[MC] Abdul M. Mian and Sarvadaman Chowla, The differential equations satisfied by certain functions, *J. Indian Math. Soc.* **8** (1944), 27–28; available at https://tinyurl.com/y7jqsk6d.

[Mis] Marni Mishna, *Analytic combinatorics: a multidimensional approach*, CRC Press, Boca Raton, FL, 2020, 229 pp.

[Moo] Justin T. Moore, Fast growth in the Følner function for Thompson's group F, *Groups Geom. Dyn.* **7** (2013), 633–651.

[MF] M. Ram Murty and Brandon Fodden, *Hilbert's tenth problem*, AMS, Providence, RI, 2019, 237 pp.

[Müt23] Torsten Mütze, Combinatorial Gray codes - an updated survey, *Electronic Journal of Combniatorics* **30** (2023), pp. 1-93.

[Naor] Assaf Naor, Metric dimension reduction: a snapshot of the Ribe program, in *Proc. ICM Rio de Janeiro*, Vol. I, World Sci., Hackensack, NJ, 2018, 759–837.

[NY] Assaf Naor and Robert Young, Vertical perimeter versus horizontal perimeter, *Annals of Math.* **188** (2018), 171–279.

[Odl] Andrew M. Odlyzko, Asymptotic enumeration methods, in *Handbook of Combinatorics*, Vol. 2, Elsevier, Amsterdam, 1995, 1063–1229.

[OEIS] Neil Sloane (ed.), *The on-line encyclopedia of integer sequences* ,oeis.org.

[OH93] Mitsunori Ogiwara and Lane Hemachandra, A complexity theory for feasible closure properties, *Journal ofComputer and System Sciences* **46** (1993), pp. 295-325.

[OHa90] K. M. O'Hara, Unimodality of Gaussian coefficients: a constructive proof, *J. Combin. Theory, Ser. A* **53** (1990), pp. 29–52.

[Pak] Igor Pak, Complexity problems in enumerative combinatorics, in *Proc. ICM Rio de Janeiro*, Vol. IV, World Sci., Hackensack, NJ, 2018, 3153–3180.

[PP] Igor Pak and Greta Panova, Strict unimodality of q-binomial coefficients, *Comptes Rendus Acad. Sci. Paris, Ser. I. Math.*, **351** (2013), no. 11-12, 415-418.

[PS1] Igor Pak and David Soukup, Algebraic and arithmetic properties of the cogrowth-sequence of nilpotent groups, preprint (2022). `arxiv:2210.09419`

[Par] Walter Parry, Growth series of some wreath products, *Trans. AMS* **331** (1992), 751–759.

[PS2] Christophe Pittet and Laurent Saloff-Coste, Random walks on finite rank solvable groups, *J. Eur. Math. Soc.* **5** (2003), 313–342.

[Pól] Georg Pólya, Über eine Aufgabe der Wahrscheinlichkeitsrechnung betreffend die Irrfahrt im Straßennetz (in German), *Math. Ann.* **84** (1921), 149–160.

[Poo1] Bjorn Poonen, Undecidability in number theory, *Notices AMS* **55** (2008), no. 3, 344–350.

[Poo2] Bjorn Poonen, Undecidable problems: a sampler, in *Interpreting Gödel*, Cambridge Univ. Press, Cambridge, UK, 2014, 211–241.

[Pre20] Matthew Pressland, Mutation of frozen Jacobian algebras, J. Algebra 546 (2020).

[PG] Andrew E. Price and Anthony J. Guttmann, Numerical studies of Thompson's group F and related groups, *Internat. J. Algebra Comput.* **29** (2019), 179–243.

[Pro82] Robert A. Proctor, Solution of Two Difficult Combinatorial Problems with Linear Algebra, *The American Mathematical Monthly* **89** (1982), no. 10, 721–734.

[Rob] Raphael M. Robinson, Undecidability and nonperiodicity for tilings of the plane, *Invent. Math.* **12** (1971), 177–209.

[RY] Eric Rowland and Reem Yassawi, Automatic congruences for diagonals of rational functions, *J. Théor. Nombres Bordeaux* **27** (2015), 245–288.

[Rus88] Frank Ruskey, Research problems 90 and 91, *Discrete Mathematics* **70** (1988), pp. 111-112.

[Rus92] Frank Ruskey, Generating linear extensions of posets by transpositions,Journal of Combinatorial Theory,Series B54(1992), pp. 77-101.

[Rus03] Frank Ruskey, *Combinatorial generation*. Book draft, 2003.

[Sap] Mark Sapir, Asymptotic invariants, complexity of groups and related problems, *Bull. Math. Sci.* **1** (2011), 277–364.

[Sha] Michael Shapiro, Growth of a $PSL_2\mathbf{R}$ manifold group, *Math. Nachr.* **167** (1994), 279–312.

[STWZ] Vivek Shende, David Treumann, Harold Williams, and Eric Zaslow, Cluster varieties from Legendrian knots, *Duke Math. J.* **168** (2019), no. 15, pp. 2801- 2871.

[SS06] Evgenia Soprunova and Frank Sottile, Lower bounds for real solutions to sparse polynomial systems, *Advances in Mathematics* **204** (2006), pp. 116-151.

[Sou1] David Soukup, Complexity of ice quiver mutation equivalence, *Annals of Combinatorics* (2023).

[Sou2] David Soukup, Complexity of sign imbalance, parity of linear extensions, and height 2 posets, preprint, 9 pp. `arxiv:2311.02203`

[Sta87] Dennis Stanton, Unimodality and Young's lattice, *Journal of Combinatorial Theory, Series A* **54** (1987), pp. 41-53.

[Sta97a] Grzegorz Stachowiak, Finding parity difference by involutions, *Discrete Mathematics* **163** (1997), pp. 139-151.

[Sta97b] Richard Stanley,Enumerative Combinatorics, Vol. 1, Cambridge Univ. Press, Cambridge, MA, 1997.

[Sta1] Richard P. Stanley, *Enumerative Combinatorics*, vol. 1 (Second ed.) and vol. 2, Cambridge Univ. Press, 2012 and 1999.

[Sta05] Richard Stanley, Some remarks on sign-balanced and maj-balanced posets, *Advances in Applied Mathematics* **34** (2005), pp. 880-902.

[Sta2] Richard P. Stanley, D-finiteness of certain series associated with group algebras, in *Oberwolfach Rep.* **11** (2014), 708; available at tinyurl.com/4rrsfwx6

[Sto] Michael Stoll, Rational and transcendental growth series for the higher Heisenberg groups, *Invent. Math.* **126** (1996), 85–109.

[Syl78] J. J. Sylvester, Proof of the hitherto undemonstrated Fundamental Theorem of Invariants, *Philosophical Magazine* **5** (1878), 178–188; reprinted in *Coll. Math. Papers*, vol. 3, Chelsea, New York, 1973, pp. 117–126; available at `http://tinyurl.com/c94pphj`

[Tro95] William Trotter, Partially ordered sets, inHandbook of combinatorics, vol. 1, Elsevier, Amsterdam, 1995, 433–480.

[Ufn] Victor A. Ufnarovski, Combinatorial and asymptotic methods in algebra, in *Algebra VI*, Springer, Berlin, 1995, 1–196.

[Whi01] Dennis White, Sign-balanced posets.Journal of Combinatorial Theory, Series A95, (2001), pp. 1-38.

[WZ] Herbert S. Wilf and Doron Zeilberger, An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities, *Invent. Math.* **108** (1992), 575–633.

[Woe] Wolfgang Woess, *Random walks on infinite graphs and groups*, Cambridge Univ. Press, Cambridge, UK, 2000, 334 pp.

[YA] Adam Yedidia and Scott Aaronson, A relatively small Turing machine whose behavior is independent of set theory, *Complex Systems* **25** (2016), 297–327.

[Zei] Doron Zeilberger, A holonomic systems approach to special functions identities, *J. Comput. Appl. Math.* **32** (1990), 321–368.