ALGEBRAIC AND ARITHMETIC PROPERTIES OF THE COGROWTH SEQUENCE OF NILPOTENT GROUPS

IGOR PAK* AND DAVID SOUKUP*

Abstract. We prove that congruences of the cogrowth sequence in a unitriangular group $\mathrm{UT}(m, \mathbb{Z})$ are undecidable. This is in contrast with abelian groups, where the congruences of the cogrowth sequence are decidable. As an application, we conclude that there is no algorithm to present the cogrowth series as the diagonal of a rational function.

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 3.

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

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

the number of products of generators equal to one. The sequence $\{\mathrm{cog}_{\mathcal{S}}(n)\}$ 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 upper triangular matrices with 1's on the diagonal.

Theorem 1.1 (Main theorem). *Let $m, a \geq 1$ be integers, and let p be a prime. The following problem is undecidable: Given symmetric generating sets $\mathcal{S}, \mathcal{T}$ in $\mathrm{UT}(m, \mathbb{Z})$, determine whether*

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

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

This is a rare undecidabe 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 1.2. *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*

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

October 12, 2022.

*Department of Mathematics, UCLA, Los Angeles, CA 90095. Email: {pak,soukup}@math.ucla.edu.

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

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

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 $\sum_{n\ge 0} b(n,\ldots,n)\, t^n$.

Theorem 1.3. *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* $\mathrm{Cog}_{\mathcal{S}}(t)$ *as a diagonal of a rational function P/Q, for some polynomials $P, Q \in \mathbb{Z}[x_1,\ldots,x_k]$, $k \ge 1$. Moreover, the result holds for $m \le 9.6 \cdot 10^{85}$.*

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 $\mathrm{Cog}_{\mathcal{S}}(t)$ is always *D-finite*, i.e. a solution of an ODE with polynomial coefficients. Christol's Conjecture 3.1 (see below), reduces the problem to whether $\mathrm{Cog}_{\mathcal{S}}(t)$ is always a diagonal of a rational function. Until now, no progress has been made in this direction.

Remark 1.4. Let us place our theorem in context. 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 §6.3. It is also possible and even likely, that *for all* $m \ge 3$ and all symmetric generating sets $\mathcal{S}$ of $\mathrm{UT}(m,\mathbb{Z})$, the cogrowth series is not a diagonal. Theorem 1.3 gives no contradiction with that.

Additionally, 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 1.3 shows is that there is no *constructive proof* that the cogrowth series it is always a diagonal.

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 $\mathrm{PSL}(2,\mathbb{R})$ 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* $H_2 \subset \mathrm{UT}(4,\mathbb{Z})$ and two generating sets so that one growth series is rational while another is non-algebraic. Curiously, for the (usual) Heisenberg group $H_1 = \mathrm{UT}(3,\mathbb{Z})$, the growth series is always rational [DS].

(3) After Pólya's work, *lattice walks* on $\mathbb{Z}^d$ have been intensely studied with 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 combinatorics context, and in [Aom, FTS] in an 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, interest in the problem has come from Kontsevich's question whether the cogrowth series is always D-finite on linear groups, see [Sta2]. Note that by *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 [PS], that for every symmetric generating set $\mathcal{S}$, the cogrowth satisfies

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

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

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

see [Woe, §3.B, §15.B] and references therein. Now *Jungen's theorem* [Jun], implies that for the cogrowth series is not algebraic for even $d(G)$. For odd $d(G) \ge 5$, only a weaker result is known, 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 algebraic and D-finite GFs with the same asymptotics, 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 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

[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.

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 §6.6. Our Theorem 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 $H_1 = \mathrm{UT}(3,\mathbb{Z})$ [DLS, GMO]; the proofs of this result are similarly based on Hilbert's 10th problem, cf. §6.3.

1.3. **Paper structure.** After a few notation in Section 2, we start with a technology of generating functions in Section 3. There, we give quick proofs of Theorem 1.2 from the Adamczewski–Bell theorem (Theorem 3.3), and of Theorem 1.3 from the Main Theorem 1.1. There, we also formulate Theorem 3.5 on a possible non-D-algebraic cogrowth series for $\mathrm{UT}(m,\mathbb{Z})$. We then prove Main Theorem 1.1 in a lengthy Section 4. The proof of Theorem 3.5 is given in Section 5. We conclude with final remarks and open problems in Section 6.

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

$$\binom{\boldsymbol{a}}{\boldsymbol{b}} := \binom{a_1}{b_1} \cdots \binom{a_k}{b_k}. \tag{2.1}$$

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 $s_1 \cdots s_n = 1$.

3. Cogrowth series

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

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

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 $\operatorname{Cog}_{\mathcal{S}}(t) = \sum_{n \geq 0} \tbinom{2n}{n}^2 t^{2n}$ 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:

Conjecture 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] and an explicit form ADE 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.

3.2. **Proofs of Theorems 1.2 and 1.3.** We start with the following two results.

Theorem 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 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 <u>decidable</u>:*

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

[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 $\tbinom{2n}{n}^2 \sim \frac{1}{\pi n} 16^n$. Jungen's theorem can be used to show that the cogrowth series is non-algebraic *for all* generating sets of $\mathbb{Z}^2$.

Theorems 1.2 and 1.3 now follows easily by a combination of these results and the Main Theorem 1.1.

Proof of Theorem 1.2. Note that the proof of Theorem 3.2 in [Kuk2, §5.1] is completely constructive, giving $\mathrm{Cog}_{\mathcal{S}} = \operatorname{diag} P_1/Q_1$ and $\mathrm{Cog}_{\mathcal{T}} = \operatorname{diag} P_2/Q_2$ for some explicit $P_1, P_2, Q_1, Q_2 \in \mathbb{Z}[x_1, \ldots, x_2]$. 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 3.3 to $C(t)$ with all possible $1 \leq b < p^a$, 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 1.3. Let $p = 2$, $a = 40$, and let $G = \mathrm{UT}(m,\mathbb{Z})$ be as in Theorem 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: $\mathrm{Cog}_{\mathcal{S}}(t) - \mathrm{Cog}_{\mathcal{T}}(t) = \operatorname{diag} P/Q$, for every two symmetric generating sets $\mathcal{S}$ and $\mathcal{T}$ of G, and some computable multivariate polynomials P, Q. By Theorem 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. □

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 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 $i \geq 1$,*
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. $\rho_i \equiv a \mod 2^b$,*
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:*

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

Theorem 3.5. *Suppose Conjecture 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 3.5 in Section 5. The proof is based on the following result of independent interest. It also explains the nature of assumptions in the conjecture.

Lemma 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 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]

4. Proof of Theorem 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 4.1 we show that words of a particular structure can compute the value of f at integers. Then, in Lemmas 4.3 and 4.4 we extend our matrices so that this computation is true for a broader class of words.

Next, Lemmas 4.8 and 4.12 allows us to turn the question of Theorem 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.

4.1. **Polynomials via matrix products.**

We start with the following key lemma.

Lemma 4.1. *Let $f \in \mathbb{Z}[x_1, \dots, x_k]$ and let $\mathrm{D} := \deg f$. Then there exists matrices $P, Q, A_1, \dots, A_k \in \mathrm{UT}(m, \mathbb{Z})$ for some $m \leq (\mathrm{D}+1)\binom{\mathrm{D}+k}{k} + 2$, such that*

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

for all

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

Proof. Denote $\boldsymbol{x} = (x_1, \dots, x_k)$ and recall the multi-index notation (2.1). Write $f(\boldsymbol{x})$ in the binomial basis $\{\binom{\boldsymbol{x}}{\boldsymbol{d}} : \boldsymbol{d} \in \mathbb{N}^k\}$ as follows:

$$f(\boldsymbol{x}) \;=\; \sum_{|\boldsymbol{d}| \leq \mathrm{D}} b_{\boldsymbol{d}} \binom{\boldsymbol{x}}{\boldsymbol{d}} \qquad \text{for some} \qquad b_{\boldsymbol{d}} \in \mathbb{Z}, \;\; \boldsymbol{d} \in \mathbb{N}^k. \tag{4.1}$$

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:

$$J_q \;=\; \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \qquad \text{and} \qquad (J_q)^p \;=\; \begin{bmatrix} 1 & \binom{p}{1} & \binom{p}{2} & \cdots & \binom{p}{q-2} & \binom{p}{q-1} \\ 0 & 1 & \binom{p}{1} & \cdots & \binom{p}{q-3} & \binom{p}{q-2} \\ 0 & 0 & 1 & \cdots & \binom{p}{q-3} & \binom{p}{q-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \binom{p}{1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}. \tag{4.2}$$

Now, for each $\boldsymbol{d} = (d_1, \dots, d_k)$ in the sum in (4.1), define matrices $B_{\boldsymbol{d},i} \in \mathrm{UT}(|\boldsymbol{d}|+1, \mathbb{Z})$ as follows:

$$\begin{cases} B_{\boldsymbol{d},1} \;:=\; J_{d_1+1} \oplus I_{d_2 + \ldots + d_k} \\ B_{\boldsymbol{d},2} \;:=\; I_{d_1} \oplus J_{d_2+1} \oplus I_{d_3 + \ldots + d_k} \\ \qquad \vdots \\ B_{\boldsymbol{d},k} \;:=\; I_{d_1 + \ldots + d_{k-1}} \oplus J_{d_k+1} \end{cases} \tag{4.3}$$

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

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

$$[B_{\boldsymbol{d}}]_{1,|\boldsymbol{d}|+1} = \sum_{(j_1,\ldots,j_{k+1})\,:\, j_1=1,\, j_{k+1}=|\boldsymbol{d}|+1} \big[B_{\boldsymbol{d},1}^{x_1}\big]_{j_1,j_2} \big[B_{\boldsymbol{d},2}^{x_2}\big]_{j_2,j_3} \cdots \big[B_{\boldsymbol{d},k}^{x_k}\big]_{j_k,j_{k+1}} . \tag{4.4}$$

We investigate which of the terms in the sum (4.4) survive. Since all the $B_{\boldsymbol{d},i}$ are upper triangular we can only have a nonzero term if $j_1 \le j_2 \le \cdots \le j_{k+1}$. 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

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

Therefore, there is only one nonzero term in the sum (4.4), 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 (4.2), this gives

$$[B_{\boldsymbol{d}}]_{1,|\boldsymbol{d}|+1} = \big[J_{d_1+1}^{x_1}\big]_{1,d_1+1} \cdots \big[J_{d_k+1}^{x_k}\big]_{1,d_k+1} = \tbinom{x_1}{d_1+1-1} \cdots \tbinom{x_k}{d_k+1-1} = \tbinom{\boldsymbol{x}}{\boldsymbol{d}}. \tag{4.5}$$

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 (4.1). The top-right corner of PAQ is

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

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 (4.5) this becomes

$$[PAQ]_{1,m} = \sum_{\boldsymbol{d}} [A]_{\alpha_{\boldsymbol{d}}, \beta_{\boldsymbol{d}}} b_{\boldsymbol{d}} = \sum_{\boldsymbol{d}} [B_{\boldsymbol{d}}]_{1,|\boldsymbol{d}|+1} b_{\boldsymbol{d}} = \sum_{\boldsymbol{d}} b_{\boldsymbol{d}} \binom{\boldsymbol{x}}{\boldsymbol{d}} = f(\boldsymbol{x}). \tag{4.6}$$

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 (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 (4.6).

To summarize, M is of the form

$$M = \begin{bmatrix} 1 & [P]_{1,2} & [P]_{1,3} & [P]_{1,4} & \cdots & [P]_{1,m-1} & f(\boldsymbol{x}) \\ 0 & 1 & 0 & 0 & \cdots & 0 & \xi_1(\boldsymbol{x}) \\ 0 & 0 & 1 & 0 & \cdots & 0 & \xi_2(\boldsymbol{x}) \\ 0 & 0 & 0 & 1 & \cdots & 0 & \xi_3(\boldsymbol{x}) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \tag{4.7}$$

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 (4.7) by P^{-1} to get

$$MP^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & f(\boldsymbol{x}) \\ 0 & 1 & 0 & 0 & \cdots & \xi_1(\boldsymbol{x}) \\ 0 & 0 & 1 & 0 & \cdots & \xi_2(\boldsymbol{x}) \\ 0 & 0 & 0 & 1 & \cdots & \xi_3(\boldsymbol{x}) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}. \tag{4.8}$$

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:

$$P^{-1}M = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & \xi_1(\boldsymbol{x}) \\ 0 & 0 & 1 & 0 & \cdots & \xi_2(\boldsymbol{x}) \\ 0 & 0 & 0 & 1 & \cdots & \xi_3(\boldsymbol{x}) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}. \tag{4.9}$$

Combining (4.8) and (4.9), 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 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*.*

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 4.1 to new matrices. Therefore the next lemmas will reduce the problem to Corollary 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 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 4.1.

Lemma 4.3. *Suppose $f \in \mathbb{Z}[x_1,\ldots,x_k]$ has degree $\mathrm{D} := \deg f$. Then there exists matrices P, Q, $A_1,\ldots,A_k \in \mathrm{UT}(m,\mathbb{Z})$ for some $m \le 4(\mathrm{D}+1)\binom{\mathrm{D}+k}{k} + 8$, such that the conclusion of Corollary 4.2 holds, and such that every word of the form*

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

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

Proof. Let $P', Q', A'_1,\ldots,A'_k$ be the matrices produced by Lemma 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

$$PW_1QW_2P^{-1}W_3Q^{-1}W_4 = \begin{bmatrix} V & 0 & 0 & 0 \\ 0 & I_m & 0 & W'_3W'_4(I_m - W'_2W'_1) \\ 0 & 0 & I_m & W'_4(I_m - W'_2W'_3) \\ 0 & 0 & 0 & W'_1W'_2W'_3W'_4 \end{bmatrix}$$

where $V = P'W'_1Q'W'_2(P')^{-1}W'_3(Q')^{-1}W'_4$. The construction in Lemma 4.1 shows that Corollary 4.2 holds.

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

$$W'_3W'_4(I_m - W'_2W'_1) = W'_4(I_m - W'_2W'_3) = 0 \quad \text{and} \quad W'_1W'_2W'_3W'_4 = I_m\,,$$

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

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

such that the conclusion of Corollary 4.2 holds, and such that every word of the form

$$PW_1QW_2P^{-1}W_3Q^{-1}W_4 \tag{4.10}$$

where $W_i \in \langle A_1^{\pm 1},\ldots,A_k^{\pm k}\rangle$, 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 $x_1,\ldots,x_k$.

Proof. Let $P', Q', A'_1,\ldots,A'_k$ be the matrices produced by Lemma 4.1. We consider the structure of matrices in $\langle (A'_1)^{\pm 1},\ldots,(A'_k)^{\pm}\rangle$ more deeply. Each consists of a collection of blocks defined as $B_{\boldsymbol{d},i}$ in (4.4). 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 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

$$W = B_{\boldsymbol{d},j_1}^{\varepsilon_1} \cdots B_{\boldsymbol{d},j_m}^{\varepsilon_m} \tag{4.11}$$

for some integer m, indices $1 \le j_m \le k$, 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 (4.11). 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 (4.11) 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 4.6. *Let $V \in \mathrm{UT}(q, \mathbb{Z})$ and let $1 < a \le b < q$. 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 $I_q + E_{1,a}VE_{b,q}V^{-1}$. This equals the right-hand side. □

To finish the proof of Lemma 4.3, we construct our matrices as follows. Let $P'', Q'', A''_1, \ldots, A''_k$ be the matrices obtained in Lemma 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

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

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 (4.10) is cogrowth. Then by Lemma 4.3 we have $W_1 = W_2^{-1} = W_3 = W_4^{-1}$. Therefore, by construction and Sublemma 4.6 all of the entries of $\Phi(W_1)$ outside of the nontrivial Jordan blocks are zero. Then, Sublemma 4.5 implies that $W_1 = A_1^{y_1} \cdots A_k^{y_k}$ for the y_i defined in Sublemma 4.5. This completes the proof of Lemma 4.3. □

Corollary 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. □

4.3. **The construction.** We are now ready to construct our generating sets $\mathcal{S}$ and $\mathcal{T}$ as in Theorem 1.1. For a fixed polynomial $f \in \mathbb{Z}[x]$, let P', Q', A'_1, $\ldots$, $A'_k \in \mathrm{UT}(m, \mathbb{Z})$ be the matrices given by Lemma 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

$$\begin{aligned} \mathcal{S} &:= \{A_1^{\pm 1}, A_2^{\pm 1}, \ldots, A_k^{\pm 1}\} \,\cup\, u \cdot \big\{P^{\pm 1}, Q^{\pm 1}\big\} \,\cup\, u^{10} \cdot \mathcal{E}_{m+3}\,, \text{ and} \\ \mathcal{T} &:= \mathcal{S} \,\cup\, u^5 \cdot \big\{R^{\pm 1}\big\}, \end{aligned} \tag{4.12}$$

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 to eliminate any word that does not fit the pattern of Lemma 4.4.

Lemma 4.8. *Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$, and define $\mathcal{S}$ and $\mathcal{T}$ as in (4.12). 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:

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

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

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

In a different direction, we have:

Corollary 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* (4.12)*. Then:*

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

Proof. By Lemma 4.8, we have:

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

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 4.4 and Corollary 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 4.11. Unfortunately, not every polynomial has a root satisfying the conditions of Corollary 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 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,* (4.13)
- ○ *$\boldsymbol{x} \in \mathbb{Z}^{k+1}$ is an integer root of $\widetilde{g}$ $\Rightarrow$ $|\boldsymbol{x}|$ is even,* (4.14)
- ○ *$\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^{k+1}$ are integer roots of $\widetilde{g}$ $\Rightarrow$ $|\boldsymbol{x}| \neq |\boldsymbol{y}|$,* (4.15)
- ○ $\deg \widetilde{g} \, \le \, \max\{2 \deg g, 4k + 12\}$. (4.16)

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 (4.16) 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 (4.13).

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 (4.14).

On the other hand, observe that

$$\bigl||\boldsymbol{r}| \,-\, v^{k+3}\bigr| \,\le\, \sum_{i=1}^{k} |y_i| \,+\, \left|\sum_{i=1}^{k} y_i v^{i+1} \,+\, \sum_{i=1}^{k} y_i\right| \,\le\, \sum_{i=1}^{k} |y_i|\,\bigl(2+v^{i+1}\bigr)$$
$$\le\, (2+v^{k+1}) \sum_{i=1}^{k} |y_i| \,\le\, (2+v^{k+1})\frac{v}{4} \,\le\, v^{k+3}-(v-1)^{k+3}\,.$$

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 (4.15). This finishes the proof of the lemma. □

We can now complete the proof of Theorem 1.1. Suppose an algorithm exists that determines whether or not, for arbitrary generating sets $\mathcal{S}$ and $\mathcal{T}$, we have

$$\exists n\ge 0 \;:\; \mathrm{cog}_{\mathcal{S}}(n) \,\not\equiv\, \mathrm{cog}_{\mathcal{T}}(n) \mod p^a. \tag{4.17}$$

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 4.12. Then construct $\mathcal{S}$ and $\mathcal{T}$ with $f=\widetilde{g}$ and $u=16$ as in Lemma 4.4. By Corollaries 4.9 and 4.10, polynomial $\widetilde{g}$, and thus f, has a root if and only if (4.17) 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. Sun [Sun]) the Diophantine problem over $\mathbb{Z}$ is undecidable for $\deg g=192$ and $k=63$. Then $\deg\widetilde{g}=384$, which by Lemma 4.4 gives the desired bound $m\le 9.6\cdot 10^{85}$. This completes the proof of Theorem 1.1. □

Remark 4.13. In fact, Jones [Jon] 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.

5. D-algebraic

The previous sections gave us information about the parity of cogrowth sequences. We first prove Lemma 3.6 where the parity information is enough to conclude that a sequence is not D-algebraic. We then deduce Theorem 3.5.

5.1. **Proof of Lemma 3.6.** Let $\Lambda(t)=\sum\lambda_n t^n$, and suppose that Λ satisfies an algebraic differential equation. Then there exist positive integers C and D together with a finite family of polynomials $\{\Pi_{c,d}\}_{0\le c\le C,0\le d\le D}$, 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:

$$\sum_{c,d}\ \sum_{\nu\vdash(n-c)\,:\,|\nu|=d} \Gamma_{\nu,n}\,\lambda_1\cdots\lambda_d \,=\, 0 \qquad \text{for all } n, \tag{5.1}$$

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 $n_{\alpha_1}, \dots, n_{\alpha_\ell}$, 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 (5.1). Indeed, consider the equality modulo 2^{V+1}. Letting $\nu = \{n_{\alpha_1}, \dots, n_{\alpha_\ell}\}$, 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 (5.1). 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 (5.1) has exactly one term which is not congruent to zero modulo 2^{V+1}, a contradiction. Hence our sequence cannot be D-algebraic. □

5.2. **Proof of Theorem 3.5.** Suppose we have a polynomial f satisfying the conditions prescribed in Conjecture 3.4. Construct $A_1, \dots, A_k$ and P, Q, R as in the proof of Theorem 1.1. Suppose for the sake of contradiction that $\operatorname{cog}_{\mathcal{S}}(n)$ and $\operatorname{cog}_{\mathcal{T}}(n)$ 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 $\{A_1^{\pm 1}, \dots, A_k^{\pm 1}\}$. Define ω_n to be the number of words in $\mathcal{W}$ of length n.

Lemma 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 $\boldsymbol{x} = (x_1, \dots, x_k)$ 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:

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

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 $\{A_1^{\pm 1}, \dots, A_k^{\pm 1}\}$ together with their charged versions.

Lemma 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

$$2^d - x_i \leq v \leq 2^d. \tag{5.2}$$

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 (5.2) to hold for all W's and x's. That implies

$$|n - 4 - e| \leq 4|\boldsymbol{x}|, \tag{5.3}$$

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 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 3.6.

Indeed, let $n_i = |\rho_i|/2$. Conditions (1), (2) and (3) of Lemma 3.6 follow from the assumptions of Theorem 3.5 and Corollary 4.10. Therefore $\{\lambda_n\}$ cannot be D-algebraic. And condition (4) of Lemma 3.6 follows from the above computation plus assumption (4) of Conjecture 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. □

6. Final remarks and open problems

6.1. **Grappling with undecidability.** To further understand the meaning of our Main Theorem 1.1, we state the following corollary:

Corollary 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] *:*

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

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

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 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], 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 of 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.

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 holds for *some* nilpotent group and its families of generating sets, then the "using multiple copies of extra generators" trick used in §4.3

6.3. **Heisenberg group.** For the Heisenberg group $H_1 = \mathrm{UT}(3, \mathbb{Z})$ 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 §1.2, there is a deeper reason why H_1 has simpler structure than the higher Heisenberg group $H_2 \subset \mathrm{UT}(4, \mathbb{Z})$, see [NY]. In fact, from metric geometry point of view, group H_2 is the "most distorted" relative to the abelian group, see [Naor]. Additionally, every equation is decidable in H_1 [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_2 or $\mathrm{UT}(4, \mathbb{Z})$ is a better place to start than H_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 §1.2). 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.

6.5. **Abelian groups.** Kuksov's Theorem 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 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.

6.6. **Christol's conjecture.** There is a healthy debate in the literature about the validity of Christol's Conjecture 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 1.3 in this setting.

[6] We stopped at three towers for clarity. We could have e.g. $\mathrm{Tow}(\phi)$ of towers, of course.

6.7. **Explicit construction.** The construction of generating sets in Corollary 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.

Acknowledgements. We are grateful Artëm Chernikov, Mark van Hoeij, Yuri Matiyasevich and Boris Moroz for discussions and helpful comments. Special thanks to Boris Adamczewski and Jason Bell for telling us about paper [AB], and to Andrew Marks for pointing out a gap in our original argument. The second author was partially supported by the NSF.

This paper was finished soon after the death of Mark Sapir. Over the years, the first author had many conversations with Mark, whose wit and generosity were delightful and educational. We dedicate this paper to his memory.

References

[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.

[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.

[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.

[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.

[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.

[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.

[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.

[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 $\mathrm{BS}(N,N)$ is D-finite, *Internat. J. Algebra Comput.* **24** (2014), 171–187.

[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.

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

[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.

[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 *Multicomponent 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.

[HHR] Søren Haagerup, Uffe Haagerup, 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`.

[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.

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

[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.

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

[Mat1] Yuri V. Matiyasevich, *Hilbert's tenth problem*, 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.

[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.

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

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

[PS] 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.

[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.

[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.

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

[OEIS] Neil J. A. Sloane, The Online Encyclopedia of Integer Sequences, oeis.org.

[Sha] Michael Shapiro, Growth of a $\mathrm{PSL}_2\mathbf{R}$ manifold group, *Math. Nachr.* **167** (1994), 279–312.

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

[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.

[Sun] Zhi-Wei Sun, Further results on Hilbert's tenth problem, *Sci. China Math.* **64** (2021), 281–306.

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

[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.