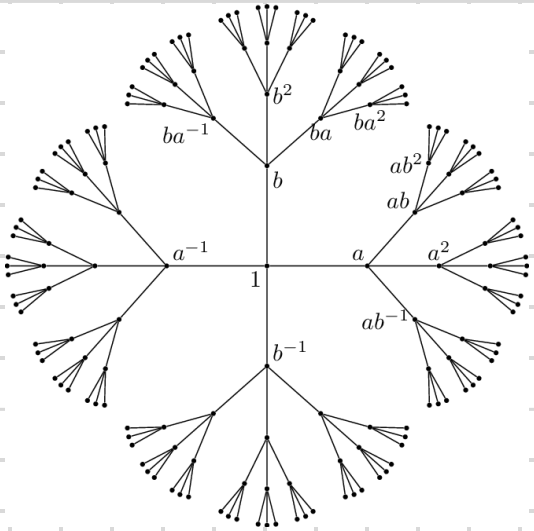
IHP (Dec 9 , 2022)

Transcendence and combinatorics

What do we know about the cogrowth sequence?

Igor Pak, UCLA

Joint work with David Soukup



Plan of the talk:

0) What to do with combinatorial sequences?
1) What is the cogrowth sequence and why study it?
2) Recent results

Main thing to remember:

We are only beginning to understand the subject!

Combinatorial sequences:

OEIS now has over 300,000 sequences!

Our policy has been to include all interesting sequences, no matter how obscure the reference. [N.J.A. Sloane, S. Plouffe, EIS, 1995]

[The EIS contains] *the unrelenting cascade of numbers,* [..] *lists Hard, Disallowed and Silly sequences.* [Richard Guy, 1997]

A307468 Cogrowth sequence for the Heisenberg group.

1, 4, 28, 232, 2156, 21944, 240280, 2787320, 33820044, 424925872, 5486681368, 72398776344

(my only sequence in OEIS)

AUTHOR Igor Pak, Apr 09 2019

STATUS approved

Ad hoc combinatorial sequences

$$
\begin{aligned}
a_n &= \#\text{ of triangulations of a convex } n\text{-gon} = \tfrac{1}{n+1}\tbinom{2n}{n} \\
a_n &= \#\text{ of domino tilings of } [n \times n] = \det M_n \\
a_n &= \#\text{ of connected labeled graphs on } n \text{ vertices} \leftarrow \text{RR} \\
a_n &= \#\text{ of triangulations of a } n \times n \text{ grid} = \gamma^{n^2(1+o(1))}
\end{aligned}
$$

Families of sequences

$$
\begin{aligned}
a_n &= \#\text{ walks } (0,0) \to (0,0) \text{ in } \mathbb{N}^2 \text{ using } n \text{ steps } \{(1,1),(1,0),(-1,0),(-1,-1)\} \\
&\quad \leftarrow \text{Gessel walks} \\
a_n &= \#\text{ walks } (0,0) \to (0,0) \text{ in } \mathbb{N}^2 \text{ using } n \text{ steps } \{(1,1),(-1,0),(0,-1)\} \\
&\quad \leftarrow \text{Kreweras walks}
\end{aligned}
$$

Combinatorial sequences:

First Question: Does $\mathcal{A}(t) = \sum_n a_n t^n$ have a *formula*?

Second Question: What is a *formula*?

Classes of combinatorial sequences

(1) ***rational*** GF $\mathcal{A}(t) = P(t)/Q(t),\ \ P, Q \in \mathbb{Z}[t]$.

E.g. $a_n := \mathrm{Fib}(n),\ \ \mathcal{A}(t) = 1/(1-t-t^2)$.

(2) ***algebraic*** GF $c_0\mathcal{A}^k + c_1\mathcal{A}^{k-1} + \ldots + c_k = 0,\ c_i \in \mathbb{Z}[t]$.

E.g. $a_n := \mathrm{Cat}(n),\ \ \mathcal{A}(t) = (1-\sqrt{1-4t})/2t$.

(3) ***Diagonals*** $\mathcal{A}(t) = \operatorname{diag} P/Q,\ \ P, Q \in \mathbb{Z}[x_1, \ldots, x_k]$.

$$\mathcal{B} = \sum_{(i_1,\ldots,i_k)} b(i_1,\ldots,i_k)\, x_1^{i_1} \cdots x_n^{i_k} \quad \Longrightarrow \quad \operatorname{diag}\mathcal{B} := \sum_{n=0}^{\infty} b(n,\ldots,n)\, t^n$$

E.g. *Delannoy numbers* $\{D_n\}$ and *Apéry numbers* $\{A_n\}$

$$D_n := \sum_{k=0}^{n} \binom{n+k}{n-k}\binom{2k}{k} \quad \text{and} \quad A_n := \sum_{k=0}^{n}\sum_{j=0}^{k} \binom{n}{k}\binom{n+k}{k}\binom{k}{j}^3$$

Classes of combinatorial sequences

(4) ***D-finite*** GF $c_0\mathcal{A} + c_1\mathcal{A}' + \ldots + c_k\mathcal{A}^{(k)} = 0$, $c_i \in \mathbb{Z}[t]$.

E.g. $a_n :=$ # involutions in S_n, $a_n = a_{n-1} + (n-1)a_{n-2}$.

The sequences $\{a_n\}$ are called ***P-recursive***

(5) ***D-algebraic*** GF $Q\big(t, \mathcal{A}, \mathcal{A}', \ldots, \mathcal{A}^{(k)}\big) = 0$, $Q \in \mathbb{Z}[t, x_0, x_1, \ldots, x_k]$

E.g. $a_n = \#\{\sigma(1) < \sigma(2) > \sigma(3) < \ldots \in S_n\}$, $\mathcal{A}'' = \mathcal{A} \cdot \mathcal{A}'$.

Also $p(n) =$ # integer partitions of n. Then $F(t) = \sum_n p(n)t^n$ satisfies:

$$\begin{aligned} 4F^3F'' + 5tF^3F''' + t^2F^3F^{(4)} - 16F^2(F')^2 - 15tF^2F'F'' - 39t^2F^2(F'')^2 \\ + 20t^2F^2F'F''' + 10tF(F')^3 + 12t^2F(F')^2F'' + 6t^2(F')^4 = 0. \end{aligned}$$

(Jacobi, Ramanujan)

Classes of combinatorial sequences

(4) ***D-finite*** GF $c_0\mathcal{A} + c_1\mathcal{A}' + \ldots + c_k\mathcal{A}^{(k)} = 0$, $c_i \in \mathbb{Z}[t]$.

E.g. $a_n := \#$ involutions in S_n, $a_n = a_{n-1} + (n-1)a_{n-2}$.

The sequences $\{a_n\}$ are called ***P-recursive***

(5) ***D-algebraic*** GF $Q\big(t, \mathcal{A}, \mathcal{A}', \ldots, \mathcal{A}^{(k)}\big) = 0$, $Q \in \mathbb{Z}[t, x_0, x_1, \ldots, x_k]$

E.g. $a_n = \#\{\sigma(1) < \sigma(2) > \sigma(3) < \ldots \in S_n\}$, $\mathcal{A}'' = \mathcal{A} \cdot \mathcal{A}'$.

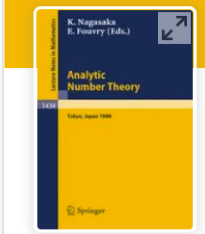
$$\textit{Rational} \subsetneq \textit{Algebraic} \subsetneq \textit{Diagonal} \subsetneq \textit{D-finite} \subsetneq \textit{D-algebraic}$$

Christol's conjecture:

$$a_n \in \mathbb{N},\ \ a_n \leq c^n \ \ \forall\ n \in \mathbb{N}$$

$$\{a_n\} \in \text{D-finite} \implies \{a_n\} \in \text{Diagonal}$$

$$\sum_{n=0}^{\infty} \binom{2n}{n} t^{2n} = \operatorname{diag} \frac{1}{1-x-y}$$



Analytic Number Theory pp 45–64 | Cite as

Globally bounded solutions of differential equations

Christol Gilles

"Conjecture 4.
Every D-finite globally bounded function is the diagonal of a rational function."

State of the art:

(1) **Remarkable successes** proving/disproving formulas in *enumerative combinatorics*

(counting walks, trees, maps, etc.)

(2) **Minor successes** proving/disproving formulas in *number theory*

E.g. $\mathcal{P}(t) = \sum_n p_n t^n \in$ D-finite ($p_n :=$ n-th prime). [Flajolet–Gerhold–Salvy, 2005]

Is $\mathcal{P}(t)$ D-algebraic? (surely not!?)

Also $\theta(t) = \sum_n t^{n^2} \in$ D-algebraic [Jacobi, 1848]

OTOH $\theta(t) \notin$ T-algebraic $\leftarrow$ version of $\mathbb{N}$–D–algebraic [Drmota–P., 2023+]

Is $\sum_n t^{n^3} \in$ D-algebraic? (surely not!?)

(3) **Moderate successes** proving/disproving formulas in *geometric group theory*

(this talk)

Growth and cogrowth sequences

Definition:

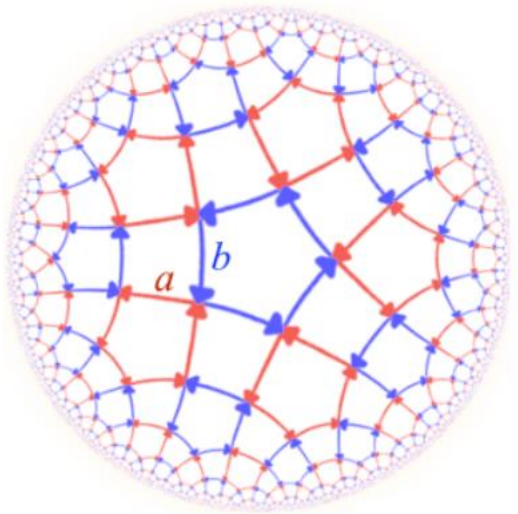
Let G be a finitely generated group, $G = \langle S \rangle$, where $S = S^{-1}$ symmetric generating set

$$\textit{length}: \qquad \ell(g) := \min\{\ell : g = s_1 \cdots s_\ell,\ (s_1, \ldots, s_\ell) \in S^\ell\}$$

$$\textit{growth sequence}: \qquad \mathrm{growth}_S(n) := \left|\left\{g \in G : \ell(g) \le n\right\}\right|$$

$$\textit{cogrowth sequence}: \qquad \mathrm{cog}_S(n) := \left|\left\{(s_1, \ldots, s_n) \in S^n : s_1 \cdots s_n = 1\right\}\right|$$

$$\mathcal{G}_S(t) := \sum_{n=0}^{\infty} \mathrm{growth}_S(n) t^n \qquad \mathcal{C}_S(t) := \sum_{n=0}^{\infty} \mathrm{cog}_S(n) t^n \quad \leftarrow ???$$



Growth sequences vs. cogrowth sequences

Observation: *growth sequence* can be harder to compute than the *cogrowth sequence* (think matrix groups)

Note: *much more is known about* the *cogrowth sequence!*

Examples:

1) $G = \mathbb{Z}$, $S = \{\pm 1\}$, $\mathrm{growth}_S(n) = 2n + 1$

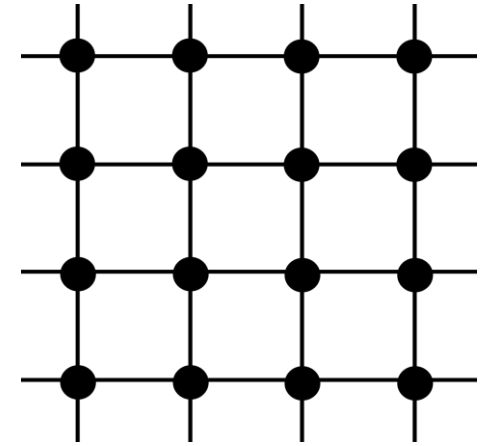
$\mathrm{cog}_S(2n) = \binom{2n}{n}$, $\mathrm{cog}_S(2n+1) = 0$,

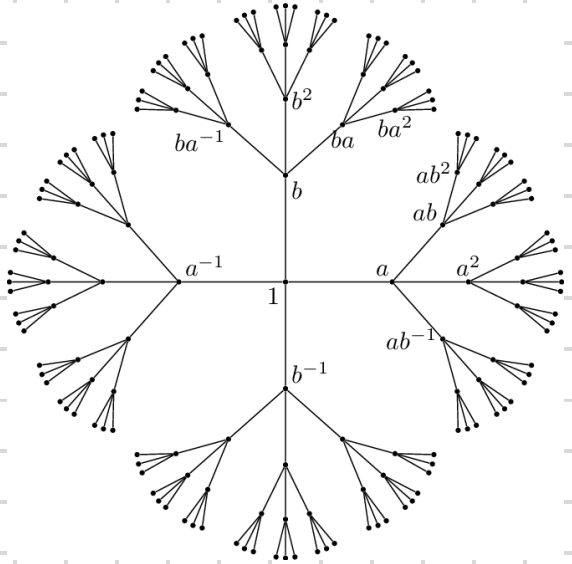
2) $G = \mathbb{Z}^2$, $S = \{(\pm 1, 0), (0, \pm 1)\}$, $\mathrm{growth}_S(n) = 2n^2 + 2n + 1$,

$\mathrm{cog}_S(2n) = \binom{2n}{n}^2$, $\mathrm{cog}_S(2n+1) = 0$,

3) $G = F_2$, $S = \{a, a^{-1}, b, b^{-1}\}$, $\mathrm{growth}_S(n) = (4^n - 1)/3$,

$\mathcal{C}_S(t) = 3/\left(1 + 2\sqrt{1 - 12t^2}\right)$





Properties of growth sequences:

(1) $A_1 + \text{growth}_S(C_1 n) \leq \text{growth}_{S'}(n) \leq A_2 + \text{growth}_S(C_2 n) \quad \forall S, S'$, where $C_1, C_2 > 0$
(asymptotics is independent of the generating set)

(2) $\exists$ uncountably many f.g. groups $\implies$ $\exists$ non-D-algebraic growth sequences

(3) $\exists$ groups of polynomial, exponential, intermediate growth (*Grigorchuk groups*)

(4) linear groups have polynomial or exponential growth (*Tits alternative*, *Milnor–Wolf theorem*)

(5) groups of polynomial growth are virtually nilpotent (*Gromov theorem*)

(6) for many classes of groups $\mathcal{G}_S \in$ Rational $\forall\ S$ (abelian, hyperbolic, H_3)

(7) $\exists$ examples $\mathcal{G}_S \in$ Rational and $\mathcal{G}_{S'} \notin$ Algebraic
(nonamenable [Shapiro, 1994], nilpotent [Stoll, 1996])

Properties of cogrowth sequences:

(1) $A_1 + \mathrm{cog}_S(C_1 n) \leq \mathrm{cog}_{S'}(n) \leq A_2 + \mathrm{cog}_S(C_2 n) \quad \forall S, S'$, where $C_1, C_2 > 0$

(asymptotics is independent of the generating set)

(2) G is finite $\iff$ $\mathcal{C}_S \in$ Rational [Kuksov'98] (in fact, $\mathbb{N}$-Rational)

(3) G is abelian $\implies$ $\mathcal{C}_S \in$ Diagonal (folklore for $\mathbb{Z}^d$, [Kuksov'98])

(4) $G = F_k \implies \mathcal{C}_S \in$ Algebraic ([Aomoto'84], [Figà-Talamanca, Steger'94], [Haiman'93])

(5) $G \in$ solvable, exponential growth $\implies \mathcal{C}_S \notin$ D-finite $\forall S$ [Garrabrant–P.'17]

This resolved *Kontsevich's question*: Is $\mathcal{C}_S \in$ D-finite $\forall$ linear G?

(6) $G \in$ intermediate growth $\implies \mathcal{C}_S \notin$ D-finite $\forall S$ [Bell–Mishna'20]

Open problems for cogrowth sequences:

(1) Does there exist finitely presented G with $\mathcal{C}_S \notin$ D-algebraic?

(2) Does there exist G with $\mathcal{C}_S \in$ Algebraic but $\mathcal{C}_{S'} \notin$ Algebraic?

(same question for Diagonal, D-finite, D-algebraic)

(3) Are there (not virtually abelian) *nilpotent* G with $\mathcal{C}_S \notin$ Diagonal?

(same question for D-finite, D-algebraic)

(3′) Are there (not virtually abelian) *nilpotent* G with $\mathcal{C}_S \in$ Diagonal?

(same question for D-finite, D-algebraic)

Today: We came *really close* to resolving (3)

Unitriagular group:

$$\mathrm{UT}(3,\mathbb{Z}) = H_3$$

$$S := \left\{ \begin{pmatrix} 1 & \pm 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \pm 1 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

$$\mathrm{UT}(m,\mathbb{Z}) := \begin{bmatrix} 1 & \mathbb{Z} & \mathbb{Z} & \cdots & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} & \cdots & \mathbb{Z} & \mathbb{Z} \\ 0 & 0 & 1 & \cdots & \mathbb{Z} & \mathbb{Z} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \mathbb{Z} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}_{m \times m}$$

$$\mathrm{cog}_S(2n) = \#\text{ walks } \gamma : O \to O \text{ in } \mathbb{Z}^2 \text{ with } \quad \mathrm{signed\_area}(\gamma) = 0$$

A307468 Cogrowth sequence for the Heisenberg group.

1, 4, 28, 232, 2156, 21944, 240280, 2787320, 33820044, 424925872, 5486681368, 72398776344

Cogrowth sequences of unitriangular groups:

(1) $m = 3,\ G = \mathrm{UT}(3, \mathbb{Z}) = H_3 \implies \mathrm{cog}_S(2n) \sim C|S|^n/n^2$

$\implies \mathcal{C}_S \notin$ Algebraic [Jungen'31]

(2) $m = 6,\ G = \mathrm{UT}(6, \mathbb{Z}) \implies \mathrm{cog}_S(2n) \sim C|S|^n/n^{35/2}$

$\implies \mathcal{C}_S \notin$ $\mathbb{N}$-algebraic [Banderier–Drmota'15]

(3) **Conjecture:** $\mathcal{C}_S \notin$ D-algebraic for all $m \geq 3$ and all S

(4) **Open:** $\exists\ \mathcal{C}_S \notin$ Diagonal for some $m \geq 3$ and S

(5) **Open:** $\exists\ \mathcal{C}_S \in$ D-algebraic for some $m \geq 3$ and S

New results

Main Theorem

For a fixed sufficiently large integer m, 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 $\mathcal{C}_S(t)$ as diag P/Q, for some $P, Q \in \mathbb{Z}[x_1, \ldots, x_k]$, and $k \geq 1$.

Moreover, the result holds for some $m \leq 9.6 \cdot 10^{85}$.

Moral: Even if $\mathcal{C}_S \in$ Diagonal for all $\langle S \rangle = \mathrm{UT}(m,\mathbb{Z})$, the proof would be *ineffective*.

In fact, the claim "$\mathcal{C}_S \in$ Diagonal for all $m \geq 3$ and all S" could be independent of ZFC

New results

Theorem 1.

There exist $m \geq 3$, $a \geq 1$, and prime p, s.t. the following problem is undecidable:

Given finite symmetric generating sets S, T in $\mathrm{UT}(m, \mathbb{Z})$, determine whether

$$\forall n \in \mathbb{N} \ : \ \mathrm{cog}_S(n) \equiv \mathrm{cog}_T(n) \mod p^a.$$

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

Theorem 2.

Let $a \geq 1$, let p be a prime, and let G be a finitely generated abelian group.

The following problem is decidable:

Given finite symmetric generating sets S, T in G, determine whether

$$\forall n \in \mathbb{N} \ : \ \mathrm{cog}_S(n) \equiv \mathrm{cog}_T(n) \mod p^a.$$

Proof of Theorem 2

Theorem 2.

Let $a \geq 1$, let p be a prime, and let G be a finitely generated abelian group.

The following problem is decidable:

Given finite symmetric generating sets S, T in G, determine whether

$$\forall n \in \mathbb{N} \ : \ \mathrm{cog}_S(n) \equiv \mathrm{cog}_T(n) \mod p^a.$$

Lemma 1. [Kuksov, 1998]

Let $G = \langle S \rangle$ be an abelian group, $S = S^{-1}$. Then $\mathcal{C}_S(t) \in$ Diagonal.

Lemma 2. [Adamczewski–Bell, 2013]

Let $C(t) = \sum_{n \geq 0} c_n t^n \in$ Diagonal, let p be a prime, and let $a \geq 1$, $b \geq 0$.

The following problem is decidable:

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

Understanding Theorem 1

Corollary 1.

For some integer $m \leq 9.6 \cdot 10^{85}$, *there are symmetric g.s.* S, T *of* $\mathrm{UT}(m, \mathbb{Z})$, *such that the following problem is independent of ZFC:*

$$\forall n \in \mathbb{N} \ : \ \mathrm{cog}_S(n) \equiv \mathrm{cog}_T(n) \mod 2^{40}$$

Corollary 2.

For some integer $m \leq 9.6 \cdot 10^{85}$, *there are symmetric g.s.* S, T *of* $\mathrm{UT}(m, \mathbb{Z})$, *s.t.*

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

but the first time the inequality holds is for $n > \mathrm{Tow}(\mathrm{Tow}(\mathrm{Tow}(\phi)))$, *where* $\phi := \phi(\mathcal{S}) + \phi(\mathcal{T})$ *is the sum of absolute values of matrix entries, and* $\mathrm{Tow}(N)$ *is the tower of 2's of length* N.

Theorem 1 implies Main Theorem

Main Theorem

For a fixed sufficiently large integer m, 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 $\mathcal{C}_S(t)$ as diag P/Q, for some $P, Q \in \mathbb{Z}[x_1, \ldots, x_k]$, and $k \geq 1$.

Moreover, the result holds for some $m \leq 9.6 \cdot 10^{85}$.

PROOF BY CONTRADICTION

Lemma 2. [Adamczewski–Bell, 2013]

Let $C(t) = \sum_{n\geq 0} c_n t^n \in$ Diagonal, let p be a prime, and let $a \geq 1$, $b \geq 0$.

The following problem is decidable:

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

Towards the proof of Theorem 1

Hilbert's tenth problem

From Wikipedia, the free encyclopedia

Theorem (unsolvability of Hilbert's tenth problem). *One* CANNOT *construct an algorithm that would determine, for an arbitrary Diophantine equation, whether or not it has a solution in integers.*

[Martin Davis, Yuri Matiyasevich, Hilary Putnam and Julia Robinson, 1970]

Main idea: embedding Diophantine equations into the cogrowth

Towards the proof of Theorem 1

Main Lemma

Let $f \in \mathbb{Z}[x_1, \ldots, x_k]$ with $D = \deg f \geq 2$. Then for some

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

there exists matrices $P, Q, A_1, \ldots, A_k \in \mathrm{UT}(m, \mathbb{Z})$, s.t. every word of the form

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

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 integer root of f, i.e. $f(x_1, \ldots, x_k) = 0$.

Dreaming beyond diagonals

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 $\operatorname{bin}(z)$ 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. $\rho_i/2 \equiv a \mod 2^b$,*
(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:*

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

Theorem 4. *Suppose Conjecture 3.4 holds. Then there exists $m \geq 1$ and a symmetric g.s. S of $\mathrm{UT}(m, \mathbb{Z})$, s.t. the cogrowth series $\mathcal{C}_S(t) \notin$ D-algebraic.*

Dreaming beyond diagonals

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.

Thank you!