

WORDS IN LINEAR GROUPS, RANDOM WALKS, AUTOMATA AND P-RECURSIVENESS

SCOTT GARRABRANT* AND IGOR PAK*

July 6, 2016

ABSTRACT. Let S be a generating set of a finitely generated group $G = \langle S \rangle$. Denote by a_n the number of words in S of length n that are equal to 1. We show that the *cogrowth sequence* $\{a_n\}$ is not always P-recursive. This is done by developing new combinatorial tools and using known results in computability and probability on groups.

1. INTRODUCTION

An integer sequence $\{a_n\}$ is called *polynomially recursive*, or *P-recursive*, if it satisfies a non-trivial linear recurrence relation of the form

$$(*) \quad q_0(n)a_n + q_1(n)a_{n-1} + \dots + q_k(n)a_{n-k} = 0,$$

for some $q_i(x) \in \mathbb{Z}[x]$, $0 \leq i \leq k$. The study of P-recursive sequences plays a major role in modern Enumerative and Asymptotic Combinatorics, see e.g. [FS, Ges, Odl, S1]. They have *D-finite* (also called *holonomic*) generating series

$$\mathcal{A}(t) = \sum_{n=0}^{\infty} a_n t^n,$$

and various asymptotic properties (see Section 5 below).

Fix a finitely generated group G and a generating (multi-) set S , i.e. $G = \langle S \rangle$. Let $a_n = a_n(G, S)$ be the number of words in S of length n equal to 1. In this case $\{a_n\}$ is called the *cogrowth sequence* and $\mathcal{A}(t) = \mathcal{A}_{G,S}(t)$ the *cogrowth series*. They were introduced by Polya in 1921 in probabilistic context of random walks on graphs, and by Kesten in 1959 in the context of amenability [Kes]. They have been computed exactly in numerous examples (see below). The asymptotic properties of cogrowth sequences of finitely generated groups were studied by Grigorchuk, Cohen, Varopoulos and many others (see §6.1).

The analytic properties of the cogrowth series $\mathcal{A}_{G,S}(t)$ and its relation to group properties remain largely mysterious. The series is rational for finite groups (and only finite groups [K1]), algebraic for free groups $G = F_k$ (see [Hai]) and the dihedral group (see [H1]). The series is D-finite for $G = \mathbb{Z}^k$, many other abelian groups (see [H1, H2]), and the *Baumslag-Solitar groups* $G = \text{BS}(k, k)$, where $\text{BS}(m, n) = \langle a, b \mid a^m b = b a^n \rangle$ (see [ERVW]). Until this work not a single example of non-D-finite cogrowth series has been given.

Theorem 1. *Group $F_2 \times F_2$ has finite generating multiset S , i.e. $G = \langle S \rangle$, such that the sequence $\{a_n(G, S)\}$ is not P-recursive.*

Theorem 2. *Let $G \subset \text{GL}(k, \mathbb{Z})$ be an amenable linear group of exponential growth, and let $S = S^{-1}$ be a symmetric generating set. Then the sequence $\{a_n(G, S)\}$ is not P-recursive.*

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

Note that Theorem 1 gives an example for a non-amenable group. In fact, the proof implies that there are many such examples. On the other hand, Theorem 2 gives many examples for amenable groups, which are very different asymptotically (cf. §6.1). The following corollary can be deduced from either theorem.

Corollary 3. *There exists a finitely generated subgroup $G \subset \mathrm{SL}(4, \mathbb{Z})$ and a finite generating set S , i.e. $G = \langle S \rangle$, such that the sequence $\{a_n(G, S)\}$ is not P-recursive.*

The proof of Theorem 1 is completely self-contained and based on ideas from computability. Roughly, we give an explicit construction of a finite state automaton with two stacks and a non-P-recursive sequence of accepting path lengths (see Section 3). We then convert this automaton into a generating set $S \subset F_2 \times F_2$, see Section 4. The resulting groups are non-amenable and have cogrowth sequence as unwieldy as desired modulo 2. The key part of the proof is a new combinatorial lemma giving an obstruction to P-recursiveness (see Section 2). As a consequence, we show that being P-recursive is not invariant under quasi-isometry (Theorem 8), i.e. can depend on a generating set S .

Proof of Theorem 2 is analytic in nature, and is the opposite of being self-contained. We prove that for all polycyclic groups of exponential growth and all symmetric generating sets $S = S^{-1}$ the cogrowth sequence is not P-recursive. This approach is restricted to amenable linear groups as in the theorem, and applies also to *Grigorchuk groups* of intermediate growth, the *lamplighter groups* $\mathbb{Z}^d \wr \mathbb{Z}_2$ and the Baumslag-Solitar groups $\mathrm{BS}(k, 1)$, where $k \geq 2$.

In this proof we interpret the problem in a probabilistic language, and obtain the result as a combination of a number of advanced and technical results in analysis, analytic number theory, probability and group theory. Denote by $p(n) = a_n(G, S)/|S|^n$ the probability of return after n steps of a random walk on the corresponding Cayley graph $\mathrm{Cay}(G, S)$. Finding the asymptotics of $p(n)$ as $n \rightarrow \infty$ is a classical problem in probability (see e.g. [Pete, Woe]). Since P-recursiveness of $\{a_n\}$ implies P-recursiveness of $\{p(n)\}$, and much is known about the asymptotic of both $p(n)$ and P-recursive sequences, this connection can be exploited to obtain non-P-recursive examples (see Section 5). See also Section 6 for final remarks and historical background behind the two proofs.

2. PARITY OF P-RECURSIVE SEQUENCES

In this section, we give a simple obstruction to P-recursiveness.

Lemma 4. *Let $\{a_n\}$ be a P-recursive integer sequence. Consider the infinite binary word $\mathbf{w} = w_1 w_2 \dots$ defined by $w_n = a_n \bmod 2$. Then, there exists a finite binary word v which is not a subword of w .*

Proof. Let $\eta(n)$ denote the largest integer r such that $2^r | n$. By definition, there exist polynomials $q_0, \dots, q_k \in \mathbb{Z}[n]$, such that

$$a_n = \frac{1}{q_0(n)} (a_{n-1} q_1(n) + \dots + a_{n-k} q_k(n)), \quad \text{for all } n > k.$$

Let ℓ be any integer such that $q_i(\ell) \neq 0$ for all i . Similarly, let m be the smallest integer such that $2^m > k$, and $m > \eta(q_i(\ell))$ for all i . Finally, let $d > 0$ be such that $\eta(q_d(\ell)) \leq \eta(q_i(\ell))$ for all $i > 0$.

Consider all n such that:

$$(\star) \quad n = \ell \bmod 2^m, \quad w_{n-d} = 1 \quad \text{and} \quad w_{n-i} = 0 \quad \text{for all } i \neq 0, d.$$

Note that $\eta(q_i(n)) = \eta(q_i(\ell))$ for all i , since $q_i(n) = q_i(\ell) \bmod 2^m$ and $\eta(q_i(\ell)) < m$. We have

$$\eta(a_n) = \eta(a_{n-1} q_1(\ell) + \dots + a_{n-k} q_k(\ell)) - \eta(q_0(\ell)).$$

Since $\eta(a_{n-d}q_d(\ell)) < \eta(a_{n-i}q_i(\ell))$ for all $i \neq d$, this implies that

$$\eta(a_n) = \eta(a_{n-d}q_d(\ell)) - \eta(q_0(\ell)) = \eta(q_d(\ell)) - \eta(q_0(\ell)).$$

Therefore, $w_n = 1$ if and only if $\eta(q_d(\ell)) = \eta(q_0(\ell))$. This implies that w_n is independent of n , and must be the same for all n satisfying (\star) . In particular, this means that at least one of the words $0^{k-d}10^{d-1}1$ and $0^{k-d}10^d$ cannot appear in \mathbf{w} ending at a location congruent to ℓ modulo 2^m .

Consider the word $v = (0^{k-d}10^k10^{d-1})^{2^m}$. Note that $0^{k-d}10^k10^{d-1}$ has odd length, and contains both $0^{k-d}10^{d-1}1$ and $0^{k-d}10^d$ as subwords. Therefore, the word v contains both $0^{k-d}10^{d-1}1$ and $0^{k-d}10^d$ in every possible starting location modulo 2^m . This implies that v cannot appear as a subword of \mathbf{w} . \square

3. BUILDING AN AUTOMATON

In this section we give an explicit construction of a finite state automaton with the number of accepting paths given by a binary sequence which does not satisfy the conditions of Lemma 4.

Let $X \simeq F_3$ be the free group generated by $x, 1_x,$ and 0_x . Similarly, let $Y \simeq F_3$ be the free group generated by $y, 1_y,$ and 0_y .

Define a directed graph Γ on vertices $\{s_1, \dots, s_8\}$, and with edges as shown in Figure 1. Some of the edges in Γ are labeled with elements of $X, Y,$ or both. For a path γ in Γ , denote by $\omega_X(\gamma)$ the product of all elements of X in γ , and by $\omega_Y(\gamma)$ denote the product of all elements of Y in γ . By a slight abuse of notation, while traversing γ we will use ω_X and ω_Y to refer to the product of all elements of X and Y , respectively, on edges that have been traversed so far.

Finally, let b_n denote the number of paths in Γ from s_1 to s_8 of length n , such that $\omega_X(\gamma) = \omega_Y(\gamma) = 1$. For example, the path

$$\gamma : s_1 \xrightarrow{xy} s_1 \rightarrow s_2 \xrightarrow{1_y x^{-1}} s_4 \xrightarrow{1_y^{-1} 1_x} s_4 \xrightarrow{y^{-1}} s_5 \rightarrow s_6 \xrightarrow{1_x^{-1}} s_8$$

is the unique such path of length 7, so $b_7 = 1$.

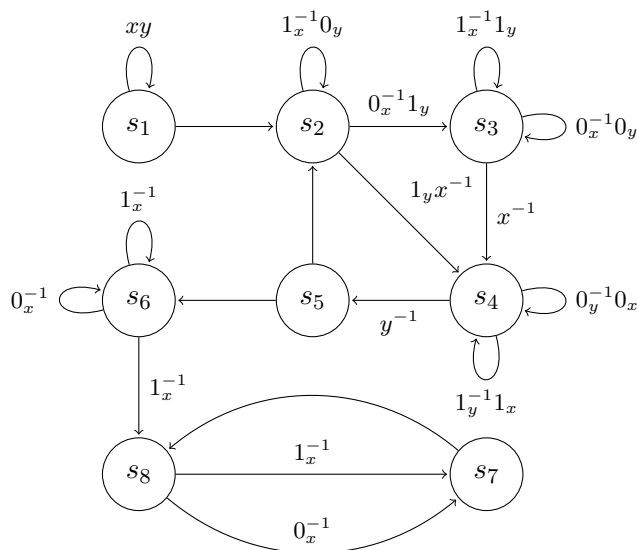


FIGURE 1. The graph Γ .

Lemma 5. *For every $n \geq 1$, we have $b_n \in \{0, 1\}$. Moreover, every finite binary word is a subword of $\mathbf{b} = b_1 b_2 \dots$.*

Proof. To simplify the presentation, we split the proof into two parts.

(a) The structure of paths. Let γ be a path from s_1 to s_8 . Denote by k the number of times γ traverses the loop $s_1 \xrightarrow{xy} s_1$. The value of ω_X after traversing these k loops is x^k , and the value of ω_Y is y^k .

There must be k instances of the edge $s_4 \xrightarrow{y^{-1}} s_5$ in γ to cancel out the y^k . Further, any time the path traverses this edge, the product ω_Y must change from some y^j to y^{j-1} , with no 0_y or 1_y terms. Therefore, every time γ enters the vertex s_4 , it must traverse the two loops $s_4 \xrightarrow{1_y^{-1}1_x} s_4$ and $s_4 \xrightarrow{0_y^{-1}0_x} s_4$ enough to replace any 0_y and 1_y terms in ω_Y with 0_x and 1_x terms in ω_X . This takes the binary word at the end of ω_Y , and moves it to the end of ω_X in the reverse order.

Similarly, any time γ traverses the edge $s_3 \xrightarrow{x^{-1}} s_4$ or $s_2 \xrightarrow{1_y x^{-1}} s_4$, the product ω_X must change from some x^j to x^{j-1} , with no 0_x or 1_x terms. Every time γ enters the vertex s_2 , it must remove all 0_x and 1_x terms from ω_X before transitioning to s_4 . The s_2 and s_3 vertices ensure that as this binary word is deleted from ω_X , another binary word is written at the end of ω_Y such that the reverse of the binary word written at the end of ω_Y is one greater as a binary integer than the word removed from the end of ω_X .

Every time γ traverses the edge $s_4 \xrightarrow{y^{-1}} s_5$, the number written in binary at the end of ω_X is incremented by one. Thus, after traversing this edge k times, the X word will consist of k written in binary, and ω_Y will be the identity. At this point, γ will traverse the edge $s_5 \xrightarrow{y^{-1}} s_6$.

After entering the vertex s_6 , all of the 0_x and 1_x terms from ω_X will be removed. Each time a 1_x term is removed, γ can move to the vertex s_8 . From s_8 , the 0_x and 1_x terms will continue to be removed, but γ will traverse two edges for every term removed, thus moving at half speed. After all of these terms are removed, the products $\omega_X(\gamma)$ and $\omega_Y(\gamma)$ are equal to identity, as desired.

(b) The length of paths. Now that we know the structure of paths through Γ , we are ready to analyze the possible lengths of these paths. There are only two choices to make in specifying a path γ : first, the number $k = k(\gamma)$ of times the loop from s_1 to itself is traversed, and second, the number $j = j(\gamma)$ of digits still on $\omega_X(\gamma)$ immediately before traversing the edge from s_6 to s_8 . The number j must be such that the j -th binary digit of k is a 1.

When γ reaches s_5 for the first time, it has traversed $k + 4$ edges. In moving from the i -th instance of s_5 along γ to the $(i + 1)$ -st instance of s_5 , the number of edges traversed is $3 + \lceil 1 + \log_2(i) \rceil + \lceil 1 + \log_2(i + 1) \rceil$, three more than the sum of the number of binary digits in i and $i + 1$. Therefore, the number of edges traversed by the time γ reaches s_6 is equal to

$$k + 5 + \sum_{i=1}^{k-1} (3 + \lceil 1 + \log_2(i) \rceil + \lceil 1 + \log_2(i + 1) \rceil).$$

If $j = 1$, the edge from s_6 to s_8 is traversed at the last possible opportunity and $\lceil 1 + \log_2(k) \rceil$ more edges are traversed. However, if $j > 1$, there are an additional $j - 1$ edges traversed, since the s_7 and s_8 states do not remove ω_X terms as efficiently as s_6 . In total, this gives $|\gamma| = L(k(\gamma), j(\gamma))$, where

$$L(k, j) = j - 1 + \lceil 1 + \log_2(k) \rceil + k + 5 + \sum_{i=1}^{k-1} (3 + \lceil 1 + \log_2(i) \rceil + \lceil 1 + \log_2(i + 1) \rceil).$$

This simplifies to

$$L(k, j) = j + 6k + 2 \sum_{i=1}^k \lceil \log_2 i \rceil.$$

Since $1 \leq j \leq \lfloor 1 + \log_2(k) \rfloor$, we have $L(k+1, 1) > L(k, j)$ for all possible values of j . Thus, there are no two paths of the same length, which proves the first part of the lemma.

Furthermore, we have $b_n = 1$ if and only if $n = L(k, j)$ for some $k \geq 1$ and j such that the j -th binary digit of k is a 1. Thus, the binary subword of \mathbf{b} at locations $L(k, 1)$ through $L(k, \lfloor 1 + \log_2(k) \rfloor)$ is exactly the integer k written in binary. This is true for every positive integer k , so \mathbf{b} contains every finite binary word as a subword. \square

Example 6. For $k = 3$ and $j = 2$, we have $L(k, j) = 24$. This corresponds to the unique path in Γ of length 24:

$$\begin{aligned} s_1 \xrightarrow{xy} s_1 \xrightarrow{xy} s_1 \xrightarrow{xy} s_1 \rightarrow s_2 \xrightarrow{1_y x^{-1}} s_4 \xrightarrow{1_y^{-1} 1_x} s_4 \xrightarrow{y^{-1}} s_5 \rightarrow s_2 \\ \xrightarrow{1_x^{-1} 0_y} s_2 \xrightarrow{1_y x^{-1}} s_4 \xrightarrow{1_y^{-1} 1_x} s_4 \xrightarrow{0_y^{-1} 0_x} s_4 \xrightarrow{y^{-1}} s_5 \rightarrow s_2 \xrightarrow{0_x^{-1} 1_y} s_3 \xrightarrow{1_x^{-1} 1_y} s_3 \\ \xrightarrow{x^{-1}} s_4 \xrightarrow{1_y^{-1} 1_x} s_4 \xrightarrow{1_y^{-1} 1_x} s_4 \xrightarrow{y^{-1}} s_5 \rightarrow s_6 \xrightarrow{1_x^{-1}} s_8 \xrightarrow{1_x^{-1}} s_7 \rightarrow s_8. \end{aligned}$$

4. PROOF OF THEOREM 1

4.1. From automata to groups. To simplify working with multisets, we work with the corresponding elements of the group algebra $\mathbb{Z}[G]$. We start with the following technical lemma.

Lemma 7. *Let $G = F_{11} \times F_3$. There exists an element $u \in \mathbb{Z}[G]$, such that $[1]u^{2n+1}$ is always even, and $\mathbf{w} = w_1 w_2 \dots$ given by $w_n = \left(\frac{1}{2}[1]u^{2n+1}\right) \bmod 2$, is a infinite binary word that contains every finite binary word as a subword.*

Proof. We suggestively label the generators of F_{11} as $\{s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, x, 0_x, 1_x\}$ and label the generators of F_3 as $\{y, 0_y, 1_y\}$. Consider the following set S of 19 elements of G :

$$\begin{array}{lll} (1) z_1 = s_1^{-1} x y s_1, & (7) z_7 = s_3^{-1} x^{-1} s_4, & (13) z_{13} = s_5^{-1} s_6, \\ (2) z_2 = s_1^{-1} s_2, & (8) z_8 = s_2^{-1} 1_y x^{-1} s_4, & (14) z_{14} = s_6^{-1} 1_x^{-1} s_6, \\ (3) z_3 = s_2^{-1} 1_x^{-1} 0_y s_2, & (9) z_9 = s_4^{-1} 1_y^{-1} 1_x s_4, & (15) z_{15} = s_6^{-1} 0_x^{-1} s_6, \\ (4) z_4 = s_2^{-1} 0_x^{-1} 1_y s_3, & (10) z_{10} = s_4^{-1} 0_y^{-1} 0_x s_4, & (16) z_{16} = s_6^{-1} 1_x^{-1} s_8, \\ (5) z_5 = s_3^{-1} 1_x^{-1} 1_y s_3, & (11) z_{11} = s_4^{-1} y^{-1} s_5, & (17) z_{17} = s_7^{-1} s_8, \\ (6) z_6 = s_3^{-1} 0_x^{-1} 0_y s_3, & (12) z_{12} = s_5^{-1} s_2, & (18) z_{18} = s_8^{-1} 1_x^{-1} s_7, \\ & & (19) z_{19} = s_8^{-1} 0_x^{-1} s_7. \end{array}$$

Let Γ be as defined in the previous section. For every edge from $s_i \xrightarrow{r} s_j$ in Γ , there is one element of S equal to $s_i^{-1} r s_j$. We show that the number of ways to multiply n terms from S to get $s_1^{-1} s_8$ is exactly b_n .

First, we show that there is no product of terms in S whose F_{11} component is the identity. Assume that such a product exists, and take one of minimal length. If there are two consecutive terms in this product such that s_i at the end of one term does not cancel the s_j^{-1} at the start of the following term, then either the s_i must cancel with a s_i^{-1} before it or the s_j^{-1} must cancel with a s_j after it. In both cases, this gives a smaller sequence of terms whose product must have F_{11} component equal to the identity. If the s_i at the end of each term cancels the s_j^{-1} at the beginning of the next term, then this product corresponds to a cycle $\gamma \in \Gamma$ such that $\omega_X(\gamma)$ is the identity. Straightforward analysis of Γ shows that no such cycle exists, so there is no product of terms in S whose product F_{11} component equal to the identity.

This also means that the s_i at the end of each term must cancel the s_j^{-1} at the start of the following term, since otherwise either the s_i must cancel with a s_i^{-1} before it or the s_j^{-1} must cancel with a s_j after it, forming a product of terms in S whose F_{11} component is equal to the identity.

Since each s_i cancels with an s_i^{-1} at the start of the following term, the product must correspond to a path $\gamma \in \Gamma$. If γ is from s_i to s_j , the product will evaluate to $s_i^{-1}\omega_X(\gamma)\omega_Y(\gamma)s_j$. Therefore, the number of ways to multiply n terms from S to get $s_1^{-1}s_8$ is equal to b_n .

We can now define $u \in \mathbb{Z}[G]$ as

$$u = 2s_8^{-1}s_1 + \sum_{z_i \in S} z_i.$$

We claim that $\frac{1}{2}[1]u^{2n+1} = b_{2n} \pmod{2}$. We already showed that one cannot get 1 by multiplying only elements of S , so the $2s_8^{-1}s_1$ term must be used at least once. If this term is used more than once, then the contribution to $[1]u^{2n+1}$ will be 0 mod 4. Therefore, we need only consider the cases where this term is used exactly once, so $\frac{1}{2}[1]u^{2n+1}$ is equal modulo 2 to the number of products of the form

$$(\star\star) \quad 2 = z_{i_1} \dots z_{i_{k-1}} (2s_8^{-1}s_1) z_{i_{k+1}} \dots z_{i_{2n+1}}.$$

This condition holds if and only if

$$z_{i_{k+1}} \dots z_{i_{2n+1}} z_{i_1} \dots z_{i_{k-1}} = s_1^{-1}s_8,$$

which can be achieved in b_{2n} ways.

There are $2n+1$ choices for the location k of the $2s_8^{-1}s_1$ term, and for each such k , there are b_{2n} solutions to $(\star\star)$. This gives

$$\frac{1}{2}[1]u^{2n+1} = (2n+1)b_{2n} = b_{2n} \pmod{2},$$

which implies $w_n = b_{2n}$. By Lemma 7, we conclude that \mathbf{w} is an infinite binary word which contains every finite binary word as a subword. \square

4.2. Counting words mod 2. Here we deduce the main result of this paper and then give an application.

Proof of Theorem 1. Let $S \subset F_{11} \times F_3$ be as in the proof of Lemma 7. Let $G = \langle S \rangle$ and observe that $a_n = [1]u^n = a_n(G, S)$. By Lemma 7, the number a_{2n+1} is always even, and the word $\mathbf{w} = w_1w_2\dots$ given by $w_n = \frac{1}{2}a_{2n+1} \pmod{2}$ is an infinite binary word which contains every finite binary word as a subword. Therefore, by Lemma 4, the sequence $\{\frac{1}{2}a_{2n+1}\}$ is not P-recursive. Since P- recursivity is closed under taking a subsequence consisting of every other term, the sequence $\{a_n\}$ is also not P-recursive.

Now realize $F_{11} \times F_3$ as a subgroup of $F_2 \times F_2$ and add standard generators of $F_2 \times F_2$ to S repeated 4 times. This would not change parity of $\frac{1}{2}a_{2n+1}(G, S)$, which completes the proof. \square

Proof of Corollary 3. Observe that $\mathrm{SL}(2, \mathbb{Z})$ contains Sanov's subgroup isomorphic to F_2 (see e.g. [dlH]), and $\mathrm{SL}(4, \mathbb{Z})$ contains $\mathrm{SL}(2, \mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z})$ as a subgroup. \square

Theorem 8. *Group $G = F_2 \times F_2$ has two generating multisets S_1 and S_2 , i.e. $G = \langle S_1 \rangle = \langle S_2 \rangle$, such that $\{a_n(G, S_1)\}$ is P-recursive, while $\{a_n(G, S_2)\}$ is not P-recursive.*

Proof. Denote by X_1 and X_2 the standard generating sets of two copies of F_2 in G . Let $S_1 = (X \times 1) \cup (1 \times Y)$,

$$w_1 = \sum_{x \in X_1} x, \quad w_2 = \sum_{x \in X_2} x.$$

Recall that if $\{c_n\}$ is P-recursive, then so is $\{c_n/n!\}$ and $\{c_n \cdot n!\}$. Observe that

$$\sum_{n=0}^{\infty} [1]u_1^n \frac{t^n}{n!} = \left(\sum_{n=0}^{\infty} [1]w_1^n \frac{t^n}{n!} \right) \left(\sum_{n=0}^{\infty} [1]w_2^n \frac{t^n}{n!} \right).$$

Recall that $\{[1]w_1^n\}$ and $\{[1]w_2^n\}$ are algebraic, and thus P-recursive, by Haiman's theorem [Hai]. This implies that $\{a_n(G, S_1) = [1]u_1^n\}$ is also P-recursive, as desired.

Now, let $S_2 = 4S_1 \cup S$, where S is the set constructed in the proof of Lemma 7, and $4S_1$ means that each element of S_1 is taken 4 times. Observe that $[1]u_2^n = [1]u^n \bmod 4$, where u is as in the proof of Theorem 2. This implies that $\{a_n(G, S_2) = [1]u_2^n\}$ is not P-recursive, and finishes the proof. \square

5. ASYMPTOTICS OF P-RECURSIVE SEQUENCES AND THE RETURN PROBABILITIES

5.1. Asymptotics. The asymptotics of general P-recursive sequences is understood to be a finite sum of terms

$$A(n!)^s \lambda^n e^{Q(n^\gamma)} n^\alpha (\log n)^\beta,$$

where $s, \gamma \in \mathbb{Q}$, $\alpha, \lambda \in \overline{\mathbb{Q}}$, $\beta \in \mathbb{N}$, and $Q(\cdot)$ is a polynomial. This result goes back to Birkhoff and Trjitzinsky (1932), and also Turrittin (1960). Although there are several gaps in these proofs, they are closed now, notably in [Imm]. We refer to [FS, §VIII.7], [Odl, §9.2] and [Pak] for various formulations of general asymptotic estimates, an extensive discussion of priority issues and further references.

For the integer P-recursive sequences which grow at most exponentially, the asymptotics have further constraints summarized in the following theorem.

Theorem 9. *Let $\{a_n\}$ be an integer P-recursive sequence defined by $(*)$, and such that $a_n < C^n$ for some $C > 0$ and all $n \geq 1$. Then*

$$a_n \sim \sum_{i=1}^m A_i \lambda_i^n n^{\alpha_i} (\log n)^{\beta_i},$$

where $\alpha_i \in \mathbb{Q}$, $\lambda_i \in \overline{\mathbb{Q}}$ and $\beta_i \in \mathbb{N}$.

The theorem is a combination of several known results. Briefly, the generating series $\mathcal{A}(t)$ is a G -function in a sense of Siegel (1929), which by the works of André, Bombieri, Chudnovsky, Dwork and Katz, must satisfy an ODE which has only regular singular points and rational exponents (see a discussion in [And, p. 719] and an overview in [Beu]). We then apply the Birkhoff–Trjitzinsky theorem, which in the regular case has a complete and self-contained proof (see Theorem VII.10 and subsequent comments in [FS]). We refer to [Pak] for further references and details.

5.2. Probability of return. Let G be a finitely generated group. A generating set S is called *symmetric* if $S = S^{-1}$. Let H be a subgroup of G of finite index. It was shown by Pittet and Saloff-Coste [PS3], that for two symmetric generating sets S and S' , $\langle S \rangle = G$ and $\langle S' \rangle = H$, we have

$$(\diamond) \quad C_1 p_{G,S}(\alpha_1 n) < p_{H,S'}(n) < C_2 p_{G,S}(\alpha_2 n),$$

for all $n > 0$ and fixed constants $C_1, C_2, \alpha_1, \alpha_2 > 0$. For $G = H$, this shows, qualitatively, that the asymptotic behavior of $p_{G,S}(n)$ is a property of a group.

Denote by $\gamma_{G,S}(n)$ the (word) *growth function* sequence, defined as the number of elements $g \in G$ at distance $d_{G,S}(g) = n$ from 1 in the Cayley graph $\text{Cay}(G, S)$. We assume the reader is familiar with standard definitions of groups of polynomial, exponential and intermediate growth (see e.g. [dlH, GriP]).

The following results summarize what is known for large classes of groups.

Theorem 10. *Let G be a finitely generated group and S a symmetric generating set.*

(i) *If G has polynomial growth, the return probabilities are also polynomial:*

$$A_1 n^{-d} < p_{G,S}(2n) < A_2 n^{-d},$$

for some $A_1, A_2 > 0$ and $d \in \mathbb{N}$.

(ii) *If G is polycyclic and has exponential growth, the return probabilities are mildly exponential:*

$$A_1 \rho_1^{\sqrt[3]{n}} < p_{G,S}(2n) < A_2 \rho_2^{\sqrt[3]{n}},$$

for some $A_1, A_2 > 0$ and $0 < \rho_1, \rho_2 < 1$. More generally, same bounds hold for all solvable groups of exponential growth with finite Prüfer rank.

(iii) *The above upper bound extends to all groups of intermediate growth:*

$$p_{G,S}(2n) < A \rho^{n^{\alpha/(\alpha+2)}}, \quad \text{for all } \gamma_{G,S}(n) > B c^{n^\alpha},$$

where $A, B > 0$, $c > 1$ and $0 < \alpha, \rho < 1$.

(iv) *If G is non-amenable, the return probabilities are exponential:*

$$A_1 \rho_1^n < p_{G,S}(2n) < A_2 \rho_2^n,$$

for some $A_1, A_2 > 0$ and $0 < \rho_1, \rho_2 < 1$.

The theorem is a compilation of several known results. The non-amenable case (iv) is proved by Kesten [Kes] (see also [Woe] and §6.1). In the polynomial case (i), the lower bound follows from the CLT by Crépel and Raugi [CR], while the upper bound was proved by Varopoulos using the Nash inequality [V1] (see also [V3]). For amenable groups of exponential and intermediate growth, the upper bound is due to Varopoulos [V2]. For polycyclic groups of exponential growth, the lower bound is due to Alexopoulos [Ale]. The generalization to finite rank was given by Pittet and Saloff-Coste [PS5]. We refer to [PS4] and [Woe, §15] for proofs and further references, and to [PS2] for a generalization to discrete subgroups of groups of Lie type.

The following theorem includes results on the probability of return for several amenable groups of special interest which are not covered by the theorem.

Theorem 11. (i) *For the solvable Baumslag–Solitar groups $G = \text{BS}(k, 1)$, $k \geq 2$, and symmetric generating sets S , the return probabilities are mildly exponential:*

$$A_1 \rho_1^{\sqrt[3]{n}} < p_{G,S}(2n) < A_2 \rho_2^{\sqrt[3]{n}},$$

for some $A_1, A_2 > 0$ and $0 < \rho_1, \rho_2 < 1$.

(ii) *Let $L(d, H) = \mathbb{Z}^d \wr H$ be the lamplighter group, where H is a finite abelian group and $d \geq 1$. For symmetric generating set S of $L(d, H)$, the return probabilities are mildly exponential:*

$$A_1 \rho_1^{n^{d/(d+2)}} < p_{L,S}(2n) < A_2 \rho_2^{n^{d/(d+2)}},$$

for some $A_1, A_2 > 0$ and $0 < \rho_1, \rho_2 < 1$.

Part (i) is proved in [Woe, §15.C], and part (ii) is given in [PS1]. Our final result in this subsection is a weak general bound relating the growth function and the probability of return.

Proposition 12. *For every group G and symmetric generating set S , we have:*

$$p_{G,S}(2n) \geq \frac{1}{\gamma_{G,S}(2n)}.$$

In other words, the probability of return is greater than the probability of any other element reached by the random walk. For the proof, see e.g. [AS2, p. 157].

5.3. Applications to P-recursiveness. Recall that if the return probability sequence $\{p_{G,S}(2n)\}$ is not P-recursive, then so is the cogrowth sequence $\{a_n(G, S)\}$.

Conjecture 13. *Let G be an amenable group of superpolynomial growth, and let S be a symmetric generating set. Then the probability of return sequence $\{p_{G,S}(n)\}$ is not P-recursive.*

Theorem 14. *The conjecture above holds for the following classes of groups:*

- (1) *virtually solvable groups of exponential growth with finite Prüfer rank,*
- (2) *amenable linear groups of superpolynomial growth,*
- (3) *for groups of weakly exponential growth*

$$Ae^{n^\alpha} < \gamma_{G,S}(n) < Be^{n^\beta},$$

where $A, B > 0$, and $0 < \alpha, \beta < 1$,

- (4) *the Baumslag-Solitar groups $G = \text{BS}(k, 1)$, $k \geq 2$,*
- (5) *the lamplighter groups $L(d, H) = \mathbb{Z}^d \wr H$, where H is a finite abelian group and $d \geq 1$.*

Part (2) of the theorem implies Theorem 2 in the introduction. Note here that by the main result in [LMS], groups in (1) are exactly those with polynomial subgroup growth. Note also that the (first) *Grigorchuk group* \mathbb{G} has weakly exponential growth (see e.g. [dlH, GriP] and §6.4). Note also that in contrast to Theorem 8, the non-P-recursiveness here holds *for all* S as above (cf. §6.5).

Proof. For (1), use tight bounds in Theorem 10(ii). Now observe that Theorem 9 forbids mildly exponential terms $\rho^{\sqrt[3]{n}}$ in the asymptotics of $p(2n) = a_n/|S|^n$, giving a contradiction. Parts (4) and (5) follow similarly from two parts of Theorem 11.

For (2), by the Tits alternative, the group G must be virtually solvable of exponential growth (see e.g. [dlH]). By the *quasi-isometry* (\diamond) , we can assume that G is solvable. By Mal'tsev's theorem (see e.g. [Sup, Thm. 22.7]), the group G is polycyclic. This reduces (2) to (1).

Finally, for (3) we combine the upper bound in Theorem 11(iii), and the lower bound in Proposition 12. The details are straightforward. \square

To obtain Corollary 3 from Theorem 2, consider the following explicit example. Let $H \subset \text{SL}(3, \mathbb{Z})$ be a linear group of exponential growth:

$$H = \left\{ \begin{pmatrix} x_{1,1} & x_{1,2} & y_1 \\ x_{2,1} & x_{2,2} & y_2 \\ 0 & 0 & 1 \end{pmatrix} \text{ s.t. } \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^k, k \in \mathbb{Z} \right\}$$

(see e.g. [Woe, §15.B]). Observe that $H \simeq \mathbb{Z} \times \mathbb{Z}^2$, and therefore H is solvable. Thus, H has a natural symmetric generating set

$$E = \left\{ \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 0 & \pm 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \pm 1 \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

By Theorem 14(2), the probability of return sequence $\{p_{H,E}(n)\}$ is not P-recursive, as desired.

6. FINAL REMARKS

6.1. The *cogrowth rate* is defined as follows:

$$\rho(G, S) = \lim_{n \rightarrow \infty} a_n(G, S)^{1/n}.$$

Kesten's theorem says that for a symmetric generating set $S = S^{-1}$, we have $\rho(G, S) = |S|$ if and only if G is amenable [Kes]. This explains subexponential behavior of the probability of return $p_{G,S}(n)$ in theorems 10 and 11. This is also the motivation for having both theorems 1 and 2. Let us mention that if $\{a_n(G, S)\}$ is P-recursive, then $\rho(G, S)$ is algebraic, but the opposite is

false by Theorem 2. Since the proof of Theorem 1 is based on the parity considerations, our tools are not strong enough to construct an example with $\rho(G, S) \notin \overline{\mathbb{Q}}$. It would be interesting to find such an example.

Let us mention that the cogrowth functions of Kesten and Grigorchuk–Cohen are somewhat different as the latter does not allow walks to backtrack (see e.g. [Sap, §5.8]). In this paper we use Kesten’s definition (cf. [ERVW, H1, H2, K1, K2]). We refer to [Pete, Woe] for an overview of an extensive body of work on probability on infinite groups.

6.2. Our original motivation was in resolving a question by Maxim Kontsevich, who asked whether $\{a_n\}$ is always P-recursive when $G \subseteq \mathrm{GL}(k, \mathbb{Z})$, see [S2]. In response to the draft of this paper, Ludmil Katzarkov, Maxim Kontsevich and Richard Stanley asked us if the examples we construct satisfy *algebraic differential equations* (ADE), see e.g. [S1, Exc. 6.63]. In a forthcoming paper [GP2] extending our first proof, we construct groups for with the non-ADE cogrowth series. Note that the second proof cannot be easily extended since little is known about the asymptotics of integer ADE sequences.

6.3. The motivation behind the proof of Theorem 1 lies in the classical result of Mihaïlova that $G = F_2 \times F_2$ has an undecidable group membership problem [Mih]. In fact, we conjecture that the problem whether $\{[1]u^n\}$ is P-recursive is undecidable. We refer to [Hal] for an extensive survey of decidable and undecidable matrix problems.

6.4. In connection with part (3) of Theorem 14, let us mention that groups of intermediate growth do not necessarily have weakly exponential growth. Many constructions going back to Grigorchuk work in 1980s show that $\gamma(n)$ can be subexponential, but as close to exponential as necessary, and in fact have oscillatory behavior (on a $\log_n \log$ scale). We refer to [Bri, BE, KP] for the recent work on the subject, and to [dlH, GriP] for the introduction.

The results of Theorem 14(3) can in fact be extended to all groups with growth

$$\gamma_{G,S}(n) < Be^{n/f(n)}, \quad \text{where } f(n) \rightarrow \infty \text{ as } n \rightarrow \infty.$$

This gives a superpolynomial lower bound for $p_{G,S}(n)$. For the upper bound, one needs to use an explicit superpolynomial lower bound on the growth given in [ST] and apply the tools in [V2] (cf. [Woe, §15.A]). We omit the details.

6.5. The results of Theorem 8 and Theorem 14 suggest that P-recursive for all generating sets is a rigid property which holds for very few classes of group. It would be interesting to see if it holds for all nilpotent groups.

6.6. Lemma 4 can be rephrased to say that the *subword complexity function* $c_{\mathbf{w}}(n) < 2^n$ for some n large enough (see e.g. [AS1, BLRS]). This is likely to be far from optimal. For example, for the Catalan numbers $C_n = \frac{1}{n+1} \binom{2n}{n}$, we have $\mathbf{w} = 101000100000001\dots$. In this case, it is easy to see that the word complexity function $c_{\mathbf{w}}(n) = \Theta(n)$, cf. [DS]. It would be interesting to find sharper upper bounds on the maximal growth of $c_{\mathbf{w}}(n)$, when \mathbf{w} is the infinite parity word of a P-recursive sequence. Note that $c_{\mathbf{w}}(n) = \Theta(n)$ for all automatic sequences [AS1, §10.2], and that the exponentially growing P-recursive sequences modulo almost all primes are automatic provided deep conjectures of Bombieri and Dwork, see [Chr].

6.7. The integrality assumption in Theorem 9 cannot be removed as the following example shows. Denote by a_n the number of *fragmented permutations*, defined as partitions of $\{1, \dots, n\}$ into ordered lists of numbers (see sequence A000262 in [OEIS]). It is P-recursive since

$$a_n = (2n - 1)a_{n-1} - (n - 1)(n - 2)a_{n-2} \quad \text{for all } n > 2.$$

The asymptotics is given in [FS, Prop. VIII.4]:

$$\frac{a_n}{n!} \sim \frac{1}{2\sqrt{e\pi}} e^{2\sqrt{n}} n^{-3/4}.$$

This implies that the theorem is false for the *rational*, at most exponential P-recursive sequence $\{a_n/n!\}$, since in this case we have mildly exponential terms. To understand this, note that $\sum_n a_n t^n/n!$ is not a *G*-function since the *lcm* of denominators of $a_n/n!$ grow superexponentially.

6.8. Proving that a combinatorial sequence is not P-recursive is often difficult even in the most classical cases. We refer to [B+, BRS, BP, FGS, Kla, MR] for various analytic arguments. As far as we know, this is the first proof by a computability argument. In a different direction, we found further applications of Lemma 4 to disprove the long standing Noonan–Zeilberger conjecture in enumerative combinatorics [GP1].

Acknowledgments: We are grateful to Misha Ershov, Martin Kassabov, Maxim Kontsevich, Andrew Marks, Marni Mishna, Robin Pemantle, Bruno Salvy, Andy Soffer, Jed Yang and Doron Zeilberger for interesting discussions. Special thanks to Jean-Paul Allouche, Matthias Aschenbrenner, Cyril Banderier, Alin Bostan, Mireille Bousquet-Mélou, Martin Kassabov, Nick Katz, Christophe Pittet, Laurent Saloff-Coste and Richard Stanley, for many useful remarks on the early draft of the paper, and help with the references. Some additional interesting references in group theory were provided to us by the anonymous referees. The first author was partially supported by the University of California Eugene V. Cota-Robles Fellowship; the second author was partially supported by the NSF.

REFERENCES

[AS1] J.-P. Allouche and J. Shallit, *Automatic sequences*, Cambridge U. Press, Cambridge, UK, 2003.
 [AS2] N. Alon and J. H. Spencer, *The probabilistic method* (third ed.), John Wiley, Hoboken, NJ, 2008.
 [Ale] G. Alexopoulos, A lower estimate for central probabilities on polycyclic groups, *Canad. J. Math.* **44** (1992), 897–910.
 [And] Y. André, Séries Gevrey de type arithmétique. I. Théorèmes de pureté et de dualité (in French), *Ann. of Math.* **151** (2000), 705–740.
 [B+] C. Banderier, M. Bousquet-Mélou, A. Denise, P. Flajolet, D. Gardy and D. Gouyou-Beauchamps, Generating functions for generating trees, *Discrete Math.* **246** (2002), 29–55.
 [BE] L. Bartholdi and A. Erschler, Groups of given intermediate word growth, *Ann. Inst. Fourier (Grenoble)* **64** (2014), 2003–2036.
 [BLRS] J. Berstel, A. Lauve, C. Reutenauer and F. Saliola, *Combinatorics on Words: Christoffel Words and Repetitions in Words*, AMS, Providence, RI, 2009.
 [Beu] F. Beukers, *E-functions and G-functions*, course notes (2008); available from the Southwest Center for Arithmetic Geometry website <http://swc.math.arizona.edu/aws/2008/>
 [BRS] A. Bostan, K. Raschel and B. Salvy, Non-*D*-finite excursions in the quarter plane, *J. Combin. Theory, Ser. A* **121** (2014), 45–63.
 [BP] M. Bousquet-Mélou and M. Petkovšek, Walks confined in a quadrant are not always *D*-finite, *Theoret. Comput. Sci.* **307** (2003), 257–276.
 [Bri] J. Brioussé, Behaviors of entropy on finitely generated groups, *Ann. Probab.* **41** (2013), 4116–4161.
 [Chr] G. Christol, Globally bounded solutions of differential equations, in *Lecture Notes in Math.* **1434**, Springer, Berlin, 1990, 45–64.
 [CR] P. Crépel and A. Raugi, Théorème central limite sur les groupes nilpotents (in French), *Ann. Inst. H. Poincaré Sect. B* **14** (1978), 145–164.
 [ERVW] M. Elder, A. Rehnitz, E. J. Janse van Rensburg and T. Wong, The cogrowth series for $BS(N, N)$ is *D*-finite, *Internat. J. Algebra Comput.* **24** (2014), 171–187.
 [dlH] P. de la Harpe, *Topics in Geometric Group Theory*, University of Chicago Press, Chicago, 2000.
 [DS] E. Deutsch and B. E. Sagan, Congruences for Catalan and Motzkin numbers and related sequences, *J. Number Theory* **117** (2006), 191–215.
 [FGS] P. Flajolet, S. Gerhold and B. Salvy, On the non-holonomic character of logarithms, powers, and the *n*th prime function, *Electron. J. Combin.* **11** (2004/06), A2, 16 pp.
 [FS] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge Univ. Press, Cambridge, 2009.
 [GP1] S. Garrabrant and I. Pak, Pattern avoidance is not P-recursive, [arXiv:1505.06508](https://arxiv.org/abs/1505.06508)
 [GP2] S. Garrabrant and I. Pak, Combinatorial sequences which are not ADE, in preparation.
 [Ges] I. Gessel, Symmetric Functions and P-Recursiveness, *J. Combin. Theory, Ser. A* **53** (1990), 257–285.
 [GriP] R. Grigorchuk and I. Pak, Groups of intermediate growth: an introduction, *Enseign. Math.* **54** (2008), 251–272.

- [Hai] M. Haiman, Noncommutative rational power series and algebraic generating functions, *European J. Combin.* **14** (1993), 335–339.
- [Hal] V. Halava, Decidable and Undecidable Problems in Matrix Theory, *TUCS Tech. Report* **127** (1997), 62 pp.
- [H1] S. P. Humphries, Cogrowth of groups and the Dedekind–Frobenius group determinant, *Math. Proc. Cambridge Philos. Soc.* **121** (1997), 193–217.
- [H2] S. P. Humphries, Cogrowth of groups and a matrix of Redheffer, *Linear Algebra Appl.* **265** (1997), 101–117.
- [Imm] G. K. Immink, Reduction to canonical forms and the Stokes phenomenon in the theory of linear difference equations, *SIAM J. Math. Anal.* **22** (1991), 238–259.
- [KP] M. Kassabov and I. Pak, Groups of oscillating intermediate growth, *Ann. of Math.* **177** (2013), 1113–1145.
- [Kes] H. Kesten, Symmetric random walks on groups, *Trans. AMS* **92** (1959), 336–354.
- [Kla] M. Klazar, Irreducible and connected permutations, *ITI Series Preprint* **122** (2003), 24 pp.; available at <http://kam.mff.cuni.cz/~klazar/irre.pdf>
- [K1] D. Kuksov, On rationality of the cogrowth series, *Proc. AMS* **126** (1998), 2845–2847.
- [K2] D. Kuksov, Cogrowth series of free products of finite and free groups, *Glasg. Math. J.* **41** (1999), 19–31.
- [LMS] A. Lubotzky, A. Mann and D. Segal, Finitely generated groups of polynomial subgroup growth, *Israel J. Math.* **82** (1993), 363–371.
- [Mih] K. A. Mihailova, The occurrence problem for direct products of groups, *Mat. Sb.* **70** (1966), 241–251.
- [MR] M. Mishna and A. Rechnitzer, Two non-holonomic lattice walks in the quarter plane, *Theoret. Comput. Sci.* **410** (2009), 3616–3630.
- [Odl] A. M. Odlyzko, Asymptotic enumeration methods, in *Handbook of Combinatorics*, Vol. 2, Elsevier, Amsterdam, 1995, 1063–1229.
- [OEIS] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, <http://oeis.org>.
- [Pak] I. Pak, Asymptotics of combinatorial sequences, a survey in preparation.
- [Pete] G. Pete, *Probability and Geometry on Groups*, Lecture notes for a graduate course, 2013, 203 pp.; available at <http://www.math.bme.hu/~gabor/PGG.pdf>
- [PS1] C. Pittet and L. Saloff-Coste, Amenable groups, isoperimetric profiles and random walks, in *Geometric group theory down under*, de Gruyter, Berlin, 1999, 293–316.
- [PS2] C. Pittet and L. Saloff-Coste, Random walk and isoperimetry on discrete subgroups of Lie groups, in *Sympos. Math.* **XXXIX**, Cambridge Univ. Press, Cambridge, 1999, 306–319.
- [PS3] C. Pittet and L. Saloff-Coste, On the stability of the behavior of random walks on groups, *J. Geom. Anal.* **10** (2000), 713–737.
- [PS4] C. Pittet and L. Saloff-Coste, A survey on the relationships between volume growth, isoperimetry, and the behavior of simple random walk on Cayley graphs, with examples; preprint (2001), available at <http://www.math.cornell.edu/~lsc/articles.html>
- [PS5] C. Pittet and L. Saloff-Coste, Random walks on finite rank solvable groups, *Jour. EMS* **5** (2003), 313–342.
- [Sap] M. V. Sapir, *Combinatorial algebra: syntax and semantics*, Springer, Cham, 2014.
- [ST] Y. Shalom and T. Tao, A finitary version of Gromov’s polynomial growth theorem, *Geom. Funct. Anal.* **20** (2010), 1502–1547.
- [S1] R. P. Stanley, *Enumerative Combinatorics*, Vol. 1 and 2, Cambridge Univ. Press, Cambridge, UK, 1997 and 1999.
- [S2] R. P. Stanley, D-finiteness of certain series associated with group algebras, in *Oberwolfach Rep.* **11** (2014), 708; available at <http://tinyurl.com/lza6v2e>
- [Sup] D. A. Suprunenko, *Matrix groups*, AMS, Providence, RI, 1976.
- [V1] N. Th. Varopoulos, Théorie du potentiel sur des groupes et des variétés (in French), *C.R. Acad. Sci. Paris Sér. I Math.* **302** (1986), no. 6, 203–205.
- [V2] N. Th. Varopoulos, Groups of superpolynomial growth, in *Harmonic analysis*, Springer, Tokyo, 1991, 194–200.
- [V3] N. Th. Varopoulos, Analysis and geometry on groups, in *Proc. ICM Kyoto*, Math. Soc. Japan, Tokyo, 1991, 951–957.
- [Woe] W. Woess, *Random walks on infinite graphs and groups*, Cambridge U. Press, Cambridge, 2000.