J. Group Theory **24** (2021), 1043–1053
DOI 10.1515/jgth-2020-0066 © de Gruyter 2021

Diameters of random Cayley graphs of finite nilpotent groups

Daniel El-Baz* and Carlo Pagano

Communicated by Christopher W. Parker

Abstract. We prove the existence of a limiting distribution for the appropriately rescaled diameters of random undirected Cayley graphs of finite nilpotent groups of bounded rank and nilpotency class, thus extending a result of Shapira and Zuck which dealt with the case of abelian groups. The limiting distribution is defined on a space of unimodular lattices, as in the case of random Cayley graphs of abelian groups. Our result, when specialised to a certain family of unitriangular groups, establishes a very recent conjecture of Hermon and Thomas. We derive this as a consequence of a general inequality, showing that the diameter of a Cayley graph of a nilpotent group is governed by the diameter of its abelianisation.

1 Introduction

Metric properties of graphs are important in the study of networks. A key example is given by the diameter of a graph, which is defined to be the longest distance among the pairs of vertices of the graph.

A natural family of graphs is provided by Cayley graphs of groups. For certain finite simple groups and generating sets, upper bounds on the diameter show logarithmic growth. That is sharp since one always has a logarithmic lower bound, which essentially comes from the fact that finitely generated groups always have at most exponential growth. The motivation for proving such upper bounds is Babai's conjecture [2, Conjecture 1.7], which postulates the existence of a constant $a > 0$ such that, for every finite simple group G and every generating set S, one has $\operatorname{diam}(\Gamma(G, S)) \leq (\log |G|)^a$.

In contrast, Amir and Gurel-Gurevich [1] started investigating the diameter of cyclic groups $\mathbb{Z}/q\mathbb{Z}$ with respect to a random set S of generators of fixed size, say $k \geq 2$. The fact that finitely generated abelian groups of rank k have growth of

The authors wish to thank the Max Planck Institute for Mathematics in Bonn for its financial support, great working conditions and an inspiring atmosphere. Daniel El-Baz is supported by the Austrian Science Fund (FWF), projects Y-901 and F-5512. Carlo Pagano is grateful to the Glasgow mathematics department for financial support.

order a polynomial of degree k in the radius is reflected in a simple lower bound of the order of $q^{1/k}$; furthermore, they obtain that, for any function f going to infinity with q, the probability that the diameter of the random Cayley graph is bigger than $f(q)q^{1/k}$ goes to 0 as $q \to \infty$. That led them to conjecture that, as $q \to \infty$, the random variables given by the diameter of the corresponding random Cayley graph, when rescaled by $q^{1/k}$, converge in distribution.

Marklof and Strömbergsson [6] introduced a strategy relating that problem to an equidistribution theorem in homogeneous dynamics and were able to prove a version of that conjecture in which the cyclic group itself was also taken at random (with $q \in \mathbb{Z} \cap [1, Q]$). Inspired by that approach, Shapira and Zuck [7] settled that conjecture and further extended it from finite cyclic groups to arbitrary finite abelian groups of bounded rank. In the present article, we obtain the analogous result for finite nilpotent groups with bounded rank and nilpotency class.

Recall that, for a group G, one can inductively define the filtration of subgroups $\mathbb{Z}_{\geq 1} \ni i \mapsto G^{(i)}$ – called the lower central series – given by $G^{(1)} = G$ and for $i \geq 1$, $G^{(i+1)} = [G, G^{(i)}]$. A group is said to be nilpotent if there exists $i \geq 1$ such that $G^{(i)} = \{\mathrm{id}\}$. In that case, the nilpotency class of G is defined to be the smallest positive integer c such that $G^{(c+1)} = \{\mathrm{id}\}$. For a group G and a symmetric generating set $S \subset G$, we denote by $\Gamma(G, S)$ the Cayley graph of G with respect to S.

Theorem 1.1. *Let $k > r \geq 1$ and $c \geq 1$ be integers. Let $\{G_n\}_{n \in \mathbb{Z}_{\geq 1}}$ be a sequence of finite nilpotent groups of rank at most r, nilpotency class at most c and with $\lim_{n \to \infty} |G_n| = \infty$. Choosing a subset S uniformly at random among all symmetric generating subsets of G_n of size k, then as $n \to \infty$, the random variables*

$$\frac{\mathrm{diam}(\Gamma(G_n, S))}{|G_n^{\mathrm{ab}}|^{\frac{1}{k}}}$$

converge in distribution.

A version of this theorem which also contains a fairly explicit description of the limiting distribution is given as Theorem 3.1.

In recent work, Hermon and Thomas [5] investigated random walks on certain finite unitriangular groups, defined for $q, d \in \mathbb{Z}_{\geq 2}$, to be the group of $d \times d$ matrices over $\mathbb{Z}/q\mathbb{Z}$ which are upper triangular and whose diagonal entries are all 1; that group is denoted by $H_{q,d}$. Those are special examples of finite nilpotent groups.

Hermon and Thomas establish a concentration result for the *typical distance* – a function of a parameter $\beta \in (0, 1)$ defined as the smallest radius of a ball centred at the identity which is enough to cover a proportion β of the group – of the random

Cayley graphs of those unitriangular groups, which they show concentrates around the value it takes for the abelianisation of $H_{q,d}$ when the number of generators diverges (or is at least large enough as a function of d); combined with the simple lower bound on the diameter coming from the growth of the group, which is of the same order, that led them to conjecture the existence of a limiting distribution for the diameters of those graphs with that particular rescaling.

As a consequence of Theorem 1.1, we establish their conjecture.[1]

Theorem 1.2. *Let $q \geq 2, d \geq 2$ and $k \geq d$. Let $\{Z_1(q), \dots, Z_k(q)\}$ be chosen uniformly and independently among all symmetric generating k-subsets of $H_{q,d}$, and write $\Delta_{Z(q)}(k)$ for the diameter of the random Cayley graph with those generators. As $q \to \infty$, the random variables*

$$\frac{\Delta_{Z(q)}(k)}{q^{\frac{d-1}{k}}}$$

converge in distribution.

We state a more precise version of the above as Theorem 3.2 which also includes an explicit description of the limiting distribution in terms of the space of k-dimensional unimodular lattices. The latter is the same as the limiting distribution for the random undirected Cayley graph of the finite abelian group $(\mathbb{Z}/q\mathbb{Z})^{d-1}$ with k generators chosen uniformly at random, which was obtained by Shapira and Zuck. Note that the distribution is also the same as that from the paper by Marklof and Strömbergsson (for random undirected circulant graphs with respect to k generators), in which they make use of the description in terms of random unimodular lattices in $\mathbb{R}^k$ to derive quantitative properties of the limiting distribution such as tail estimates.

Indeed, our strategy for proving those theorems consists in establishing a general inequality for the diameter of a Cayley graph on a finite nilpotent group, which essentially shows that this diameter is governed by the diameter of the abelianisation. This is done in Section 2. The crucial step is Proposition 2.1. In that proposition, we take advantage of the well-known phenomenon of *distortion* in nilpotent groups, that is the possibility of rewriting N times a nested commutator of length i in time $O(N^{\frac{1}{i}})$ modulo nested commutators of length at least $i+1$, for a positive integer N. The upper bound in Proposition 2.1 is reminiscent of the formula of Bass and Guivarc'h for the growth in finitely generated nilpotent group [4, Appendix], which indeed relies on the same phenomenon of distortion. We remark

[1] Their paper only deals with q prime and directed graphs; ours treats arbitrary $q \geq 2$ but undirected graphs.

that a very similar argument can be found in the proof of [3, Lemma 4.11].[2] This upper bound leads us to wonder whether $q^{\frac{d-1}{ik}}$ is the correct scale for the diameters (with respect to the ambient metric on the group) of the i-th term of the lower central series of undirected Cayley graphs of $H_{q,d}$ with respect to a random generating set. In the concluding section, we ask this and a few related questions.

2 Diameters of finite nilpotent groups

2.1 Diameters of a group and its quotients

For a finite group G with symmetric generating set S, a normal subgroup H of G and a normal subgroup N of H, we view H and N as metric subspaces of the Cayley graphs $\Gamma(G, S)$, which allows us to define the diameters of N and H with respect to S, which we denote respectively by $\operatorname{diam}(H, S)$ and $\operatorname{diam}(N, S)$.

This metric also induces one on the quotient $\frac{H}{N}$ and allows us to define the diameter of that group with respect to the projections of the elements of S onto $\frac{H}{N}$, which we denote by $\operatorname{diam}\big(\frac{H}{N}, S\big)$.

When $H = G$, that last quotient coincides as a metric space with the Cayley graph of $\frac{G}{N}$ with respect to the projections of the elements of S in $\frac{G}{N}$.

The following lemma relates those three quantities.

Lemma 2.1. *For every finite group G with symmetric generating set S, every normal subgroup H of G and every normal subgroup N of H, we have*

$$\operatorname{diam}\Big(\frac{H}{N}, S\Big) \leq \operatorname{diam}(H, S) \leq \operatorname{diam}\Big(\frac{H}{N}, S\Big) + \operatorname{diam}(N, S).$$

Proof. The lower bound on $\operatorname{diam}(H, S)$ follows from the definition.

We now prove the upper bound. Fix two elements h_1 and h_2 in H. Define

$$d_1 = \operatorname{diam}\Big(\frac{H}{N}, S\Big) \quad \text{and} \quad d_2 = \operatorname{diam}(N, S).$$

By definition of d_1, we find $x_1, \dots, x_{s_1} \in S$ with $s_1 \leq d_1$ such that there exists $n \in N$ such that

$$x_1 \cdots x_{s_1} h_1 = n h_2. \tag{2.1}$$

For that $n \in N$ and by definition of d_2, we find $y_1, \dots, y_{s_2} \in S$ with $s_2 \leq d_2$ connecting id to n, that is

$$y_1 \cdots y_{s_2} = n. \tag{2.2}$$

[2] We thank Matthew Tointon for pointing out this reference to us after receiving a first draft of this paper.

Combining (2.1) and (2.2), we get

$$y_{s_2}^{-1} \cdots y_1^{-1} x_1 \cdots x_{s_1} h_1 = h_2,$$

which means that the distance between h_1 and h_2 via elements of S is at most $s_1 + s_2$ which is itself at most $d_1 + d_2$, hence the claim. □

2.2 Multilinear maps attached to groups

In this section, we briefly recall (part of) the multilinear structure present on a group G.

For x, y in G, we denote $[x, y] = xyx^{-1}y^{-1}$. Observe that $[x, y]^{-1} = [y, x]$. Furthermore, if z is also in G, then we have $[x, zy] = [x, z][x, y][z, [y, x]]^{-1}$. Observe that if z, y are taken to be in $G^{(i)}$ for some $i \in \mathbb{Z}_{\geq 1}$, this last identity tells us that the commutator pairing

$$G \times \frac{G^{(i)}}{G^{(i+1)}} \to \frac{G^{(i+1)}}{G^{(i+2)}}$$

is bilinear in the second entry (observe that, by definition, $\frac{G^{(j)}}{G^{(j+1)}}$ is an abelian group for any positive integer j). A similar computation shows that this pairing factors through $G^{(2)}$ in the first coordinate and is bilinear in both entries for the map

$$\frac{G^{(1)}}{G^{(2)}} \times \frac{G^{(i)}}{G^{(i+1)}} \to \frac{G^{(i+1)}}{G^{(i+2)}}.$$

Hence, in total, we get a homomorphism $(G^{\mathrm{ab}})^{\otimes i} \twoheadrightarrow \frac{G^{(i)}}{G^{(i+1)}}$, defined by the multilinear map from $(G^{\mathrm{ab}})^i \to \frac{G^{(i)}}{G^{(i+1)}}$ sending the vector $(g_1, \ldots, g_i)$ to the class of $[g_1, [g_2, \ldots, [g_{i-1}, g_i], \ldots]$ modulo $G^{(i+1)}$. In particular, notice that if S generates G, then nested commutators among elements of S of length i generate $\frac{G^{(i)}}{G^{(i+1)}}$.

2.3 Comparing diameters

We shall need the following elementary lemma.

Lemma 2.2. *Let i be a positive integer. Then there exist positive integers C_i, n_i such that, for any $\lambda \in \mathbb{Z}_{\geq 1}$, one can find $a_1, \ldots, a_{n_i}, r$ in $\mathbb{Z}_{\geq 0}$ such that*

$$\lambda = a_1^i + \cdots + a_{n_i}^i + r,$$

with $r \leq C_i \lambda^{1/i}$.

Proof. Observe that one can find a constant D_i such that, for each positive integer λ, one has a representation $\lambda = a_1^i + r_1$, with $r_1 \leq D_i \lambda^{\frac{i-1}{i}}$: to this end, take $a_1 := \lfloor \lambda^{1/i} \rfloor$, and apply the binomial expansion to the worst-case scenario $\lambda = (\lfloor \lambda^{1/i} \rfloor + 1)^i - 1$. Hence, iterating this, we obtain that, for each j in $\mathbb{Z}_{\geq 1}$, there are non-negative integers $a_1, \ldots, a_j, r_j$ such that $\lambda = a_1^i + \cdots + a_j^i + r_j$, with

$$r_j \leq D_i^{\sum_{h=0}^{j-1} (\frac{i-1}{i})^h} \lambda^{(\frac{i-1}{i})^j}.$$

Choosing j such that $\left(\frac{i-1}{i}\right)^j < \frac{1}{i}$ yields the desired conclusion. □

Proposition 2.1. *For every finite group G, every symmetric generating set $S \subset G$ of size $s \in \mathbb{Z}_{\geq 2}$ and every $i \geq 1$, we have*

$$\operatorname{diam}\left(\frac{G^{(i)}}{G^{(i+1)}}, S\right) = O_{i,s}\left(\operatorname{diam}(\Gamma(G^{\mathrm{ab}}, S))^{1/i}\right).$$

Proof. We show that, for each $h \in \frac{G^{(i)}}{G^{(i+1)}}$, there exist $y_1, \ldots, y_d$ in S such that $h \equiv y_1 \cdots y_d \bmod \mathrm{G}^{(\mathrm{i}+1)}$, with $d = O_{i,s}(\operatorname{diam}(\Gamma^{\mathrm{ab}}, S)^{1/i})$. By Section 2.2, we can find $(\lambda_f)_{f:[i]\to S} \in \mathbb{Z}^{[i]\to S}$ such that

$$h = \sum_{f:[i]\to S} \lambda_f [f(1), [\ldots, [\ldots, f(i)]]].$$

By multilinearity, we can collect the last entries of the nested commutators for each choice of the first $i-1$ entries and obtain for each $g\colon [i-1] \to S$ an element y_g in G^{ab} such that

$$h = \sum_{g:[i-1]\to S} [g(1), [\ldots, [g(i-1), y_g]]]. \tag{2.3}$$

Now, for each $g\colon [i-1] \to S$, rewrite

$$y_g = \sum_{x \in S} \lambda(x, g)[x]_{G^{\mathrm{ab}}}$$

with

$$\sum_{x \in S} |\lambda(x, g)| \leq \operatorname{diam}(\Gamma(G^{\mathrm{ab}}, S)). \tag{2.4}$$

Using multilinearity once again, we have

$$[g(1), [\ldots, [g(i-1), y_g]]] = \sum_{x \in S} [g(1), [\ldots, [g(i-1), \lambda(x, g)[x]_{G^{\mathrm{ab}}}]]].$$

Rewrite, for each $x \in S$, using Lemma 2.2,

$$\begin{aligned}
&\operatorname{sgn}(\lambda(x,g))|\lambda(x,g)|[g(1),[\ldots,[g(i-1),[x]_{G^{\mathrm{ab}}}]]]\\
&\quad= \operatorname{sgn}(\lambda(x,g))\Bigl(\sum_{h=1}^{n_i} a_h^i + r\Bigr)\cdot[g(1),[\ldots,[g(i-1),[x]_{G^{\mathrm{ab}}}]]]\\
&\quad= \operatorname{sgn}(\lambda(x,g))\Bigl(\Bigl(\sum_{h=1}^{n_i}[a_h g(1),[\ldots,[a_h g(i-1),a_h[x]_{G^{\mathrm{ab}}}]]]\Bigr)\\
&\qquad\qquad + r\cdot[g(1),[\ldots,[g(i-1),[x]_{G^{\mathrm{ab}}}]]]\Bigr).
\end{aligned}$$

In the last equality, each of the $n_i + 1$ summands are $O_i(|\lambda(x,g)|^{1/i})$; hence the g-th term of the sum (2.3) has length at most $O_i(\sum_{x\in S}|\lambda(x,g)|^{1/i})$, which is $O_i(\operatorname{diam}(\Gamma(G^{\mathrm{ab}},S))^{1/i})$ by Jensen's inequality and recalling (2.4). Summing over all g, we thus get an upper bound of $s^{i-1}O_i(\operatorname{diam}(\Gamma(G^{\mathrm{ab}},S))^{1/i})$, which is $O_{s,i}(\operatorname{diam}(\Gamma(G^{\mathrm{ab}},S)^{1/i})$ as claimed. □

Corollary 2.1. *Let G be a finite nilpotent group of class $c \in \mathbb{Z}_{\geq 1}$. Let $S \subset G$ be a symmetric generating set of size $s \in \mathbb{Z}_{\geq 2}$. We have*

$$\begin{aligned}
\operatorname{diam}(\Gamma(G^{\mathrm{ab}},S)) &\leq \operatorname{diam}(\Gamma(G,S))\\
&\leq \operatorname{diam}(\Gamma(G^{\mathrm{ab}},S)) + O_{c,s}\Bigl(\sqrt{\operatorname{diam}(\Gamma(G^{\mathrm{ab}},S))}\Bigr).
\end{aligned}$$

Proof. By the left-hand side of the inequality in Lemma 2.1, the left-hand side follows immediately.

Using the right-hand side of the inequality in Lemma 2.1 inductively for the terms of the lower central series, we obtain

$$\operatorname{diam}(\Gamma(G,S)) \leq \sum_{i\geq 1}\operatorname{diam}\Bigl(\frac{G^{(i)}}{G^{(i+1)}},S\Bigr).$$

Appealing to Proposition 2.1 now yields the desired conclusion. □

3 The case of unitriangular groups and more general sequences of nilpotent groups

In this section, we apply Corollary 2.1 to determine the limiting distribution of the appropriately rescaled diameters of random Cayley graphs of finite nilpotent groups of bounded rank and class.

The resulting theorem below is a generalisation of [7, Theorem 1.2], which corresponds to the case $c = 1$ of our result. As the reader shall soon see, however, our proof consists of a reduction to that case by means of Corollary 2.1.

Theorem 3.1. *Let $k > r \geq 1$ and $c \geq 1$ be integers. Let $\{G_n\}_{n \in \mathbb{Z}_{\geq 1}}$ be a sequence of finite nilpotent groups of rank at most r, nilpotency class at most c and with $|G_n|$ approaching infinity as n goes to infinity.*

Choosing a subset S uniformly at random among all symmetric generating subsets S of G_n of size k, then as $n \to \infty$, we have that the random variables

$$\frac{\operatorname{diam}(\Gamma(G_n, S))}{|G_n^{\mathrm{ab}}|^{\frac{1}{k}}}$$

converge in distribution. Moreover,

$$\frac{\operatorname{diam}(\Gamma(G_n, S))}{|G_n^{\mathrm{ab}}|^{\frac{1}{k}}} \xrightarrow[n\to\infty]{\mathrm{d}} \operatorname{diam}(\mathbb{R}^k/L),$$

where the random variable on the right-hand side is defined by choosing L at random in the space $\mathrm{SL}_k(\mathbb{R})/\mathrm{SL}_k(\mathbb{Z})$ of unimodular lattices in $\mathbb{R}^k$ with respect to the Haar probability measure and the diameter on the right-hand side is with respect to the ℓ^1 metric.

Proof. For $n \geq 1$, $r \geq 1$ and $k > r$, denote the random variable

$$\frac{\operatorname{diam}(\Gamma(G_n, S))}{|G_n^{\mathrm{ab}}|^{\frac{1}{k}}}$$

by X_n and the random variable

$$\frac{\operatorname{diam}(\Gamma(G_n^{\mathrm{ab}}, S))}{|G_n^{\mathrm{ab}}|^{\frac{1}{k}}}$$

by X_n^{ab}.

Applying Corollary 2.1 to the finite nilpotent group G_n (of class at most c) thus yields the inequalities

$$X_n^{\mathrm{ab}} \leq X_n \leq X_n^{\mathrm{ab}} + O_{k,c}\left(\frac{\sqrt{X_n^{\mathrm{ab}}}}{|G_n^{\mathrm{ab}}|^{\frac{1}{2k}}}\right). \tag{3.1}$$

We next remark that we must have that $|G_n^{\mathrm{ab}}|$ approaches infinity as n goes to infinity. Indeed, from Section 2.2, it follows immediately that there are finitely many nilpotent groups of bounded nilpotency class and bounded size of the abelianisation, and this would contradict the fact that $|G_n|$ tends to infinity as n goes to infinity. This is also explained in [3, Lemma 4.13]. Moreover, observe that the groups G_n^{ab} trivially have rank bounded by r. We are therefore in a position to use

[7, Theorem 1.2] to deduce that X_n^{ab} converges in distribution to the random variable defined on the space of k-dimensional unimodular lattices as in the statement of our theorem, say X.

Note also that

$$\left(\frac{\sqrt{X_n^{\mathrm{ab}}}}{|G_n^{\mathrm{ab}}|^{\frac{1}{2k}}}\right)_n$$

converges in probability to 0.

The right-hand side of (3.1) is therefore of the form $X_n^{\mathrm{ab}} + \varepsilon_n$ with $X_n^{\mathrm{ab}} \xrightarrow{\mathrm{d}} X$ and $\varepsilon_n \xrightarrow{\mathrm{P}} 0$. It follows from Slutsky's lemma that $X_n^{\mathrm{ab}} + \varepsilon_n \xrightarrow{\mathrm{d}} X$.

This finishes the proof. □

We now use Theorem 3.1 with the sequence of finite nilpotent groups $H_{q,d}$ of upper triangular $d \times d$ matrices over $\mathbb{Z}/q\mathbb{Z}$ with 1 on the diagonal: they are of nilpotency class $d-1$ and $H_{q,d}^{\mathrm{ab}} \simeq (\mathbb{Z}/q\mathbb{Z})^{d-1}$. We thus obtain the following theorem and, in doing so, a proof of [5, Conjecture 7] along with an explicit description of the limiting distribution.

Theorem 3.2. *Let $q \geq 2, d \geq 2$ and $k \geq d$. Choosing a subset S uniformly at random among all symmetric generating subsets S of $H_{q,d}$ of size k, then as $q \to \infty$, we have that the random variables*

$$\frac{\operatorname{diam}(\Gamma(H_{q,d}, S))}{q^{(d-1)/k}}$$

converge in distribution. Moreover,

$$\frac{\operatorname{diam}(\Gamma(H_{q,d}, S))}{q^{(d-1)/k}} \xrightarrow[q\to\infty]{\mathrm{d}} \operatorname{diam}(\mathbb{R}^k/L),$$

where the random variable on the right-hand side is defined by choosing L at random in the space $\mathrm{SL}_k(\mathbb{R})/\mathrm{SL}_k(\mathbb{Z})$ of unimodular lattices in $\mathbb{R}^k$ with respect to the Haar probability measure and the diameter on the right-hand side is with respect to the ℓ^1 metric.

4 Concluding remarks

Let i be in $\mathbb{Z}_{\geq 2}$. One can then ask the following related questions.

Questions. What is the correct order of magnitude of $\operatorname{diam}(H_{q,d}^{(i)}, S)$? Is the power $q^{\frac{d-1}{ik}}$ suggested by the upper bound of Proposition 2.1 sharp (to hold in probability)?

We only remark that, using the same type of argument based on growth that one uses to show the logarithmic behaviour as a general lower bound, one can establish as a pointwise lower bound a much smaller power of q, depending on i. Such a trivial estimate can be slightly improved using the equidistribution theorem in [7] and basic facts about the shortest vector statistics on spaces of unimodular lattices. However, the resulting gain on the power of q is still not enough to reach $q^{\frac{d-1}{ik}-\varepsilon}$ as a pointwise lower bound.

One can also ask about the difference $\operatorname{diam}(\Gamma(H_{q,d}, S)) - \operatorname{diam}(\Gamma(H_{q,d}^{\mathrm{ab}}, S))$. Corollary 2.1 gives an upper bound for this quantity. We ask the following.

Question. Can one give a sharp lower bound for the quantity

$$\operatorname{diam}(\Gamma(H_{q,d}, S)) - \operatorname{diam}(\Gamma(H_{q,d}^{\mathrm{ab}}, S))$$

(to hold in probability)?

Finally, what about those questions for more general sequences $\{G_n\}_{n\in\mathbb{Z}_{\geq 1}}$ of finite nilpotent groups as in Theorem 3.1?

Acknowledgments. We thank Jonathan Hermon for a helpful email on his work with Sam Olesker-Taylor (formerly Thomas) [5]. We are also grateful to him for pointing out that, in a previous version of this paper, there was an inaccuracy in the rounding off with i-th powers at the end of the proof of Proposition 2.1. We further thank both Jonathan Hermon and Sam Olesker-Taylor for their careful reading of a previous version our manuscript and suggesting a few corrections. We also thank Matthew Tointon for encouraging us to state our main result in the generality of Theorem 3.1, for providing us with references to his work and for helpful feedback. We are grateful to Uri Shapira, Mima Stanojkovski and Andreas Strömbergsson for feedback on a previous version of this work that led to an improvement of the presentation.

Bibliography

[1] G. Amir and O. Gurel-Gurevich, The diameter of a random Cayley graph of $\mathbb{Z}_q$, *Groups Complex. Cryptol.* **2** (2010), no. 1, 59–65.

[2] L. Babai and A. Seress, On the diameter of permutation groups, *European J. Combin.* **13** (1992), no. 4, 231–243.

[3] E. Breuillard and M. C. H. Tointon, Nilprogressions and groups with moderate growth, *Adv. Math.* **289** (2016), 1008–1055.

[4] M. Gromov, Groups of polynomial growth and expanding maps, *Publ. Math. Inst. Hautes Études Sci* (1981), no. 53, 53–73.

[5] J. Hermon and S. Thomas, Random Cayley graphs I: Cutoff and geometry for Heisenberg groups, preprint (2019), https://arxiv.org/abs/1911.02974.

[6] J. Marklof and A. Strömbergsson, Diameters of random circulant graphs, *Combinatorica* **33** (2013), no. 4, 429–466.

[7] U. Shapira and R. Zuck, Asymptotic metric behavior of random Cayley graphs of finite abelian groups, *Combinatorica* **39** (2019), no. 5, 1133–1148.

Received May 3, 2020; revised January 10, 2021.

Author information

Corresponding author:
Daniel El-Baz, Institute of Analysis and Number Theory, TU Graz,
Steyrergasse 30, 8010 Graz, Austria.
E-mail: danielelbaz88@gmail.com

Carlo Pagano, Max Planck Institute for Mathematics,
Vivatsgasse 7, 53111 Bonn, Germany;
and School of Mathematics and Statistics, University of Glasgow,
G12 8QQ, United Kingdom.
E-mail: carlein90@gmail.co