© Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **32** (2021). Number 2, pp. 226–235
DOI:10.12958/adm1506

Maximal subgroup growth of a few polycyclic groups*

A. Kelley and E. Wolfe

Communicated by R. A. Grigorchuk

Abstract. We give here the exact maximal subgroup growth of two classes of polycyclic groups. Let $G_k = \langle x_1, x_2, \ldots, x_k \mid x_i x_j x_i^{-1} x_j \text{ for all } i < j \rangle$, so $G_k = \mathbb{Z} \rtimes (\mathbb{Z} \rtimes (\mathbb{Z} \rtimes \cdots \rtimes \mathbb{Z}))$. Then for all integers $k \geqslant 2$, we calculate $m_n(G_k)$, the number of maximal subgroups of G_k of index n, exactly. Also, for infinitely many groups H_k of the form $\mathbb{Z}^2 \rtimes G_2$, we calculate $m_n(H_k)$ exactly.

Introduction

Let G be a finitely generated group. We denote by $a_n(G)$ the number of subgroups of G of index n (which is necessarily finite), and we denote by $m_n(G)$ the number of maximal subgroups of G of index n. Subgroup growth is the study of the growth of different subgroup counting functions in groups, such as $a_n(G)$, $m_n(G)$, and $s_n(G) := \sum_{k=1}^{n} a_k(G)$.

People have made great progress in understanding subgroup growth. One highlight is the classification of all finitely generated groups for which $a_n(G)$ is bounded above by a polynomial in n (see chapter 5 in [7]). Also, Jaikin-Zapirain and Pyber made a significant advance in [3], where they give a "semi-structural characterization" of groups G for which $m_n(G)$ is bounded above by a polynomial in n.

*This paper was done with the support of the Student Collaborative Research grant at Colorado College.

2020 MSC: 20E07.

Key words and phrases: maximal subgroup growth, polycyclic groups, semidirect products.

For calculating the *word* growth in a group with polynomial growth, the degree is given by a nice, simple formula. However, for subgroup growth, it is often very challenging, given a group G of polynomial subgroup growth, to calculate its degree of polynomial growth *deg(G)*:

$$\deg(G) = \inf\{\alpha \mid a_n(G) \leqslant n^\alpha \text{ for all large } n\} = \limsup \frac{\log a_n(G)}{\log n}.$$

Similarly, for groups G with polynomial maximal subgroup growth, it is often difficult to determine $\mathrm{mdeg}(G)$, where

$$\mathrm{mdeg}(G) = \inf\{\alpha \mid m_n(G) \leqslant n^\alpha \text{ for all large } n\} = \limsup \frac{\log m_n(G)}{\log n}.$$

Progress has been made in both areas. In [9], Shalev calculated $\deg(G)$ exactly for certain metabelian groups and for all virtually abelian groups. In [6], the first author calculated $\mathrm{mdeg}(G)$ for some metabelian groups, and in [4] he does so for all virtually abelian groups.

The groups G for which $\mathrm{mdeg}(G)$ is known are rare, and rarer still are groups for which an exact formula for $m_n(G)$ is known. In [2], Gelman gives a beautiful, exact formula for $a_n(\mathrm{BS}(a,b))$, assuming $\gcd(a,b)=1$, where $\mathrm{BS}(a,b)$ is the Baumslag-Solitar group having presentation $\langle x, y \mid y^{-1}x^a y = x^b\rangle$. Gelman's argument can be easily modified to give an exact formula for $m_n(BS(a,b))$, where again $\gcd(a,b)=1$. (Alternatively, a different argument, that explains why $\gcd(a,b)=1$ is such a nice assumption, is given by the first author in [5].)

Since there are so few groups G for which $m_n(G)$ has been calculated, this paper gives exact formulas for two infinite classes of polycyclic groups.

For $k \geqslant 2$, consider the group G_k with presentation

$$\langle x_1, x_2, \ldots, x_k | x_i x_j x_i^{-1} x_j \text{ for all } i < j\rangle.$$

Then G_k has the form $\mathbb{Z} \rtimes (\mathbb{Z} \rtimes (\mathbb{Z} \rtimes \cdots \rtimes \mathbb{Z}))$, where the ith $\mathbb{Z}$, reading from right to left, is generated by x_i. Note that the Hirsch length of G_k is k, and so if $i \neq j$, then $G_i \ncong G_j$. In Theorem 3, we calculate $m_n(G_k)$ exactly for $k \geqslant 2$.

Let G_2 be as above. Note that G_2 is the Baumslag-Solitar group $\mathrm{BS}(1,-1)$, also known as the fundamental group of the Klein bottle. We will write $G_2 = \mathbb{Z} \rtimes \mathbb{Z}$ as $\langle b\rangle \rtimes \langle a\rangle$ instead of $\langle x_2\rangle \rtimes \langle x_1\rangle$. For $k \in \mathbb{Z}$, we will define the group H_k, which is of the form $\mathbb{Z}^2 \rtimes G_2$. The generator a acts (by conjugation) on $\mathbb{Z}^2$ by multiplication by the matrix $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and the generator b acts (by conjugation) on $\mathbb{Z}^2$ by multiplication by the matrix $B_k = \left(\begin{smallmatrix} 0 & 1 \\ -1 & k \end{smallmatrix}\right)$. Then in Theorem 9, we calculate $m_n(H_k)$ exactly for all $k \in \mathbb{Z}$. A consequence of this theorem is that among the groups H_k, there are infinitely many that are pairwise non-isomorphic. Also, it is interesting that $\operatorname{mdeg}(H_2) = 2$, but $\operatorname{mdeg}(H_k) = 1$ for all $k \neq 2$.

One reason for studying the two families $\{G_k\}_{k\geqslant 2}$ and $\{H_k\}_{k\in\mathbb{Z}}$ is that the first author thinks that it might be possible to extend the methods of [6] to apply to the class of polycyclic groups. In particular, it might be feasible to give an exact formula for $\operatorname{mdeg}(G)$ when G is a group of the form $A_k \rtimes (A_{k-1} \rtimes (A_{k-2} \rtimes \ldots \rtimes A_1))$, where each A_i is a finitely generated abelian group. Another reason why we chose the particular infinite families we did is that (besides G_2) they appeared to be the easiest such groups to work with that aren't of the form $A_2 \rtimes A_1$.

1. Groups of the form $\mathbb{Z} \rtimes (\mathbb{Z} \rtimes (\mathbb{Z} \rtimes \cdots \rtimes \mathbb{Z}))$

For a group $G = N \rtimes H$ with N abelian, to calculate $m_n(G)$, it is useful to consider the H-module structure given by G on N. See Lemma 5 from [6].

Let G_k be as in the introduction, and let $G_1 = \mathbb{Z}$. For a group G and N a G-module, recall that a function $\delta : G \to N$ is called a derivation (or a 1-cocycle) if $\delta(gh) = \delta(g) + g \cdot \delta(h)$ for all $g, h \in G$. The set of derivations from G to N is denoted $\operatorname{Der}(G, N)$. In the following lemma, we will use the fact that if $\delta \in \operatorname{Der}(G, N)$, then for $g \in G$, we have $\delta(g^{-1}) = -g^{-1}\delta(g)$ which follows from the fact that $\delta(g^{-1}g) = \delta(1) = 0$.

Lemma 1. *Let S be a G_k-module. There is a one-to-one correspondence between the set $\operatorname{Der}(G_k, S)$ and the set Δ of all functions $\delta : \{x_1, x_2, \ldots x_k\} \to S$ satisfying*

$$(1 - x_j^{-1})\delta(x_i) = (-x_i - x_j^{-1})\delta(x_j) \quad \textit{for all } i,\ j \textit{ with } i < j. \qquad (*)$$

Proof. If $\delta \in \Delta$, then exercise 3(a) in [1] (pg. 90) (or Lemma 2.20 from [4]), gives us a unique derivation $\delta : F_k \to S$, where F_k is the free group on k generators and the action of F_k on S is the induced action. So by slight abuse of notation, by taking δ in Δ, we mean the derivation of the free group F_k that corresponds to the map $\delta \in \Delta$.

Let δ be an element either of $\operatorname{Der}(G_k, S)$ or of Δ. We will show that $\delta(x_i x_j x_i^{-1} x_j) = 0$ for all $i < j$ if and only if $(*)$ holds. Fix i and j with

$i < j$. Then

$$\begin{aligned}\delta(x_i x_j x_i^{-1} x_j) &= \delta(x_i) + x_i\delta(x_j) + x_i x_j \delta(x_i^{-1}) + x_i x_j x_i^{-1}\delta(x_j)\\ &= \delta(x_i) + x_i\delta(x_j) - x_i x_j x_i^{-1}\delta(x_i) + x_j^{-1}\delta(x_j)\\ &= \delta(x_i) + x_i\delta(x_j) - x_j^{-1}\delta(x_i) + x_j^{-1}\delta(x_j)\\ &= (\delta(x_i) - x_j^{-1}\delta(x_i)) - (-x_i\delta(x_j) - x_j^{-1}\delta(x_j))\\ &= (1 - x_j^{-1})\delta(x_i) - (-x_i - x_j^{-1})\delta(x_j)\end{aligned}$$

If $\delta \in \mathrm{Der}(G_k, S)$, then $\delta(x_i x_j x_i^{-1} x_j) = 0$ because $\delta(1) = 0$, and so $(*)$ holds. Conversely, if $\delta \in \Delta$, then that $(*)$ holds implies $\delta(x_i x_j x_i^{-1} x_j) = 0$ for all $i < j$, in which case Lemma 2.19 from [4], which is basically exercise 4(a) in [1] (pg. 90), gives a derivation δ from G_k to S.

□

Lemma 2. *Consider $\mathbb{Z}/p\mathbb{Z}$, a simple G_k-module, where each generator x_i of G_k acts on $\mathbb{Z}/p\mathbb{Z}$ by multiplication by -1. Then*

$$|\mathrm{Der}(G_k, \mathbb{Z}/p\mathbb{Z})| = \begin{cases} 2^k & \textit{if } p = 2 \\ p & \textit{if } p \neq 2. \end{cases}$$

Proof. If $p = 2$, then the action of G_k on $\mathbb{Z}/2\mathbb{Z}$ is trivial, and so $|\mathrm{Der}(G_k, \mathbb{Z}/2\mathbb{Z})| = |\mathrm{Hom}(G_k, \mathbb{Z}/2\mathbb{Z})|$, which is 2^k.

Next, suppose $p \neq 2$. The action of $(1 - x_i^{-1})$ and $(-x_i - x_j^{-1})$ on $\mathbb{Z}/p\mathbb{Z}$ is multiplication by 2, which is invertible since $p \neq 2$. So $(*)$ from Lemma 1 becomes $2\delta(x_i) = 2\delta(x_j)$ for all $i < j$, which simplifies to $\delta(x_i) = \delta(x_j)$ for all $i < j$.

So by Lemma 1, we may choose a derivation by picking $\delta(x_k)$ to be any element of $\mathbb{Z}/p\mathbb{Z}$, and then letting $\delta(x_i) = \delta(x_k)$ for all $i < k$. Thus $|\mathrm{Der}(G_k, \mathbb{Z}/p\mathbb{Z})| = |\mathbb{Z}/p\mathbb{Z}| = p$. □

Theorem 3. *Let G_k be as above. Then*

$$m_n(G_k) = \begin{cases} 1 + (k-1)n & \textit{if } n \textit{ is a prime with } n > 2 \\ 2^k - 1 & \textit{if } n = 2 \\ 0 & \textit{if } n \textit{ is not prime.} \end{cases} \qquad (**)$$

Proof. Consider N, the subgroup of G_k generated by x_k. Then $N \cong \mathbb{Z}$, and $N \trianglelefteq G_k$ with $G_k/N \cong G_{k-1}$. So, N is a G_{k-1}-module. Since $G_k \cong N \rtimes G_{k-1}$, Lemma 5 from [6] gives us

$$m_n(G_k) = m_n(G_{k-1}) + \sum_{N_0} |\mathrm{Der}(G_{k-1}, N/N_0)|$$

where the sum is over all maximal submodules N_0 of N of index n. Of course, the maximal submodules of N are precisely the subgroups of prime index. Thus if n is not prime, then $m_n(G_k) = 0$; this follows by induction on k.

Fix a prime p. For both cases $p > 2$ and $p = 2$, we proceed by induction on k.

First, let $p > 2$, and let $k = 1$. Then $m_p(G_1) = 1 = 1 + (k-1)p$. Assume $(**)$ holds for $k = a$. Then $m_p(G_a) = 1 + (a-1)p$. Consider $k = a+1$. We have

$$m_p(G_{a+1}) = m_p(G_a) + \sum_{N_0} |\mathrm{Der}(G_a, N/N_0)|.$$

By Lemma 2, $\sum_{N_0} |\mathrm{Der}(G_a, N/N_0)| = p$. So $m_p(G_{a+1}) = 1+(a-1)p+p = 1 + (a+1-1)p$, the desired result.

Finally, let $p = 2$, and let $k = 1$. Then $m_2(G_1) = 1 = 2^1 - 1$. Assume $(**)$ holds for $k = a$. Then $m_2(G_a) = 2^a - 1$. Consider $k = a+1$. Then $m_2(G_{a+1}) = m_2(G_a) + |\mathrm{Der}(G_a, \mathbb{Z}/2\mathbb{Z})|$. By Lemma 2, $|\mathrm{Der}(G_a, \mathbb{Z}/2\mathbb{Z})| = 2^a$. Thus $m_2(G_{a+1}) = 2^a - 1 + 2^a = 2^{a+1} - 1$, the desired result. □

2. Some groups of the form $\mathbb{Z}^2 \rtimes (\mathbb{Z} \rtimes \mathbb{Z})$

Next, we will define the groups H_k, which are of the form $\mathbb{Z}^2 \rtimes (\mathbb{Z} \rtimes \mathbb{Z})$. We will write $G_2 = \mathbb{Z} \rtimes \mathbb{Z}$ as $\langle b \rangle \rtimes \langle a \rangle$ instead of $\langle x_2 \rangle \rtimes \langle x_1 \rangle$. Recall that $G_2 = \langle a, b | aba^{-1}b \rangle$. To form a group of the form $\mathbb{Z}^2 \rtimes (\mathbb{Z} \rtimes \mathbb{Z})$, what we need is an action of G_2 on $\mathbb{Z}^2$, and so, we just need to find matrices $A, B \in \mathrm{GL}_2(\mathbb{Z})$ such that $ABA^{-1}B = I_2$. With this, we can say that the action (by conjugation) of the generator a on $\mathbb{Z}^2$ is multiplication by the matrix A, and the generator b acts (by conjugation) on $\mathbb{Z}^2$ by multiplication by the matrix B.

We will take $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Let $B = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$. Then $ABA^{-1}B = \begin{pmatrix} y^2 + wz & yz + xz \\ wy + xw & wz + x^2 \end{pmatrix}$, and we will find solutions which make this equal I_2. We thus have $y^2 + wz = 1$, $wz + x^2 = 1$, $wy + xw = 0$ (equivalently, $w = 0$ or $x + y = 0$), and $yz + xz = 0$ (equivalently, $z = 0$ or $x + y = 0$). Also, we have $wz - xy = \pm 1$. One way to solve these equations is to let $w = 0$. Then $x, y = \pm 1$. Take $x = 1$. If we take $y = -1$, then z can be any integer.

Let the group H_k be the group formed when we take B to be $B_k = \begin{pmatrix} 0 & 1 \\ -1 & k \end{pmatrix}$. Our choice of A and B is in part to make calculating $m_n(H_k)$ be as simple as possible, but other choices could also be considered.

For a module M, we let $N \leqslant M$ denote that N is a submodule of M.

Lemma 4. *Consider $\mathbb{Z}^2$ to be a G_2-module as above. Let M be a maximal submodule of $\mathbb{Z}^2$. Then $p\mathbb{Z}^2 \leqslant M$ for some prime p.*

Proof. First, recall that every maximal subgroup of a polycyclic group has prime power index; this follows, for example, from the proof of Result 5.4.3 (iii) in [8].

Let H_k be as above, so $H_k = \mathbb{Z}^2 \rtimes G_2$. We claim that M yields a maximal subgroup of H_k with index equal to $[\mathbb{Z}^2 : M]$. Indeed, we have that $H_k/M \cong (\mathbb{Z}^2/M) \rtimes G_2$. Thus $\mathbb{Z}^2/M$ has a complement in $(\mathbb{Z}^2/M) \rtimes G_2$, which by Lemma 3 of [6] must be maximal and of index $[\mathbb{Z}^2 : M]$. Then just take its preimage in H_k.

Since M yields a maximal subgroup of H_k with index equal to $[\mathbb{Z}^2 : M]$ and H_k is polycyclic, we must have $[\mathbb{Z}^2 : M] = p^j$ for some prime p. Therefore, $p^j\mathbb{Z}^2 \leqslant M$. Consider the group $\mathbb{Z}^2/p^j\mathbb{Z}^2$. Its Frattini subgroup is $p\mathbb{Z}^2/p^j\mathbb{Z}^2$, and therefore, $p\mathbb{Z}^2/p^j\mathbb{Z}^2 + M/p^j\mathbb{Z}^2 = M/p^j\mathbb{Z}^2$. And hence $p\mathbb{Z}^2 + M = M$, that is, $p\mathbb{Z}^2 \leqslant M$. □

For a module N and for $n_i \in N$ for $i = 1, \ldots, t$, the submodule they generate is denoted $\langle n_1, n_2, \ldots, n_t \rangle$. For a prime p, consider the submodule $M_{p,\mathbf{w}}$ of $\mathbb{Z}^2$, where $M_{p,\mathbf{w}} = \langle \left(\begin{smallmatrix} p \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ p \end{smallmatrix}\right), \mathbf{w} \rangle$, with $\mathbf{w} \in \mathbb{Z}^2$. We will assume $\mathbf{w} \notin p\mathbb{Z}^2$. Then $M_{p,\mathbf{w}}$ is a proper (and hence maximal) submodule of $\mathbb{Z}^2$ if and only if the image of $\mathbf{w}$ in $\mathbb{Z}/p\mathbb{Z}^2$ is an eigenvector of both matrices A and B_k, considered as elements of $\mathrm{GL}_2(\mathbb{F}_p)$.

Let $\mathbf{v} = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$ and $\mathbf{u} = \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right)$, and let $M_p = M_{p,\mathbf{v}}$ and $M_{p,-1} = M_{p,\mathbf{u}}$. Of course, $\mathbf{v}$ and $\mathbf{u}$ are eigenvectors of $A \in \mathrm{GL}_2(\mathbb{F}_p)$ for all p. (And $\mathbf{v} \equiv \mathbf{u} \pmod 2$. Hence, $M_2 = M_{2,-1}$.)

Lemma 5. *With the above notation, we have that M_p is a maximal submodule of $\mathbb{Z}^2$ if and only if $p \mid k-2$. Also, $M_{p,-1}$ is a maximal submodule of $\mathbb{Z}^2$ if and only if $p \mid k+2$. Further, $M_{p,\mathbf{w}}$ is not a proper submodule of $\mathbb{Z}^2$ unless $M_{p,\mathbf{w}} = M_p$ or $M_{p,-1}$. Thus, $p\mathbb{Z}^2$ is a maximal submodule of $\mathbb{Z}^2$ if and only if $p \nmid (k-2)(k+2)$. Finally there are no maximal submodules of $\mathbb{Z}^2$ besides (the appropriate) M_p, $M_{p,-1}$, and $p\mathbb{Z}^2$.*

Proof. Let $\mathbf{v}$ and $\mathbf{u}$ be as above, but consider them as elements of $\mathbb{Z}^2/p\mathbb{Z}^2$. We have that $B_k\mathbf{v} = \left(\begin{smallmatrix} 1 \\ k-1 \end{smallmatrix}\right)$, and so $B_k\mathbf{v} = \lambda\mathbf{v}$ for some $\lambda \in \mathbb{Z}$ if and only if $k-1 \equiv 1 \pmod p$, i.e. if and only if $p \mid k-2$.

Also, $B_k\mathbf{u} = \binom{-1}{-1-k}$, and since multiples of $\mathbf{u}$ are characterized by the sum of their coordinates being $0 \pmod{p}$, $B_k\mathbf{u} = \lambda\mathbf{u}$ for some $\lambda \in \mathbb{Z}$ if and only if $-1-1-k \equiv 0 \pmod{p}$, which is equivalent to $p \mid k+2$.

That no other $M_{p,\mathbf{w}}$ is a proper submodule of $\mathbb{Z}^2$ follows from the fact that any eigenvector of A is a multiple of $\mathbf{v}$ or of $\mathbf{u}$.

Next, let $p \nmid (k-2)(k+2)$. Since neither M_p nor $M_{p,-1}$ is a maximal submodule of $\mathbb{Z}^2$ and neither is any other $M_{p,\mathbf{w}}$, we have that $p\mathbb{Z}^2$ is a maximal submodule of $\mathbb{Z}^2$. And if $p \mid (k-2)(k+2)$, then $p \mid k-2$ or $p \mid k+2$, in which case M_p or $M_{p,-1}$ is a proper submodule of $\mathbb{Z}^2$ that properly contains $p\mathbb{Z}^2$.

The final statement of this lemma follows from the previous parts of this lemma, together with Lemma 4; indeed it follows from Lemma 4 that any maximal submodule is either $p\mathbb{Z}^2$ or of the form $M_{p,\mathbf{w}}$. □

For a module N, we let $\tilde{m}_n(N)$ denote the number of maximal submodules of N of index n.

Corollary 6. *We have*

$$\tilde{m}_n(\mathbb{Z}^2) = \begin{cases} 1 & \text{if } n \text{ is a prime } p, \text{ and } p \mid (k-2)(k+2) \\ 1 & \text{if } n = p^2 \text{ for some prime } p, \text{ and } p \nmid (k-2)(k+2) \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Note that if $p \mid k-2$ and $p \mid k+2$, then $k-2 \equiv k+2 \pmod{p}$, whence $p = 2$. And using the previous notation, recall that $M_2 = M_{2,-1}$.

This corollary then follows from Lemma 5. □

Lemma 7. *Consider G_2 with presentation $\langle a, b \mid aba^{-1}b \rangle$, as described above. Let S be a G_2-module. Then there is a one-to-one correspondence between the set $\mathrm{Der}(G_2, S)$ and the set of functions $\delta : \{a, b\} \to S$ satisfying*

$$(1 - b^{-1})\delta(a) = (-a - b^{-1})\delta(b). \qquad (***)$$

Proof. This follows from Lemma 1. □

Lemma 8. *Fix k, and let $\mathbb{Z}^2$ have the G_2-module structure given above. For a given prime p, define S as either $\mathbb{Z}^2/M_p$, $\mathbb{Z}^2/M_{p,-1}$ or $\mathbb{Z}^2/p\mathbb{Z}^2$ such that S is simple (see Lemma 5). Any simple quotient of $\mathbb{Z}^2$ must be some such S. Then*

$$|\mathrm{Der}(G_2, S)| = \begin{cases} |S|^2 = p^2 & \text{if } p \mid k-2 \\ |S| = p & \text{if } p \mid k+2 \text{ and } p > 2 \\ |S| = p^2 & \text{if } p \nmid (k-2)(k+2). \end{cases}$$

Proof. That any simple quotient of $\mathbb{Z}^2$ is some such S follows from Lemma 5.

Let $\delta \in \mathrm{Der}(G_2, S)$ (to be specified later). The element $1-b^{-1}$ in $(***)$ from Lemma 7 acts on $\delta(a)$ by multiplication by the matrix $I_2 - B_k^{-1} = \left(\begin{smallmatrix} 1-k & 1 \\ -1 & 1 \end{smallmatrix}\right)$ which has determinant $2-k$, and the element $-a-b^{-1}$ acts by multiplication by the matrix $-A - B_k^{-1} = \left(\begin{smallmatrix} -k & 0 \\ -2 & 0 \end{smallmatrix}\right)$.

First, suppose $p \nmid k-2$. Then by Lemma 5, either $M_{p,-1}$ or $p\mathbb{Z}^2$ is a maximal submodule of $\mathbb{Z}^2$, depending on whether or not $p \mid k+2$. Notice that if $p=2$, then $p \mid k+2$ implies $p \mid k-2$, and hence if $p \mid k+2$, then $p > 2$ (because we are assuming here that $p \nmid k-2$).

In this case, $I_2 - B_k^{-1}$ is invertible, considered as a 2×2 matrix over $\mathbb{F}_p$. Hence $(***)$ from Lemma 7 may be written as

$$\delta(a) = (I_2 - B_k^{-1})^{-1}(-A - B_k^{-1})\delta(b).$$

And so in this case, we are free to choose $\delta(b)$ to be any element of S, and then this determines what $\delta(a)$ must be. Thus we would have $|\mathrm{Der}(G_2, S)| = |S|$. If $p \mid k+2$, then $S = \mathbb{Z}^2/M_{p,-1}$, and $|S| = p$. If $p \nmid k+2$, then $S = \mathbb{Z}^2/p\mathbb{Z}^2$, and $|S| = p^2$.

Next, suppose that $p \mid k-2$. Then $I_2 - B_k^{-1} \equiv \left(\begin{smallmatrix} -1 & 1 \\ -1 & 1 \end{smallmatrix}\right)$ and $-A - B_k^{-1} \equiv \left(\begin{smallmatrix} -2 & 0 \\ -2 & 0 \end{smallmatrix}\right) \pmod p$. Also, $p \mid k-2$ implies (by Lemma 5) that M_p is a maximal submodule of $\mathbb{Z}^2$. By Corollary 6, we have that $\tilde{m}_p(\mathbb{Z}^2) \leqslant 1$, and thus $S = \mathbb{Z}^2/M_p$.

We have that $\{\left(\begin{smallmatrix} i \\ 0 \end{smallmatrix}\right) : 0 \leqslant i < p\}$ is a complete set of representatives of $\mathbb{Z}^2/M_p$. Then letting $\delta(a) = \left(\begin{smallmatrix} i \\ 0 \end{smallmatrix}\right) + M_p$ and $\delta(b) = \left(\begin{smallmatrix} j \\ 0 \end{smallmatrix}\right) + M_p$, we have that equation $(***)$ from Lemma 7 holds because $(I_2 - B_k^{-1})\left(\begin{smallmatrix} i \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -i \\ -i \end{smallmatrix}\right) \in M_p$ and $(-A - B_k^{-1})\left(\begin{smallmatrix} j \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -2j \\ -2j \end{smallmatrix}\right) \in M_p$. And so both $(1-b^{-1})\delta(a)$ and $(-a-b^{-1})\delta(b)$ are the trivial element of $\mathbb{Z}^2/M_p$. Therefore, in this case, we have $|S|^2$ options for a derivation from G_2 to S.

□

Theorem 9. *We have*

$$m_n(H_k) = \begin{cases} n^2+n+1 & \text{if } n \text{ is prime, and } n \mid k-2 \\ 2n+1 & \text{if } n \text{ is prime, and } n \mid k+2 \text{ with } p > 2 \\ n+1 & \text{if } n \text{ is prime, and } n \nmid (k-2)(k+2) \\ n & \text{if } n = p^2 \text{ for some prime } p, \text{ and} \\ & \qquad\qquad p \nmid (k-2)(k+2) \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Consider $\mathbb{Z}^2 \trianglelefteq \mathbb{Z}^2 \rtimes G_2$. By Lemma 5 from [6], we have

$$m_n(H_k) = m_n(G_2) + \sum_{N_0} |\mathrm{Der}(G_2, \mathbb{Z}^2/N_0)| \tag{1}$$

where the sum is over all maximal submodules N_0 of $\mathbb{Z}^2$ of index n. Also, by Theorem 3, we have

$$m_n(G_2) = \begin{cases} n+1 & \text{if } n \text{ is a prime} \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

We have that Lemma 8 and Corollary 6 together imply that

$$\sum_{N_0} |\mathrm{Der}(G_2, \mathbb{Z}^2/N_0)| = \begin{cases} n^2 & \text{if } n \text{ is prime, and } n \mid k-2 \\ n & \text{if } n \text{ is prime and } n \mid k+2 \text{ with } n > 2 \\ n & \text{if } n = p^2 \text{ for some prime } p\text{, and} \\ & \qquad p \nmid (k-2)(k+2) \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

The present theorem follows from (1) by adding (2) and (3). □

For $n \in \mathbb{Z}$, let $\pi(n)$ denote the set of prime numbers dividing n. Then a consequence of Theorem 9 is that for $i, j \in \mathbb{Z}$, if $\pi(i-2) \neq \pi(j-2)$ or $\pi(i+2) \neq \pi(j+2)$, then $H_i \ncong H_j$. Also, note that $\mathrm{mdeg}(H_2) = 2$ (because $\pi(0)$ is the set of all primes), and for all $k \neq 2$, $\mathrm{mdeg}(H_k) = 1$.

Acknowledgment

We would like to thank the referee for a detailed referee report that helped us improve this paper.

References

[1] K. Brown. *Cohomology of groups*. Springer-Verlag, New York, 1982.

[2] E. Gelman. (2005). Subgroup growth of Baumslag-Solitar groups. *J. Group Theory*, 8(no. 6), 801–806.

[3] A. Jaikin-Zapirain and L. Pyber. (2011). Random generation of finite and profinite groups and group enumeration. *Ann. of Math. (2)*, 173(no. 2):769–814.

[4] A. Kelley. *Maximal Subgroup Growth of Some Groups*. PhD thesis, State University of New York at Binghamton, (2017).

[5] A. Kelley. (2020). Subgroup growth of all Baumslag-Solitar groups. *New York J. of Math.*, 218–229; http://nyjm.albany.edu/j/2020/26-11.html.

[6] A. Kelley. Maximal subgroup growth of some metabelian groups. To appear in *Comm. Algebra.* Preprint (2018), https://arxiv.org/abs/1807.03423.

[7] A. Lubotzky and D. Segal. *Subgroup growth.* Birkhauser Verlag, Basel, 2003.

[8] D. Robinson. *A course in the theory of groups.* Springer-Verlag, New York, second edition, 1996.

[9] A. Shalev. (1999). On the degree of groups of polynomial subgroup growth. *Trans. Amer. Math. Soc.*, 351(no. 9):3793–3822.

Contact information

Andrew James Kelley
Department of Mathematics and Computer Science
14 E. Cache La Poudre St.
Colorado Springs, CO, 80903, USA
E-Mail(s): akelley2500@gmail.com

Elizabeth Ciorsdan Dwyer Wolfe
Elizabeth Wolfe 1848
Colorado College
902 N Cascade Ave
Colorado Springs, CO 80946, USA
E-Mail(s): e_wolfe@coloradocollege.edu

Received by the editors: 03.12.2019
and in final form 04.01.2021.