LINEAR DIOPHANTINE EQUATIONS AND CONJUGATOR LENGTH IN 2-STEP NILPOTENT GROUPS

M. R. BRIDSON AND T. R. RILEY

Abstract. We establish upper bounds on the lengths of minimal conjugators in 2-step nilpotent groups. These bounds exploit the existence of small integral solutions to systems of linear Diophantine equations. We prove that in some cases these bounds are sharp. This enables us to construct a family of finitely generated 2-step nilpotent groups $(G_m)_{m\in\mathbb{N}}$ such that the conjugator length function of G_m grows like a polynomial of degree $m+1$.

2020 Mathematics Subject Classification: 20F65, 20F10, 20F18

Key words and phrases: nilpotent groups, conjugator length, linear Diophantine equations

1. Introduction

In this article we will explore the difficulty of the conjugacy problem in 2-step nilpotent groups, using normal forms to convert each instance of the problem into a system of linear Diophantine equations. A natural measure of the difficulty of the conjugacy problem in a finitely generated group G is its *conjugator length function*

$$\mathrm{CL}(n) \;=\; \max\left\{\mathrm{CL}(u,v) \mid \text{ words } u \text{ and } v \text{ with } u\sim v \text{ in } G \text{ and } |u|+|v|\leq n\right\},$$

where $u\sim v$ denotes conjugacy in G and $\mathrm{CL}(u,v)$ is defined to be the length $|w|$ of a shortest word w such that $uw=wv$ in G. The precise values of the function $\mathrm{CL}(n)$ depend on the choice of finite generating set, but the $\simeq$ class of $\mathrm{CL}(n)$ does not, where $\simeq$ is the following standard equivalence relation on functions $f,g:\mathbb{N}\to\mathbb{N}$: by definition, $f\preceq g$ if there exists $C>0$ such that $f(n)\leq Cg(Cn+C)+C$ for all $n\in\mathbb{N}$; if $f\preceq g$ and $g\preceq f$ then $f\simeq g$. If $\mathrm{CL}(n)\simeq n^d$, then one says that $\mathrm{CL}(n)$ is *polynomial of degree d*.

Here and in a companion article [BR] we describe the first families of groups to exhibit the following behaviour.

Theorem 1. *For all integers $d\geq 1$ there is a finitely presented group with conjugator length function $\mathrm{CL}(n)\simeq n^d$.*

The groups Γ_d we use to prove this theorem in [BR] are standard lattices in the much-studied model filiform groups. The proof that $\mathrm{CL}_{\Gamma_d}(n)\simeq n^d$ proceeds by induction on d; it relies on the fact that Γ_d is isomorphic to Γ_{d+1} modulo its cyclic

---

Date: 31 May 2025.

The first author thanks the Mathematics Department of Stanford University for its hospitality. The second author gratefully acknowledges the financial support of the National Science Foundation (NSF OIA-2428489).

centre, and hence on the fact that Γ_d is nilpotent of class d. The proof involves a careful analysis of the geometry of cyclic subgroups and centralisers in Γ_d.

The groups G_m that we will construct here to prove Theorem 1 are of a quite different nature. First of all, they are not drawn from a well known family of prototypes: they are bespoke, designed for the sole purpose of ensuring that their conjugator length functions are polynomial of arbitrary degree. The construction of G_m is not overtly geometric and the tools that we use to study these groups involve no geometry. The crucial property of G_m is that the Diophantine equations that arise from comparing normal forms for certain elements in the group have a simple recursive structure that enables us to establish a lower bound on $\mathrm{CL}_{G_d}(n)$. In a subsequent article we shall explain how this property can be exploited so as to construct amalgamated free products with more exotic conjugator length functions.

A further noteworthy feature of the groups G_m is that they are all *nilpotent of class* 2. Thus they reveal a sharp difference in behaviour between the word problem and the conjugacy problem: for a finitely generated nilpotent group G of class c, the Dehn function, which measures the complexity of the word problem, is polynomial of degree at most $c+1$ (see [GHR03, Gro96]); but we now know that the conjugator length function of G can be polynomial of any degree, even when $c = 2$.

Our groups G_m are central extensions

$$1 \to \mathbb{Z}^m \to G_m \to \mathbb{Z}^{m+2} \to 1$$

of $\mathbb{Z}^{m+2} = \langle a_1, \ldots, a_m, b_1, b_2 \rangle$ by $\mathbb{Z}^m = \langle c_1, \ldots, c_m \rangle$.

Theorem 2. *For $m \geq 1$, the group*

$$G_m \ := \left\langle \begin{array}{l} a_1, \ldots, a_m \\ b_1, b_2 \\ c_1, \ldots, c_m \end{array} \;\middle|\; \begin{array}{l} a_i a_j = a_j a_i \textit{ for all } i, j \\ b_1 b_2 = b_2 b_1 \\ b_1 a_i = a_i b_1 c_i \quad \textit{for} \quad i = 1, \ldots, m \\ b_2 a_i = a_i b_2 c_{i+1}^{-1} \quad \textit{for} \quad i = 1, \ldots, m-1 \\ b_2 a_m = a_m b_2 \\ c_i c_j = c_j c_i, \quad a_i c_j = c_j a_i, \quad b_i c_j = c_j b_i \textit{ for all } i, j \end{array} \right\rangle$$

has $\mathrm{CL}(n) \simeq n^{m+1}$.

The upper bound in Theorem 2 is a special case of the following general result.

Theorem 3. *The conjugator length functions of finitely generated class-2 nilpotent groups can be bounded from above as follows. Let G be a finitely generated group that is a central extension*

$$1 \to Z \to G \to A \to 1$$

where A is abelian and

$$Z \ \cong \ \mathbb{Z}^m \times T$$

where T is a finite abelian group. Then G has $\mathrm{CL}(n) \preceq n^{m+1}$.

The context of this theorem among prior literature on conjugator length functions of nilpotent groups is as follows. Ji, Ogle, and Ramsey [JOR10] argued that the conjugator length functions of finitely generated class-2 nilpotent groups G grows at most polynomially. Macdonald, Myasnikov, Nikolaev, and Vassileva [MMNV22, Thm. 4.7] proved polynomial upper bounds for the conjugator length functions of finitely generated nilpotent groups. Their argument gives an upper bound of $2^m(6mc^2)^{m^2}$ on the degree, where c is the class and m is the number of elements in what they call a *Mal'cev basis* for the group. In the case of a class-2 nilpotent group G with center Z, the union of a basis for Z and a set of elements of G that map to a basis for G/Z is a Mal'cev basis.

The tighter bounds that we get in the class-2 case will be obtained by carefully reducing each search for conjugators (where they are known to exist) to a consistent system of linear Diophantine equations, and then applying a result of Borosh, Flahive, Rubin, and Treybig [BFRT89] that bounds the size of the smallest integral solution.

For more background and information about conjugator length functions, we refer the reader to our survey article with Andrew Sale [BRS]. In that article we proved that the conjugator length function of the 3-dimensional integral Heisenberg group $\mathcal{H}_3(\mathbb{Z})$ is quadratic. The techniques that we deploy here are inspired in part by the proof of that result. In fact, the group G_1 in Theorem 2 is $\mathcal{H}_3(\mathbb{Z}) \times \mathbb{Z}$ with the $\mathbb{Z}$-factor being generated by b_2.

2. Conjugacy in class-2 nilpotent groups

Our aim here is to prove Theorem 3. We have a finitely generated group G that is a central extension

$$1 \to Z \to G \to A \to 1$$

with A abelian and

$$Z \;\cong\; \mathbb{Z}^m \times C_{o_1} \times \cdots \times C_{o_l},$$

where each C_{o_i} is a cyclic group of finite order o_i. Let $r = m + l$.

We express A as a direct sum of cyclic groups and choose preimages $a_1, \ldots, a_k \in G$ for generators of these cyclic groups. We also fix $c_1, \ldots, c_r \in Z$ so that $c_1, \ldots, c_m$ generate the $\mathbb{Z}^m$ summand and c_{m+j}, for $j = 1, \ldots, l$, generates the summand C_{o_j}. This gives us a set of generators $S = \{a_1, \ldots, a_k, c_1, \ldots, c_m\}$ for G. Indeed, G admits a normal form in which each element is expressed uniquely in the form

$$a_1^{x_1} \cdots a_k^{x_k} \; c_1^{z_1} \cdots c_r^{z_r}, \tag{1}$$

with $x_i, z_i \in \mathbb{Z}$ for all i with $0 \le z_{m+j} < o_j$ for $j = 1, \ldots, l$ and $0 \le x_i < o(a_i)$ if the image of a_i in A has finite order $o(a_i)$.

For all $1 \le i, j \le k$, all $1 \le s \le m$, and all $1 \le s' \le l$, there exist unique integers γ_{ijs} and $\gamma_{ij(m+s')}$ such that $[a_i, a_j] = c_1^{\gamma_{ij1}} \cdots c_r^{\gamma_{ijr}}$ in G and $0 \le \gamma_{ij(m+s')} < o_{s'}$. Note that $\gamma_{iis} = 0$ and $\gamma_{ijs} = -\gamma_{jis}$. Also $\gamma_{iis'} = 0$ and, modulo $o_{s'}$, $\gamma_{ijs'} = -\gamma_{jis'}$. Let

$$L \;=\; \max_{ij} \left\{ |\gamma_{ij1}| + \cdots + |\gamma_{ijr}| \mid 1 \le i < j \le k \right\}.$$

Suppose $n \in \mathbb{N}$ and consider words u and v on S such that $|u| + |v| \le n$ and $u \sim v$ in G. We rewrite u and v to express them (as elements of G) in normal form

$$u \;=\; a_1^{\alpha_1} \cdots a_k^{\alpha_k} \; c_1^{p_1} \cdots c_r^{p_r} \quad \text{and} \quad v \;=\; a_1^{\alpha_1} \cdots a_k^{\alpha_k} \; c_1^{q_1} \cdots c_r^{q_r}. \tag{2}$$

For all i, the exponents of a_i in the normal forms of u and of v agree, because the images of u and v in A are equal.

We will need bounds on the exponents in (2) in terms of n. To obtain the normal forms of u and v, we first push all their occurrences of $a_1^{\pm 1}$ to the left using the identities[1] $a_1 a_j = a_j a_1 [a_1, a_j]$ and $a_1^{-1} a_j = a_j a_1^{-1} [a_1, a_j]^{-1}$, moving commutators to the end of the word as they are produced, using the fact that they are central in G. We then push all occurrences of $a_2^{\pm 1}$ to the left and place them after the power of a_1 that we have gathered; then we push letters $a_3^{\pm 1}$ and so on. The total number of times we push one letter $a_i^{\pm 1}$ past another $a_j^{\pm 1}$ to get it in the correct position is less than n^2, and each push creates one commutator. We use the relations $[a_i, a_j] = c_1^{\gamma_{ij1}} \cdots c_r^{\gamma_{ijr}}$ to rewrite the commutators that are created in terms of the letters $c_1, \ldots, c_r$, then, using the fact that they are central, we shuffle the $c_1, \ldots, c_r$ into order. It follows from this description that $|\alpha_1| + \cdots + |\alpha_k| \le n$, and for all $i = 1, \ldots, m$,

$$|p_i|, |q_i| \;\le\; Ln^2, \tag{3}$$

and, for all $j = 1, \ldots, l$,

$$|p_{m+j}|, |q_{m+j}| \;<\; o_j \tag{4}$$

per the normal form (1).

If $w \in G$ conjugates u to v, then so does wc for every $c \in \langle c_1, \ldots, c_m \rangle$, because the c_i are central. Thus $u \sim v$ implies there exist $x_1, \ldots, x_k \in \mathbb{Z}$ so that for $w = a_1^{x_1} \cdots a_k^{x_k}$,

$$w^{-1} u w \;=\; v \tag{5}$$

in G. By expressing $w^{-1}uw$ in normal form (1) and comparing the powers of each c_i to the powers in the normal form for v, we find that (5) is equivalent to a system of linear Diophantine equations

$$\begin{array}{ccccccccc}
m_{1,1}x_1 & + & \cdots & + & m_{1,k}x_k & & & = & q_1 - p_1 \\
 & & & & & & & \vdots & \\
m_{m,1}x_1 & + & \cdots & + & m_{m,k}x_k & & & = & q_m - p_m \\
m_{m+1,1}x_1 & + & \cdots & + & m_{m+1,k}x_k & + \; o_1 x_{k+1} & & = & q_{m+1} - p_{m+1} \\
 & & & & & & & \vdots & \\
m_{r,1}x_1 & + & \cdots & + & m_{r,k}x_k & & + \; o_l x_{k+l} & = & q_r - p_r.
\end{array}$$

Here, for all i, the i-th equation counts the c_i. The additional term $o_j x_{k+j}$ present in equations $m+1$ through r accounts for c_{m+j} having order o_j — we need this because we are interested in integer solutions, not solutions modulo o_i. Recalling that $r = m + l$ and setting $d = k + l$, we write this system in the more concise form $M\mathbf{x} = \mathbf{b}$ by defining the $r \times d$ matrix M and the vectors $\mathbf{x} \in \mathbb{Z}^d$ and $\mathbf{b} \in \mathbb{Z}^r$ by:

$$M \;=\; \begin{pmatrix}
m_{1,1} & \cdots & m_{1,k} & & & \\
\vdots & & \vdots & & & \\
m_{m,1} & \cdots & m_{m,k} & & & \\
m_{m+1,1} & \cdots & m_{m+1,k} & o_1 & & \\
\vdots & & \vdots & & \ddots & \\
m_{m+l,1} & \cdots & m_{m+l,k} & & & o_l
\end{pmatrix}, \quad \mathbf{x} \;=\; \begin{pmatrix} x_1 \\ \\ \vdots \\ \\ x_d \end{pmatrix}, \quad \mathbf{b} \;=\; \begin{pmatrix} q_1 - p_1 \\ \\ \vdots \\ \\ q_r - p_r \end{pmatrix}.$$

[1] Our commutator convention is $[a, b] = a^{-1}b^{-1}ab$.

We claim that

$$|m_{ij}| \leq kLn, \tag{6}$$

for all $1 \leq i \leq r$ and all $1 \leq j \leq k$. In order to prove this claim, we consider how one transforms $w^{-1}uw$ into normal form, starting from the concatentation of the normal forms for u and $w^{\pm 1}$,

$$w^{-1}uw = (a_k^{-x_k} \cdots a_1^{-x_1})\ (a_1^{\alpha_1} \cdots a_k^{\alpha_k}\ c_1^{p_1} \cdots c_r^{p_r})\ (a_1^{x_1} \cdots a_k^{x_k}).$$

First assume $x_1 > 0$, so the first letter of w is a_1. We want to move this letter past u and cancel it with the terminal a_1^{-1} in w^{-1}. Pushing a_1 past the central generators $c_1, \ldots, c_r$ has no effect, while the total effect of pushing a_1 past the syllables $a_1^{\alpha_1}$, $\ldots$, $a_k^{\alpha_k}$ is to increase the exponent of c_i (for $1 \leq i \leq r$) by

$$\sigma_{i1} = \sum_{t=1}^{k} \alpha_t \gamma_{1ti}.$$

If $x_1 < 0$ then the first letter of w is a_1^{-1} and pushing it past u to cancel with the terminal letter of w^{-1} will decrease the exponent of c_i by $-\sigma_{i1}$. Whatever the signs, moving $a_1^{x_1}$ past u to cancel with the terminal $a_1^{-x_1}$ in w^{-1} will add $\sigma_{i1}x_1$ to the exponent of c_i. If we continue in this manner until each syllable $a_1^{x_1}$, $\ldots$, $a_k^{x_k}$ of w has been moved past u and cancelled with the corresponding $a_1^{-x_1}$, $\ldots$, $a_k^{-x_k}$ (respectively) in w^{-1}, the total change in the exponent of c_i will be

$$\sum_{j=1}^{k} \sigma_{ij} x_j \quad \text{where} \quad \sigma_{ij} = \sum_{t=1}^{k} \alpha_t \gamma_{jti}. \tag{7}$$

At the end of this process (after shuffling the $c_1, \ldots, c_r$ that have been generated into the correct positions) we have the normal form for v, so the first sum in (7) equals $q_i - p_i$ modulo the order of c_i. It follows from this discussion that for all $1 \leq i \leq r$ and all $1 \leq j \leq k$,

$$m_{ij} = \sigma_{ij} = \sum_{t=1}^{k} \alpha_t \gamma_{jti},$$

which means that $|m_{ij}| \leq kL \max_t |\alpha_t| \leq kLn$, as claimed.

Next we will pursue a change of variables which will have the effect of replacing the matrix M by a matrix M' which differs in that the entries in the lower-left block — that is, the $m_{m+j,t}$ for $j = 1, \ldots, l$ and $t = 1, \ldots, k$ — are reduced to uniformly bounded values. To this end, for all such j and t, define $s_{m+j,t}$ and $r_{m+j,t}$ to be the integers such that

$$m_{m+j,t} \ = \ s_{m+j,t} o_j + r_{m+j,t} \ \text{ and } \ 0 \leq r_{m+j,t} < o_j. \tag{8}$$

Let $P \in \mathrm{SL}_d(\mathbb{Z})$ be the lower-triangular matrix

$$P = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ -s_{m+1,1} & \cdots & -s_{m+1,k} & 1 & & \\ \vdots & & \vdots & & \ddots & \\ -s_{m+l,1} & \cdots & -s_{m+l,k} & & & 1 \end{pmatrix}$$

and define

$$M' := MP = \begin{pmatrix} m_{1,1} & \cdots & m_{1,k} & & & \\ \vdots & & \vdots & & & \\ m_{m,1} & \cdots & m_{m,k} & & & \\ r_{m+1,1} & \cdots & r_{m+1,k} & o_1 & & \\ \vdots & & \vdots & & \ddots & \\ r_{m+l,1} & \cdots & r_{m+l,k} & & & o_l \end{pmatrix}.$$

We know that there exists $\mathbf{x}$ satisfying $M\mathbf{x} = \mathbf{b}$ because $u \sim v$ in G. So there exists $\mathbf{x}' = P^{-1}\mathbf{x} \in \mathbb{Z}^d$ satisfying $M'\mathbf{x}' = \mathbf{b}$. Next we will apply a theorem of Borosh, Flahive, Rubin, and Treybig to the system $M'\mathbf{x}' = \mathbf{b}$.

Theorem 4 ([BFRT89])**.** *For all $r > 0$, there exists $C > 0$, such that, for all $r \times d$ integer matrices K of row-rank r and all $\mathbf{b} \in \mathbb{Z}^r$, if there is a solution $\mathbf{x} \in \mathbb{Z}^d$ to the system of r linear Diophantine equations $K\mathbf{x} = \mathbf{b}$, then there is a solution $\mathbf{x} \in \mathbb{Z}^d$ whose entries all have absolute value at most the maximum of the absolute values of the $r \times r$ minors of $[K : \mathbf{b}]$.*

Assume, as required for Theorem 4, that M' has full row-rank r. We bound the absolute values of $r \times r$ minors of $[M' : \mathbf{b}]$ as follows. Suppose N is an $r \times r$ matrix obtained from by deleting some columns of $[M' : \mathbf{b}]$. Now consider expanding $\det N$ along the final column of N, which is the only one that could be $\mathbf{b}$. We get that $\det N = \sum_{\sigma \in \mathrm{Sym}(r)} \mathrm{sign}(\sigma)\pi_\sigma$ where each π_σ is a product of r entries of N, one from each of the r-rows—and among these r entries, exactly one comes from the final column of N. The absolute values of the terms from rows $1 \leq i \leq m$ are at most kLn by (6), with the possible single exception of one coming from $\mathbf{b}$, which is most $2Ln^2$ by (3); the absolute values of the terms from rows $m+j$ for $1 \leq j \leq l$ are less than o_j by (8), with the possible exception of one coming from $\mathbf{b}$, which is less than $2o_j$ by (4). So, for a suitable constant $C > 0$,

$$|\det N| \;\leq\; r!\,(kLn)^{m-1}\,\left(\max\left\{kLn, 2Ln^2\right\}\right)\,2o_1\cdots o_l \;\leq\; Cn^{m+1},$$

and Theorem 4 tells us that the system $M'\mathbf{x}' = \mathbf{b}$ has a solution $\mathbf{x}'$ whose entries all satisfy $|x_i'| \leq Cn^{m+1}$.

Now for $1 \leq i \leq k$, the entry x_i of $\mathbf{x} = P\mathbf{x}'$ is x_i'. Thus we obtain a word $w = a_1^{x_1} \cdots a_k^{x_k}$ of length at most a constant times n^{m+1} such that $uw = wv$ in G.

Finally, suppose that the row-rank of M' is $\hat{r} < r$. Then some row of M' is a $\mathbb{Q}$-linear combination of the other rows, and so, because $M'\mathbf{x}' = \mathbf{b}$ is consistent, the same row in $[M' : \mathbf{b}]$ is the same $\mathbb{Q}$-linear combination of the other rows. So removing this row does not alter the set of solutions. We discard rows in this manner until we have replaced M' with a matrix of full row-rank $\hat{r}$. Theorem 4 then tells us that there is a solution $\mathbf{x}'$ with $|x'_1|, \ldots, |x'_d|$ all at most the maximum of the absolute values of the $\hat{r} \times \hat{r}$ minors for the redacted matrix, which then leads to a stronger bound than the one we derived above.

This completes our proof of Theorem 3. $\square$

3. Conjugator length in the groups G_m

The group

$$G_m \ := \ \left\langle \begin{array}{l|l} & a_i a_j = a_j a_i \text{ for all } i,j \\ a_1,\ldots,a_m & b_1 b_2 = b_2 b_1 \\ b_1, b_2 & b_1 a_i = a_i b_1 c_i \ \text{ for } \ i = 1,\ldots,m \\ c_1,\ldots,c_m & b_2 a_i = a_i b_2 c_{i+1}^{-1} \ \text{ for } \ i=1,\ldots,m-1 \\ & b_2 a_m = a_m b_2 \\ & c_i c_j = c_j c_i, \ \ a_i c_j = c_j a_i, \ \ b_i c_j = c_j b_i \text{ for all } i,j \end{array} \right\rangle$$

is a central extension of $\mathbb{Z}^{m+2} = \langle a_1, \ldots, a_m, b_1, b_2 \rangle$ by $\mathbb{Z}^m = \langle c_1, \ldots, c_m \rangle$.

Elements w of G_m can be expressed uniquely per the normal form

$$w \ = \ a_1^{x_1} \cdots a_m^{x_m} \ b_1^{y_1} b_2^{y_2} \ c_1^{z_1} \cdots c_m^{z_m} \tag{9}$$

with $x_1, \ldots, x_m, y_1, y_2, c_1, \ldots, c_m \in \mathbb{Z}$.

Proof of Theorem 2. Theorem 3 tells that $\mathrm{CL}(n) \preceq n^{m+1}$, so what remains to be proved is that $\mathrm{CL}(n) \succeq n^{m+1}$. Suppose $n \in \mathbb{N}$. Let $u = b_1 b_2^n \ a_1^{-n} b_1^{-n} a_1^n b_1^n$ and $v = b_1 b_2^n$. Then

$$|u| + |v| \ = \ 2 + 6n \tag{10}$$

and $u = b_1 b_2^n c_1^{-n^2}$ in G_m. For w as in (9), we use the defining relations for G_m to calculate the normal forms of uw and wv, pushing the letters a_i then b_i to the left and remembering that the c_i are central:

$$\begin{aligned} uw \ &= \ b_1 b_2^n c_1^{-n^2} \ a_1^{x_1} \cdots a_m^{x_m} \ b_1^{y_1} b_2^{y_2} \ c_1^{z_1} \cdots c_m^{z_m} \\ &= \ a_1^{x_1} \cdots a_m^{x_m} \ b_1^{y_1+1} b_2^{y_2+n} \ c_1^{x_1+z_1-n^2} c_2^{x_2 - n x_1 + z_2} \cdots c_m^{x_m - n x_{m-1} + z_m}, \end{aligned}$$

$$\begin{aligned} wv \ &= \ a_1^{x_1} \cdots a_m^{x_m} \ b_1^{y_1} b_2^{y_2} \ c_1^{z_1} \cdots c_m^{z_m} \ b_1 b_2^n \\ &= \ a_1^{x_1} \cdots a_m^{x_m} \ b_1^{y_1+1} b_2^{y_2+n} \ c_1^{z_1} \cdots c_m^{z_m}. \end{aligned}$$

Now, $uw = wv$ in G_m if and only if the exponents of $c_1, \ldots, c_m$ in their normal forms agree, and that amounts to the system of equations

$$\begin{array}{ccccccccccc} & x_1 & & & & & & & & = & n^2 \\ - & n x_1 & + & x_2 & & & & & & = & 0 \\ & & \ddots & & \ddots & & & & & & \vdots \\ & & & - & n x_{m-2} & + & x_{m-1} & & & = & 0 \\ & & & & & - & n x_{m-1} & + & x_m & = & 0 \end{array}$$

with no constraints on $y_1, y_2, z_1, \ldots, z_m$. This system has the unique solution $x_i = n^{i+1}$ for all i. So

$$w_0 \ = \ a_1^{n^2} a_2^{n^3} \cdots a_m^{n^{m+1}} \tag{11}$$

satisfies $uw_0 = w_0 v$ in G_m. Moreover, *any* word w such that $uw = wv$ in G_m has the same image as w_0 under the retraction $G_m \twoheadrightarrow \langle a_1, \ldots, a_m \rangle \cong \mathbb{Z}^m$ (which has kernel $\langle b_1, b_2, c_1, \ldots, c_m \rangle$), so w must contain at least n^{m+1} occurrences of the letter a_m. Therefore $\mathrm{CL}(u, v) \geq n^{m+1}$ and, in light of (10), $\mathrm{CL}(n) \succeq n^{m+1}$. □

References

[BFRT89] I. Borosh, M. Flahive, D. Rubin, and B. Treybig. A sharp bound for solutions of linear Diophantine equations. *Proc. Amer. Math. Soc.*, 105(4):844–846, 1989.

[BR] M. R. Bridson and T. R. Riley. The lengths of conjugators in the model filiform groups. In preparation.

[BRS] M. R. Bridson, T. R. Riley, and A. Sale. Conjugator length in finitely presented groups. In preparation.

[GHR03] S. M. Gersten, D. F. Holt, and T. R. Riley. Isoperimetric functions for nilpotent groups. *GAFA*, 13:795–814, 2003.

[Gro96] M. Gromov. *Carnot-Carathéodory spaces seen from within*, volume 144 of *Progress in Mathematics*, pages 79–323. Birkhäuser, 1996.

[JOR10] R. Ji, C. Ogle, and B. Ramsey. Relatively hyperbolic groups, rapid decay algebras and a generalization of the Bass conjecture. *J. Noncommut. Geom.*, 4(1):83–124, 2010. With an appendix by Ogle.

[MMNV22] J. Macdonald, A. Myasnikov, A. Nikolaev, and S. Vassileva. Logspace and compressed-word computations in nilpotent groups. *Trans. Amer. Math. Soc.*, 375(8):5425–5459, 2022. arXiv:1503.03888.

Martin R. Bridson
Mathematical Institute, Andrew Wiles Building, Oxford OX2 6GG, United Kingdom
bridson@maths.ox.ac.uk, https://people.maths.ox.ac.uk/bridson/

Timothy R. Riley
Department of Mathematics, 310 Malott Hall, Cornell University, Ithaca, NY 14853, USA
tim.riley@math.cornell.edu, http://www.math.cornell.edu/~riley/