LOGARITHMIC GIRTH EXPANDER GRAPHS OF $SL_n(\mathbb{F}_p)$

GOULNARA ARZHANTSEVA AND ARINDAM BISWAS*

Abstract. We provide an explicit construction of finite 4-regular graphs $(\Gamma_k)_{k\in\mathbb{N}}$ with girth $\Gamma_k \to \infty$ as $k \to \infty$ and $\frac{\operatorname{diam}\Gamma_k}{\operatorname{girth}\Gamma_k} \leqslant D$ for some $D > 0$ and all $k \in \mathbb{N}$. For each fixed dimension $n \geqslant 2$, we find a pair of matrices in $SL_n(\mathbb{Z})$ such that (i) they generate a free subgroup, (ii) their reductions mod p generate $SL_n(\mathbb{F}_p)$ for all sufficiently large primes p, (iii) the corresponding Cayley graphs of $SL_n(\mathbb{F}_p)$ have girth at least $c_n \log p$ for some $c_n > 0$. Relying on growth results (with no use of expansion properties of the involved graphs), we observe that the diameter of those Cayley graphs is at most $O(\log p)$. This gives infinite sequences of finite 4-regular Cayley graphs of $SL_n(\mathbb{F}_p)$ as $p \to \infty$ with large girth and bounded diameter-by-girth ratio. These are the first explicit examples in all dimensions $n \geqslant 2$ (all prior examples were in $n = 2$). Moreover, they happen to be expanders. Together with Margulis' and Lubotzky-Phillips-Sarnak's classical constructions, these new graphs are the only known explicit logarithmic girth Cayley graph expanders.

1. Introduction

The *girth* of a graph is the edge-length of its shortest non-trivial cycle (it is assigned to be infinity for an acyclic graph). The *diameter* of a graph is the greatest edge-length distance between any pair of its vertices. We regard a countable graph Γ as a sequence of its connected components $\Gamma = (\Gamma_k)_{k\in\mathbb{N}}$ each of which is endowed with the edge-length distance.

Definition 1.1 (large girth graph, cf. [Big98]). *A graph $\Gamma = (\Gamma_k)_{k\in\mathbb{N}}$ is* large girth *if* $\operatorname{girth}\Gamma_k \to \infty$, *and it is* logarithmic girth *if there exists a constant $c > 0$ such that for all $k \in \mathbb{N}$:*

$$\operatorname{girth}\Gamma_k \geqslant c \log |\Gamma_k|.$$

Definition 1.2 (dg-bounded graph [AT18]). *A graph $\Gamma = (\Gamma_k)_{k\in\mathbb{N}}$ is* dg-bounded *if there exists a constant $D > 0$ such that for all $k \in \mathbb{N}$:*

$$\frac{\operatorname{diam}\Gamma_k}{\operatorname{girth}\Gamma_k} \leqslant D.$$

A dg-bounded graph with uniformly bounded degree r satisfies $\operatorname{girth}\Gamma_k \geqslant \frac{1}{D}\operatorname{diam}\Gamma_k$ and $\operatorname{diam}\Gamma_k \geqslant \log_r(|\Gamma_k|-1)$, for $r \geqslant 3$, while $\operatorname{diam}\Gamma_k \geqslant \frac{1}{2}(|\Gamma_k|-1)$ for $r = 2$. Hence, for such a graph, $\operatorname{girth}\Gamma_k \to \infty$, whenever $|\Gamma_k| \to \infty$ as $k \to \infty$.

In this paper, we focus on large girth dg-bounded graphs with uniformly bounded degree $r \geqslant 2$. For $r = 2$, a growing sequence of cycle graphs is an easy example of such a graph. A major theoretical and practical challenge is to build large girth dg-bounded graphs for $r \geqslant 3$.

The *existence* of r-regular large girth dg-bounded graphs $\Gamma = (\Gamma_k)_{k\in\mathbb{N}}$, for each $r \geqslant 3$, is a classical result. For instance, first, one can show the existence of large girth graphs using the probabilistic argument of Erdős-Sachs [ES63] (see also [Sac63] for a recursive, on the degree r, construction) or by taking iterated mod 2-covers of a given graph (each iteration doubles the girth) and then,

1991 *Mathematics Subject Classification.* 20G40, 05C25, 20E26, 20F65.

Key words and phrases. Large girth graphs, expander graphs, diameter, special linear group, coarse embedding, thin matrix group.

This research was partially supported by the European Research Council (ERC) grant of Goulnara Arzhantseva, “ANALYTIC” grant agreement no. 259527.

following Biggs [Big98, Lemma 3.1], prove that the diameter of the graph with the minimal number of vertices among all graphs of a given degree $r \geqslant 2$ and of girth at least $g \geqslant 3$ is at most g (giving $D = 1$ for such a graph, called a 'cage'). However, this does not provide concrete examples and the resulting graphs are not necessarily Cayley graphs.

The first *explicit* examples for $r \geqslant 3$ are given by suitable Cayley graphs of $SL_2(\mathbb{F}_p)$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ are the integers $\bmod\, p$ for a prime p. Namely, the famous explicit construction of large girth graphs by Margulis [Mar82] is made of 4-regular Cayley graphs $\Gamma_p = Cay(SL_2(\mathbb{F}_p), \{A_p, B_p\})$ with matrices A_p, B_p being images of Sanov's generators of the free group (see below for notation and Section 3 for details). It satisfies $\operatorname{girth} \Gamma_p \geqslant C \log |\Gamma_p|$ for $C > 0$ and it is dg-bounded as by Selberg's theorem [Sel65], combined with the transfer principle of Brooks [Bro86] and Burger [Bur86], they form an infinite expander family as $p \to \infty$. Then $\operatorname{diam} \Gamma_p = O(\log |\Gamma_p|)$ because every expander has logarithmic diameter. Alternatively, the celebrated Lubotzky-Phillips-Sarnak [LPS88] graphs, $\Gamma_q = Cay(PGL_2(\mathbb{F}_q), \{S_1, S_2, \dots, S_{p+1}\})$ as $q \to \infty$, where p, q are distinct primes congruent to 1 $\bmod 4$ with the Legendre symbol $\left(\frac{p}{q}\right) = -1$ and $S_1, \dots, S_{p+1}$ are suitable $p+1$ matrices, form a Ramanujan family (hence, an expander family) and they satisfy $\operatorname{girth} \Gamma_q \geqslant 4 \log_p q - \log_p 4$ with $|\Gamma_q| = q(q^2 - 1)$. Therefore, they are $(p+1)$-regular large girth dg-bounded Cayley graphs. Observe that both of these examples are in *dimension 2* (i.e., in 2×2 matrices), they are of logarithmic girth, and the expansion property is used to conclude the dg-boundedness. Moreover, these constructions of Margulis and Lubotzky-Phillips-Sarnak (and their slight variants, again in dimension 2) have been, up to now, the only known explicit large girth dg-bounded expanders among the Cayley graphs.

Our aim is to provide an explicit construction of 4-regular large girth dg-bounded Cayley graphs of $SL_n(\mathbb{F}_p)$ as $p \to \infty$, for *all dimensions* $n \geqslant 2$. Concretely, we shall give an extensive description of two-element generating sets of $SL_n(\mathbb{F}_p)$ that induce the required properties of the Cayley graphs. We formulate now our main result, indicate several corollaries (among others, constructions of $2k$-regular examples for *all* $k \geqslant 2$) and explain the motivation for this work.

Magic matrices in dimension $n \geqslant 2$:

$$\text{Let } A = \begin{pmatrix} 1 & a & 0 & 0 & \dots & 0 \\ 0 & 1 & a & 0 & \dots & 0 \\ 0 & 0 & 1 & a & \dots & 0 \\ \vdots & & & & & \vdots \\ & & & & \dots & a \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 & 0 & \dots & & 0 \\ b & 1 & 0 & \dots & & 0 \\ 0 & b & 1 & \dots & & 0 \\ 0 & 0 & b & \dots & & 0 \\ \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b & 1 \end{pmatrix} \in SL_n(\mathbb{Z}) \text{ with } a, b \geqslant 2.$$

We denote by A_p and B_p their reductions modulo a prime p and by $\langle A, B \rangle \leqslant SL_n(\mathbb{Z})$ and $\langle A_p, B_p \rangle \leqslant SL_n(\mathbb{F}_p)$ the subgroups generated by these matrices.

Main Theorem. *The matrices A and B satisfy the following.*

I. Freeness:
- *For $n = 2$, $\langle A, B \rangle$ is free;*
- *For $n = 3$, $\forall l \geqslant 4$, $\langle A^l, B^l \rangle$ is free;*
- *For each $n \geqslant 4$, $\forall l \geqslant 3(n-1)$, $\langle A^l, B^l \rangle$ is free.*

II. Generation $\bmod\, p$:
- *For $n = 2$, $\forall p$ prime with $a, b \not\equiv 0 (\bmod\, p)$, we have $\langle A_p, B_p \rangle = SL_2(\mathbb{F}_p)$;*
- *For $n = 3$, $a \equiv 1 (\bmod\, 3), b \equiv -1 (\bmod\, 3), \forall l = 4^k, k \in \mathbb{N}$, we have $\langle A_p^l, B_p^l \rangle = SL_3(\mathbb{F}_p)$ for $p = 3$ and all primes $p > K$, where K is a constant;*

- *For each $n \geqslant 4$, $\forall q$ prime with $n \equiv 1(\operatorname{mod} q)$ and a, b with $a \equiv 1(\operatorname{mod} q), b \equiv 1(\operatorname{mod} q)$, $\forall l \in \{1\} \cup \{q^{k+1}+1 : k \in \mathbb{N}, k \geqslant t,$ with $t \in \mathbb{N}$ given by $q^t \leqslant n < q^{t+1}\}$, we have $\langle A_p^l, B_p^l\rangle = SL_n(\mathbb{F}_p)$ for $p = q$ and all primes $p > L$, where $L = L(n, a, b, l)$ is a constant.*

III. Girth and diameter:
For each of the following choices of the parameters:

- *if $n = 2$, $l = 1$, then $\forall p$ prime with $a, b \not\equiv 0(\operatorname{mod} p)$;*
- *if $n = 3$, $a \equiv 1(\operatorname{mod} 3), b \equiv -1(\operatorname{mod} 3), \forall l = 4^k, k \in \mathbb{N}$, then for $p = 3$ and all primes $p > K$, where K is a constant;*
- *if $n \geqslant 4$ is fixed, $\forall q$ prime with $n \equiv 1(\operatorname{mod} q)$, and a, b with $a \equiv 1(\operatorname{mod} q), b \equiv 1(\operatorname{mod} q)$, $\forall l \in \{q^{k+1}+1$ if $q \neq 2$ and $q^{k+2}+1$ if $q = 2 : k \in \mathbb{N}, k \geqslant t,$ with $t \in \mathbb{N}$ given by $q^t \leqslant n < q^{t+1}\}$, then for $p = q$ and all primes $p > L$, where $L = L(n, a, b, l)$ is a constant,*

we have

$$\operatorname{girth} Cay(SL_n(\mathbb{F}_p), \{A_p^l, B_p^l\}) \geqslant c_n \log p \ \textit{ and } \ \operatorname{diam} Cay(SL_n(\mathbb{F}_p), \{A_p^l, B_p^l\}) = O(\log p),$$

where $c_n = c_n(a, b, l)$ is a constant.

In particular, $\Gamma_p^{n,l}(a, b) = Cay(SL_n(\mathbb{F}_p), \{A_p^l, B_p^l\})$ as $p \to \infty$ is a large girth dg-bounded graph, whenever n and l are as above.

Moreover, it is an expander. In addition, all the above constants K, L, c_n and that of $O(\log p)$ term are effective.

Taking specific dimension n and power l of our matrices gives, for instance, the following sequences of 4-regular large girth dg-bounded graphs:

$$\Gamma_p^{3,4}(4,2) = Cay(SL_3(\mathbb{F}_p), \{\begin{pmatrix}1&4&0\\0&1&4\\0&0&1\end{pmatrix}^4, \begin{pmatrix}1&0&0\\2&1&0\\0&2&1\end{pmatrix}^4\}) \text{ as } p \to \infty$$

and

$$\Gamma_p^{4,10}(4,4) = Cay(SL_4(\mathbb{F}_p), \{\begin{pmatrix}1&4&0&0\\0&1&4&0\\0&0&1&4\\0&0&0&1\end{pmatrix}^{10}, \begin{pmatrix}1&0&0&0\\7&1&0&0\\0&7&1&0\\0&0&7&1\end{pmatrix}^{10}\}) \text{ as } p \to \infty.$$

The graphs produced by the Main Theorem and the proof itself provide explicit examples relevant to various subjects. For instance, in each dimension $n \geqslant 3$, every free subgroup $\langle A^l, B^l\rangle$ from the Main Theorem is an example of a *thin* matrix group. No explicit examples of thin free subgroups of $SL_n(\mathbb{Z})$ for $n \geqslant 3$ were previously known. Also, the 4-regular graphs $\Gamma_p^{n,l}(a, b)$ have $2k$-regular counterparts $\Gamma_p^{n,l}(a, b; k)$, on the same vertex set! Moreover, differing conceptually from the prior examples in dimension 2 (because produced by a thin group in contrast to an arithmetic group in case $n = 2$), our expanders are concrete test graphs in the quest for large girth *super-expanders*. We discuss all these corollaries in detail, together with the corresponding open questions, in Section 6.

A classical application of explicit large girth graphs, and specifically logarithmic girth graphs, is in the coding theory, e.g. to the LDPC codes, as pioneered by Margulis [Mar82]. Besides being a purely combinatorial challenge in a higher dimension in contrast to known results in dimension 2, with potential applications in computer science, our motivation to find explicitly such graphs comes from several recent results in geometric group theory and in metric geometry. For instance, uniformly bounded degree $r \geqslant 3$ large girth dg-bounded graphs are required in the constructions of infinite finitely generated groups with prescribed subgraphs in their Cayley graphs, so-called 'infinite monster groups'. A foundational example is Gromov's random groups that contain infinite expander families in their Cayley graphs [Gro03, AD08]. Gromov's monster groups do not coarsely embed into a Hilbert space and are counterexamples to an important conjecture in topology, the Baum-Connes conjecture with coefficients [HLS02]. For a more recent result on monster groups see [AT18] (where it is essential to have the large girth dg-bounded graph made of Cayley graphs) and references therein. In all these constructions the imposed large girth and dg-boundedness of graphs ensure the existence of appropriate small cancellation labelings of their edges. This in turn guarantees a suitable embedding of such a graph into the Cayley graph of the group (whose generators are labeling letters and relators are defined by the labels of closed cycles). On the other hand, some results in metric geometry use directly large girth and dg-boundedness (no additional labeling is required). For example, in [Ost12], the author constructs the first examples of regular large girth graphs with uniformly bounded ℓ_1 distortion. Namely, given a uniformly bounded degree large girth dg-bounded graph, he applies the results of [AGS12] to the mod 2-cover of such a graph to conclude a uniform bound on the ℓ_1 distortion. Graphs with uniformly bounded ℓ_1 distortion are useful, for instance, in the theory of approximation algorithms.

Notation. Throughout the text, we denote by $Cay(G, S)$ the Cayley graph of a group G with respect to a generating set $S \subseteq G$. In particular, $Cay(G, S \sqcup S^{-1})$ is the same graph even if a given S is not symmetric.

Acknowledgments. We thank Peter Sarnak for indicating that free subgroups from our Main Theorem are thin matrix groups, see Section 6, Alex Lubotzky for pointing out that our result also yields r-regular logarithmic girth Cayley expander graphs, for all even integer $r \geqslant 4$, see Corollaries 6.1 and 6.2 and Nikolay Nikolov for attracting our attention to Nori's result [N87]. We are grateful to the anonymous referees for detailed comments and useful suggestions.

2. Strategy of the proof and expansion properties

Our strategy has an advantage to guarantee the expansion properties of our graphs as a byproduct of previously known strong results about expanders defined through finite quotients of Zariski dense subgroups of $SL_n(\mathbb{Z})$.

In detail, the proof of Main Theorem consists of four steps. For each of the choices of dimension, $n = 2, 3$ and $n \geqslant 4$, we prove that our matrices $A, B \in SL_n(\mathbb{Z})$ satisfy the following:

(i) A^l and B^l generate a free subgroup in $SL_n(\mathbb{Z})$ for each $l \geqslant 1$ as in the Main Theorem ($l = 1$ for $n = 2$),

(ii) A^l_p, B^l_p, their reduction mod p, generate $SL_n(\mathbb{F}_p)$ for all sufficiently large primes p,

(iii) girth $Cay(SL_n(\mathbb{F}_p), \{A^l_p, B^l_p\}) \geqslant c_n \log p$ for some $c_n > 0$;

In addition, we deduce:

(iv) $Cay(SL_n(\mathbb{F}_p), \{A^l_p, B^l_p\})$ as $p \to \infty$ is an expander.

Each of these assertions is new for our pair of matrices in case $n \geqslant 3$ and it seems no explicit matrices have been known with the properties (i)–(iii), and (i)–(iv), for $n \geqslant 3$.

We proceed as follows. For each of the choices of dimension, we first show properties (i) and (ii), and then use them and known results about growth of small subsets in $SL_n(\mathbb{F}_p)$ to obtain a logarithmic bound on the diameter of the Cayley graphs. We do not use the expansion properties of the involved graphs as our focus is large girth dg-bounded graphs and, a priori, such graphs need not be expanders. The logarithmic bound on the diameter together with (iii) gives the required large girth with bounded diameter-by-girth ratio. Although, our strategy is similar in all dimensions, dimension $n = 3$ appears to be exceptional. Note also a smaller value of l we can allow in this case in Main Theorem.

In dimension $n = 2$, we moreover have property (ii) for *all* primes p such that $a, b \not\equiv 0 (\bmod p)$. For all *sufficiently large* primes p, (ii) can be obtained from (i) by the Matthews-Vaserstein-Weisfeiler theorem [MVW84] as the free subgroup of $SL_2(\mathbb{Z})$ is non-elementary, and hence Zariski dense. We do not use this deep result in our proof of (ii) for $n = 2$ but present an easy direct argument for the sake of completeness.

In dimension $n \geqslant 3$, in contrast to the two-dimensional case, assertion (i) does not yield (ii) since in higher dimensions freeness does not imply Zariski dense, so [MVW84] does not apply immediately. However, our computations show that assertion (ii) holds for a suitable prime p. This, combined with [W91] (see also [Lub99]), implies that our free subgroup $\langle A^l, B^l \rangle$ is indeed Zariski dense, and, hence, by [MVW84], (ii) holds for all sufficiently large primes p.

The expansion properties of our sequence of Cayley graphs have not been known previously. Observe that generators A^l_p, B^l_p of $SL_n(\mathbb{F}_p)$ are *not* images[1] of generators of $SL_n(\mathbb{Z})$. However, as explained, using (i) for $n = 2$ and (i)-(ii) for $n \geqslant 3$, the free subgroup $\langle A^l, B^l \rangle$ is Zariski dense. It follows by [BG08] for $n = 2$ and by [BV12] for $n \geqslant 3$ that $Cay(SL_n(\mathbb{F}_p), \{A^l_p, B^l_p\})$ as $p \to \infty$ is indeed an expander. It appears to be the first explicit expander in dimension $n \geqslant 3$ which is large girth dg-bounded, by the Main Theorem.

3. Dimension $n = 2$

The results of this section are certainly known to specialists, although formulations available in the literature often restrict to the cases $|a| = |b| = 2$ or $|a| = |b|$. In our setting, a and b can differ and we present arguments for completeness.

3.1. Girth.

Our magic matrices are 2-by-2 matrices $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$. Enlarging the set of possible a, b, we take $a, b \in \mathbb{Z}, |a|, |b| \geqslant 2$. It is an easy consequence of the ping-pong lemma that the subgroup generated by these matrices $\langle A, B \rangle \leqslant SL_2(\mathbb{Z})$ is free.

Lemma 3.1 (Ping-pong [LS01, Ch.III, Prop.12.2])**.** *Let G be a group acting on a set X, let Γ_1, Γ_2 be two subgroups of G, and let $\Gamma = \langle \Gamma_1, \Gamma_2 \rangle$ be the subgroup of G generated by Γ_1 and Γ_2. Suppose $|\Gamma_1| \geqslant 3$ and $|\Gamma_2| \geqslant 2$. Suppose there exist two disjoint non-empty subsets of X, say X_1 and X_2 with*

$$\gamma(X_1) \subset X_2 \ \ \forall \gamma \in \Gamma_2, \gamma \neq 1 \text{ and } \gamma(X_2) \subset X_1 \ \ \forall \gamma \in \Gamma_1, \gamma \neq 1.$$

Then Γ is isomorphic to the free-product $\Gamma_1 * \Gamma_2$.

Corollary 3.2 (Sanov's theorem)**.** *$\langle A, B \rangle \leqslant SL_2(\mathbb{Z})$ is free.*

Proof. Consider the usual action of $SL_2(\mathbb{Z})$ on $X = \mathbb{Z}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : x, y \in \mathbb{Z} \right\}$. Let $\Gamma_1 = \langle A \rangle, \Gamma_2 = \langle B \rangle$, $X_1 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : |x| > |y| \right\}$ and $X_2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 : |y| > |x| \right\}$ be two disjoint non-empty subsets of X.

Let $\gamma_1 \in \Gamma_1$ and $\gamma_2 \in \Gamma_2$. Then $\gamma_1 = \begin{pmatrix} 1 & k_1 a \\ 0 & 1 \end{pmatrix}$ and $\gamma_2 = \begin{pmatrix} 1 & 0 \\ k_2 b & 1 \end{pmatrix}$ for some $k_1, k_2 \in \mathbb{Z} \backslash \{0\}$. Clearly, $\gamma_1(X_2) = \left\{ \begin{pmatrix} x + k_1 a y \\ y \end{pmatrix} : |y| > |x| \right\}$ and $|x| < |y| \Rightarrow |x + k_1 a y| > |y|$ since $|k_1 a| \geqslant 2$ (the assumption $|a| \geqslant 2$ is essential). Hence, $\gamma_1(X_2) \subset X_1 \ \forall \gamma_1 \in \Gamma_1 \backslash \{1\}$. Similarly, $\gamma_2(X_1) \subset X_2 \ \ \forall \gamma_2 \in \Gamma_2 \backslash \{1\}$ (with the use of assumption $|b| \geqslant 2$). The ping-pong lemma applies and we are done as $\Gamma_1 \cong \Gamma_2 \cong \mathbb{Z}$. □

[1] For $n \geqslant 3$, $G = SL_n(\mathbb{Z})$ has Kazhdan's property (T), hence any generating set S and a nested family of finite index normal subgroups $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots$ with $\bigcap_{n=0}^{\infty} G_n = \{1\}$ naturally provide an infinite expander $\bigsqcup_{n=0}^{\infty} Cay(G/G_n, S_n)$, where S_n is the canonical image of S. Such expanders are neither of large girth, nor dg-bounded.

Note that for $a = b = 1$, the subgroup $\langle A, B\rangle$ is not free. For $|a| = |b| = 2$, it is of finite index in $SL_2(\mathbb{Z})$, while for $|a| = |b| > 2$ it is of infinite index in $SL_2(\mathbb{Z})$.

The main result of this subsection is Proposition 3.3. This fact is originally due to Margulis for $a = b = 2$ [Mar82], cf. [DSV03, Appendix A]. We give our computation, which is a bit more explicit in view of its generalization to higher dimensions.

Proposition 3.3. *Let p be a prime. Then* $\operatorname{girth} Cay(\langle A_p, B_p\rangle, \{A_p, B_p\}) \geqslant C\log p$ *for a constant* $C = C(a, b) > 0$.

Proof. The girth is the length of the shortest non-trivial cycle in $Cay(\langle A_p, B_p\rangle, \{A_p, B_p\})$. Hence, it is the minimum length of the non-trivial word in the generators $\{A_p^{\pm 1}, B_p^{\pm 1}\}$ which represents the identity of $\langle A_p, B_p\rangle$.

Starting at the identity of $\langle A_p, B_p\rangle$, we consider all non-trivial paths in the Cayley graph which return to the identity. We aim to show that the length of all such paths in $Cay(\langle A_p, B_p\rangle, \{A_p, B_p\})$ is at least $C\log p$ for some $C > 0$, whenever a, b are integers such that $a, b \not\equiv 1(\operatorname{mod} p)$ and $a, b \not\equiv 0(\operatorname{mod} p)$. These assumptions on p are not restrictive as a, b are fixed, so there are finitely many excluded primes and the values of the corresponding girths are bounded above by a constant.

The proof is an explicit analysis of the growth of the products

$$\prod_{1\leqslant i\leqslant k} (A^{l_i}B^{m_i}) \in SL_2(\mathbb{Z}),\ i, k \in \mathbb{N},\ l_i, m_i \in \mathbb{Z}\backslash\{0\},$$

where

$$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix},\ a, b \not\equiv 1(\operatorname{mod} p) \text{ and } a, b \not\equiv 0(\operatorname{mod} p).$$

We have $A^{l_i} = \begin{pmatrix} 1 & l_i a \\ 0 & 1 \end{pmatrix}, B^{m_i} = \begin{pmatrix} 1 & 0 \\ m_i b & 1 \end{pmatrix}$ $\forall l_i, m_i \in \mathbb{Z}\backslash\{0\}$, which gives

$$A^{l_1}B^{m_1} = \begin{pmatrix} l_1m_1ab + 1 & l_1a \\ m_1b & 1 \end{pmatrix},$$

$$A^{l_1}B^{m_1}A^{l_2}B^{m_2} = \begin{pmatrix} (l_1m_1l_2m_2)(ab)^2 + (l_1m_1 + l_1m_2 + l_2m_2)ab + 1 & (l_1m_1l_2)a^2b + (l_1 + l_2)a \\ (m_1l_2m_2)ab^2 + (m_1 + m_2)b & (m_1l_2)ab + 1 \end{pmatrix},$$

and in general if we have the product of $2k$ terms then each entry of the matrix is a polynomial in a, b. Let us denote these polynomials by $P_{11}(a, b), P_{12}(a, b), P_{21}(a, b), P_{22}(a, b)$ such that

$$\prod_{1\leqslant i\leqslant k} A^{l_i}B^{m_i} = \begin{pmatrix} P_{11}(a, b) & P_{12}(a, b) \\ P_{21}(a, b) & P_{22}(a, b) \end{pmatrix},\ l_i, m_i \in \mathbb{Z}\backslash\{0\}\,\forall i$$

then, by induction on k, one can obtain the explicit forms of the polynomials $P_{ij}(a, b), 1 \leqslant i, j \leqslant 2$. For instance, P_{11} has the form,

$P_{11}(a, b) = 1 + a_2(ab) + a_4(ab)^2 + \ldots + a_{2k}(ab)^k$, where, for $1 \leqslant r \leqslant k$, we have

$$a_{2r} = \sum_{1\leqslant j_r\leqslant i_r<\ldots<j_2\leqslant i_2<j_1\leqslant i_1\leqslant k} m_{i_1}l_{j_1}m_{i_2}l_{j_2}\cdots m_{i_r}l_{j_r}.$$

Since A, B generate a free group, $\prod_{1\leqslant i\leqslant k} A^{l_i}B^{m_i} \neq \mathrm{id}$ in $SL_2(\mathbb{Z})$ and so starting from the identity a necessary condition for the path along this product to reach the identity in $Cay(\langle A_p, B_p\rangle, \{A_p, B_p\})$ is $|P_{ij}(a, b)| > p$, for some $1 \leqslant i, j \leqslant 2$. Let k denote the length of such a path. Then,

$$|P_{ij}(a, b)| \leqslant M^k|(ab + 1)|^k,$$

where $M = \max\{|l_i|, |m_i| : 1 \leqslant i \leqslant k\}$. This yields a constant $C = C(a,b) > 0$ such that

$$k > C \log p.$$

From the above it is also clear that the same holds when $l_1 = 0$ or $m_k = 0$. Since Cayley graphs are vertex transitive and we have shown that starting from the identity it takes the product of at least $C \log p$ matrices of the form $A_p^{\pm 1}, B_p^{\pm 1}$ to reach the identity non-trivially, we conclude that the girth of $Cay(\langle A_p, B_p\rangle, \{A_p, B_p\})$ is at least $C \log p$. □

3.2. **Diameter.** The diameter problem for the finite (simple) linear groups has been studied extensively and there exists a vast literature on the subject. We follow our strategy from Section 2 and make sure that our elements A_p and B_p generate the entire $SL_2(\mathbb{F}_p)$. In dimension 2, this fact is easy.

Lemma 3.4. *$\langle A_p, B_p\rangle = SL_2(\mathbb{F}_p)$ for all primes p.*

Proof. Fix a prime p and note that $A^l \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod p$ and $B^m \equiv \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \pmod p$ for some $1 \leqslant l, m \leqslant p$. Since the mod p reduction $SL_2(\mathbb{Z}) \twoheadrightarrow SL_2(\mathbb{F}_p)$ is surjective and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ generate $SL_2(\mathbb{Z})$, then their mod p reduction generate $SL_2(\mathbb{F}_p)$. It follows that $\langle A_p, B_p\rangle = SL_2(\mathbb{F}_p)$, for all primes p. □

In contrast, it is a highly non-trivial fact that the diameter of $Cay(SL_2(\mathbb{F}_p), \{A_p, B_p\})$ is $O(\log p)$. As alluded to in the introduction, one way is to use the expansion properties of the sequence as $p \to \infty$. Another way is to apply the circle method to show that any element of $SL_2(\mathbb{F}_p)$ lifts to an element of $SL_2(\mathbb{Z})$ having word representation of $O(\log p)$ [LPS88] (see also [Lar03] for an efficient algorithm, although it gives $O(\log p \log\log p)$ only). We take yet an alternative way and use an aspect of the seminal work of Helfgott [Hel08].

Theorem 3.5 (Helfgott [Hel08])**.** *Let p be a prime. Let S be any generating set of $SL_2(\mathbb{F}_p)$. Then the Cayley graph $Cay(SL_2(\mathbb{F}_p), S)$ has diameter $O((\log p)^c)$, where c and the implied constant are absolute.*

To establish this theorem Helfgott showed the following result.

Proposition 3.6 (Key proposition [Hel08])**.** *Let p be a prime. Let S be a subset of $SL_2(\mathbb{F}_p)$ not contained in any proper subgroup.*

(1) Assume that $|S| < p^{3-\delta}$ for some fixed $\delta > 0$. Then

$$|S^3| > c|S|^{1+\epsilon}$$

where $c > 0$ and $\epsilon > 0$ depend only on δ.

(2) Assume that $|S| > p^\delta$ for some fixed $\delta > 0$. Then there is an integer $k > 0$, depending only on δ, such that every element of $SL_2(\mathbb{F}_p)$ can be expressed as a product of at most k elements of $S \sqcup S^{-1}$.

We now obtain the required upper bound on the diameter of our graphs.

Lemma 3.7. *The diameter of $Cay(SL_2(\mathbb{F}_p), \{A_p, B_p\})$ is $O(\log p)$, where the implied constant depends on a and b.*

Proof. By Lemma 3.4, the group $\langle A, B\rangle$ surjects onto $SL_2(\mathbb{F}_p)$. We know that $\langle A, B\rangle$ is a free subgroup in $SL_2(\mathbb{Z})$ and the girth of $Cay(SL_2(\mathbb{F}_p), \{A_p, B_p\})$ is at least $c \log p$ for some constant $c = c(a,b) > 0$. Therefore, denoting $S = \{A_p^{\pm 1}, B_p^{\pm 1}\}$, we have

$$|S^{\frac{c}{6}\log p}| \geqslant 3^{\frac{c}{6}\log p}.$$

Choosing $S' = S^{\frac{c}{6}\log p}$, we find ourselves in (2) of Proposition 3.6 (with $\delta < \frac{c}{6}\log 3$), and hence $(S')^k = SL_2(\mathbb{F}_p)\ \forall p$, where k depends only on δ. Therefore, $S^{kc\log p} = SL_2(\mathbb{F}_p)$, which means that the diameter of $Cay(SL_2(\mathbb{F}_p), \{A_p, B_p\})$ is $O(\log p)$. □

Since we have a generating set which is free in $SL_2(\mathbb{Z})$ the growth of balls in $SL_2(\mathbb{F}_p)$ is fast at the beginning (up to girth scale). Therefore, we only used part (2) of Proposition 3.6 in the preceding proof. This estimate on the diameter (with the same argument) also appeared, for example, in [Hel08, Corollary 6.3].

Corollary 3.8. *Let $a, b \in \mathbb{Z}\backslash\{0,1\}$. The diameter-by-girth ratio of the sequence of Cayley graphs of $G = SL_2(\mathbb{F}_p)$ with respect to $S = \{A_p^{\pm1}, B_p^{\pm1}\}$, as $p \to \infty$, where $A = \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}, B = \begin{pmatrix}1 & 0\\ b & 1\end{pmatrix}$ is bounded by a constant.*

Proof. By Proposition 3.3 and Lemma 3.7, there exist constants $K_1 = K_1(a,b) > 0$ and $K_2 = K_2(a,b) > 0$ such that $\operatorname{girth} Cay(G,S) > K_1 \log p$ and $\operatorname{diam} Cay(G,S) < K_2 \log p$, respectively. Hence, $\frac{\operatorname{diam} Cay(G,S)}{\operatorname{girth} Cay(G,S)} < \frac{K_2}{K_1}$. □

4. Dimension $n = 3$

4.1. **Girth.** For $n = 3$ the situation is more complicated. The primary difficulty is to find suitable candidates for our free subgroup in $SL_3(\mathbb{Z})$. The existence of such free subgroups is a well-known fact but explicit examples seem not to be present in the literature. Indeed, apart from a few special cases the ping-pong lemma, Lemma 3.1, is the universal way one can establish that two elements generate a non-abelian free subgroup. The challenge with the ping-pong lemma is that it is a non-trivial problem to find an explicit description of disjoint non-empty subspaces X_1 and X_2 such that $\gamma_1(X_2) \subset X_1$ and $\gamma_2(X_1) \subset X_2$. In higher dimensions, each of the sets X_1 and X_2 might be a union of smaller subsets. We get around this difficulty by a direct computation on growth of some products. We show that fourth powers of our A and B generate a free group inside $SL_3(\mathbb{Z})$. Then we use them to produce a new large girth dg-bounded sequence of finite Cayley graphs.

Proposition 4.1. *Fix $a, b \in \mathbb{N}, a, b \geqslant 2$. Let $A, B \in SL_3(\mathbb{Z})$ be such that*

$$A = \begin{pmatrix}1 & a & 0\\ 0 & 1 & a\\ 0 & 0 & 1\end{pmatrix}, B = \begin{pmatrix}1 & 0 & 0\\ b & 1 & 0\\ 0 & b & 1\end{pmatrix}$$

Then $\langle A^4, B^4\rangle$ is a free subgroup of $SL_3(\mathbb{Z})$.

Proof. Let $X = A^4 = \begin{pmatrix}1 & 4a & 6a^2\\ 0 & 1 & 4a\\ 0 & 0 & 1\end{pmatrix}$ and $Y = B^4 = \begin{pmatrix}1 & 0 & 0\\ 4b & 1 & 0\\ 6b^2 & 4b & 1\end{pmatrix}$. We claim that $\langle X, Y\rangle$ is a free subgroup of $SL_3(\mathbb{Z})$. We study products of the form $X^{r_1}Y^{s_1}\cdots X^{r_k}Y^{s_k}$ for any $r_i, s_i \in \mathbb{Z}\backslash\{0\}, k \in \mathbb{N}$. The crucial step is to show that

$$\big(X^{r_1}Y^{s_1}\big)\big(X^{r_2}Y^{s_2}\big)\cdots\big(X^{r_k}Y^{s_k}\big) \neq \mathrm{id} \text{ in } SL_3(\mathbb{Z}),\ \forall r_i, s_i \in \mathbb{Z}\backslash\{0\}, k \in \mathbb{N}.$$

Clearly,

$$X^{r_i}Y^{s_i} = \begin{pmatrix}1 & 4ar_i & \frac{4r_ia^2(4r_i-1)}{2}\\ 0 & 1 & 4ar_i\\ 0 & 0 & 1\end{pmatrix} \times \begin{pmatrix}1 & 0 & 0\\ 4bs_i & 1 & 0\\ \frac{4s_ib^2(4s_i-1)}{2} & 4bs_i & 1\end{pmatrix}$$

$$= 4abr_is_i\begin{pmatrix}ab(4r_i-1)(4s_i-1) + 4 + \frac{1}{4abr_is_i} & 2a(4r_i-1) + \frac{1}{bs_i} & \frac{a(4r_i-1)}{2bs_i}\\ 2b(4s_i-1) + \frac{1}{ar_i} & 4 + \frac{1}{4abr_is_i} & \frac{1}{bs_i}\\ \frac{b(4s_i-1)}{2ar_i} & \frac{1}{ar_i} & \frac{1}{4abr_is_i}\end{pmatrix} = 4r_is_i(4r_i-1)(4s_i-1)\times$$

$$\begin{pmatrix} x^2+\frac{4x}{(4r_i-1)(4s_i-1)}+\frac{1}{4r_is_i(4r_i-1)(4s_i-1)} & \frac{2xa}{(4s_i-1)}+\frac{a}{s_i(4r_i-1)(4s_i-1)} & \frac{a^2}{2s_i(4s_i-1)} \\ \frac{2xb}{(4r_i-1)}+\frac{b}{r_i(4r_i-1)(4s_i-1)} & \frac{4x}{(4r_i-1)(4s_i-1)}+\frac{1}{4r_is_i(4r_i-1)(4s_i-1)} & \frac{a}{s_i(4r_i-1)(4s_i-1)} \\ \frac{b^2}{2r_i(4r_i-1)} & \frac{b}{r_i(4r_i-1)(4s_i-1)} & \frac{1}{4r_is_i(4r_i-1)(4s_i-1)} \end{pmatrix},$$

where $x = ab \geqslant 4$. Thus, the above expression is equal to

$$4r_is_i(4r_i-1)(4s_i-1)N_i,$$

where

$$N_i = \begin{pmatrix} x^2+\frac{4x}{(4r_i-1)(4s_i-1)}+\frac{1}{4r_is_i(4r_i-1)(4s_i-1)} & \frac{2xa}{(4s_i-1)}+\frac{a}{s_i(4r_i-1)(4s_i-1)} & \frac{a^2}{2s_i(4s_i-1)} \\ \frac{2xb}{(4r_i-1)}+\frac{b}{r_i(4r_i-1)(4s_i-1)} & \frac{4x}{(4r_i-1)(4s_i-1)}+\frac{1}{4r_is_i(4r_i-1)(4s_i-1)} & \frac{a}{s_i(4r_i-1)(4s_i-1)} \\ \frac{b^2}{2r_i(4r_i-1)} & \frac{b}{r_i(4r_i-1)(4s_i-1)} & \frac{1}{4r_is_i(4r_i-1)(4s_i-1)} \end{pmatrix} \forall i \in \mathbb{N}$$

denotes the normalised form of the product $X^{r_i}Y^{s_i}$.

It is easy to check that denoting $N_i = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, we have the (anti-)lexicographic ordering among the elements from left to right and from top to bottom in the sense that $|a_{11}| > |a_{12}| > |a_{13}| > |a_{23}| > |a_{33}|, |a_{11}| > |a_{12}| > |a_{22}| > |a_{23}| > |a_{33}|$, etc. In fact, we have stronger inequalities on the bounds of the values taken by $a_{ij}, \forall 1 \leqslant i,j \leqslant 3$. We have:

(1) $x^2 + \frac{x}{2} > a_{11} > x^2 - \frac{x}{2}$
(2) $\frac{2}{3}xa + \frac{a}{9} \geqslant |a_{12}|$
(3) $\frac{2}{3}xa + \frac{x}{9a} \geqslant |a_{21}|$
(4) $\frac{a^2}{6} > a_{13} > 0$
(5) $\frac{a^2}{6} > a_{31} > 0$
(6) $\frac{4x}{9} + \frac{1}{9} > |a_{22}|$
(7) $\frac{a}{8} > |a_{23}| > 0$
(8) $\frac{b}{8} > |a_{32}| > 0$
(9) $\frac{1}{4} > a_{33} > 0$

If $N = N_1N_2\cdots N_k$ has the first coefficient > 1, then it will imply $\left(X^{r_1}Y^{s_1}\right)\left(X^{r_2}Y^{s_2}\right)\cdots\left(X^{r_k}Y^{s_k}\right) \neq$ id in $SL_3(\mathbb{Z})$, $\forall r_i, s_i \in \mathbb{Z}\backslash\{0\}, k \in \mathbb{N}$.

Let $Z = \begin{pmatrix} A & B_1 & C_1 \\ B_2 & D & E_1 \\ C_2 & E_2 & F \end{pmatrix} \in SL_3(\mathbb{Z})$ be such that $A > |B_1| + |C_1| + 1$.

Claim 4.2. *$Z \cdot N_1 \cdot N_2 \cdots N_k$ has the same form as Z.*

Proof of claim. Let $Z' = Z \cdot N_i$ for some $i \in \mathbb{N}$. First we check that Z' has the same form as Z.

$$Z' = \begin{pmatrix} A' & B_1' & C_1' \\ B_2' & D' & E_1' \\ C_2' & E_2' & F' \end{pmatrix} = \begin{pmatrix} A & B_1 & C_1 \\ B_2 & D & E_1 \\ C_2 & E_2 & F \end{pmatrix} \times \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

By the inequalities on the $a_{rs}, 1 \leqslant r,s \leqslant 3$, we know that

(1) $A' = Aa_{11} + B_1a_{21} + C_1a_{31} > (x^2 - \frac{x}{2})A - (\frac{2}{3}xa + \frac{x}{9a})|B_1| - \frac{a^2}{6}|C_1|$
(2) $B_1' = Aa_{12} + B_1a_{22} + C_1a_{32} < (\frac{2}{3}xa + \frac{a}{9})A + (\frac{4x}{9} + \frac{1}{9})|B_1| + \frac{b}{8}|C_1|$
(3) $C_1' = Aa_{13} + B_1a_{23} + C_1a_{33} < \frac{a^2}{6}A + \frac{a}{8}|B_1| + \frac{1}{4}|C_1|$

We would like to show that $A' > |B_1'| + |C_1'| + 1$ under the assumption that $A > |B_1| + |C_1| + 1$. Substituting the above inequalities we get that if we can show

$$\begin{aligned}\left(x^2 - \frac{x}{2}\right) A - \left(\frac{2}{3}xa + \frac{x}{9a}\right)|B_1| - \frac{a^2}{6}|C_1| > \left(\frac{2}{3}xa + \frac{a}{9}\right) A + \left(\frac{4x}{9} + \frac{1}{9}\right)|B_1| \\ + \frac{b}{8}|C_1| + \frac{a^2}{6}A + \frac{a}{8}|B_1| + \frac{1}{4}|C_1| + 1,\end{aligned} \tag{4.1}$$

then we are done. We know that $x = ab \geqslant 2a$. If $x > 2a$ (equivalently $b > 2$), then rearranging and simplifying the above expression we see that if we can show

$$(x^2 - 1 - xa)A > xa|B_1| + xa|C_1| + 1,$$

then we are done. Indeed, the above holds under the assumption $A > |B_1| + |C_1| + 1$ (if $x \geqslant 2a + 1$). For $x = 2a$, a direct substitution in (4.1) shows that it holds under this assumption.

The claim follows by induction on k, using the above assertion on Z' twice. Indeed, the base of the induction is the above considerations for $Z \cdot N_1$. Then if $Z \cdot N_1 \cdot N_2 \cdots N_{i-1}$ has the same form as Z, this assertion gives that $Z \cdot N_1 \cdot N_2 \cdots N_i$ has the same form as Z as well.

□

Thus, $N = N_1 \cdots N_k$ cannot be identity in $SL_3(\mathbb{Z})$ for any $k \in \mathbb{N}$. Also, N has the same form as Z. Since X^r is not of this form, it follows that $N \neq X^r$ for any $r \in \mathbb{Z}$. Therefore, products of the form $N \cdot X^r$ cannot be identity either. The case of $Y^s \cdot N \neq \mathrm{id}$ is clear from the fact that we consider reduced words in $X^{\pm 1}$ and $Y^{\pm 1}$. So, $Y^s \cdot N = \mathrm{id} \implies NY^s = \mathrm{id}$ which either has the same form as above or reduces to a power of X or of Y. Both of these elements are of infinite order so their powers cannot be identity. The remaining case of products of form $Y^s \cdot N \cdot X^r$ reduces to the already considered. This concludes the fact that $\langle X, Y\rangle \leqslant SL_3(\mathbb{Z})$ is a free subgroup. □

Our proof of Proposition 4.1 actually gives the following stronger statement.

Theorem 4.3. *Let $A, B \in SL_3(\mathbb{Z})$ be such that*

$$A = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}, \ B = \begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ 0 & b & 1 \end{pmatrix}, \ a, b \geqslant 2.$$

Then $\langle A^l, B^l \rangle$, $\forall l \geqslant 4$, is a free subgroup of $SL_3(\mathbb{Z})$.

Theorem 4.4. *Fix $a, b \geqslant 2$ and let p be a prime. Then there exists a constant $C = C(a, b) > 0$, such that* $\operatorname{girth} Cay(\langle A_p^4, B_p^4\rangle, \{A_p^4, B_p^4\}) \geqslant C \log p$.

Proof. Let again $X = A^4 = \begin{pmatrix} 1 & 4a & 6a^2 \\ 0 & 1 & 4a \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = B^4 = \begin{pmatrix} 1 & 0 & 0 \\ 4b & 1 & 0 \\ 6b^2 & 4b & 1 \end{pmatrix}$.

Using the previous expression for products

$$X^{r_i} Y^{s_i} = \begin{pmatrix} 1 & 4ar_i & \frac{4r_i a^2 (4r_i - 1)}{2} \\ 0 & 1 & 4ar_i \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 \\ 4bs_i & 1 & 0 \\ \frac{4s_i b^2 (4s_i - 1)}{2} & 4bs_i & 1 \end{pmatrix}$$

$$= 4abr_i s_i \begin{pmatrix} ab(4r_i - 1)(4s_i - 1) + 4 + \frac{1}{4abr_i s_i} & 2a(4r_i - 1) + \frac{1}{bs_i} & \frac{a(4r_i - 1)}{2bs_i} \\ 2b(4s_i - 1) + \frac{1}{ar_i} & 4 + \frac{1}{4abr_i s_i} & \frac{1}{bs_i} \\ \frac{b(4s_i - 1)}{2ar_i} & \frac{1}{ar_i} & \frac{1}{4abr_i s_i} \end{pmatrix} = 4r_i s_i (4r_i - 1)(4s_i - 1) \times$$

$$\begin{pmatrix} x^2 + \frac{4x}{(4r_i-1)(4s_i-1)} + \frac{1}{4r_is_i(4r_i-1)(4s_i-1)} & \frac{2xa}{(4s_i-1)} + \frac{a}{s_i(4r_i-1)(4s_i-1)} & \frac{a^2}{2s_i(4s_i-1)} \\ \frac{2xb}{(4r_i-1)} + \frac{b}{r_i(4r_i-1)(4s_i-1)} & \frac{4x}{(4r_i-1)(4s_i-1)} + \frac{1}{4r_is_i(4r_i-1)(4s_i-1)} & \frac{a}{s_i(4r_i-1)(4s_i-1)} \\ \frac{b^2}{2r_i(4r_i-1)} & \frac{b}{r_i(4r_i-1)(4s_i-1)} & \frac{1}{4r_is_i(4r_i-1)(4s_i-1)} \end{pmatrix}$$

$$= 4r_is_i(4r_i-1)(4s_i-1)N_i,$$

where $x = ab \geqslant 4$ and $\forall i \in \mathbb{N}$,

$$N_i = \begin{pmatrix} x^2 + \frac{4x}{(4r_i-1)(4s_i-1)} + \frac{1}{4r_is_i(4r_i-1)(4s_i-1)} & \frac{2xa}{(4s_i-1)} + \frac{a}{s_i(4r_i-1)(4s_i-1)} & \frac{a^2}{2s_i(4s_i-1)} \\ \frac{2xb}{(4r_i-1)} + \frac{b}{r_i(4r_i-1)(4s_i-1)} & \frac{4x}{(4r_i-1)(4s_i-1)} + \frac{1}{4r_is_i(4r_i-1)(4s_i-1)} & \frac{a}{s_i(4r_i-1)(4s_i-1)} \\ \frac{b^2}{2r_i(4r_i-1)} & \frac{b}{r_i(4r_i-1)(4s_i-1)} & \frac{1}{4r_is_i(4r_i-1)(4s_i-1)} \end{pmatrix}.$$

In general,

$$\prod_{1\leqslant i\leqslant k} X^{r_i}Y^{s_i} = 4^k \prod_{1\leqslant i\leqslant k} r_is_i(4r_i-1)(4s_i-1)N_i = 4^k \prod_{1\leqslant i\leqslant k} r_is_i(4r_i-1)(4s_i-1)\cdot N,$$

with $N = \prod_{1\leqslant i\leqslant k} N_i$. Denoting $N = \begin{pmatrix} N_{11} & N_{12} & N_{13} \\ N_{21} & N_{22} & N_{23} \\ N_{31} & N_{32} & N_{33} \end{pmatrix}$, it is clear that N_{11} is $O(x^{2k})$, and hence reduction modulo p gives us that k should be at least $C\log p$ for some $C > 0$. Again, we can assume here that $a, b \not\equiv 0 (\mathrm{mod}\, p)$ and $a, b \not\equiv 1 (\mathrm{mod}\, p)$: the finitely many excluded primes p are taken into account by enlarging constant C if necessary. Thus, the girth of the graph is at least $C\log p$ for some $C > 0$. □

4.2. **Diameter.** Fix $a \equiv 1 (\mathrm{mod}\, 3)$ and $b \equiv -1 (\mathrm{mod}\, 3)$. We shall show that $\langle A_p^4, B_p^4 \rangle = SL_3(\mathbb{F}_p)$ for all sufficiently large primes p. For this we use a result on the Zariski density and the following proposition.

Proposition 4.5. *Let* $a \equiv 1 (\mathrm{mod}\, 3)$ *and* $b \equiv -1 (\mathrm{mod}\, 3)$. *Then* mod 3 *reduction of the matrices* $X = A^4 = \begin{pmatrix} 1 & 4a & 6a^2 \\ 0 & 1 & 4a \\ 0 & 0 & 1 \end{pmatrix}$ *and* $Y = B^4 = \begin{pmatrix} 1 & 0 & 0 \\ 4b & 1 & 0 \\ 6b^2 & 4b & 1 \end{pmatrix}$ *generate* $SL_3(\mathbb{F}_3)$.

Proof. After reducing mod 3, we have to show that

$$X \equiv \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} (\mathrm{mod}\, 3) \text{ and } Y \equiv \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} (\mathrm{mod}\, 3)$$

generate $SL_3(\mathbb{F}_3)$. For we give an algorithm how to attain elementary matrices of $SL_3(\mathbb{F}_3)$ while taking certain products of our matrices $X^{\pm 1}$ and $Y^{\pm 1}$. This goes as follows:

(1) Calculate $C_1 = YXY^{-1}X^{-1} \equiv \begin{pmatrix} 2 & -1 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix} (\mathrm{mod}\, 3)$. Similarly,

$$C_2 = Y^{-1}X^{-1}YX \equiv \begin{pmatrix} 2 & 0 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} (\mathrm{mod}\, 3), \quad C_1^{-1} = C_3 \equiv \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{pmatrix} (\mathrm{mod}\, 3),$$

$$C_2^{-1} = C_4 \equiv \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -1 \\ -1 & 0 & 2 \end{pmatrix} (\mathrm{mod}\, 3).$$

(2) This implies $C_1C_2^{-1} = YXY^{-1}X^{-2}Y^{-1}XY \equiv \begin{pmatrix} -1 & -1 & 5 \\ 0 & 1 & -1 \\ 0 & 0 & -1 \end{pmatrix} \pmod 3 \implies$
$C_1C_2^{-1}X \equiv \begin{pmatrix} -1 & -2 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \pmod 3$ and $(C_1C_2^{-1}X)^2 \equiv \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod 3$.
Thus, we can get the matrices $T_1 \equiv \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod 3$ and $T_2 \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \pmod 3$.

(3) Let $T = [T_2, T_1]^{\,2} \equiv \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \pmod 3$ and $Z = T \times C_4 \equiv \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \pmod 3$. Then $Z \times T_1^{-1}$ gives us

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \pmod 3.$$

Similarly, we get the other elementary matrices. It is standard that the elementary matrices generate $SL_n(\mathbb{Z})$ for all $n \geqslant 1$. Thus, mod 3 reduction of A^4 and B^4 indeed generate $SL_3(\mathbb{F}_3)$. □

Remark 4.6. Proposition 4.5 sheds light on our choice of the power of A and B to be 4. The number 3 in $a \equiv 1 (\bmod 3)$ and $b \equiv -1 (\bmod 3)$ is not mandatory, any prime $q \geqslant 3$ works. Indeed, if we fix a prime q, $a \equiv 1(\bmod q)$ and $b \equiv -1(\bmod q)$, and take the power of A and B to be $q+1$, then our algorithm from the preceding proof extends and we get the elementary matrices in $SL_3(\mathbb{F}_q)$.

We now state an essential criterion that ensures that $\bmod\, p$ reduction of the matrices X and Y generate $SL_3(\mathbb{F}_p)$ for almost all primes p. We use a formulation from [Lub99] (as we mentioned in Section 2, this result follows using [W91] and [MVW84]). We keep the original notation, e.g. here A denotes a subset.

Proposition 4.7 (Lubotzky [Lub99])**.** *Let $A = \{a_i\}_{i \in I}$ be a subset of $SL_n(\mathbb{Z})$. Assume that for some prime p, the reduction modulo p of A generates the subgroup $SL_n(\mathbb{F}_p)$. If $n = 2$ assume $p \neq 2$ or 3, if $n = 3$ or 4 assume $p \neq 2$. Then for almost every prime q, reduction modulo q of A generates the subgroup $SL_n(\mathbb{F}_q)$.*

This amazing result gives the existence of a constant $q(n, A, p)$ such that given n, A, and p as in the preceding proposition, A generates $SL_n(\mathbb{F}_q)$ for every prime $q \geqslant q(n, A, p)$. The proof in [Lub99] uses the Strong Approximation theorem for linear groups and it is not constructive. In particular, it does not provide estimates on the possible value of $q(n, A, p)$. However, recent effective variants of the Strong Approximation theorem, see [Bre15, Theorem 2.3] and [GV12, Appendix A], both based on Nori's quantitative proof of the strong approximation [N87], imply that the value of $q(n, A, p)$ is effective, i.e., it can be computed from the given parameters by an algorithm.

Proposition 4.8. *Let a and b be fixed so that $a \equiv 1(\bmod 3)$ and $b \equiv -1(\bmod 3)$. Then $\langle A_p^4, B_p^4 \rangle = SL_3(\mathbb{F}_p)$ for almost every prime p, i.e., for every prime $p \geqslant q(3, \{X, Y\}, 3)$.*

Proof. Use Proposition 4.5 and Proposition 4.7 to get the existence of $q(3, \{X, Y\}, 3)$. □

Thus, we have that $\{A^4, B^4\}$ generate a free subgroup in $SL_3(\mathbb{Z})$ and also that $\{A_p^4, B_p^4\}$ generate $SL_3(\mathbb{F}_p)$ for almost all primes p. We can now estimate the diameter using a result similar to Proposition 3.6 but for higher dimensions. It was first shown by Helfgott for dimension 3 and later

[2] For elements g, h in a group G, the commutator $[g, h]$ is equal to $g^{-1}h^{-1}gh$.

generalised to all bounded dimensions by Pyber–Szabo [PS16] and Breuillard–Green–Tao [BGT11]. We state it as formulated in [BGT11].

Proposition 4.9 (Breuillard–Green–Tao [BGT11], Corollary 2.4)**.** *Let $d \in \mathbb{N}$. Then there are $\epsilon(d) > 0, C_d > 0$ such that for every absolutely almost simple algebraic group G with $\dim(G) \leqslant d$ defined over a finite field k, and every finite subset A in $G(k)$ generating $G(k)$, and for all $0 < \epsilon < \epsilon(d)$, one of the following two statements holds:*

(1) $|A| >_d |G(k)|^{1-C_d\epsilon}$,
(2) $|A^3| \geqslant |A|^{1+\epsilon}$,

where $X >_d Y$ denotes $X > C(d)Y$ and $C(d)$ is some constant depending only on d.

Since our set $\{A^4, B^4\}$ generates a free subgroup in $SL_3(\mathbb{Z})$ and the girth of $Cay(SL_3(\mathbb{F}_p), \{A_p^4, B_p^4\})$ is at least $C \log p$ we argue like in the proof of Lemma 3.7 and use at most a constant times Proposition 4.9(2) to get a set $S' = S^{O(\log p)}$ with $|S'| \geqslant |G|^{1-\delta}$ for some constant δ. Then applying the following result of Gowers to the subset S' (with the minimal degree of the non-trivial representation as chosen in [BGT11, Theorem 7.1]), we conclude that $(S')^3 = SL_3(\mathbb{F}_p)$, and, hence,

$$\operatorname{diam} Cay(SL_3(\mathbb{F}_p), \{A_p^4, B_p^4\}) \text{ is } O(\log p),$$

where the implied constant depends on a and b.

Proposition 4.10 (Gowers [Gow08], Lemma 5.1; cf. Nikolov–Pyber [NP11], Corollary 1)**.** *Let G be a group of order n, such that the minimal degree of a nontrivial representation is k. If A, B, C are three subsets of G such that $|A||B||C| > \frac{n^3}{k}$, then there is a triple $(a, b, c) \in A \times B \times C$ such that $ab = c$.*

Same argument as in the proof of Corollary 3.8 but using Theorem 4.4 and the preceding conclusion on the diameter gives the required result.

Corollary 4.11. *The sequence $Cay(SL_3(\mathbb{F}_p), \{A_p^4, B_p^4\})$ as $p \to \infty$ is large girth dg-bounded.*

5. Dimension $n \geqslant 4$

5.1. **Girth.** We first show the following proposition which deals with the case $n = 4$.

Proposition 5.1. *Let $A = \begin{pmatrix} 1 & a & 0 & 0 \\ 0 & 1 & a & 0 \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ b & 1 & 0 & 0 \\ 0 & b & 1 & 0 \\ 0 & 0 & b & 1 \end{pmatrix} \in SL_4(\mathbb{Z})$ with $a, b \geqslant 2$. Then $\forall l \geqslant 6$, $\langle A^l, B^l \rangle$ is a free subgroup in $SL_4(\mathbb{Z})$.*

Proof. In general,

$$A^k = \begin{pmatrix} 1 & \binom{k}{1}a & \binom{k}{2}a^2 & \binom{k}{3}a^3 \\ 0 & 1 & \binom{k}{1}a & \binom{k}{2}a^2 \\ 0 & 0 & 1 & \binom{k}{1}a \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where $\binom{k}{r}$ denotes the usual binomial coefficient.
Fix $l \geqslant 6$. Proceeding as in Proposition 4.1 we see that, for $r_i, s_i \in \mathbb{Z}\backslash\{0\}$, if

$$Z_i = (A^l)^{r_i}(B^l)^{s_i} = \begin{pmatrix} Z_{11_i}(a,b) & Z_{12_i}(a,b) & Z_{13_i}(a,b) & Z_{14_i}(a,b) \\ Z_{21_i}(a,b) & Z_{22_i}(a,b) & Z_{23_i}(a,b) & Z_{24_i}(a,b) \\ Z_{31_i}(a,b) & Z_{32_i}(a,b) & Z_{33_i}(a,b) & Z_{34_i}(a,b) \\ Z_{41_i}(a,b) & Z_{42_i}(a,b) & Z_{43_i}(a,b) & Z_{44_i}(a,b) \end{pmatrix},$$

then

$$\begin{pmatrix} Z_{11_i}(a,b) & Z_{12_i}(a,b) & Z_{13_i}(a,b) & Z_{14_i}(a,b) \\ Z_{21_i}(a,b) & Z_{22_i}(a,b) & Z_{23_i}(a,b) & Z_{24_i}(a,b) \\ Z_{31_i}(a,b) & Z_{32_i}(a,b) & Z_{33_i}(a,b) & Z_{34_i}(a,b) \\ Z_{41_i}(a,b) & Z_{42_i}(a,b) & Z_{43_i}(a,b) & Z_{44_i}(a,b) \end{pmatrix} = \begin{pmatrix} 1 & \binom{lr_i}{1}a & \binom{lr_i}{2}a^2 & \binom{lr_i}{3}a^3 \\ 0 & 1 & \binom{lr_i}{1}a & \binom{lr_i}{2}a^2 \\ 0 & 0 & 1 & \binom{lr_i}{1}a \\ 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ \binom{ls_i}{1}b & 1 & 0 & 0 \\ \binom{ls_i}{2}b^2 & \binom{ls_i}{1}b & 1 & 0 \\ \binom{ls_i}{3}b^3 & \binom{ls_i}{2}b^2 & \binom{ls_i}{1}b & 1 \end{pmatrix} =$$

$$\begin{pmatrix} \binom{lr_i}{3}\binom{ls_i}{3}a^3b^3 + \binom{lr_i}{2}\binom{ls_i}{2}a^2b^2 + \binom{lr_i}{1}\binom{ls_i}{1}ab + 1 & \binom{lr_i}{3}\binom{ls_i}{2}a^3b^2 + \binom{lr_i}{2}\binom{ls_i}{1}a^2b + \binom{lr_i}{1}a & \binom{lr_i}{3}\binom{ls_i}{1}a^3b + \binom{lr_i}{2}a^2 & \binom{lr_i}{3}a^3 \\ \binom{lr_i}{2}\binom{ls_i}{3}a^2b^3 + \binom{lr_i}{1}\binom{ls_i}{2}ab^2 + \binom{ls_i}{1}b & \binom{lr_i}{2}\binom{ls_i}{2}a^2b^2 + \binom{lr_i}{1}\binom{ls_i}{1}ab + 1 & \binom{lr_i}{2}\binom{ls_i}{1}a^2b + \binom{lr_i}{1}a & \binom{lr_i}{2}a^2 \\ \binom{lr_i}{1}\binom{ls_i}{3}ab^3 + \binom{ls_i}{2}b^2 & \binom{lr_i}{1}\binom{ls_i}{2}ab^2 + \binom{ls_i}{1}b & \binom{lr_i}{1}\binom{ls_i}{1}ab + 1 & \binom{lr_i}{1}a \\ \binom{ls_i}{3}b^3 & \binom{ls_i}{2}b^2 & \binom{ls_i}{1}b & 1 \end{pmatrix}$$

For $r_i, s_i \in \mathbb{Z}\backslash\{0\}, l \geqslant 6$ we have that the coefficient $\binom{lr_i}{3}\binom{ls_i}{3}$ of the highest degree term (a^3b^3) of $Z_{11_i}(a,b)$ is non-vanishing. We shall use this fact to show that arbitrary products of Z_i's are non-trivial group elements.

Claim 5.2. *$\forall k \in \mathbb{N}$, $\prod_{i=1}^{k} Z_i \neq \mathrm{id}$ in $SL_4(\mathbb{Z})$.*

Proof of claim. We argue by induction on k. Clearly in Z_1, we have

$$|Z_{11_1}| > |Z_{12_1}| + |Z_{13_1}| + |Z_{14_1}| + 1,$$

which is the basis of induction. Let the inequality hold for

$$Z = Z_1Z_2\cdots Z_k = \begin{pmatrix} Z_{11}(a,b) & Z_{12}(a,b) & Z_{13}(a,b) & Z_{14}(a,b) \\ Z_{21}(a,b) & Z_{22}(a,b) & Z_{23}(a,b) & Z_{24}(a,b) \\ Z_{31}(a,b) & Z_{32}(a,b) & Z_{33}(a,b) & Z_{34}(a,b) \\ Z_{41}(a,b) & Z_{42}(a,b) & Z_{43}(a,b) & Z_{44}(a,b) \end{pmatrix},$$

i.e., $|Z_{11}| > |Z_{12}| + |Z_{13}| + |Z_{14}| + 1$. Then for $Z' = Z \times Z_{k+1} = Z \times (A^l)^{r_{k+1}}(B^l)^{s_{k+1}}$ we have that

$$|Z'_{11}| > |Z'_{12}| + |Z'_{12}| + |Z'_{13}| + 1,$$

by the same argument as in the proof of Claim 4.2 in Proposition 4.1. □

This claim implies that $\forall k \in \mathbb{N}$, $T = \prod_{i=1}^{k} A^{lr_i}B^{ls_i}$ for $l \geqslant 6, r_i, s_i \in \mathbb{Z}\backslash\{0\}$ has the property that

$$|T_{11}| > |T_{12}| + |T_{13}| + |T_{14}| + 1.$$

Clearly, this implies that $T \neq B^s$ and $T \neq A^r$ for any $r, s \in \mathbb{Z}$. Note that A and B are of infinite order in $SL_4(\mathbb{Z})$. Thus, we have that $\langle A^l, B^l\rangle$ is a free subgroup of $SL_4(\mathbb{Z})$ for any $l \geqslant 6$. □

For an arbitrary $n \geqslant 4$, we have the following theorem

Theorem 5.3. *Let* $A = \begin{pmatrix} 1 & a & 0 & 0 & \dots & 0 \\ 0 & 1 & a & 0 & \dots & 0 \\ 0 & 0 & 1 & a & \dots & 0 \\ \vdots & & & & & \vdots \\ & & & & \dots & a \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$ *and* $B = \begin{pmatrix} 1 & 0 & 0 & \dots & & 0 \\ b & 1 & 0 & \dots & & 0 \\ 0 & b & 1 & \dots & & 0 \\ 0 & 0 & b & \dots & & 0 \\ \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b & 1 \end{pmatrix} \in SL_n(\mathbb{Z})$ *with* $a, b \geqslant 2$. *Then* $\langle A^l, B^l\rangle$ $\forall l \geqslant 3(n-1)$ *is a free subgroup of* $SL_n(\mathbb{Z})$.

Proof. Proceed as in the proof of Proposition 5.1 or see the Appendix (Section 7). □

Remark 5.4. A more refined analysis of the inequalities can show that $\langle A^l, B^l\rangle$, $\forall l > 2n$, is a free subgroup in $SL_n(\mathbb{Z})$, at the cost of making the proof longer. However, since we are interested in giving explicit examples of dg-bounded graphs of large girth, as long as we give some explicit constant $C(n) > 0$ (depending only on dimension n) such that $\langle A^l, B^l\rangle$, $\forall l \geqslant C(n)$, is a free subgroup in $SL_n(\mathbb{Z})$ we are done. By Theorem 5.3, $C(n) = 3(n-1)$ has this property.

Theorem 5.5. *Fix $n \geqslant 4, l \geqslant 3(n-1)$. There exists a constant $C > 0$ such that for all primes p we have* $\operatorname{girth} Cay(\langle A_p^l, B_p^l\rangle, \{A_p^l, B_p^l\}) \geqslant C \log p$.

Proof. By Theorem 5.3, $\{A^l, B^l\}$ generate a free subgroup in $SL_n(\mathbb{Z})$. It follows that a product

$$(A^l)^{r_1}(B^l)^{s_1}\cdots(A^l)^{r_k}(B^l)^{s_k}$$

can become identity in $SL_n(\mathbb{F}_p)$ only if the entry in the $(1,1)^{\text{th}}$ position of $(A^l)^{r_1}(B^l)^{s_1}\cdots(A^l)^{r_k}(B^l)^{s_k}$ is strictly larger than p (again, without loss of generality, $a, b \not\equiv 0(\operatorname{mod} p)$ and $a, b \not\equiv 1(\operatorname{mod} p)$). Arguing as in the proof of Theorem 4.4, we see that this term has order $O(a^{nk+1}b^{nk+1})$. It follows that there exists a constant C (independent of p) such that $k > C\log p$. Thus, the girth is at least $C \log p$. □

5.2. **Diameter.** To estimate the diameter we first show that there exist infinitely many numbers $l \in \mathbb{N}$ such that $\langle A_p^l, B_p^l\rangle = SL_n(\mathbb{F}_p)$ for all sufficiently large primes p and fixed n.

Fix a prime q with $n \equiv 1(\operatorname{mod} q)$. We have already seen that $\forall l \geqslant 3(n-1), \langle A^l, B^l\rangle$ is a free subgroup of $SL_n(\mathbb{Z})$, where as usual $a, b \geqslant 2$. We shall first reduce our matrices

$$A = \begin{pmatrix} 1 & a & 0 & 0 & \dots & 0 \\ 0 & 1 & a & 0 & \dots & 0 \\ 0 & 0 & 1 & a & \dots & 0 \\ \vdots & & & & & \vdots \\ & & & & \dots & a \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 & 0 & \dots & & 0 \\ b & 1 & 0 & \dots & & 0 \\ 0 & b & 1 & \dots & & 0 \\ 0 & 0 & b & \dots & & 0 \\ \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b & 1 \end{pmatrix} \in SL_n(\mathbb{Z})$$

to matrices

$$A_q = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 \\ \vdots & & & & & \vdots \\ & & & & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \text{ and } B_q = \begin{pmatrix} 1 & 0 & 0 & \dots & & 0 \\ 1 & 1 & 0 & \dots & & 0 \\ 0 & 1 & 1 & \dots & & 0 \\ 0 & 0 & 1 & \dots & & 0 \\ \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \end{pmatrix} \in SL_n(\mathbb{F}_q).$$

Obviously, $a, b \equiv 1(\operatorname{mod} q)$ ensures this. Moreover, keeping this values of a and b fixed, and using a classical result of Lucas, Theorem 5.6, we can guarantee that there are infinitely many powers l of A, B which reduce $\operatorname{mod} q$ to these same matrices in $SL_n(\mathbb{F}_q)$.

Theorem 5.6 (Lucas [Luc78])**.** *A binomial coefficient $\binom{\alpha}{\beta}$ is divisible by a prime q if and only if at least one of the base q digits of β is greater than the corresponding digit of α.*

We know that

$$A^k = \begin{pmatrix} 1 & \binom{k}{1}a & \binom{k}{2}a^2 & & \dots & \binom{k}{n-1}a^{n-1} \\ 0 & 1 & \binom{k}{1}a & \binom{k}{2}a^2 & \dots & \binom{k}{n-2}a^{n-2} \\ 0 & 0 & 1 & \binom{k}{1}a & \dots & \binom{k}{n-3}a^{n-3} \\ \vdots & & & & & \vdots \\ & & & & \dots & \binom{k}{1}a \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

We want the binomial coefficients $\binom{k}{i}$ $\forall 1 < i \leqslant n-1$ to be divisible by q. By Lucas' result, Theorem 5.6, a binomial coefficient $\binom{k}{i}$ is divisible by a prime q if and only if at least one of the base q digits of i is greater than the corresponding digit of k. So expressing $k = a_r q^r + \ldots + a_1 q + 1 \cdot q^0$ and the i's for $2 \leqslant i \leqslant n-1$ similarly we see that it is sufficient to choose k so that all the a_j's are 0 till the place where the base q representation of $n-1$ ends. For example, for $q = 2$ and $n = 7 = 2^2 + 2 + 1$ we can take k to be in $\{1, 2^3+1, 2^4+1, \ldots\}$. See Theorem 5.10 for more details.

Thus, we get the matrices

$$A_q = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 \\ \vdots & & & & & \vdots \\ & & & & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \text{ and } B_q = \begin{pmatrix} 1 & 0 & 0 & \dots & & 0 \\ 1 & 1 & 0 & \dots & & 0 \\ 0 & 1 & 1 & \dots & & 0 \\ 0 & 0 & 1 & \dots & & 0 \\ \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \end{pmatrix} \in SL_n(\mathbb{F}_q)$$

as images under $\bmod q$ reduction of matrices $\{A^k, B^k\}$ which in addition generate a free subgroup in $SL_n(\mathbb{Z})$ (if we choose k to be a sufficiently large power bigger than $3(n-1)$). The trick now is to show that these matrices $\{A_q, B_q\}$ generate $SL_n(\mathbb{F}_q)$. For all but $n = 4$ this fact follows from the following result (whose proof is non-constructive).

Theorem 5.7 (Gow-Tamburini [GT93])**.** *If $n \geqslant 2, n \neq 4$, then the above matrices A_q, B_q viewed as elements of $SL_n(\mathbb{Z})$ generate $SL_n(\mathbb{Z})$. When $n = 4$, they generate a subgroup of index 8 in $SL_4(\mathbb{Z})$.*

For infinitely many values of n in a suitable form (when n is of the form $q^t + 1, t \in \mathbb{N}$), we give a constructive proof of the required fact. Our arguments also handle the exceptional case $n = 4$ (because $4 = 3 + 1$), where Theorem 5.7 does not apply.

Proposition 5.8. *Let $n \geqslant 4$, fix a prime q with $n = q^t + 1$ and $t \in \mathbb{N}$. Let*

$$A' = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 \\ \vdots & & & & & \vdots \\ & & & & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \text{ and } B' = \begin{pmatrix} 1 & 0 & 0 & \dots & & 0 \\ 1 & 1 & 0 & \dots & & 0 \\ 0 & 1 & 1 & \dots & & 0 \\ 0 & 0 & 1 & \dots & & 0 \\ \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \end{pmatrix} \in SL_n(\mathbb{F}_q).$$

Then $\langle A', B' \rangle = SL_n(\mathbb{F}_q)$.

Proof. The prime q is fixed. We make all the operations in $\mathbb{F}_q$. Consider the matrices

$$A' = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 1 \\ 0 & \dots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } B' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 1 & 1 & 0 & 0 \\ 0 & \dots. & 0 & 0 & 1 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \in SL_{q^t+1}(\mathbb{F}_q).$$

Then

$$(B')^{q^t} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 0 \\ 1 & \dots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \langle A', B' \rangle.$$

We have

$$X = B'^{-1}A'(B')^{q^t}A'^{-1}B'A' \equiv \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \langle A', B' \rangle$$

$$\Rightarrow X_1 = A'X^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 1 \\ 0 & \dots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \langle A', B' \rangle.$$

Similarly,

$$Y_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots. & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \in \langle A', B' \rangle.$$

The matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ generate $SL_2(\mathbb{Z})$, hence we have

$$Y = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 & x & y \\ 0 & \dots & 0 & 0 & 0 & z & t \end{pmatrix} \in \langle A', B' \rangle, \forall x, y, z, t \text{ with } xt - yz \equiv 1 (\operatorname{mod} q).$$

This implies

$$A' \times Y = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 1 \\ 0 & \dots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 & x & y \\ 0 & \dots & 0 & 0 & 0 & z & t \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & x & y \\ 0 & \dots & 0 & 0 & 0 & x+z & t+y \\ 0 & \dots & 0 & 0 & 0 & z & t \end{pmatrix} \in \langle A', B' \rangle.$$

Choosing $x = 0, y = -1, t = 1, z = 1$ we have $xt - yz \equiv 1 (\operatorname{mod} q)$ we get

$$Z = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 0 & -1 \\ 0 & \dots & 0 & 0 & 0 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \in \langle A', B' \rangle, \text{ and hence } Y_1^{-1} Z = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 0 & -1 \\ 0 & \dots & 0 & 0 & 0 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \langle A', B' \rangle.$$

Also,

$$[X^{-1}, X_1^{-1}] = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 0 & 1 \\ 0 & \dots & 0 & 0 & 0 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \langle A', B' \rangle.$$

$$\text{Let } T = [X^{-1}, X_1^{-1}] Y_1^{-1} Z = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \langle A, B \rangle. \text{ Then,}$$

$$A' T^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 1 \\ 0 & \dots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \langle A', B' \rangle \implies X_1^{-1} A T^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & 0 & 0 & 1 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 1 & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \langle A', B' \rangle.$$

In such a way we get the standard elementary matrix $E_{i,i+1} \in \langle A', B' \rangle \, \forall 1 \leqslant i \leqslant n-1$. Now it is easy to see that we can get all the elementary matrices $E_{i,j}, 1 \leqslant i, j \leqslant n$ and since elementary matrices generate $SL_n(\mathbb{F}_q)$, we are done. □

Proposition 5.9. *Let $n \geqslant 2$ be any integer and let q be a prime with $n \equiv 1(\operatorname{mod} q)$. Let*

$$A' = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 \\ \vdots & & & & & \vdots \\ & & & & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \text{ and } B' = \begin{pmatrix} 1 & 0 & 0 & \dots & & 0 \\ 1 & 1 & 0 & \dots & & 0 \\ 0 & 1 & 1 & \dots & & 0 \\ 0 & 0 & 1 & \dots & & 0 \\ \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \end{pmatrix} \in SL_n(\mathbb{F}_q).$$

Then $\langle A', B' \rangle = SL_n(\mathbb{F}_q)$.

Proof. We apply Theorem 5.7 to A', B' over $\mathbb{Z}$ instead of $\mathbb{F}_q$. Then we do the $\operatorname{mod} q$ reduction $SL_n(\mathbb{Z}) \twoheadrightarrow SL_n(\mathbb{F}_q)$ and conclude by Proposition 5.8. □

Theorem 5.10. *For each integer $n \geqslant 4$, let q be a prime with $n \equiv 1(\operatorname{mod} q)$ and let*

$$A = \begin{pmatrix} 1 & a & 0 & 0 & \dots & 0 \\ 0 & 1 & a & 0 & \dots & 0 \\ 0 & 0 & 1 & a & \dots & 0 \\ \vdots & & & & & \vdots \\ & & & & & \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ b & 1 & 0 & \dots & 0 \\ 0 & b & 1 & \dots & 0 \\ \vdots & & & & \vdots \\ & & & & \\ 0 & 0 & \dots & b & 1 \end{pmatrix} \in SL_n(\mathbb{Z})$$

with $a, b \geqslant 2$ and $a, b \equiv 1(\bmod\ q)$. Then there exist constants $K = K(n, a, b), K_1 = K_1(n, a, b)$ such that for all primes $p > K$, the mod p *reduction of $S = \{(A^{q^{k+2}+1})^{\pm 1}, (B^{q^{k+2}+1})^{\pm 1}\}$ with $k \in \mathbb{N}$, $k \geqslant t$ with $t \in \mathbb{N}$ given by $q^t \leqslant n < q^{t+1}$, generate $SL_n(\mathbb{F}_p)$ and the diameter-by-girth ratio of the sequence of Cayley graphs $Cay(SL_n(\mathbb{F}_p), S)$ is less than K_1.*

Proof. The proof has two parts.

(1) Generation: For each integer $n \geqslant 4$, we are given a prime q with $n \equiv 1(\operatorname{mod} q)$, and the matrices A and B in $SL_n(\mathbb{Z})$. Let t denote the highest power of q in the base q representation of n. We would like to obtain the matrices

$$A_q = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 \\ \vdots & & & & & \vdots \\ & & & & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \text{ and } B_q = \begin{pmatrix} 1 & 0 & 0 & \dots & & 0 \\ 1 & 1 & 0 & \dots & & 0 \\ 0 & 1 & 1 & \dots & & 0 \\ 0 & 0 & 1 & \dots & & 0 \\ \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \end{pmatrix} \in SL_n(\mathbb{F}_q)$$

as words in A and B reduced modulo q. By Lucas result, Theorem 5.6, we see that

$$A^{rq^{(t+1)}+1}(\operatorname{mod} q) = A_q \text{ and } B^{rq^{(t+1)}+1}(\operatorname{mod} q) = B_q \text{ in } SL_n(\mathbb{F}_q)$$

for all integers r. By Proposition 5.9, it follows that the group generated by these matrices coincides with $SL_n(\mathbb{F}_q)$. By Proposition 4.7, we have $\langle A^{rq^{(t+1)}+1}, B^{rq^{(t+1)}+1} \rangle = SL_n(\mathbb{F}_p)$ for all positive integers r and all primes $p > K$, where K is a constant.

(2) Freeness: By Theorem 5.3, we know that $\langle A^l, B^l \rangle$ is free in $SL_n(\mathbb{Z})$ for all $l \geqslant 3(n-1)$. This implies that the girth of the corresponding sequence of Cayley graphs is at least $C_2 \log p$ for some constant $C_2 > 0$.

It remains to make sure that $rq^{t+1} + 1 \geqslant 3(n-1)$. If $q \geqslant 3$, then choosing r to be equal to positive powers of q gives us the required bound. For $q = 2$, choose $r = q^2$.

Since S generates a free subgroup in $SL_n(\mathbb{Z})$, by Proposition 4.9, the diameter of $SL_n(\mathbb{F}_p)$ with respect to the mod p reduction of generators from S is $\leqslant C_1 \log p$, where $C_1 > 0$ is a constant. We know already that the girth is at least $C_2 \log p$. Thus, the diameter-by-girth ratio is $\leqslant \frac{C_1}{C_2} = K_1$. □

Lemma 5.11 (Effectiveness of the constants). *The constants K, L, c_n and that of $O(\log p)$ term of Main Theorem are effective.*

Proof. The constants K and L are effective by recent works of Breuillard [Bre15, Theorem 2.3] and Golsefidy-Varjú [GV12, Appendix A], see our explanation following Proposition 4.7. The constant c_n is also effective, [Mar82, section 6]. For the constant in the $O(\log p)$ term of the upper bound on the diameter (let us call it d_n) we proceed as follows. Given a generating set $S = \{A_p^{\pm l}, B_p^{\pm l}\}$ of $G = SL_n(\mathbb{F}_p)$, using our results on the large girth of $Cay(SL_n(\mathbb{F}_p), \{A_p^l, B_p^l\})$, we have $|S^{\frac{c_n}{6}\log p}| \geqslant 3^{\frac{c_n}{6}\log p} = |G|^t$ for some $0 < t < 1$. Taking $A = S^{\frac{c_n}{6}\log p}$ and using a result of Pyber-Szabó [PS16, Theorem 2], applied to $SL_n(\mathbb{F}_p)$, we have

$$\text{either } |A^3| > |A|^{1+\epsilon(n)}, \text{ or } A^3 = G,$$

where $\epsilon(n)$ is effective. If we are in the former case then applying the above inequality k times we will fall into the latter case whenever k is large enough. It follows from $|A| \geqslant |G|^t$ and Proposition 4.10 that such a constant k is given by $t(1+\epsilon(n))^k = 99/100$. Since $\epsilon(n)$ is effective, we conclude that k, and hence $d_n = 3k$, are effective. □

Combining results proved throughout Sections 3–5, we obtain all the statements of our Main Theorem except expansion. As explained in Section 2, the fact that our graphs $\Gamma_p^{n,l}(a,b)$ as $p \to \infty$ are indeed expanders is a by-product of our results about freeness (for $n = 2$) and about freeness and generation mod p (for $n \geqslant 3$), using [BG08] and [BV12], respectively.

6. Further results and questions

In dimension $n \geqslant 3$, every free subgroup $\langle A^l, B^l\rangle$ from our Main Theorem is an explicit example of a *thin* matrix group which is, by definition, a finitely generated subgroup of $GL_n(\mathbb{Z})$ which is of infinite index in the $\mathbb{Z}$-points of its Zariski closure in GL_n. Indeed, it follows from our proof that the integral Zariski closure of $\langle A^l, B^l\rangle$ is $SL_n(\mathbb{Z})$, see Section 2. On the other hand, $\langle A^l, B^l\rangle$ is of infinite index in $SL_n(\mathbb{Z})$ because, for $n \geqslant 3$, $SL_n(\mathbb{Z})$ is not virtually free. For applications of thin matrix groups in many diophantine and geometric problems, see [Sar14] and references therein. For a recent characterization of thin matrix groups, see [LV17] and for a concise invitation and examples in dimension 2, 3 and 4, see [KLLR18]. Our Main Theorem gives infinitely many explicit examples of thin matrix groups in each dimension $n \geqslant 3$.

Corollary 6.1 ($2k$-regular logarithmic girth expanders). *Let $n \geqslant 2$ and $l \geqslant 1$ be as in III of Main Theorem. For every integer $k \geqslant 2$, there exist $S_1, \ldots, S_k \in \langle A^l, B^l\rangle$ such that the sequence of Cayley graphs $\Gamma_p^{n,l}(a,b;k) = Cay(SL_n(\mathbb{F}_p), \{(S_1)_p, \ldots, (S_k)_p\})$ as $p \to \infty$ is a $2k$-regular large girth dg-bounded graph. Moreover, it is a $2k$-regular logarithmic girth expander.*

Proof. For $k = 2$, we set $S_1 = A^l, S_2 = B^l$ since 4-regular graphs $\Gamma_p^{n,l}(a,b) = Cay(SL_n(\mathbb{F}_p), \{A_p^l, B_p^l\})$ as $p \to \infty$ from our Main theorem form such expander. For each $k \geqslant 3$, take a subgroup of index $k-1$ in $\langle A^l, B^l\rangle \leqslant SL_n(\mathbb{Z})$. Since $\langle A^l, B^l\rangle$ is free and Zariski dense, this subgroup is also free and Zariski dense. By Nielsen-Schreier formula [LS01, Ch.I, Prop.3.9], it has rank k. We denote the subgroup by F_k and its free generators by $S_1, \ldots, S_k$. The Cayley graph of F_k with respect to these free generators is $2k$-regular. By the Matthews-Vaserstein-Weisfeiler theorem [MVW84], for all sufficiently large prime numbers p, the mod p reduction of $S_1, \ldots, S_k$ generate the entire $SL_n(\mathbb{F}_p)$ as F_k is Zariski dense. Therefore, by same arguments as in the previous sections, we conclude that the diameter of $Cay(SL_n(\mathbb{F}_p), \{(S_1)_p, \ldots, (S_k)_p\})$ is $O(\log p)$ as F_k is free and the entire $SL_n(\mathbb{F}_p)$ is generated, its girth is logarithmic as F_k is free, and the sequence is an expander as $p \to \infty$ because F_k is Zariski dense. □

Up to a slight modification both in the formulation and in the proof of the preceding corollary, we obtain a large girth dg-bounded expander sequence of 2k-regular congruence quotients. Let $\ell \in \mathbb{Z}$ be an arbitrary integer and $SL_n(\mathbb{Z}) \twoheadrightarrow SL_n(\mathbb{Z}/\ell\mathbb{Z}) : S_i \mapsto (S_i)_\ell$ be the congruence surjection.

Corollary 6.2 ($2k$-regular logarithmic girth congruence quotients)**.** *Let $n \geqslant 2$ and $l \geqslant 1$ be as in III of Main Theorem. For every integer $k \geqslant 2$, there exist $S_1, \ldots, S_k \in \langle A^l, B^l\rangle$ such that the sequence of Cayley graphs $\Lambda_\ell^{n,l}(a,b;k) = Cay(\langle (S_1)_\ell, \ldots, (S_k)_\ell\rangle, \{(S_1)_\ell, \ldots, (S_k)_\ell\})$ as $\ell \to \infty$ is a $2k$-regular large girth dg-bounded graph. Moreover, it is a $2k$-regular logarithmic girth expander and there exists an integer ℓ_0 with $\langle (S_1)_\ell, \ldots, (S_k)_\ell\rangle = SL_n(\mathbb{Z}/\ell\mathbb{Z})$ if ℓ is coprime with ℓ_0.*

Proof. Let $S_1, \ldots, S_k$ be as in the proof of Corollary 6.1 so that $\langle S_1, \ldots, S_k\rangle \leqslant SL_n(\mathbb{Z})$ is free of rank k and Zariski dense. The logarithmic girth follows as previously from freeness, the expansion and the existence of ℓ_0 is by [BV12, Theorem 1]. For ℓ coprime with ℓ_0, the logarithmic upper estimates on the diameter, and hence, dg-boundedness of $\Lambda_\ell^{n,l}(a,b;k)$ follows from the expansion. For an arbitrary ℓ, when possibly $\langle (S_1)_\ell, \ldots, (S_k)_\ell\rangle < SL_n(\mathbb{Z}/\ell\mathbb{Z})$ is a proper subgroup, such estimates are immediate from expansion. □

The matrices $S_1, \ldots, S_k$ in Corollaries 6.1 and 6.2 can be given explicitly as concrete words in generators A^l and B^l (it is easy to produce generators of a finite index subgroup in a free group). However, in Corollary 6.2, algebraic features of a proper subgroup $\langle (S_1)_\ell, \ldots, (S_k)_\ell\rangle < SL_n(\mathbb{Z}/\ell\mathbb{Z})$ can vary and the subgroup itself is not so explicit, whence our use of expansion for diameter estimates in this case. However, we believe that a combination of our strategy with analysis of such Zariski dense subgroups from [BV12, Theorem 1] can yield the required estimates on the diameter with no use of expansion properties of the involved graphs.

Our graphs are in all dimensions $n \geqslant 2$ and clearly not isomorphic to each other whenever the dimensions are different. Moreover, we can make them distinct from the large-scale geometry point of view. Indeed, taking suitable subsequences in $\Gamma_p^{n,l}(a,b) = Cay(SL_n(\mathbb{F}_p), \{A_p^l, B_p^l\})$ as $p \to \infty$ yields graphs in distinct regular[3] equivalence classes; subsequences in a given dimension n or in distinct dimensions $n_1, \ldots, n_N$. Therefore, our large girth dg-bounded Cayley graphs of $SL_n(\mathbb{F}_p)$ as $p \to \infty$ viewed for each $n \geqslant 2$ over a suitable subsequence of primes are not coarsely equivalent to each other. These are the first such explicit examples in all dimensions.

Corollary 6.3 (regularly/coarsely distinct logarithmic girth expanders)**.** *Let $n, n_1, \ldots, n_N \geqslant 2$ arbitrary dimensions and $l \geqslant 1$ as in III of Main Theorem, $N \in \mathbb{N}$. Let $\mathbb{P}$ be the set of all primes.*

- *(i) There exists an infinite subset $P \subseteq \mathbb{P}$ such that for any infinite subsets $Q, Q' \subseteq P$ with $Q \setminus Q'$ infinite, there is no regular map from $\Gamma_p^{n,l}(a,b)$ as $p \to \infty$, $p \in Q$ to $\Gamma_p^{n,l}(a,b)$ as $p \to \infty$, $p \in Q'$.*
- *(ii) There exist infinite subsets $P_1, \ldots, P_N \subseteq \mathbb{P}$ such that for any infinite subsets $Q, Q' \subseteq \cup_{i=1}^N P_i$ with $Q \setminus Q'$ infinite, there is no regular map from $\Gamma_p^{n_i,l}(a,b)$ as $p \to \infty$, $p \in Q$ to $\Gamma_p^{n_j,l}(a,b)$ as $p \to \infty$, $p \in Q'$.*

Proof. (i) We choose $P \subseteq \mathbb{P}$ such that for each $p \in P$ and the next prime in the subsequence $q \in P$, we have girth $\Gamma_q^{n,l}(a,b) > |\Gamma_p^{n,l}(a,b)|$ and $|\Gamma_q^{n,l}(a,b)|/|\Gamma_p^{n,l}(a,b)| \to \infty$ as $p \to \infty$. This is possible as the graph is large girth. Then the statement is immediate by Theorem 2.8 of [Hum17] applied to $\Gamma_p^{n,l}(a,b)$ as $p \to \infty, p \in P$. This yields $2^{\aleph_0}$ regular equivalence classes of large girth dg-bounded expanders in each dimension n.

[3] A map between graphs is *regular* if it is Lipschitz and pre-images of vertices have uniformly bounded cardinality. Two graphs are *regularily equivalent* if there exist two regular maps: from one graph to the other, and back.

(ii) We take the union $\Gamma_p = \cup_{i=1}^{N} \Gamma_p^{n_i,l}(a,b)$ as $p \to \infty$, $p \in \cup_{i=1}^{N} \mathbb{P}$ of N sequences of our graphs in the chosen dimensions $n_1, \ldots, n_N$. Since the graphs are large girth and the assumptions on girth and cardinality required by [Hum17, Theorem 2.8] are transitive, we can choose the required infinite subsets $P_1, \ldots, P_N \subseteq \mathbb{P}$ successively for $n_1, \ldots, n_N$. □

There is much flexibility in the formulation of the preceding corollary. In particular, there are numerous choices for subsets $P, P_1, \ldots, P_N$ and parameters l, a, b can vary for distinct dimensions. The analogous result holds for graphs $\Gamma_p^{n,l}(a,b;k)$ and $\Lambda_\ell^{n,l}(a,b;k)$ defined in Corollaries 6.1 and 6.2.

The following question is highly intriguing. Again, $n \geqslant 2$ and $l \geqslant 1$ are as in III of Main Theorem. An expander is called a *super-expander* if it is an expander with respect to every super-reflexive Banach space [MN14]. In particular, such a graph does not coarsely embed into any uniformly convex Banach space.

Question 6.4 (super-expansion). *Is $\Gamma_p^{n,l}(a,b) = Cay(SL_n(\mathbb{F}_p), \{A_p^l, B_p^l\})$ as $p \to \infty$ a super-expander?*

This is open for $n = 2$ and $l = 1$, hence, also for Magulis' expander [Mar82]. Currently available super-expanders, produced using a strong Banach variant of Kazhdan's property (T) [Laf08, Laf09], an iterative zig-zag type combinatorial construction [MN14], or by means of warped cones, see e.g. [NS17], are all of finite girth. A positive answer to Question 6.4 for at least one choice of parameters n and l will allow, for instance, to build an infinite 'super monster' *group* (like that from [Gro03, AD08] but with respect to group actions on super-reflexive Banach spaces): a finitely generated group which does not admit a coarse embedding into any uniformly convex Banach space. This is of great interest in the context of the Novikov conjecture [KYu06].

Question 6.4 is a large girth counterpart of well-known question, for each $n \geqslant 3$, whether or not the sequence of congruence quotients $Cay(SL_n(\mathbb{Z}/\ell\mathbb{Z}), S_\ell)$, as $\ell \to \infty$ is a super-expander; S_ℓ denotes the canonical image of a finite generating set S of $SL_n(\mathbb{Z})$. However, for each $n \geqslant 3$, our expander $Cay(SL_n(\mathbb{F}_p), \{A_p^l, B_p^l\})$ as $p \to \infty$ is not coarsely equivalent to $Cay(SL_n(\mathbb{F}_p), S_p)$ as $p \to \infty$. Indeed, the sequence of marked finite groups $(SL_n(\mathbb{F}_p), S_p)$ as $p \to \infty$ converges to $(SL_n(\mathbb{Z}), S)$, then by [Kun16, Corollary 5], the sequence $Cay(SL_n(\mathbb{F}_p), S_p)$ as $p \to \infty$ is not coarsely embeddable into our sequence $Cay(SL_n(\mathbb{F}_p), \{A_p^l, B_p^l\})$ as $p \to \infty$. Therefore, a conjectural Banach property (T) of $SL_n(\mathbb{Z}), n \geqslant 3$ does not apply to conclude super-expansion of our expander (although, it would apply to the congruence quotients) and entirely new methods have to be designed in order to answer Question 6.4.

Since all three explicit constructions of large girth dg-bounded Cayley graphs, Margulis'[Mar82], Lubotzky-Phillips-Sarnak' [LPS88], and our's, happen to be expanders and, in addition, of logarithmic girth, in the next question we wonder if this is always the case. Restricting to Cayley graphs of finite quotients of a non Zariski dense subgroup of $SL_n(\mathbb{Z})$ or of $Sp_{2n}(\mathbb{Z})$ (cf. [LSTX17]), or of another algebraic group are interesting instances of this question.

Question 6.5 (large girth dg-bounded graphs with no expansion). *Does there exist a large girth dg-bounded graph made of $r \geqslant 3$ regular Cayley graphs that is not an expander? Moreover, with no weakly embedded expander? Furthermore, that is not a generalized expander?*

Our final question explores possible metric embeddings differences between random graph expanders and known explicit constructions of large girth dg-bounded expanders. We refer to [MN15] for the terminology and for the amazing results which yielded the question to us.

Question 6.6 (random vs explicit). *Does there exist a Hadamard space (M, d_M) such that $\Gamma_p^{n,l}(a,b) = Cay(SL_n(\mathbb{F}_p), \{A_p^l, B_p^l\})$ as $p \to \infty$ is an expander with respect to (M, d_M) yet a random regular graph is not expander with respect to (M, d_M)?*

The main outcome of [MN15] is a Hadamard space (N, d_N) and a sequence of 3-regular graphs $(\Lambda_n)_{n\in\mathbb{N}}$ that is an expander with respect to (N, d_N) yet a random regular graph is not an expander with respect to (N, d_N). The construction of graphs $(\Lambda_n)_{n\in\mathbb{N}}$ is by a zig-zag iteration and it is neither large girth nor made of Cayley graphs. The Hadamard space (N, d_N) is the Euclidean cone over a suitable large girth dg-bounded graph (obtained from a random regular graph by removing a portion of edges). If our graph $\Gamma_p^{n,l}(a, b)$ as $p \to \infty$ is expander with respect to this (N, d_N), then we have an affirmative answer to the preceding question. This would give the first large girth example of this kind versus the 'small girth' construction from [MN15]. In addition, a positive answer to the preceding question (with a Hadamard space (M, d_M) that differs from a Hilbert space and that is possibly not such a cone) would also allow us to apply the main result of [NS11] to our graphs and such a space (M, d_M). This would yield first examples of groups with strong fixed point properties on such (M, d_M): namely, finitely generated groups such that, almost surely, any of its isometric action on (M, d) has a common fixed point.

7. Appendix

For an interested reader, we give a detailed proof of Theorem 5.3.

Proof of Theorem 5.3. Fix $(n-1) = k \in \mathbb{N}$ and consider the matrix $A^{lr_i}B^{ls_i}$ with $l \geqslant 3k$ and $r_i, s_i \in \mathbb{Z}\backslash\{0\}$. Let $a, b \in \mathbb{N}$ with $a, b \geqslant 2$. Suppose

$$\mathcal{P}_i = A^{lr_i}B^{ls_i} = \begin{pmatrix} P_{11}(a,b) & P_{12}(a,b) & \dots & P_{1n}(a,b) \\ P_{21}(a,b) & P_{22}(a,b) & \dots & P_{2n}(a,b) \\ P_{31}(a,b) & P_{32}(a,b) & \dots & P_{3n}(a,b) \\ \vdots & & & \vdots \\ & & \dots & P_{(n-1)n}(a,b) \\ P_{n1}(a,b) & P_{n2}(a,b) & \dots & P_{nn}(a,b) \end{pmatrix} \in SL_n(\mathbb{Z}),$$

where the polynomials $P_{uv}(a, b), 1 \leqslant u, v \leqslant n$ satisfy

- $P_{11}(a,b) = \binom{lr_i}{k}\binom{ls_i}{k}a^k b^k + \binom{lr_i}{k-1}\binom{ls_i}{k-1}a^{k-1}b^{k-1} + \dots + \binom{lr_i}{3}\binom{ls_i}{3}a^3b^3 + \binom{lr_i}{2}\binom{ls_i}{2}a^2b^2 + \binom{lr_i}{1}\binom{ls_i}{1}ab + 1$
- $P_{12}(a,b) = \binom{lr_i}{k}\binom{ls_i}{k-1}a^k b^{k-1} + \binom{lr_i}{k-1}\binom{ls_i}{k-2}a^{k-1}b^{k-2} + \dots + \binom{lr_i}{3}\binom{ls_i}{2}a^3b^2 + \binom{lr_i}{2}\binom{ls_i}{1}a^2b^1 + \binom{lr_i}{1}a$

  $\dots$

  and in general
- $P_{uv}(a,b) = \Sigma_{u'=u,v'=v}^{u'=k+2-v,v'=k+1}\binom{lr_i}{k-u'+1}\binom{ls_i}{k-v'+1}a^{k-u'+1}b^{k-v'+1}$ with $u \leqslant v$
- $P_{uv}(a,b) = \Sigma_{u'=u,v'=v}^{u'=k+1,v'=k+2-u}\binom{lr_i}{k-u+1}\binom{ls_i}{k-v+1}a^{k-u'+1}b^{k-v'+1}$ with $u > v$

  $\dots$
- $P_{nn}(a,b) = 1$

Then we have the following inequalities for $l \geqslant 3k$

(1) $1 - \frac{1}{15} \leqslant \frac{P_{11}(a,b)}{\binom{lr_i}{k}\binom{ls_i}{k}a^k b^k} \leqslant 1 + \frac{1}{15}$

(2) $|\frac{P_{12}(a,b)}{\binom{lr_i}{k}\binom{ls_i}{k}a^k b^k}| \leqslant \frac{1}{4}(1 + \frac{1}{4^2} + \frac{1}{4^4} + \dots + \frac{1}{4^{2k-2}}) < \frac{1}{4}.\frac{16}{15}$

$\dots$

and in general

(3) $|\frac{P_{uv}(a,b)}{\binom{lr_i}{k}\binom{ls_i}{k}a^k b^k}| \leqslant \frac{1}{4^{u+v-2}}.\frac{16}{15}\ \forall uv > 1$

We proceed as in the $n = 4$ case and consider

$$Z = \prod_{i=1}^{t}\mathcal{P}_i = \prod_{i=1}^{t}A^{lr_i}B^{ls_i}, \text{ for some } t \in \mathbb{N}, r_i, s_i \in \mathbb{Z}\backslash\{0\}.$$

We shall show, by induction, that $|z_{11}| > |z_{12}| + ... + |z_{1n}| + 1$, where the $z_{ij}, 1 \leqslant i, j \leqslant n$ denote the elements of the matrix Z.
From the above inequalities it is clear that $\Sigma_{v=2}^{n} |\frac{P_{1v}(a,b)}{\binom{lr_i}{k}\binom{ls_i}{k} a^k b^k}| < \frac{1}{2}$ which means

$$\frac{1}{\binom{lr_i}{k}\binom{ls_i}{k} a^k b^k} + \Sigma_{v=2}^{n} \left| \frac{P_{1v}(a,b)}{\binom{lr_i}{k}\binom{ls_i}{k} a^k b^k} \right| < \frac{P_{11}(a,b)}{\binom{lr_i}{k}\binom{ls_i}{k} a^k b^k}$$

and in turn implies that the inductive assumption (basis of induction) holds.
For the main step of the induction suppose we are already given

$$Z = \begin{pmatrix} z_{11} & z_{12} & \cdots & z_{1n} \\ z_{21} & z_{22} & \cdots & z_{2n} \\ \vdots & \vdots & & \vdots \\ z_{n1} & z_{n2} & \cdots & z_{nn} \end{pmatrix}$$

with $|z_{11}| > |z_{12}| + \cdots + |z_{1n}| + 1$.
Let

$$Z' = \begin{pmatrix} z'_{11} & z'_{12} & \cdots & z'_{1n} \\ z'_{21} & z'_{22} & \cdots & z'_{2n} \\ \vdots & \vdots & & \vdots \\ z'_{n1} & z'_{n2} & \cdots & z'_{nn} \end{pmatrix} = Z \times A^{lr_{t+1}} B^{ls_{t+1}}.$$

Expand the first row of Z', i.e., $z'_{1j}, 1 \leqslant j \leqslant n$ in terms of the first row of Z, $z_{1j}, 1 \leqslant j \leqslant n$ and the elements of the matrix $A^{lr_{t+1}} B^{ls_{t+1}}$. Then we can conclude by considering the inductive assumption $|z_{11}| > |z_{12}| + \cdots + |z_{1n}| + 1$ and the above inequalities for the matrix $A^{lr_{t+1}} B^{ls_{t+1}}$ that

$$|z'_{11}| > |z'_{12}| + \cdots + |z'_{1n}| + 1.$$

□

7.1. **Data availability.** Not applicable as the results presented in this manuscript rely on no external sources of data or code.

References

[AD08] G. Arzhantseva and T. Delzant, *Examples of random groups*, available on the authors' websites, 2008.

[AGS12] G. Arzhantseva, E. Guentner, and J. Špakula, *Coarse non-amenability and coarse embeddings*, Geom. Funct. Anal. **22** (2012), no. 1, 22–36.

[AT18] G. Arzhantseva and R. Tessera, *Admitting a coarse embedding is not preserved under group extensions*, Int. Math. Res. Not. IMRN 2019, no. 20, 6480–6498.

[Big98] N. Biggs, *Constructions for cubic graphs with large girth*, Electron. J. Combin. **5** (1998), Article 1, 25 pp.

[BG08] J. Bourgain and A. Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math. (2) **167** (2008), no. 2, 625–642.

[BV12] J. Bourgain and P. P. Varjú, *Expansion in* $SL_d(\mathbf{Z}/q\mathbf{Z})$, *q arbitrary*, Invent. Math. **188** (2012), no. 1, 151–173.

[Bre15] E. Breuillard, *Approximate subgroups and super-strong approximation*, Groups St Andrews 2013, London Math. Soc. Lecture Note Ser., vol. 422, Cambridge Univ. Press, Cambridge, 2015, pp. 1–50.

[BGT11] E. Breuillard, B. Green, and T. Tao, *Approximate subgroups of linear groups*, Geom. Funct. Anal. **21** (2011), no. 4, 774–819.

[Bro86] R. Brooks, *The spectral geometry of a tower of coverings*, J. Diff. Geometry **23** (1986), 97–107.

[Bur86] M. Burger, *Petites valeurs propres du Laplacien et topologie de Fell*, doctoral thesis (1986), Econom Druck AG (Basel).

[DSV03] G. Davidoff, P. Sarnak, A. Valette, *Elementary number theory, group theory, and Ramanujan graphs*, London Mathematical Society Student Texts, 55. Cambridge University Press, Cambridge, 2003.

[ES63] P. Erdős and H. Sachs, *Reguläre Graphen gegebener Taillenweite mit minimaler Knotenzahlare Graphen gegebener Taillenweite mit minimaler Knotenzahl*, Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg Math.-Natur. Reihe **12** (1963), 251–257.

[GV12] A. S. Golsefidy and P. P. Varjú, *Expansion in perfect groups*, Geom. Funct. Anal. **22** (2012), no. 6, 1832–1891.

[GT93] R. Gow and M. C. Tamburini, *Generation of* $\mathrm{SL}(n, \mathbf{Z})$ *by a Jordan unipotent matrix and its transpose*, Linear Algebra Appl. **181** (1993), 63–71.

[Gow08] W. T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. **17** (2008), no. 3, 363–387.

[Gro03] M. Gromov, *Random walk in random groups*, Geom. Funct. Anal. **13** (2003), no. 1, 73–146.

[Hel08] H. A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) **167** (2008), no. 2, 601–623.

[HLS02] N. Higson, V. Lafforgue, and G. Skandalis, *Counterexamples to the Baum-Connes conjecture*, Geom. Funct. Anal. **12** (2002), no. 2, 330–354.

[Hum17] D. Hume, *A continuum of expanders*, Fund. Math. **238** (2017), no. 2, 143–152.

[KYu06] G. Kasparov, G. Yu, *The coarse geometric Novikov conjecture and uniform convexity*, Adv. Math., 206 (2006), 1–56.

[KLLR18] A. Kontorovich, D. D. Long, A. Lubotzky, A.W. Reid, *What Is ... A Thin Group?*, Notices Amer. Math. Soc. **66** (2019), no. 6, 905–910.

[Kun16] G. Kun, *On sofic approximations of property (T) groups*, (2016), arxiv:1606.04471.

[Laf08] V. Lafforgue, *Un renforcement de la propriété (T)*, Duke Math. J. **143** (2008), no. 3, 559–602.

[Laf09] V. Lafforgue, *Propriété (T) renforcée banachique et transformation de Fourier rapide*, J. Topol. Anal. **1** (2009), no. 3, 191–206.

[LSTX17] A. Landesman, A. Swaminathan, J. Tao, Y. Xu, *Lifting subgroups of symplectic groups over* $\mathbb{Z}/\ell\mathbb{Z}$, Res. Number Theory **3** (2017), Art. 14, 12 pp.

[Lar03] M. Larsen, *Navigating the Cayley graph of* $SL_2(\mathbb{F}_p)$, Int. Math. Res. Not. 2003, no. 27, 1465–1471.

[Lub99] A. Lubotzky, *One for almost all: generation of* $\mathrm{SL}(n,p)$ *by subsets of* $\mathrm{SL}(n, \mathbf{Z})$, Algebra, K-theory, groups, and education (New York, 1997), Contemp. Math., vol. 243, Amer. Math. Soc., Providence, RI, 1999, pp. 125–128.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), no. 3, 261–277.

[LV17] A. Lubotzky, T.N. Venkataramana, *The congruence topology, Grothendieck duality and thin groups*, Algebra Number Theory **13** (2019), no. 6, 1281–1298.

[Luc78] E. Lucas, *Theorie des Fonctions Numeriques Simplement Periodiques*, Amer. J. Math. **1** (1878), no. 2, 184–196.

[LS01] R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Classics in Mathematics, Springer-Verlag, Berlin, 2001, Reprint of the 1977 edition.

[Mar82] G. A. Margulis, *Explicit constructions of graphs without short cycles and low density codes*, Combinatorica **2** (1982), no. 1, 71–78.

[MVW84] C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler, *Congruence properties of Zariski-dense subgroups. I*, Proc. London Math. Soc. (3) **48** (1984), no. 3, 514–532.

[MN14] M. Mendel, A. Naor, *Nonlinear spectral calculus and super-expanders*, Publ. Math. Inst. Hautes Études Sci. **119** (2014), 1–95.

[MN15] M. Mendel, A. Naor, *Expanders with respect to Hadamard spaces and random graphs*, Duke Math. J. **164** (2015), no. 8, 1471–1548.

[NS11] A. Naor, L. Silberman, *Poincarë inequalities, embeddings, and wild groups*, Compos. Math. **147** (2011), no. 5, 1546–1572.

[NP11] N. Nikolov and L. Pyber, *Product decompositions of quasirandom groups and a Jordan type theorem*, J. Eur. Math. Soc. (JEMS) **13** (2011), no. 4, 1063–1077.

[N87] M.V. Nori. *On subgroups of* $GL_n(\mathbb{F}_p)$, Inventiones Mathematicae, **88** (1987), 257–275.

[NS17] P. Nowak, D. Sawicki, *Warped cones and spectral gaps*, Proc. Amer. Math. Soc. **145** (2017), no. 2, 817–823.

[Ost12] M. I. Ostrovskii, *Low-distortion embeddings of graphs with large girth*, J. Funct. Anal. **262** (2012), no. 8, 3548–3555.

[PS16] L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type*, J. Amer. Math. Soc. **29** (2016), no. 1, 95–146.

[Sac63] H. Sachs, *Regular graphs with given girth and restricted circuits*, J. London Math. Soc. **38** (1963), 423–429.

[Sar14] P. Sarnak, *Notes on thin matrix groups*, Thin groups and superstrong approximation, 343–362, Math. Sci. Res. Inst. Publ., 61, Cambridge Univ. Press, Cambridge, 2014.

[Sel65] A. Selberg, *On the estimation of Fourier coefficients of modular forms*, 1965 Proc. Sympos. Pure Math., Vol. VIII pp. 1–15 Amer. Math. Soc., Providence, R.I.

[W91] T. Weigel, *On the profinite completion of arithmetic groups of split type*, Lois d'algèbres et variétés algébriques (Colmar, 1991), 79–101. Travaux en Cours, 50, Hermann, Paris, 1996.

Universität Wien, Fakultät für Mathematik, Oskar-Morgenstern-Platz 1, 1090 Wien, Austria.
Email address: goulnara.arzhantseva@univie.ac.at

Universität Wien, Fakultät für Mathematik, Oskar-Morgenstern-Platz 1, 1090 Wien, Austria
Current address: Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, DK-2100 Copenhagen, Denmark
Email address: arindam.biswas@univie.ac.at; ab@math.ku.dk