On arithmetic properties of solvable Baumslag-Solitar groups

Laurent Hayez∗
Université de Neuchâtel, Switzerland
laurent.hayez@unine.ch

Tom Kaiser
Université de Neuchâtel, Switzerland
tomkaiser456@gmail.com

Alain Valette
Université de Neuchâtel, Switzerland
alain.valette@unine.ch

For $0 < \alpha \leq 1$, we say that a sequence $(X_k)_{k>0}$ of $d$-regular graphs has property $D_\alpha$ if there exists a constant $C > 0$ such that $\text{diam}(X_k) \geq C \cdot |X_k|^{\alpha}$. We investigate property $D_\alpha$ for arithmetic box spaces of the solvable Baumslag-Solitar groups $BS(1,m)$ (with $m \geq 2$): those are box spaces obtained by embedding $BS(1,m)$ into the upper triangular matrices in $GL_2(\mathbb{Z}[1/m])$ and intersecting with a family $M_{N_k}$ of congruence subgroups of $GL_2(\mathbb{Z}[1/m])$, where the levels $N_k$ are coprime with $m$ and $N_k | N_{k+1}$. We prove:

• if an arithmetic box space has $D_\alpha$, then $\alpha \leq \frac{1}{2}$;
• if the family $(N_k)_k$ of levels is supported on finitely many primes, the corresponding arithmetic box space has $D_{1/2}$;
• if the family $(N_k)_k$ of levels is supported on a family of primes with positive analytic primitive density, then the corresponding arithmetic box space does not have $D_\alpha$, for every $\alpha > 0$.

Moreover, we prove that if we embed $BS(1, m)$ in the group of invertible upper-triangular matrices $T_n(\mathbb{Z}[1/m])$, then every finite index subgroup of the embedding contains a congruence subgroup. This is a version of the congruence subgroup property (CSP).

1 INTRODUCTION

Let $G$ be a finitely generated, residually finite group. If $(H_k)_{k>0}$ is a decreasing sequence of finite index normal subgroups of $G$, with trivial intersection, and $S$ is a finite generating set of $G$, then the box space $\Box(H_k)G$ is the disjoint union of finite Cayley graphs

$$\Box(H_k)G = \bigsqcup_{k>0} \text{Cay}(G/H_k, S);$$

here by abuse of notation we identify $S$ with its image in $G/H_k$. Changing the generating set $S$ does not change the coarse geometry of the box space\footnote{In the sense that the two families of graphs are quasi-isometrically equivalent, by a family of quasi-isometries with uniform constants.} so we omit $S$ from the notation.

In the dictionary between group-theoretical properties of $G$ and metric properties of $\Box(H_k)G$ (see e.g. [7]), it is natural to look at the behaviour of the diameter of the Cayley graphs $\text{Cay}(G/H_k, S)$. Let $0 < \alpha \leq 1$. The box space $\Box(H_k)G$ satisfies property $D_\alpha$ if there is some constant $C > 0$ such that for every $k > 0$:

$$\text{diam}(\text{Cay}(G/H_k, S)) \geq C |G/H_k|^{\alpha}. \quad (1)$$

Note that property $D_\alpha$ is a coarse geometry invariant of the box space. The following is known.

Theorem 1.1. Let $G$ be a finitely generated, residually finite group.

(1) (see Cor. 1.7 and Lemma 5.1 in [1]) If some box space of $G$ has property $D_\alpha$, for some $\alpha > 0$, then $G$ virtually maps onto $\mathbb{Z}$.

∗Supported by grant 200021_188578 of the Swiss National Fund for Scientific Research
(2) (see Theorem 3 in [8]) If $G$ maps onto $\mathbb{Z}$, then for every $0 < \alpha < 1$, there exists a box space of $G$ with property $D_\alpha$.

(3) (see Proposition 5 in [8]) The group $G$ is virtually cyclic if and only if some (hence any) box space of $G$ has property $D_1$.

This paper considers the Baumslag-Solitar groups $BS(n, m)$ $(m, n > 0)$ with presentation

$$BS(n, m) = \langle a, t | ta^n t^{-1} = t^m \rangle.$$  

They all map onto $\mathbb{Z}$, by $a \mapsto 0, t \mapsto 1$. On the other hand they are known to be residually finite if and only if $n = 1$ or $n = m$: see Theorem C in [10]. It turns out that the solvable Baumslag-Solitar groups $BS(1, m)$, with $m \geq 2$, have interesting box spaces. Indeed it is well-known that $BS(1, m)$ may be viewed as a semi-direct product

$$BS(1, m) = \mathbb{Z}[1/m] \rtimes \mathbb{Z},$$

where the factor $\mathbb{Z}$ corresponds to the subgroup $\langle t \rangle$ acting by powers of $m$. We may identify this semi-direct product with the following subgroup $G_m$ of upper triangular matrices in $GL_2(\mathbb{Z}[1/m])$:

$$G_m = \left\{ \begin{pmatrix} m^k & r \\ 0 & 1 \end{pmatrix} : k \in \mathbb{Z}, r \in \mathbb{Z}[1/m] \right\}.$$  

The isomorphism is obtained by mapping $a$ to $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $t$ to $T = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$. The associated embedding of $BS(1, m)$ into $GL_2(\mathbb{Z}[1/m])$ is called the standard embedding.

In $GL_n(\mathbb{Z}[1/m])$ we may define congruence subgroups. Let $N > 0$ be coprime with $m$. The principal congruence subgroup of level $N$ is the kernel $M_N$ of the reduction modulo $N$:

$$M_N = \ker [GL_n(\mathbb{Z}[1/m]) \rightarrow GL_n(\mathbb{Z}/N\mathbb{Z})].$$

**Definition 1.2.** If $G$ is any subgroup of $GL_n(\mathbb{Z}[1/m])$, and $N > 0$ is coprime to $m$, then the congruence subgroup $G(N)$ in $G$ is

$$G(N) := G \cap M_N.$$  

For a sequence of integers such that each one divides the next one, one obtains a sequence of nested congruence subgroups, and thus a box space of $BS(1, m)$. Such box spaces deserve to be called arithmetic box spaces. We will study property $D_\alpha$ for the arithmetic box spaces of $BS(1, m)$ through the standard embedding. From Theorem 1.1, we know that for every $0 < \alpha < 1$, there exists a box space of $BS(1, m)$ with property $D_\alpha$, but what about arithmetic box spaces? We will prove that box spaces with $D_\alpha$, for $\alpha > \frac{1}{2}$, can be distinguished from arithmetic box spaces by coarse geometry. More precisely:

**Theorem 1.3.** For any $m \geq 2$, the following statements are true:

1. If an arithmetic box space $\Box(G_m(N_k))$, $G_m$ has property $D_\alpha$, then $\alpha \leq \frac{1}{2}$.
2. There exists an arithmetic box space with property $D_{1/2}$.
3. There exists an arithmetic box space of $G_m$ without property $D_\alpha$ for any $\alpha \in ]0, 1/2]$.

If $\Box(H_k), G$ are two box spaces of the same residually finite group $G$, we say that $\Box(H'_k)G$ covers $\Box(H_k)G$ if $H'_k \subset H_k$ for every $k > 0$. In this case $\text{Cay}(G/H'_k, S)$ is a Galois covering of $\text{Cay}(G/H_k, S)$.

The following proposition bridges Theorem 1.3 with part (2) of Theorem 1.1.

**Proposition 1.4.** Fix $\alpha < 1$. Any arithmetic box space of $G_m$ is covered by some box space with $D_\alpha$.  


In addition, we study how property $D_\alpha$ for an arithmetic box space depends on the prime factors of the $N$’s in the sequence of congruence subgroups $(M_N)_N$. In fact, if we denote by $D'(P)$ the analytic density of the prime factors (see Section 3.2), we prove the following.

**Theorem 1.5.** Let $\square_{(G_m(N_k))_k} G_m$ be an arithmetic box space, and let $P$ be the set of prime factors of the sequence $(N_k)_k$.

1. If $|P| < +\infty$, then $\square_{(G_m(N_k))_k} G_m$ has $D_{1/2}$;
2. If $D'(P) > 0$, then $\square_{(G_m(N_k))_k} G_m$ does not have $D_\alpha$, for every $\alpha > 0$.

Of course the choice of the standard embedding raises a natural question: how do the congruence subgroups in $BS(1,m)$ depend on the choice of the embedding $\rho$? Since congruence subgroups have finite index, this is related to a form of the **congruence subgroup property** (CSP), which we now recall.

**Definition 1.6.** Let $G$ be a subgroup of $GL_n(\mathbb{Z}[1/m])$. We say that $G$ has the CSP if every finite index subgroup in $G$ contains $G(N)$ for some $N > 0$.

Let $T_n(\mathbb{Z}[1/m])$ denote the group of upper triangular matrices in $GL_n(\mathbb{Z}[1/m])$. We shall prove:

**Theorem 1.7.** For every embedding $\rho : BS(1, m) \rightarrow T_n(\mathbb{Z}[1/m])$, the group $\rho(BS(1, m))$ has the CSP.

This result can be reformulated as follows. Taking the congruence subgroups $\rho(G_m)(N)$ as a neighbourhood basis for the identity gives a topology on $\rho(G_m)$ (namely the congruence topology relative to $\rho$) and the completion $\hat{\rho(G_m)}$ with respect to this topology is a profinite group called the congruence completion of $\rho(G_m)$. As $G_m$ is residually finite, it also embeds in its profinite completion $\hat{G_m}$ which maps onto $\hat{\rho(G_m)}$. The CSP for $\rho(G_m)$ says that the map $\hat{G_m} \rightarrow \hat{\rho(G_m)}$ is an isomorphism.

Another immediate consequence of CSP is that, if $\rho : G_m \rightarrow T_n(\mathbb{Z}[1/m])$ is an embedding, then any box space of $G_m \approx \rho(G_m)$ is covered by some arithmetic box space of $\rho(G_m)$.

When $m = p^t$ is a prime power, we also propose another approach to CSP for $BS(1, m)$: we view $BS(1, p^t)$ as a subgroup of the affine group $\mathbb{G}(\mathbb{Q})$, and this subgroup is commensurable to the group $\mathbb{G}(O_S)$ of $S$-integer points, with $S = \{p, \infty\}$. We prove:

**Proposition 1.8.** Let $H$ be a $\mathbb{Q}$-algebraic subgroup of $GL_n$, and let $\rho : \mathbb{G} \rightarrow H$ be a $\mathbb{Q}$-isomorphism. Then $\rho(BS(1, p^t))$ has CSP.

As for the structure of the paper, we will start in Section 2 by recalling some well-known facts about elementary number theory, especially concerning the multiplicative order of $m$ in $\mathbb{Z}/N\mathbb{Z}$.

We then study property $D_\alpha$ for solvable Baumslag-Solitar groups in Section 3. We begin with some metric aspects, where we estimate the diameter of the arithmetic box spaces of $BS(1, m)$, which is what we use to prove Theorem 1.3 and Proposition 1 (see Theorem 3.6). To conclude Section 3, we investigate the role of prime numbers in property $D_\alpha$ and we prove Theorem 1.5 (see Theorem 3.8).

Finally, in Section 4, we prove Theorem 1.7.

We will use Landau’s notations $O, o, \Omega, \Theta$.

## 2 SOME ELEMENTARY NUMBER THEORY

We gather some technical lemmas. First we recall some facts about greatest common divisors and lowest common multiples, which will be respectively denoted by $\gcd$ and $\lcm$.

**Proposition 2.1.** Let $\mu, a_1, \ldots, a_n \in \mathbb{N}^*$,
(1) \(\gcd(\mu \cdot a_1, \mu \cdot a_2) = \mu \cdot \gcd(a_1, a_2)\),
(2) \(\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n)\),
(3) \(\gcd(a_1, \gcd(a_2, a_3)) = \gcd(\gcd(a_1, a_2), a_3)\),
(4) \(\gcd(a_1, a_2) \cdot \lcm(a_1, a_2) = a_1 \cdot a_2\),
(5) \(\lcm(a_1, \ldots, a_n) = \lcm(\lcm(a_1, \ldots, a_{n-1}), a_n)\). \(\square\)

The following lemma generalises Proposition 2.1.(4).

**Lemma 2.2.** Let \(a_1, \ldots, a_n \in \mathbb{N}\), then

\[
\lcm(a_1, \ldots, a_n) = \frac{a_1 \cdots a_n}{\gcd(a_1 \cdots a_{n-1}, a_1 \cdots a_{n-2}a_n, \ldots, a_2 \cdots a_n)}.
\]

**Proof.** We use induction to show that Eq. (2) is valid. If \(n = 1\), the formula holds. Thus assume that the formula is true for \(n \in \mathbb{N}\), and denote by \(\Pi_n\) the set \(\{a_1 \cdots a_{n-1}, a_1 \cdots a_{n-2}a_n, \ldots, a_2 \cdots a_n\}\). Using that

\[
\gcd(\lcm(a_1, \ldots, a_n), a_{n+1}) = \gcd\left(\frac{a_1 \cdots a_n}{\gcd(\Pi_n)}, a_{n+1}\right),
\]

we obtain by a direct computation that

\[
\lcm(a_1, \ldots, a_{n+1}) = \lcm(\lcm(a_1, \ldots, a_n), a_{n+1})
= \frac{\lcm(a_1, \ldots, a_n \cdot a_{n+1})}{\gcd(\lcm(a_1, \ldots, a_n), a_{n+1})},
= \frac{a_1 \cdots a_n}{\gcd(\Pi_n) \gcd\left(\frac{a_1 \cdots a_n}{\gcd(\Pi_n)}, a_{n+1}\right)}
= \frac{a_1 \cdots a_{n+1}}{\gcd(a_1 \cdots a_n, \gcd(\Pi_n) \cdot a_{n+1})}
= \frac{a_1 \cdots a_{n+1}}{\gcd(a_1 \cdots a_n, \gcd(a_1a_3 \cdots a_{n+1}a_{n+1}, \ldots, a_2a_4 \cdots a_{n+1}) \cdot a_{n+1})}
= \frac{a_1 \cdots a_{n+1}}{\gcd(a_1 \cdots a_n, a_1a_3 \cdots a_{n+1}a_{n+1}, \ldots, a_2a_4 \cdots a_{n+1})}.
\(\square\)

We now recall the ideal structure of the ring \(\mathbb{Z}[1/m]\).

**Lemma 2.3.** Let \(I\) be a proper subgroup in \(\mathbb{Z}[1/m]\). TFAE:

1. \(I\) is an ideal in \(\mathbb{Z}[1/m]\);
2. There exists \(N > 1\) such that \(I = N\mathbb{Z}[1/m]\).

Moreover \(\mathbb{Z}[1/m]/N\mathbb{Z}[1/m] = \mathbb{Z}/N\mathbb{Z}\).

**Proof.** The non-trivial direction follows from general results about localisations of rings, viewing \(\mathbb{Z}[1/m]\) as the localisation of \(\mathbb{Z}\) with respect to powers of \(m\): the map \(I \rightarrow I \cap \mathbb{Z}\) provides a bijection between ideals of \(\mathbb{Z}[1/m]\) and ideals \(J\) in \(\mathbb{Z}\) such that \(m\) is not a zero-divisor in \(\mathbb{Z}/J\) (see Proposition 2 in section 11.3 of [4]). Finally observing that \(\mathbb{Z} + N\mathbb{Z}[1/m] = \mathbb{Z}[1/m]\), we have by a classical isomorphism theorem:

\[
\mathbb{Z}[1/m]/N\mathbb{Z}[1/m] = (\mathbb{Z} + N\mathbb{Z}[1/m])/N\mathbb{Z}[1/m] = \mathbb{Z}/(\mathbb{Z} \cap N\mathbb{Z}[1/m]) = \mathbb{Z}/N\mathbb{Z}.
\(\square\)

Lemma 2.3 allows us to work with \(\mathbb{Z}/N\mathbb{Z}\), which has a familiar ring structure. We will write \(\mathbb{Z}/N\mathbb{Z}^\times\) for the multiplicative group of \(\mathbb{Z}/N\mathbb{Z}\). We denote by \(\text{ord}_m(N)\) the multiplicative order of \(m\) in \(\mathbb{Z}/N\mathbb{Z}^\times\). We define the following function.
**Definition 2.4.** Let \( m, N \in \mathbb{N} \) be such that \( \gcd(m, N) = 1 \). Write \( m^{\ord_m(N)} = \mu N + 1 \) for some \( \mu \in \mathbb{N} \) and let the function \( \eta_N : \mathbb{N}^* \to \mathbb{N} \) be defined by

\[
\eta_N(k) = \begin{cases} 
1 & \text{if } k = 1 \\
\frac{N^{k-1}}{\gcd(m, N)} & \text{if } k \geq 2.
\end{cases}
\]

**Lemma 2.5.** Let \( m, N \in \mathbb{N} \) be such that \( \gcd(m, N) = 1 \). Write \( m^{\ord_m(N)} = \mu N + 1 \) for some \( \mu \in \mathbb{N} \). Then \( \ord_m(N^2) = \ord_m(N) \cdot \frac{N}{\gcd(\mu, N)} \), and more generally

\[
\ord_m(N^k) = \ord_m(N) \cdot \eta_N(k), \quad \forall k \geq 1.
\]  

**Proof.** The case \( k = 1 \) being obvious, let us consider \( k = 2 \), and set \( \beta = \ord_m(N) \). We show that the smallest positive integer \( \lambda \) that satisfies \( m^\lambda \equiv 1 \pmod{N^2} \) is \( \lambda = \frac{N}{\gcd(\mu, N)} \beta \). Note that \( \beta \mid \lambda \): indeed if \( m^\lambda \equiv 1 \pmod{N^2} \), then \( m^\lambda \equiv 1 \pmod{N} \) so that \( \beta \) must divide \( \lambda \) (see [6, Cor. 2 p. 79]). Thus \( \lambda = \beta \hat{\lambda} \) for some \( \hat{\lambda} \in \mathbb{N} \) and we only have to show that \( \hat{\lambda} = \frac{N}{\gcd(\mu, N)} \). We have that

\[
(m^\beta)^{\hat{\lambda}} = (\mu N + 1)^{\hat{\lambda}}
\]

\[
= \sum_{i=0}^{\hat{\lambda}} \binom{\hat{\lambda}}{i} (\mu N)^i
\]

\[
\equiv 1 + \frac{\hat{\lambda}}{\beta} \mu N \pmod{N^2}.
\]

The last line shows that the smallest \( \hat{\lambda} \) we can take to have \( m^\beta \hat{\lambda} \equiv 1 \pmod{N^2} \) must be \( \hat{\lambda} = \frac{N}{\gcd(\mu, N)} \), thus demonstrating that \( \ord_m(N^2) = \beta \cdot \frac{N^{k-1}}{\gcd(\mu, N)} \).

The same arguments can be applied to show that \( \ord_m(N^k) = \beta \cdot \frac{N^{k-1}}{\gcd(\mu, N)} \) for \( k \geq 2 \). \( \square \)

**Lemma 2.6.** Let \( k, N \in \mathbb{N}^* \). Then \( \eta_N(k) \geq N^{k-2} \).

**Proof.** If \( k = 1 \), then \( 1 \geq N^{-1} \). If \( k \geq 2 \), observe that \( \gcd(\mu, N) \leq N \) implies

\[
\frac{N^{k-1}}{\gcd(\mu, N)} \geq N^{k-2}.
\]

Denote by \( \mathcal{P} \subset \mathbb{N} \) the set of prime numbers. The following lemma gives us a formula to compute the order of \( m \) in \( \mathbb{Z}/N\mathbb{Z} \) for any \( N \in \mathbb{N} \). It is an immediate consequence of the Chinese remainder theorem.

**Lemma 2.7.** For every \( N \in \mathbb{N} \), which we write \( N = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n} \) with \( p_i \in \mathcal{P} \) and \( \beta_i \in \mathbb{N} \) for every \( i \in \{1, \ldots, n\} \), we have

\[
\ord_m(N) = \ord_m \left( p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n} \right) = \lcm \left( \ord_m \left( p_1^{\beta_1} \right), \ord_m \left( p_2^{\beta_2} \right), \ldots, \ord_m \left( p_n^{\beta_n} \right) \right).
\]  

**Lemma 2.8.** Let \( P \) be a finite set of primes, not dividing \( m \). There exists a constant \( C(m, P) > 0 \) such that, for every integer \( N \) with all prime factors in \( P \), we have:

\[
\frac{\ord_m(N)}{N} \geq C(m, P).
\]
Proof. Write $N = p_1^{eta_1} \cdots p_k^{eta_k}$, with $p_i \in P$, all different, $\beta_i > 0$ and $\eta_{p_i}$ defined as in Definition 2.4. In addition, we define the set

$$\Pi_k := \{ \text{ord}_m(p_1)\eta_{p_1}(\beta_1) \cdots \text{ord}_m(p_{k-1})\eta_{p_{k-1}}(\beta_{k-1}), \quad \text{ord}_m(p_1)\eta_{p_1}(\beta_1) \cdots \text{ord}_m(p_{k-2})\eta_{p_{k-2}}(\beta_{k-2}) \text{ord}_m(p_k)\eta_{p_k}(\beta_k), \quad \ldots \}
$$

which contains all possible products with $k - 1$ factors, each one of $\text{ord}_m(p_i)\eta_{p_i}(\beta_i)$, $i = 1, \ldots, k$. Using Lemmas 2.2, 2.5, and 2.7, we obtain

$$\text{ord}_m(N) = \frac{\text{ord}_m(p_1)\eta_{p_1}(\beta_1) \cdots \text{ord}_m(p_k)\eta_{p_k}(\beta_k)}{\gcd(\Pi_k)},$$

thus

$$\frac{\text{ord}_m(N)}{N} = \frac{\text{ord}_m(p_1)\eta_{p_1}(\beta_1) \cdots \text{ord}_m(p_k)\eta_{p_k}(\beta_k)}{N \cdot \gcd(\Pi_k)}. \quad (5)$$

Moreover, $\text{ord}_m(p_i) \geq 1$ for every $i$, and using Lemma 2.6 on each $\eta_{p_i}(\beta_i)$, we obtain from Eq. (5)

$$\frac{\text{ord}_m(N)}{N} \geq \frac{p_1^{\beta_1 - 2} \cdots p_k^{\beta_k - 2}}{p_1^{\beta_1} \cdots p_k^{\beta_k} \cdot \gcd(\Pi_k)} = \frac{1}{p_1^2 \cdots p_k^2 \cdot \gcd(\Pi_k)} > 0. \quad (6)$$

So we may take $C(m, P)$ as the minimum of the $\frac{1}{p_1^2 \cdots p_k^2 \cdot \gcd(\Pi_k)}$’s taken over all subsets $\{p_1, \ldots, p_k\}$ of $P$.

The following material will be used in the proof of Proposition 4.10.

Definition 2.9. Let $N \in \mathbb{N}$ and $N = \Pi'_{i=1} p_i^{\beta_i}$, its decomposition in prime factors. The dominant prime of $N$ is the factor $p_i$ in $P$ such that $p_i^{\beta_i} \geq p_j^{\beta_j}$ for $\forall j$. The factor $p_i^{\beta_i}$ is called the dominating factor.

Lemma 2.10. Fix $s \in (\mathbb{Z}[1/m])^\times$, with $s > 0$. There exist infinitely many integers $N > 0$, coprime to $m$, such that $s$ has odd order in the multiplicative group $(\mathbb{Z}[1/m]/N\mathbb{Z}[1/m])^\times = (\mathbb{Z}/N\mathbb{Z})^\times$.

Proof. If $s = 1$, take any $N$ coprime with $m$. So we assume $s \neq 1$ and, replacing $s$ by $s^{-1}$ if necessary, we assume $s > 1$.

Let $P$ be the set of primes dividing $m$, set $r = |P|$. Write $s = \frac{a_1}{a_2}$ with $a_1 > a_2 > 0$, coprime, and all their prime factors in $P$. For $k \in \mathbb{N}$, set $a_1^k - a_2^k = N_kq_k$, where $N_k$ is the maximal factor coprime to $m$. Observe that if a prime in $P$ divides $q_k$, it cannot simultaneously divide $a_1$ and $a_2$, since they are coprime.

It is clear that, for odd $k$, $s$ will also have odd order in $(\mathbb{Z}[1/m]/(a_1^k - a_2^k)\mathbb{Z}[1/m])^\times$, hence also in $(\mathbb{Z}[1/m]/N_k\mathbb{Z}[1/m])^\times$. It is therefore enough to prove that the map $k \mapsto N_k$ takes infinitely many values on odd integers. This will follow immediately from the following.

Claim: There is an infinite family of odd integers $k$ such that $q_k \leq (a_1^{2r} - a_2^{2r})^r$. 

□
We study the diameter of arithmetic box spaces of \( BS \) with \( \gcd \) will always assume that \( i < j \) such that the dominant primes in \( q_{k-2i} \) and \( q_{k-2j} \) are the same. We have that

\[
(s^{k-2i} - 1) - (s^{k-2j} - 1) = s^{k-2i}(s^{2(j-i)} - 1)
\]

Write \( p_i^β \) for the dominating factor of \( q_{k-2i} \). Set \( β = \min\{β_i, β_j\} \) and \( p = p_i \); say that \( β = β_i \) (otherwise replace \( i \) by \( j \)). We see that \( p^β \) divides the numerator on the left, hence it divides the numerator on the right. We note that \( p \) does not divide \( a_1 \), nor \( a_2 \), hence it must divide \( a_1^{2(j-i)} - a_2^{2(j-i)} \), which is bounded by \( (a_1^{2r} - a_2^{2r}) \). So we get \( p^β \leq (a_1^{2r} - a_2^{2r}) \) and it follows that \( q_{k-2i} \leq (a_1^{2r} - a_2^{2r})^r \). □

3 PROPERTY \( D_α \) FOR SOLVABLE BAUMSLAG-SOLITAR GROUPS

3.1 Metric aspects of solvable Baumslag-Solitar groups

We study the diameter of arithmetic box spaces of \( BS(1, m) \) according to Eq. (1). In this section, we will always assume that \( \gcd(m, N) = 1 \). We recall that every element of \( BS(1, m) \) \((m > 1)\) admits a unique normal form of the type \( t^{-1}at^j \) with \( i, j \geq 0, t \in \mathbb{Z} \) and \( t \) can be a multiple of \( m \) only if either \( i \) or \( j \) is zero. Indeed, one can rewrite \( ta \) as \( a^mt, ta^{-1} \) as \( a^{-m}t, at^{-1} \) as \( t^{-1}a^{-m} \), and \( a^{-1}t^{-1} \) as \( t^{-1}a^{-m} \) and the result follows.

The normal form of a word is usually not the geodesic form, and we want to estimate how well the normal form approximates the geodesic form.

**Proposition 3.1 ([2, Prop. 2.1]).** There exist constants \( C_1, C_2, D_1, D_2 > 0 \) such that for any \( ω = t^{-1}at^j \in BS(1, m) \) with \( t \neq 0 \), we have

\[
C_1(i + j + \log|t|) - D_1 \leq \|ω\| \leq C_2(i + j + \log|t|) + D_2
\]

where \( \| \cdot \| \) is the word metric with respect to \( \{a^{±1}, t^{±1}\} \). Moreover we may take \( C_2 = D_2 = m \).

Let \( A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \), \( T = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \) \( GL_2(\mathbb{Z}[1/m]) \), and denote by \( G_m \) the subgroup of \( GL_2(\mathbb{Z}[1/m]) \) generated by \( A \) and \( T \). In the previous section, we saw that \( BS(1, m) \cong G_m \leq GL_2(\mathbb{Z}[1/m]) \).

As mentioned before, \( BS(1, m) \cong G_m \) is a finitely generated, residually finite group that surjects onto \( \mathbb{Z} \) so that Theorem 1.1 applies and we know that for every \( 0 < α < 1 \), there exists a box space of \( G_m \) with property \( D_α \). However, we are interested in specific box spaces of \( G_m \), namely the arithmetic box spaces, or in other words, box spaces of the form \( \mathbb{C}(G_m/N_d) \), \( G_m \). To this end, we start by studying the quotients \( G_m/G_m(N) \), and then explore how the diameters evolve.

**Proposition 3.2.** Let \( N \in \mathbb{N} \) be such that \( \gcd(m, N) = 1 \). Then

\[
G_m/G_m(N) \cong \mathbb{Z}/N\mathbb{Z} \rtimes_m \mathbb{Z}/\ord_m(N)\mathbb{Z}, \quad \text{and} \quad |G_m/G_m(N)| = N \cdot \ord_m(N), \quad (7)
\]

where \( \mathbb{Z}/\ord_m(N)\mathbb{Z} \) acts on \( \mathbb{Z}/N\mathbb{Z} \) by multiplication by \( m \).

**Proof.** Consider reduction modulo \( N \):

\[
\varphi: \quad G_m \quad \xrightarrow{w = \begin{pmatrix} m^k & x \\ 0 & 1 \end{pmatrix}} \quad GL_2(\mathbb{Z}/N\mathbb{Z})
\]

The image of \( \varphi \) is clearly isomorphic to \( \mathbb{Z}/N\mathbb{Z} \rtimes_m \mathbb{Z}/\ord_m(N)\mathbb{Z} \), and of order \( N \cdot \ord_m(N) \). Moreover we have

\[
w = \begin{pmatrix} m^k & x \\ 0 & 1 \end{pmatrix} \in G_m(N) \iff m^k \equiv 1 \pmod{N} \quad \text{and} \quad x \in N\mathbb{Z}\left[\frac{1}{m}\right] \iff \varphi(w) = 1.
\]
So \( \ker(\varphi) = G_m(N) \) and the result follows from the first isomorphism theorem. \( \square \)

**Example 3.3.** Consider \( BS(1, 2) \) and \( N = 5 \). Then \( \text{ord}_2(5) = 4 \), and \( G_2/G_2(5) \cong \mathbb{Z}/5\mathbb{Z} \rtimes_2 \mathbb{Z}/4\mathbb{Z} \). The Cayley graph of the quotient is the graph drawn below, using \( a = (1, 0) \) and \( t = (0, 1) \) as generators. Note that one still needs to identify the bottom line with the upper line, and the line to the left with the line to the right.

![Cayley graph](image)

Thanks to the familiar structure of the quotient \( G_m/G_m(N) \) and Proposition 2.1 from [2], we are able to estimate the diameter of arithmetic box spaces of \( BS(1, m) \).

**Lemma 3.4.** Let \( N \geq 2 \). Then

\[
\text{diam}(\text{Cay}(G_m/G_m(N))) = \Theta(\text{ord}_m(N)).
\]

More precisely, there exists a constant \( C_m > 0 \) such that

\[
\frac{1}{3} \cdot \text{ord}_m(N) \leq \text{diam}(\text{Cay}(G_m/G_m(N))) \leq C_m \cdot \text{ord}_m(N).
\]

**Proof.** Let \( m \geq 2 \) and consider \( BS(1, m) \cong G_m \subset GL_2(\mathbb{Z}[1/m]) \). Recall that \( G_m/G_m(N) \cong \mathbb{Z}/N\mathbb{Z} \rtimes_\varphi \mathbb{Z}/\text{ord}_m(N)\mathbb{Z} \) so that \( \text{diam}(G_m/G_m(N)) = \text{diam}(\mathbb{Z}/N\mathbb{Z} \rtimes_\varphi \mathbb{Z}/\text{ord}_m(N)\mathbb{Z}) \geq \text{diam}(\mathbb{Z}/\text{ord}_m(N)\mathbb{Z}) \). Since the Cayley graph of \( \mathbb{Z}/\text{ord}_m(N)\mathbb{Z} \) is a cycle, we can roughly estimate the diameter to obtain

\[
\text{diam}(G_m/G_m(N)) \geq \frac{1}{3} \cdot \text{ord}_m(N).
\]

For the second inequality, let \( ([x], [k]) \in \mathbb{Z}/N\mathbb{Z} \rtimes_\varphi \mathbb{Z}/\text{ord}_m(N)\mathbb{Z} \) be an element realising the diameter. We rewrite \( ([x], [k]) \) as \( (m^k x) G_m(N) \). The induced metrics are always smaller in a quotient, thus

\[
\left\| \begin{pmatrix} m^k & x \\ 0 & 1 \end{pmatrix} G_m(N) \right\|_{G_m/G_m(N)} \leq \left\| \begin{pmatrix} m^k & x \\ 0 & 1 \end{pmatrix} \right\|_{G_m}.
\]

Recall that any word \( \omega \in BS(1, m) \) can be written in normal form as \( \omega = t^{-1}a^it^j \). In the quotient \( G_m/G_m(N) \), the situation is even simpler, as by the semi-direct product structure every word can be written as \( A^iT^j \) with \( 0 \leq t < N \) and \( 0 \leq j < \text{ord}_m(N) \). With \( t = x \) and \( j = k \), we identify \( (m^k x) \) with the element \( A^kT^k \) in normal form in \( G_m \). If \( x = 0 \) we get \( T^k \) and

\[
\|T^k\|_{G_m} = k < \text{ord}_m(N).
\]
Assume that \( x \neq 0. \) From Proposition 3.1, we obtain
\[
\left\| \begin{pmatrix} m^k & x \\ 0 & 1 \end{pmatrix} \right\|_{G_m} = \|A^x T^k\|_{G_m} \leq 2m(k + \log x + 1). \tag{11}
\]
Note that since \( m^{\text{ord}_m(N)} \geq N \) (equivalently \( \log(N) \leq \text{ord}_m(N) \cdot \log(m) \)) and moreover \( \log x \leq \log(N) \), Eq. (11) becomes
\[
\left\| \begin{pmatrix} m^k & x \\ 0 & 1 \end{pmatrix} \right\|_{G_m} \leq 2m(2 + \log(m)) \text{ord}_m(N). \tag{12}
\]
Setting \( C_m := 2m(2 + \log(m)) \), we obtain
\[
\text{diam}(\text{Cay}(G_m/G_m(N))) \leq C_m \cdot \text{ord}_m(N). \tag{13}
\]

**Proposition 3.5.** An arithmetic box space \( \Box (G_m(N_k))_k G_m \) has property \( D_\alpha \) if and only if \( \text{ord}_m(N_k) = \Omega(N_k^{\frac{\alpha}{1-\alpha}}) \).

**Proof.** Using Lemma 3.4:
\[
\Box (G_m(N_k))_k G_m \text{ has } D_\alpha \iff \text{diam}(G_m/G_m(N_k)) = \Omega(|G_m/G_m(N_k)|^{\alpha})
\]
\[
\iff \text{ord}_m(N_k) = \Omega(N_k^{\alpha} \cdot \text{ord}_m(N_k)^{\alpha}) \iff \text{ord}_m(N_k) = \Omega(N_k^{\frac{\alpha}{1-\alpha}}).
\]

We present here the main structure theorem for the arithmetic box spaces of \( BS(1, m) \).

**Theorem 3.6.** For any \( m \geq 2 \), the following statements hold:
1. If an arithmetic box space \( \Box (G_m(N_k))_k G_m \) has property \( D_\alpha \), then \( \alpha \leq \frac{1}{2} \).
2. There exists an arithmetic box space with property \( D_{1/2} \).
3. There exists an arithmetic box space of \( G_m \) without property \( D_\alpha \) for any \( \alpha \in [0, 1/2] \).
4. Fix \( \alpha < 1 \). Every arithmetic box space of \( G_m \) is covered by some box space with \( D_\alpha \).

**Proof.**
1. If \( \Box (G_m(N_k))_k G_m \) has property \( D_\alpha \), using \( N_k \geq \text{ord}_m(N_k) \) and Proposition 3.5, we get \( N_k = \Omega(N_k^{\frac{\alpha}{1-\alpha}}) \), which forces \( \alpha \leq \frac{1}{2} \).
2. Let \( (N_k)_k \subset \mathbb{N} \) be the sequence defined by \( N_k = (m^2 - 1)^k \). Clearly, \( N_k \mid N_{k+1} \) for every \( k \).
   We apply Lemma 2.5 with \( N = m^2 - 1 \), so that \( \text{ord}_m(m^2 - 1) = 2 \) and \( \mu = 1 \). We thus obtain:
   \[
   \text{ord}_m(N_k) = 2 \cdot (m^2 - 1)^{k-1}, \forall k \geq 1.
   \tag{14}
   \]
i.e. \( \text{ord}_m(N_k) = \Omega(N_k) \). By Proposition 3.5 the box space \( \Box (G_m(N_k))_k G_m \) has property \( D_{1/2} \).
3. We consider the sequence \( (N_k)_k \) defined by \( N_k = m^{2^k} - 1 \) and prove that the arithmetic box space \( \Box (G_m(N_k))_k G_m \) does not have property \( D_\alpha \) for any \( \alpha \in [0, 1/2] \). It is straightforward that \( N_k \mid N_{k+1} \) for every \( k \), and \( \text{ord}_m(N_k) = 2^k \). We have
   \[
   \lim_{k \to \infty} \frac{\text{ord}_m(N_k)}{N_k^{\frac{\alpha}{1-\alpha}}} = \lim_{k \to \infty} \frac{2^k}{(m^{2^k} - 1)^{\frac{\alpha}{1-\alpha}}} = 0,
   \]
i.e. \( \text{ord}_m(N_k) = o(N_k^{\frac{\alpha}{1-\alpha}}) \). By Proposition 3.5 this shows that the arithmetic box space \( \Box (G_m(m^{2^k} - 1))_k G_m \) does not have property \( D_\alpha \) for any \( \alpha \in [0, 1/2] \).
We adapt the proof of Theorem 3 in [8]. Pick an integer \( D > 0 \) with \( \frac{D}{m+1} \geq \alpha \). Let \( \Box_{G_m(N_k)} G_m \) be any arithmetic box space of \( G_m \). Define
\[
n_k = \text{ord}_m(N_k) \cdot N_k^D
\]
and
\[
M_k = \left\{ \left( \begin{array}{cc} m^{\ell n_k} & r \\ 0 & 1 \end{array} \right) : \ell \in \mathbb{Z}, \ r \in N_k \mathbb{Z}[\frac{1}{m}] \right\}.
\]
It is readily checked that \( M_k \) is a subgroup and, because \( \text{ord}_m(N_k) | n_k \), that \( M_k \) is normal in \( G_m \) and is contained in \( G(N_k) \). As \( n_k | n_{k+1} \), we have that \( \Box_{(M_k)} G_m \) is a box space which covers \( \Box_{(G_m(N_k))} G_m \).

It remains to check that \( \Box_{(M_k)} G_m \) has property \( D_\alpha \). But \( G/M_k \) maps onto the cyclic group \( \mathbb{Z}/n_k \mathbb{Z} \) so we have
\[
\text{diam}(G/M_k) \geq \text{diam}(\mathbb{Z}/n_k \mathbb{Z}) \geq \frac{n_k}{3}.
\]
On the other hand
\[
|G/M_k|^\alpha = n_k^\alpha N_k^\alpha = \text{ord}_m(N_k)^\alpha N_k^{\alpha(D+1)} \leq \text{ord}_m(N_k)N_k^D = n_k.
\]
This concludes the proof.

### 3.2 Density results

A natural question after encountering the constructions of Theorem 3.6.2 and 3.6.3 is "how many arithmetic box spaces of \( BS(1, m) \) have \( D_{1/2} \)? In the following paragraphs, we give a partial answer to this question.

Let \( (N_k)_k \subset \mathbb{N} \) be such that \( N_k | N_{k+1} \) for every \( k > 0 \), and denote by \( P_k \) the set of prime factors of \( N_k \). Moreover, we define the set of prime factors of the sequence \( (N_k)_k \) by
\[
P := \bigcup_{k=1}^{+\infty} P_k.
\]

Before stating our main result from this section, we need to introduce some definitions about the density of prime numbers. We follow Powell [11] for the terminology.

**Definition 3.7.** Let \( P \subset \mathcal{P} \) be a subset of the prime numbers. The natural primitive density of \( P \) is (if the limit exists)
\[
d'(P) := \lim_{N \to +\infty} \frac{|\{ P \leq N \mid p \in P \}|}{|\{ P \leq N \mid p \in \mathcal{P} \}|}.
\]
The analytic primitive density of \( P \) is (if the limit exists)
\[
D'(P) = \lim_{s \to 1^+} \frac{\sum_{p \in P} \frac{1}{p^s}}{\sum_{p \in \mathcal{P}} \frac{1}{p^s}}.
\]

If \( P \) is finite then \( d'(P) = D'(P) = 0 \). Suppose now that \( D'(P) > 0 \). In this case, we see that \( \sum_{p \in P} \frac{1}{p} = +\infty \), otherwise \( D'(P) \) would be equal to 0. Observe that
\[
\prod_{\rho \in P} \left( 1 - \frac{1}{\rho} \right) = 0 \iff \sum_{\rho \in P} \ln \left( 1 - \frac{1}{\rho} \right) = -\infty.
\]

But using that \( \ln(1 + x) \leq x \) for \( x > -1 \)
\[
\sum_{\rho \in P} \ln \left( 1 - \frac{1}{\rho} \right) \leq -\sum_{\rho \in P} \frac{1}{\rho} = -\infty.
\]
We recall Chernikov’s theorem (see Theorem 4.10 in [13]): if \( \mathcal{N} \) is a torsion-free nilpotent group, for every \( k \geq 1 \) the map \( N \to N : x \mapsto x^k \) is injective.

The first lemma discusses one-parameter subgroups in \( U_n(A) \).

**Lemma 4.1.** For every \( g \in U_n(A) \), there exists a unique homomorphism \( \alpha : A \to U_n(A) \) such that \( \alpha(1) = g \).

Therefore, we obtain

\[
\prod_{p \in \mathcal{P}} \left( 1 - \frac{1}{p} \right) = 0
\]

if \( D'(P) > 0 \).

**Theorem 3.8.** Let \( \square(G_m(N_k))_k G_m \) be an arithmetic box space, and let \( P \) be the set of prime factors of the sequence \( (N_k)_k \).

1. If \( |P| < +\infty \), then \( \square(G_m(N_k))_k G_m \) has \( D_{1/2} \).
2. If \( D'(P) > 0 \), then \( \square(G_m(N_k))_k G_m \) does not have \( D_\alpha \) for every \( \alpha > 0 \).

**Proof.** In view of Proposition 3.5, we must study the asymptotics of the quotient \( \frac{\text{ord}_m(N_k)}{N_k} \).

1. By Lemma 2.8, there exists a constant \( C(m, P) \) such that \( \frac{\text{ord}_m(N_k)}{N_k} \geq C(m, P) \), i.e. \( \text{ord}_m(N_k) = \Omega(N_k) \). Proposition 3.5 applies to show that \( \square(G_m(N_k))_k G_m \) has \( D_{1/2} \).
2. Assume now \( D'(P) > 0 \), pick \( N = p_1^{\beta_1} \cdots p_k^{\beta_k} \) with \( p_1, \ldots, p_k \in P \). We have \( \text{ord}_m(N) \leq \varphi(N) = |(\mathbb{Z}/N\mathbb{Z})^*| \), where \( \varphi \) denotes Euler’s totient function. Then

\[
\frac{\text{ord}_m(N)}{N} \leq \prod_{i=1}^{k} \frac{\varphi(p_i^{\beta_i})}{p_i^{\beta_i}} = \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right).
\]

In view of Eq. (16) we then get \( \text{ord}_m(N_k) = o(N_k) \), which proves the second part of the theorem thanks to Proposition 3.5.

\[ \square \]

We state here a few open questions related to the previous theorem.

- If we assume that \( d'(P) > 0 \), does the associated arithmetic box space have \( D_\alpha \) for some \( \alpha \in ]0, 1/2[ \) or not?
- What happens in the case \( |P| = +\infty \) and \( D'(P) = 0 \)?
- Given \( \alpha \in ]0, 1/2[ \), can we create an arithmetic box space with exactly \( D_\alpha \)?

## 4 CSP FOR \( BS(1, m) \)

For a subring \( A \) of \( \mathbb{Q} \), we define three subgroups of \( GL_n(A) \):

- \( T_n(A) \), the subgroup of upper triangular matrices;
- \( U_n(A) \), the unipotent subgroup, i.e. the subgroup of \( T_n(A) \) consisting of matrices with 1’s down the diagonal;
- \( D_n(A) \), the subgroup of diagonal matrices.

The map \( \Delta : T_n(A) \to D_n(A) \) taking a matrix to its diagonal, is a surjective group homomorphism with kernel \( U_n(A) \).

We will also need the set \( N_n(A) \) of upper triangular nilpotent matrices, i.e. upper triangular matrices with 0’s down the diagonal. Note that \( T_n(A) = 1_n + N_n(A) \).

### 4.1 Representations of \( A \) into \( U_n(A) \)

We recall Chernikov’s theorem (see Theorem 4.10 in [13]): if \( N \) is a torsion-free nilpotent group, for every \( k \geq 1 \) the map \( N \to N : x \mapsto x^k \) is injective.

The first lemma discusses one-parameter subgroups in \( U_n(A) \).

**Lemma 4.1.** For every \( g \in U_n(A) \), there exists a unique homomorphism \( \alpha : A \to U_n(A) \) such that \( \alpha(1) = g \).
Proof. The existence follows from Cor. 10.25 in [13]: if \( g = 1_n + X \), with \( X \in N_n(A) \), then for \( r \in A \):
\[
\alpha(r) = (1_n + X)^r = \sum_{k=0}^{\infty} \left( \begin{array}{c} r \\ k \end{array} \right) X^k = 1_n + rX + \frac{r(r-1)}{2}X^2 + ... 
\]
(note that the sum is finite as \( X^n = 0 \)). For the uniqueness, let \( \beta \) be another homomorphism with \( \beta(1) = g \); for \( r \in A \), write \( r = \frac{a}{b} \) with \( a, b \in \mathbb{Z}, b > 0 \) and \( a, b \) coprime. Then
\[
\alpha(r)^b = \alpha^b = g^a = \beta(a) = \beta(r)^b,
\]
so \( \alpha(r) = \beta(r) \) by Chernikov’s theorem. □

Definition 4.2. For a subgroup \( H \) of \( U_n(A) \), the isolator of \( H \) is:
\[
I(H) = \{ g \in U_n(A) : g^k \in H \text{ for some } k \geq 1 \}.
\]

By Theorem 3.25 in [13], \( I(H) \) is a subgroup of \( U_n(A) \). Clearly \( H \subset I(H) \).

Lemma 4.3. For \( m \geq 2 \), let \( \alpha : \mathbb{Z}[1/m] \to U_n(\mathbb{Z}[1/m]) \) be an injective homomorphism. Then \( I(\alpha(\mathbb{Z}[1/m])) \) is abelian and the exponent of the group \( I(\alpha(\mathbb{Z}[1/m]))/\alpha(\mathbb{Z}[1/m]) \) is finite.

Proof. The proof is in three steps.

1. By Lemma 4.1, there exists a unique homomorphism \( \tilde{\alpha} : \mathbb{Q} \to U_n(\mathbb{Q}) \) that extends \( \alpha \). We show that \( I(\alpha(\mathbb{Z}[1/m])) \subset \tilde{\alpha}(\mathbb{Q}) \), from which the first statement will follow. For \( g \in I(\alpha(\mathbb{Z}[1/m])) \), there exists \( k \geq 1 \) and \( r \in \mathbb{Z}[1/m] \) such that \( g^k = \alpha(r) \). Then
\[
\tilde{\alpha}(\frac{r}{k})^k = \tilde{\alpha}(r) = \alpha(r) = g^k,
\]
hence \( g = \tilde{\alpha}(\frac{k}{r}) \) by Chernikov’s theorem.

2. Let us show that there exists some non-zero \( x_0 \in \mathbb{Z}[1/m] \) such that, for \( g \in I(\alpha(\mathbb{Z}[1/m])) \), \( k \geq 1 \), \( r \in \mathbb{Z}[1/m] \):
\[
g^k = \alpha(r) \implies \frac{r}{k}x_0 \in \mathbb{Z}[1/m].
\]
Write \( \alpha(1) = 1_n + X \), with \( X \in N_n(\mathbb{Z}[1/m]) \), as in Lemma 4.1. Note that \( X \neq 0 \) as \( \alpha \) is injective. Then
\[
g = \tilde{\alpha}(\frac{r}{k}) = (1_n + X)^{\frac{k}{r}} = 1_n + \frac{r}{k}X + ...
\]
For \( 1 \leq i < n \) and an upper triangular matrix \( Y \) of size \( n \times n \), we denote by \( Y_{(i)} \) the \( i \)-th parallel to the diagonal (moving upwards from the diagonal). Let \( i \) be the smallest index such that \( X_{(i)} \neq 0 \). Since \( (X^k)_{(i)} = 0 \) for \( k \geq 2 \), we have \( g_{(i)} = \frac{r}{k}X_{(i)} \). Let \( x_0 \) be any non-zero coefficient of \( X_{(i)} \). Since \( g \in U_n(\mathbb{Z}[1/m]) \), we have \( \frac{r}{k}x_0 \in \mathbb{Z}[1/m] \) as desired.

3. Let \( \pi(m) \) be the set of primes dividing \( m \). An integer is a \( \pi(m) \)-number if all its prime divisors are in \( \pi(m) \). Write \( x_0 = \frac{b}{t} \), with \( t \) a \( \pi(m) \)-number, and \( b \in \mathbb{Z} \) is coprime to \( t \). For \( g \in I(\alpha(\mathbb{Z}[1/m])) \), with \( g^k = \alpha(r) \) as above, write \( \frac{r}{k} = \frac{a}{st} \), where \( a, s, t \) are pairwise coprime, \( s \) is a \( \pi(m) \)-number and \( t \) is coprime with \( m \). By the previous step \( \frac{r}{k}x_0 = \frac{ab}{st} \in \mathbb{Z}[1/m] \). Since \( a \) and \( t \) are coprime, this may happen only if \( t \) divides \( b \). Finally
\[
g^b = \tilde{\alpha}(\frac{r}{k})^b = \tilde{\alpha}(\frac{br}{k}) = \tilde{\alpha}(\frac{ab}{st}).
\]
But \( \frac{ab}{st} \in \mathbb{Z}[1/m] \) as \( t \) divides \( b \). This implies that \( g^b \in \alpha(\mathbb{Z}[1/m]) \), hence the exponent of \( I(\alpha(\mathbb{Z}[1/m]))/\alpha(\mathbb{Z}[1/m]) \) divides \( b \). □
4.2 Special representations of BS(1, m)

For $m \geq 2$, set $G_m = BS(1, m) = \mathbb{Z}[1/m] \rtimes \mathbb{Z}$. We will write $A_m$ for $\mathbb{Z}[1/m]$ when viewed as a normal subgroup of $G_m$.

**Definition 4.4.** A special representation of $G_m$ is an injective homomorphism $\rho : G_m \rightarrow T_n(\mathbb{Z}[1/m])$ such that $\rho(A_m) \subset U_n(\mathbb{Z}[1/m])$.

We note that the standard embedding $G_m \rightarrow T_2(\mathbb{Z}[1/m])$, is a special representation.

**Lemma 4.5.** (1) If $\rho$ is a special representation, then $\rho^{-1}(U_n(\mathbb{Z}[1/m])) = A_m$.

(2) If $m$ is even, then any injective homomorphism $\rho : G_m \rightarrow T_n(\mathbb{Z}[1/m])$ is a special representation.

**Proof.** We work with the presentation $G_m = \langle a, t | tat^{-1} = a^m \rangle$, observing that the normal subgroup $A_m$ coincides with the normal subgroup generated by $a$.

(1) Suppose by contradiction that $A_m$ is strictly contained in $\rho^{-1}(U_n(\mathbb{Z}[1/m]))$. Then there exists $k > 0$ such that $\rho(t^k) \in U_n(\mathbb{Z}[1/m])$. Consider the subgroup $H$ of $G_m$ generated by $A_m \cup \{t^k\}$, so that $\rho(H) \subset U_n(\mathbb{Z}[1/m])$. Since $\rho$ is injective, we see that $H$ is nilpotent. As $H$ also has finite index in $G_m$, we deduce that $G_m$ is virtually nilpotent, which is a contradiction.

(2) Suppose that $m$ is even and $\rho : G_m \rightarrow T_n(\mathbb{Z}[1/m])$ is an injective homomorphism. It is enough to see that $\rho(a)$ belongs to $U_n(\mathbb{Z}[1/m]) = \ker(\Delta)$. But we have $\rho(a^{-m}) = \rho([a, t]) \in [T_n(\mathbb{Z}[1/m]), T_n(\mathbb{Z}[1/m])] \subset \ker(\Delta)$.

Now the image of $\Delta$, namely $D_n(\mathbb{Z}[1/m]) \equiv (\mathbb{Z}[1/m]^\times)^n$, contains only 2-torsion; since $\Delta(\rho(a)) m^{-1} = 1_n$ and $m - 1$ is odd, we have $\Delta(\rho(a)) = 1_n$ as desired.

\[ \square \]

We now head towards CSP for special representations of $BS(1, m)$. The next lemma is proved exactly as Lemma 4 in Formanek [5], using the same ingredient, namely a number-theoretical result by Chevalley [3].

**Lemma 4.6.** Let $R$ be a subring of a number field with $R^\times$ finitely generated, let $G$ be a subgroup of $D_n(R)$. There exists a function $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ such that, if $g \in G$ satisfies $g \equiv 1_n \mod \varphi(r)$, then $g$ is an $r$-th power in $G$.

\[ \square \]

In Theorem 5 of [5], Formanek proved that, if $R$ is the ring of integers of a number field and $G$ is a subgroup of $T_n(R)$, then $G$ has CSP. The proof of the next result is inspired by Formanek’s proof.

**Proposition 4.7.** Let $\rho : G_m \rightarrow T_n(\mathbb{Z}[1/m])$ be a special representation of $BS(1, m)$. Then $\rho(G_m)$ has CSP.

**Proof.** Let $N = G_m$ be a normal subgroup of finite index $r$. Denote by $G_m^r$ the subgroup generated by $r$-th powers in $G_m$. Then $G_m^r \subset N$ by Lagrange’s theorem. Let $b$ be the exponent of $I(\rho(A_m))/\rho(A_m)$ (which is finite by Lemma 4.3), and let $e$ be the exponent of the finite group $T_n(\mathbb{Z}[1/m])/(br)^2\mathbb{Z}[1/m])$. Define then

$$M = (br)^2\varphi(re),$$

where $\varphi$ comes from Lemma 4.6 applied to $\Delta(\rho(G_m))$. We will show that if $\rho(g) \equiv 1_n \mod M$, then $g \in G_m^r$ so that $\rho(N)$ contains the congruence subgroup $\rho(G_m)(M)$.

If $\rho(g) \equiv 1_n \mod M$, in particular $\Delta(\rho(g)) \equiv 1_n \mod \varphi(er)$. By Lemma 4.6, the matrix $\Delta(\rho(g))$ is an $(er)$-th power in $\Delta(\rho(G_m))$, i.e. there exists $z \in G_m$ such that

$$\Delta(\rho(g)) = \Delta(\rho(z^{er})) = \Delta(\rho((z^e)^r)).$$
But $\rho(z^r) \equiv 1_n \mod (br)^2$, by definition of $e$, so also $\rho(z^{er}) \equiv 1_n \mod (br)^2$. On the other hand by definition of $M$ we have $\rho(g) \equiv 1_n \mod (br)^2$, so $\rho(g^{-1}z^{er}) \equiv 1_n \mod (br)^2$. Since $g^{-1}z^{er} \in \ker(\Delta) = U_n(\mathbb{Z}[1/m])$, Lemma 1 of [5] applies to guarantee that $g^{-1}z^{er}$ is a $(br)$-th power in $U_n(\mathbb{Z}[1/m])$, so we find $h \in U_n(\mathbb{Z}[1/m])$ such that

$$\rho(g^{-1}z^{er}) = h^{br}.$$  

Hence $g^{-1}z^{er} \in \rho^{-1}(U_n(\mathbb{Z}[1/m])) = A_m$ (the equality follows from the first part of Lemma 4.5). This means that $h \in I(\rho(A_m))$, so by definition of $b$ we have $h^{b} \in \rho(A_m)$, say $h^{b} = \rho(y)$ for $y \in A_m$. Then $h^{br} = \rho(y^r)$ and $\rho(g^{-1}z^{er}) = \rho(y^r)$. As $\rho$ is injective $g^{-1}z^{er} = y^r$, i.e $g = (z^r)^{y^{-r}}$, so $g \in G_m^r$.

4.3 From special representations to all injective representations in $T_n(\mathbb{Z}[1/m])$

In this section we show that for any injective representation $\rho$ of $G_m$ into $T_n(\mathbb{Z}[1/m])$, the group $\rho(G_m)$ has CSP. The main idea is to pass to subrepresentations which are special and extract information about $\rho$.

LEMMA 4.8. Let $G$ be a subgroup of $GL_n(\mathbb{Z}[1/m])$.

(1) Let $H$ be a finite index subgroup of $G$, where $H$ has CSP. If $H$ contains a congruence subgroup of $G$, then $G$ also has CSP.

(2) For $1 \leq i \leq k$, let $H_i$ be a finite index subgroup of $G$. Suppose $G = \cup_{i=1}^{k} H_i$, then if all $H_i$ have CSP, $G$ also has CSP.

PROOF. (1) Let $N$ be a finite index subgroup of $G$, then $N \cap H$ is a finite index subgroup of $H$ and thus contains some congruence subgroup of the form $H(M)$. By assumption there is some $M$ such that $G(M) \subset H$, hence we have that

$$G(M\bar{M}) \subset G(M) \cap G(\bar{M}) \subset H(M) \subset N \cap H \subset N.$$  

(2) Suppose by contradiction that $G$ does not have CSP, then there is some finite index subgroup $N$ which does not contain any congruence subgroup. However each $N \cap H_i$ contains a congruence subgroup of the form $H(M_i)$. Set $\bar{M} = \Pi_i M_i$, then there is some $g \in G(\bar{M}) \setminus N$. Note that this $g$ is necessarily in one of the $H_i$'s. So it is necessarily in $H(M_i)$. However it is not in $N \cap H_i$: a contradiction. \qed

LEMMA 4.9. Let $\rho: G_m \to T_n(\mathbb{Z}[1/m])$ be a monomorphism. Suppose $\Delta(\rho(a)) \neq 1_n$ and the diagonal of $\rho(t)$ is strictly positive, then $\rho(G_m)$ has CSP.

PROOF. Note that the subgroup $B = \langle a^2, t \rangle$ is also a Baumslag-Solitar group isomorphic to $BS(1, m)$. The restriction $\rho|_{B}$ is a special representation of $BS(1, m)$; indeed by the proof of Lemma 4.5, we have $\Delta(\rho(a))^{m-1} = 1_n$, so $\Delta(\rho(a))$ has finite order in $D_m(\mathbb{Z}[1/m])$; but the torsion subgroup of $D_m(\mathbb{Z}[1/m])$ is $\{\pm 1\}^n$, so $\Delta(\rho(a^2)) = 1_n$. By Proposition 4.7, the group $\rho(B)$ has the CSP.

We show there is some congruence subgroup of $\rho(G_m)$ that is fully contained inside $\rho(B)$. Since $\Delta(\rho(a)) \neq 1_n$, there is some $-1$ on the diagonal, suppose it appears at the $i$th position. Let $s$ be the element of $(\mathbb{Z}[1/m])^\chi$ in the $i$th position in $t$. By Lemma 2.10, we find $M > 1$, coprime with $m$, such that $s$ has odd order in $(\mathbb{Z}[1/m]/\mathbb{M}[1/m])^\chi$.

We note that if $\omega$ is a word with letters in $\{a, t\}$ representing an element of $G_m \setminus B$, then it contains an odd number of $a$'s. Hence, the element on the $i$th position on the diagonal of $\rho(\omega)$ is of the form $-s^r$ for some $r \in \mathbb{Z}$. If we suppose that $\rho(\omega) \in \rho(G_m)(M)$, then $s^r = -1 \mod M$. This is

\footnote{Formanek states this lemma for the ring of integers of a number field, but the proof only uses that the ring is commutative with characteristic 0.}
impossible since $s$ has odd order in $(\mathbb{Z}[\frac{1}{m}]/M\mathbb{Z}[1/m])^\times$ and thus cannot have a power equal to $-1$. So $\rho(\omega)$ cannot be in the corresponding congruence subgroup, i.e. $\rho(G_m)(M) \subset \rho(B)$. By Lemma 4.8, the result follows. □

We are ready to complement Proposition 4.7.

**Proposition 4.10.** For any injective homomorphism $\rho : G_m \rightarrow T_n(\mathbb{Z}[1/m])$, the group $\rho(G_m)$ has CSP.

**Proof.** Since we already know the result for $m$ even (by Proposition 4.7 and Lemma 4.5), we may and will assume that $m$ is odd.

The group $G_m$ has three subgroups $B_1 = \langle a^2, t \rangle$, $B_2 = \langle a^2, at \rangle$ and $B_3 = \langle a, t^2 \rangle$, which are all isomorphic to $BS(1, m)$ or $BS(1, m^2)$. We show that they cover $G_m$. Any element $\omega \in G_m$ can be described by a word of the form $t^{-k}a^{i}t^{ℓ}$, with $k, ℓ \in \mathbb{N}$ and $r \in \mathbb{Z}$. Replacing $\omega$ by $\omega^{-1}$ if necessary, we may assume $k \leq ℓ$.

- If $r$ is even, then $\omega \in B_1$;
- If $k$ and $ℓ$ are both even or odd, then $\omega \in B_3$; indeed $\omega = t^{-2k}(t^k a^i t^{-k})t^{k+ℓ} = t^{-2k}a^{m^k}t^{k+ℓ} \in B_3$ as $k + ℓ$ is even.
- If $r$ is odd and $k, ℓ$ do not have the same parity, then $\omega \in B_2$. Indeed

$$t^{-k}a^{i}t^{ℓ} = (t^{-1}a^{-1})^k a^{-\sum_{0}^{k-1} m^i} r^a - \sum_{0}^{k-1} m^i (at)^l = (at)^{-k} a^{-\sum_{0}^{k-1} m^i} (at)^ℓ.$$

Since $r, ℓ - k$ and $m$ are odd, the exponent of $a$ in the latter expression is even, so $\omega \in B_2$.

Note that if $\Delta(\rho(\alpha)) = 1_n$, then it is a special representation and Proposition 4.7 applies. If it is not then the restrictions of $\rho$ to $B_1$ and $B_2$ are special representations, and the restriction of $\rho$ to $B_3$ satisfies the assumptions of Lemma 4.9. Hence the $\rho(B_i)$’s all have CSP. Now simply applying Lemma 4.8 finishes the argument. □

### 4.4 An alternative approach to CSP for $BS(1, p^λ)$ ($p$ prime)

We use the language of $\mathbb{Q}$-algebraic groups. Denoting by $\mathbb{G}_a$ (resp. $\mathbb{G}_m$) the additive group (resp. the multiplicative group), we set $\mathbb{G} = \mathbb{G}_a \rtimes \mathbb{G}_m$, the affine group viewed as a subgroup of $GL_2$ via the standard embedding.

Let $p_1, ..., p_r$ be distinct primes, and let $S = \{p_1, ..., p_r, \infty\}$ be viewed as a set of places of $\mathbb{Q}$. Then the ring $O_S$ of $S$-integers in $\mathbb{Q}$ is precisely

$$O_S = \mathbb{Z}[1/p_1, ..., 1/p_r],$$

so that $O_S^\times = \{ \pm p_1^{k_1} ... p_r^{k_r} : k_1, ..., k_r \in \mathbb{Z} \}$ and

$$\mathcal{G}(O_S) = \left\{ \left( \frac{\pm p_1^{k_1} ... p_r^{k_r}}{a} \right) : k_1, ..., k_r \in \mathbb{Z}, a \in \mathbb{Z}[1/p_1, ..., 1/p_r] \right\}.$$

It is known that $\mathcal{G}(O_S)$ satisfies CSP: see formula (**) on page 108 of [12].

Note that taking $r = 1$, i.e. $S = \{p, \infty\}$ and $O_S = \mathbb{Z}[\frac{1}{p}]$, makes $BS(1, p^λ)$ appear as a finite index subgroup in $\mathcal{G}(O_S)$, namely $[\mathcal{G}(O_S) : BS(1, p^λ)] = 2t$.

**Proposition 4.11.** Let $H \subset GL_n$ be a $\mathbb{Q}$-subgroup, and let $\rho : \mathcal{G} \rightarrow H$ be a $\mathbb{Q}$-isomorphism. Then $\rho(BS(1, p^λ))$ satisfies the CSP.

**Proof.** Let $K$ be a finite index subgroup in $\rho(BS(1, p^λ))$. Since $\mathcal{G}(O_S)$ satisfies the CSP, we find $N > 0$ such that $\mathcal{G}(O_S)(N) \subset \rho^{-1}(K)$. By Lemma 3.1.1(ii) in Chapter I of [9], the subgroup $\rho(\mathcal{G}(O_S)(N))$ is an $S$-congruence subgroup in $\mathcal{H}(O_S)$, i.e. it contains $\mathcal{H}(O_S)(M)$ for some $M > 1$. Then $(\rho(BS(1, p^λ))(M) \subset \mathcal{H}(O_S)(M) \subset \rho(\mathcal{G}(O_S)(N)) \subset K$. □
REFERENCES

[1] Emmanuel Breuillard and Matthew Tointon. Nilprogressions and groups with moderate growth. *Adv. Math.*, 289:1008–1055, 2016.

[2] José Burillo and Murray Elder. Metric properties of Baumslag–Solitar groups. *International Journal of Algebra and Computation*, 25(05):799–811, 2015.

[3] Claude Chevalley. Deux théorèmes d’arithmétique. *J. Math. Soc. Japan*, 3:36–44, 1951.

[4] P.M. Cohn. *Algebra*. Wiley, 1977.

[5] Edward Formanek. Conjugate separability in polycyclic groups. *Journal of Algebra*, 42:1–10, 1976.

[6] Joseph Gallian. *Contemporary abstract algebra*. Nelson Education, 2012.

[7] Ana Khukhro. Espaces et groupes non exacts admettant un plongement grossier dans un espace de hilbert [d’apr`es arzhantseva, guentner, osajda, spakula]. *Séminaire BOURBAKI*, Exposé 1154, 71ème année, 2018.

[8] Ana Khukhro and Alain Valette. Expanders and box spaces. *Advances in Mathematics*, 314:806–834, 2017.

[9] G.A. Margulis. *Discrete subgroups of semisimple Lie groups*. Springer-Verlag, 1991.

[10] Stephen Meskin. Non-residually finite one-relator groups. *Trans. Amer. Math. Soc.*, 64:105–114, 1972.

[11] Barry J Powell. Primitive densities of certain sets of primes. *Journal of Number Theory*, 12(2):210–217, 1980.

[12] M.S. Raghunathan. On the congruence subgroup problem. *Publications mathématiques de l’I.H.E.S.*, 46:107–161, 1976.

[13] Robert B. Warfield. *Nilpotent groups*, volume 513. Springer Lecture Notes in Math., 1976.