ISRAEL JOURNAL OF MATHEMATICS **255** (2023), 109–122
DOI: 10.1007/s11856-022-2412-5

GLASNER PROPERTY FOR UNIPOTENTLY GENERATED GROUP ACTIONS ON TORI

BY

Kamil Bulinski and Alexander Fish

School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia
e-mail: kamil.bulinski@sydney.edu.au, alexander.fish@sydney.edu.au

ABSTRACT

A theorem of Glasner from 1979 shows that if $A \subset \mathbb{T} = \mathbb{R}/\mathbb{Z}$ is infinite, then for each $\epsilon > 0$ there exists an integer n such that nA is ϵ-dense and Berend–Peres later showed that in fact one can take n to be of the form $f(m)$ for any non-constant $f(x) \in \mathbb{Z}[x]$. Alon and Peres provided a general framework for this problem that has been used by Kelly–Lê and Dong to show that the same property holds for various linear actions on $\mathbb{T}^d$. We complement the result of Kelly–Lê on the ϵ-dense images of integer polynomial matrices in some subtorus of $\mathbb{T}^d$ by classifying those integer polynomial matrices that have the Glasner property in the full torus $\mathbb{T}^d$. We also extend a recent result of Dong by showing that if $\Gamma \leq \mathrm{SL}_d(\mathbb{Z})$ is generated by finitely many unipotents and acts irreducibly on $\mathbb{R}^d$, then the action $\Gamma \curvearrowright \mathbb{T}^d$ has a uniform Glasner property.

1. Introduction

In 1979 Glasner [7] showed that an infinite subset $A \subset \mathbb{T} = \mathbb{R}/\mathbb{Z}$ satisfies the property that for every $\epsilon > 0$ there exists $n \in \mathbb{N}$ such that nA is ϵ-dense in $\mathbb{T}$. This was later extended by Berend–Peres [4] in a number of ways. For example, they showed that for each non-constant polynomial $f(x) \in \mathbb{Z}[x]$ there exists $n \in \mathbb{N}$ such that $f(n)A$ is ϵ-dense in $\mathbb{T}$. This motivated them to define a set $S \subset \mathbb{N}$ to be **Glasner** if for all infinite $A \subset \mathbb{T}$ and $\epsilon > 0$ there exists an $s \in S$ such that sA is ϵ-dense. Turning our attention to more general semigroup actions on metric spaces, we extend this definition as follows.

Received March 16, 2021 and in revised form November 11, 2021

Definition 1.1: We say that a subset S of a semigroup Γ is **Glasner for an action** $\Gamma \curvearrowright X$ on a compact metric space X by continuous maps if for each infinite $Y \subset X$ and $\epsilon > 0$ there exists an $s \in S$ such that sY is ϵ-dense. We say that the action $\Gamma \curvearrowright X$ is Glasner if Γ is a Glasner set with respect to this action.

In fact, Berend–Peres realised that a more uniform notion of the Glasner property holds for this action on $\mathbb{T}$. This leads us to the following definition.

Definition 1.2: If $k : \mathbb{R}_{>0} \to \mathbb{N}$ is a function, then we say that a subset S of a semigroup Γ is k-**uniformly Glasner for an action** $\Gamma \curvearrowright X$ on a compact metric space X by continuous maps if there is an $\epsilon_0 > 0$ such that for each $0 < \epsilon < \epsilon_0$ and $Y \subset X$ with $|Y| \geq k(\epsilon)$ there exists an $s \in S$ such that sY is ϵ-dense. We say that the action $\Gamma \curvearrowright X$ is k-uniformly Glasner if Γ is a k-uniformly Glasner set with respect to this action. We will also use the phrase **uniformly Glasner** to mean k-uniformly Glasner for some unspecified $k : \mathbb{R}_{>0} \to \mathbb{N}$.

In particular, Berend–Peres showed that the multiplicative action of $\mathbb{N}$ acting on $\mathbb{T}$ is $(c_1/\epsilon)^{c_2/\epsilon}$-uniformly Glasner.[1] Moreover, they also gave a lower bound by showing that there is a set $A_\epsilon \subset \mathbb{T}$ of cardinality $c\epsilon^{-2}$ such that nA_ϵ is not ϵ-dense for all $n \in \mathbb{N}$. The seminal work of Alon–Peres [1] closed this significant difference in the lower and upper bounds by showing that in fact this action is $\epsilon^{-2-\delta}$-uniformly Glasner for all $\delta > 0$. Secondly, Alon–Peres also quantitatively improved the polynomial example by showing that if $f(x) \in \mathbb{Z}[x]$ is a non-constant polynomial of degree D, then the set $\{f(n) \mid n \in \mathbb{N}\}$ is $\epsilon^{-2D-\delta}$-uniformly Glasner for all $\delta > 0$.

The Glasner property of linear actions on a higher-dimensional torus $\mathbb{T}^d$ was studied by Kelly- Lê [10], where they used the techniques of Alon–Peres [1] to show that the natural action of the multiplicative semi-group $M_{d\times d}(\mathbb{Z})$ of $d \times d$ integer matrices on $\mathbb{T}^d$ is $c_d\epsilon^{-3d^2}$uniformly Glasner. This was later improved by Dong in [5] where he showed, using the same techniques of Alon–Peres together with the deep work of Benoist–Quint [3], that the action $\mathrm{SL}_d(\mathbb{Z}) \curvearrowright \mathbb{T}^d$ is $c_{\delta,d}\epsilon^{-4d-\delta}$-uniformly Glasner for all $\delta > 0$. Furthermore, Kelly–Lê also gave the following multidimensional generalization of the aforementioned result on the Glasner property of polynomial sequences.

[1] If $k(\epsilon, c, c_1, \ldots,)$ is an expression involving ϵ and possibly constants c, c_i etc., by $k(\epsilon)$-uniformly Glasner we always technically mean k-uniformly Glasner for the function $k(\epsilon) = k(\epsilon, c, c_1, \ldots)$ for some choice of $c, c_i > 0$.

THEOREM 1.3 (Kelly–Lê, [10, Theorem 2]): *Let $A(x) \in M_{d\times d}(\mathbb{Z}[x])$ be a matrix with integer polynomial entries. Then the following conditions are equivalent.*

(1) *The columns of $A(x)-A(0)$ are linearly independent over $\mathbb{Z}$ (as elements in $\mathbb{Z}[x]^d$) and whenever $v, w \in \mathbb{Z}^d$ are such that*

$$v \cdot (A(x) - A(0))w = 0$$

then $v \cdot A(0)w = 0$.

(2) *For any infinite subset $Y \subset \mathbb{T}^d$ there exists a subtorus (non-trivial connected closed Lie subgroup) $\mathcal{T} = \mathcal{T}(Y, A(x))$ such that for all $\epsilon > 0$ there exists an $n \in \mathbb{Z}$ such that, for some $Y_0 \subset Y$, the set*

$$A(n)Y_0 = \{A(n)y \mid y \in Y_0\}$$

is ϵ-dense in a translate of $\mathcal{T}$.

The following main result of this paper characterizes those $A(x) \in M_{d\times d}(\mathbb{Z}[x])$ which satisfy the stronger property that $\{A(n) \mid n \in \mathbb{Z}\}$ is Glasner (for the natural linear action on $\mathbb{T}^d$), i.e., it characterizes when we can take the subtorus $\mathcal{T}$ to be the full $\mathbb{T}^d$.

THEOREM 1.4: *Let $A(x) \in M_{d\times d}(\mathbb{Z}[x])$ be a matrix with integer polynomial entries. Then the following conditions are equivalent.*

(1) *For all $v \in \mathbb{Z}^d \setminus \{0\}$ and $w \in \mathbb{Z}^d \setminus \{0\}$ we have that*

$$v \cdot (A(x) - A(0))w \neq 0.$$

(2) *The set $\{A(n) \mid n \in \mathbb{Z}\}$ is $c_1\epsilon^{-c_2}$-uniformly Glasner for the linear action $M_{d\times d}(\mathbb{Z}[x]) \curvearrowright \mathbb{T}^d$ for some constants $c_1, c_2 > 0$ depending on $A(x)$. That is, for every $Y \subset \mathbb{T}^d$ with $|Y| > c_1\epsilon^{-c_2}$ there exists $n \in \mathbb{Z}$ such that $A(n)Y$ is ϵ-dense in $\mathbb{T}^d$.*

Remark 1.5: As we shall see in the (2) $\Longrightarrow$ (1) proof, in condition (2) of Theorem 1.4 one can replace $c_1\epsilon^{-c_2}$-uniformly Glasner with the weaker condition of being just Glasner. So Glasner and $c_1\epsilon^{-c_2}$-uniformly Glasner are equivalent for sets of the form $\{A(n) \mid n \in \mathbb{Z}\}$ for some $A(x) \in M_{d\times d}(\mathbb{Z}[x])$.

Let us remark that, as stated, the subtorus $\mathcal{T}$ in Theorem 1.3 depends on Y and not just $A(x)$ and the proof in [10] is not constructive as it makes use of Ramsey's Theorem on graph colourings to demonstrate the existence of such a $\mathcal{T}$. Thus it does not seem that our result can be easily derived from the result or techniques of Kelly–Lê. Note that in Theorem 2.8 we will provide an effective estimate on the uniformity (estimates on the constants c_1 and c_2).

It will be convenient to give some alternative formulations and geometrically intuitive extensions of condition (1) in Theorem 1.4.

Definition 1.6: A set $S \subset \mathbb{R}^d$ is said to be **hyperplane-fleeing** if for all proper affine subspaces H of $\mathbb{R}^d$ (i.e., $H = W + a$ for some proper vector subspace $W \subset \mathbb{R}^d$ and $a \in \mathbb{R}^d$) we have that $S \not\subset H$.

Thus, condition (1) in Theorem 1.4 is equivalent to the statement that for each non-zero $w \in \mathbb{Z}^d \setminus \{0\}$ the orbit

$$\{A(n)w \mid n \in \mathbb{Z}\}$$

is hyperplane-fleeing (as it is not a subset of the hyperplane

$$\{x \in \mathbb{R}^d \mid v \cdot x - v \cdot A(0)w = 0\}$$

for any $v \in \mathbb{Z}^d \setminus \{0\}$ and in fact any $v \in \mathbb{R}^d \setminus \{0\}$ as $A(x)$ has integer polynomial entries). This hyperplane-fleeing property of the orbits is related to the irreducibility of linear group actions. Indeed, it is easy to see that if $d > 1$, and $\Gamma \leq M_{d\times d}(\mathbb{Z})$ is a semigroup whose action on $\mathbb{R}^d$ is irreducible, then the orbit of any non-zero vector $v \in \mathbb{R}^d \setminus \{0\}$ is hyperplane-fleeing (we prove a stronger statement in Lemma 3.2). This enables us to use Theorem 1.4 to deduce the Glasner property for various irreducible representations. For instance, we recover in a more elementary way (by avoiding the deep work of Benoist–Quint [3]) the aforementioned result of Dong but with weaker (but still polynomial in ϵ^{-1}) uniformity bounds. In general, we will demonstrate that subgroups generated by a finite set of unipotent elements of $\mathrm{SL}_d(\mathbb{Z})$ that act irreducibly on $\mathbb{T}^d$ satisfy the uniform Glasner property.

THEOREM 1.7: *Let $d > 1$ and let $u_1, \ldots, u_m \in \mathrm{SL}_d(\mathbb{Z})$ be unipotent elements such that the action of the subgroup $\Gamma = \langle u_1, \ldots, u_m \rangle$ on $\mathbb{R}^d$ is irreducible. Then there exists c_1, c_2 (depending on Γ) such that the following is true: For each $\epsilon > 0$ there exists an integer $k \leq c_1\epsilon^{-c_2}$ such that for any distinct $x_1, \ldots, x_k \in \mathbb{T}^d$ there exists $\gamma \in \Gamma$ such that $\{\gamma x_1, \ldots, \gamma x_k\}$ is ϵ-dense in $\mathbb{T}^d$. In other words, the action of Γ on $\mathbb{T}^d$ is $c_1\epsilon^{-c_2}$ uniformly Glasner.*

This will follow by showing (see Proposition 3.3) that Γ contains such a polynomial satisfying the condition (1) of Theorem 1.4.

Let us now explore some examples of such subgroups other than $\mathrm{SL}_d(\mathbb{Z})$ (which is an example as $\mathrm{SL}_d(\mathbb{Z})$ is generated by the finitely many elementary matrices obtained from changing a single 0 to a 1 in the identity matrix).

THEOREM 1.8: *Let* $Q(x,y,z) = xy - z^2$ *or* $Q(x,y,z) = x^2 - y^2 - z^2$. *Let* $\Gamma = \mathrm{SO}_{\mathbb{Z}}(Q)$ *be the subgroup of* $\mathrm{SL}_d(\mathbb{Z})$ *preserving this quadratic form. Then the action of* Γ *on* $\mathbb{T}^d$ *is uniformly Glasner.*

Proof. For $Q(x,y,z) = xy - z^2$ this can be seen as follows. By identifying $(x,y,z) \in \mathbb{Z}^3$ with

$$\begin{bmatrix} z & -y \\ x & -z \end{bmatrix} \in \mathfrak{sl}_2(\mathbb{Z})$$

we see that $Q(x,y,z)$ is the determinant. But the determinant is preserved by the conjugation action (adjoint representation) of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{sl}_2(\mathbb{R})$ given by

$$\mathrm{Ad}(g)A = gAg^{-1} \quad \text{for } A \in \mathfrak{sl}_2(\mathbb{R}) \text{ and } g \in \mathrm{SL}_2(\mathbb{Z}),$$

which is irreducible. Note that $\mathrm{Ad}(u)$ is unipotent for unipotent u since u is a polynomial map and group homomorphism, $\mathrm{Ad}(\mathrm{SL}_2(\mathbb{Z}))$ thus generated by unipotents. Of course, this example generalizes to any higher dimensional adjoint representation, thus showing that it also has the uniform Glasner property. For $Q(x,y,z) = x^2 - y^2 - z^2$ one instead notices

$$Q(x,y,z) = \det \begin{pmatrix} z & -(x+y) \\ x-y & -z \end{pmatrix}.$$

Hence we may regard Q as the determinant map on the abelian subgroup

$$\left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathfrak{sl}_2(\mathbb{Z}) \mid a_{21} \equiv a_{12} \mod 2 \right\} \cong \mathbb{Z}^3.$$

Now notice that the conjugation action of

$$\left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle$$

preserves this additive subgroup and acts irreducibly on $\mathfrak{sl}_2(\mathbb{R})$. Again, the generators are unipotent hence have unipotent image under the adjoint representation, as required. ∎

We remark that these examples complement a recent work of Dong [6] where he extended his result from [5] on the Glasner property of $\mathrm{SL}_d(\mathbb{Z}) \curvearrowright \mathbb{T}^d$ by showing that the subgroups $\Gamma \leq \mathrm{SL}_d(\mathbb{Z})$ that are Zariski dense in $\mathrm{SL}_d(\mathbb{R})$ are also Glasner for the action on $\mathbb{T}^d$, but the uniform Glasner property was not established. The examples above are not Zariski dense in $\mathrm{SL}_d(\mathbb{R})$, though it is remarked in Remark 4.2 of [6] that it is possible to also extend his techniques to the case where Γ satisfies the Benoist–Quint hypothesis, which these examples do. However, these techniques are not quantitative and do not establish the uniform Glasner property provided in Theorem 1.7. It is also worth remarking that our proofs are more self-contained as they avoid the deep work of Benoist–Quint.

Acknowledgement. The authors were partially supported by the Australian Research Council grant DP210100162.

2. Hyperplane fleeing orbits implies Glasner property

In this section we prove Theorem 1.4. We start with the easier direction.

Proof of (2) $\implies$ (1) *in Theorem 1.4.* Suppose that we have $v, w \in \mathbb{Z}^d \setminus \{0\}$ such that $v \cdot (A(x))w = c$ where $c = v \cdot A(0)w$ is a constant. Let $w_m \in \mathbb{T}^d$ be the image of $\frac{1}{m}w$ and $c_m \in \mathbb{T}$ be the image of $\frac{1}{m}c$. Notice that $C = \{c_m \mid m \in \mathbb{Z}_{>0}\}$ cannot be dense in $\mathbb{T}$ because $c_m \to 0 \in \mathbb{T}$, hence avoids a non-empty open set $U \subset \mathbb{T}$. The map $f : \mathbb{T}^d \to \mathbb{T}$ given by $f(u) = v \cdot u$ is well defined, continuous and surjective with $f(A(n)w_m) = c_m$ for all $n \in \mathbb{Z}$ and $m \in \mathbb{Z}_{>0}$. Thus the infinite set $Y = \{w_m \mid m \in \mathbb{Z}_{>0}\} \subset \mathbb{T}^d$ satisfies the property that $f(A(n)Y)$ will never intersect U and so $A(n)Y$ will never intersect the non-empty open set $f^{-1}(U)$. ∎

Lemma 2.1: *If $A(x) \in M_{d\times d}(\mathbb{Z}[x])$ is a matrix of integer polynomials, then the following are equivalent.*

1. *The orbit $\{A(n)w \mid n \in \mathbb{Z}\}$ is hyperplane-fleeing for all $w \in \mathbb{Z}^d \setminus \{0\}$.*
2. *For all $w \in \mathbb{Z}^d \setminus \{0\}$, the entries of $(A(x) - A(0))w$ are polynomials in $\mathbb{Z}[x]$ that are linearly independent over $\mathbb{Z}$.*
3. *The polynomial $v^t(A(x) - A(0))w$ is non-zero for all $v, w \in \mathbb{Z}^d \setminus \{0\}$.*
4. *For all $v \in \mathbb{Z}^d \setminus \{0\}$, the entries of $v^t(A(x) - A(0))$ are polynomials in $\mathbb{Z}[x]$ that are linearly independent over $\mathbb{Z}$.*

If $w = (w_1, \dots, w_d) \in \mathbb{Z}^d$ we let $\gcd(w) = \gcd(w_1, \dots, w_d)$. If $\vec{w}_1, \dots, \vec{w}_d$ are integer vectors (of possibly different dimensions) then we identify $(\vec{w}_1, \dots, \vec{w}_d)$ with their concatenation, so $\gcd(\vec{w}_1, \dots, \vec{w}_d)$ makes sense and is equal to

$$\gcd(\gcd(\vec{w}_1), \dots, \gcd(\vec{w}_d)).$$

Proposition 2.2: *Let $v_1, \ldots, v_d \in \mathbb{Z}^r$ be linearly independent vectors. Then for all $a_1, \ldots, a_d \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$ with $\gcd(a_1, \ldots, a_d, q) = 1$ we have that*

$$\gcd(a_1 v_1 + \cdots + a_d v_d, q) \leq d! \max_i \|v_i\|_\infty^d.$$

Proof. Let $V_0 : \mathbb{Z}^d \to \mathbb{Z}^r$ be the linear map given by

$$V_0(x_1, \ldots, x_d) = \sum_{i=1}^{d} x_i v_i.$$

It is of full rank, hence there exists a full rank $d \times d$ minor of the matrix V_0, in other words there is a projection $\pi : \mathbb{Z}^r \to \mathbb{Z}^d$ of co-ordinates so that

$$V = \pi \circ V_0 : \mathbb{Z}^d \to \mathbb{Z}^d$$

is of full rank. By the Smith normal form for integer matrices, there exists a linear map $D : \mathbb{Z}^d \to \mathbb{Z}^d$ and automorphisms R and L of $\mathbb{Z}^d$ such that

$$V = LDR$$

and D is a diagonal matrix with non-zero (the kernel of V and hence D is trivial) diagonal entries satisfying the divisibility condition $D_{1,1} | D_{2,2} | \cdots | D_{d,d}$. Since automorphisms preserve divisors, we have that for $\vec{a} = (a_1, \ldots, a_d)$ with $\gcd(a_1, \ldots, a_d, q) = 1$, $\gcd(R\vec{a}, q) = 1$. Hence since all $D_{i,i} \neq 0$, we get that $\gcd(DR\vec{a}, q) \leq D_{d,d}$. Since L preserves divisors, we get that

$$\gcd(V\vec{a}, q) = \gcd(LDR\vec{a}, q) \leq D_{d,d}.$$

We have the upper bound

$$D_{d,d} \leq |\det(D)| = |\det(V)| \leq d! \max_i \|v_i\|_\infty^d.$$

Finally, since $V = \pi \circ V_0$ we have $\gcd(V_0\vec{a}, q) \leq \gcd(V\vec{a}, q)$, which completes the proof. ∎

Definition 2.3: We say that a vector $P(x) = (P_1(x), \ldots, P_r(x))$, where $P_i(x) \in \mathbb{Z}[x]$, has **multiplicative complexity** Q if for all $\vec{a} = (a_1, \ldots, a_r) \in \mathbb{Z}^r$ and $q \in \mathbb{Z}$ with $\gcd(a_1, \ldots, a_r, q) = 1$ we have that the polynomial

$$\sum_{j=1}^{D} b_j x^j = (P(x) - P(0)) \cdot \vec{a}$$

satisfies $\gcd(b_1, \ldots, b_D, q) \leq Q$.

Throughout this paper, if $A(x) \in M_{d\times d}(\mathbb{Z}[x])$ is a matrix with polynomial integer matrices, then we let $\|A(x)\|$ denote the largest absolute value of a coefficient appearing in $A(x)$.

Corollary 2.4: *Let $A(x) \in M_{d\times d}(\mathbb{Z}[x])$ be a matrix with integer polynomial entries and $w \in \mathbb{Z}^d \setminus \{0\}$ such that the entries of the row vector $w^t(A(x)-A(0))$ are elements of $\mathbb{Z}[x]$ that are linearly independent over $\mathbb{Z}$. Then $w^tA(x)$ has multiplicative complexity Q where*

$$Q = Q(A(x), w) = d! \cdot (d \cdot \|A(x) - A(0)\| \|w\|_\infty)^d.$$

Proof. Let $v_1, \ldots, v_d \in \mathbb{Z}[x]$ denote the entries of the row vector $w^t(A(x)-A(0))$. These are linearly independent over $\mathbb{Z}$ and so we may apply Proposition 2.2 by viewing v_i as an element of $\mathbb{Z}^r$, where $r-1$ is the maximal degree of the v_i, to obtain the desired estimate. ∎

Throughout this paper, we let $e(t) = \exp(2\pi i t)$. We will need the following classical bound of Hua.

Theorem 2.5 ([8], see also [9]): *For a positive integer D and $0 < \delta < \frac{1}{D}$ there exists a constant $C_{D,\delta}$ such that if $f = a_0 + a_1x + \cdots + a_Dx^D \in \mathbb{Z}[x]$ is a polynomial and q is a positive integer such that $gcd(a_1, \ldots, a_D, q) = 1$, then*

$$\Big|\frac{1}{q}\sum_{n=1}^{q} e\Big(\frac{f(n)}{q}\Big)\Big| \le C_{D,\delta}\, q^{\delta - \frac{1}{D}}.$$

We now state some extensions of tools developed by Alon–Peres [1] that have been used or slightly modified in subsequent works on the Glasner property [5], [10]. Let

$$B(M) = \{\vec{m} \in \mathbb{Z}^d \mid \vec{m} \neq \vec{0} \text{ and } \|\vec{m}\|_\infty \le M\}$$

denote the L^∞ ball of radius M in $\mathbb{Z}^d$ around $\vec{0}$ with $\vec{0}$ removed.

Proposition 2.6: *For each positive integer d there exists a constant $C_1 = C_1(d) > 0$ such that for all $\epsilon > 0$, if we set $M = \lfloor d/\epsilon \rfloor$, then the following is true: Let $\gamma_1, \ldots, \gamma_N \subset M_{d\times d}(\mathbb{Z})$ be a finite sequence of matrices and $X = \{x_1, \ldots, x_k\} \subset \mathbb{T}^d$. Suppose that $\gamma_n X$ is not ϵ-dense in $\mathbb{T}^d$ for all $n = 1, \ldots N$. Then*

$$k^2 \le \frac{C_1}{\epsilon^d} \sum_{\vec{m}\in B(M)} \sum_{1\le i,j\le k} \frac{1}{N}\sum_{n=1}^{N} e(\vec{m}\cdot \gamma_n(x_i - x_j)).$$

Proof. This is exactly Proposition 2 in [10] without the limit. See the short half-page proof that uses the exponential sum estimate from [2]. ∎

Proposition 2.7: *Fix an integer $d > 0$ and any real number $r > 0$. Then there exists a constant $C = C(d, r)$ such that the following is true: Given any distinct $x_1, \dots, x_k \in \mathbb{T}^d$, let h_q denote the number of pairs (i, j) with $1 \le i, j \le k$ such that q is the minimal (if such exists) positive integer such that $q(x_i - x_j) = 0$. Then*

$$\sum_{q=2}^{\infty} h_q q^{-r} \le C k^{2-r/(d+1)}.$$

Proof. For $r > 1$, this is a combination of Proposition 5 and Lemma 4.2 in [5], which is based on Proposition 1.3 of the Alon–Peres work [1]. It is only stated in [5] for $r > 1$ but it is in fact true for $r > 0$. We reproduce the proof for the sake of convenience and certifying that indeed only the assumption $r > 0$ is needed. Let

$$H_m = \sum_{q=2}^{m} h_q \quad \text{for } m \ge 2$$

and $H_1 = 0$. We first show that $H_m \le k m^{d+1}$. To see this, note that for each fixed i and q, there are at most q^d values of j such that $q(x_i - x_j) = 0$. Thus summing over $j = 1, \dots, k$ and then over $q = 1, \dots, m$ we get $H_m \le k m^{d+1}$. Note also that $H_m \le k^2$ for all m. Choose large enough $Q > k^{1/(d+1)}$ such that $h_q = 0$ for all $q > Q$. We have that

$$\begin{aligned}
\sum_{q=2}^{\infty} h_q q^{-r} &= \sum_{q=2}^{Q} h_q q^{-r} \\
&= \sum_{q=2}^{Q} (H_q - H_{q-1}) q^{-r} \\
&= \sum_{q=2}^{Q} H_q (q^{-r} - (q+1)^{-r}) + H_Q (Q+1)^{-r} \\
&= \sum_{2 \le q < k^{1/(d+1)}} H_q (q^{-r} - (q+1)^{-r}) \\
&\quad + \sum_{k^{1/(d+1)} \le q \le Q} H_q (q^{-r} - (q+1)^{-r}) + H_Q (Q+1)^{-r}
\end{aligned}$$

Now for the second sum use the bound $H_q \leq k^2$, telescoping and let $Q \to \infty$. Then for the first sum use the inequality $H_q \leq kq^{d+1}$ to get

$$\begin{aligned}\sum_{q=2}^{\infty} h_q q^{-r} &\leq \sum_{2\leq q<k^{1/(d+1)}} kq^{d+1}(q^{-r} - (q+1)^{-r}) + k^2 k^{-r/(d+1)} \\ &\leq k \sum_{2\leq q<k^{1/(d+1)}} rq^{d-r} + k^2 k^{-r/(d+1)} \\ &\leq Ck^{2-r/(d+1)} + k^{2-r/(d+1)}\end{aligned}$$

for some constant $C = C(d-r)$. ∎

We are now ready to prove the (1) $\Longrightarrow$ (2) direction of Theorem 1.4. We will actually prove the following stronger quantitative form.

Theorem 2.8: *For $\delta > 0$ and integers $d, D > 0$ there exists a constant $C_{\delta,d,D} > 0$ such that the following is true: Let $A(x) \in M_{d\times d}(\mathbb{Z}[x])$ be a matrix with integer polynomial entries of degree at most D such that for each $w \in \mathbb{Z}^d \setminus \{0\}$ the orbit $\{A(n)w \mid n \in \mathbb{Z}\}$ is hyperplane-fleeing. Then for each $\epsilon > 0$ and positive integers*

$$k > C_{\delta,d,D}\|A(x) - A(0)\|^{d(d+1)}\epsilon^{-2d(d+1)D-d(d+1)-\delta}$$

we have that whenever $x_1, \ldots, x_k$ are k distinct elements of $\mathbb{T}^d$, then there exists an integer n such that $\{A(n)x_1, \ldots, A(n)x_k\}$ is ϵ-dense in $\mathbb{T}^d$.

Proof. Fix $\epsilon > 0$ and assume that no such n exists. We will obtain an upper bound for k by applying Proposition 2.6 with $\gamma_n = A(n)$ and letting $N \to \infty$ in the upper bound. We claim that if $x_i - x_j$ is irrational and $\vec{m} \in B(M)$, where $M = \lfloor d/\epsilon \rfloor$ as in Proposition 2.6, then

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(\vec{m} \cdot \gamma_n(x_i - x_j)) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(\vec{m}^t A(n)(x_i - x_j)) = 0.$$

To see this, first note that the row vector

$$\vec{m}^t(A(x) - A(0)) = [P_1(x), \ldots, P_d(x)]$$

has linearly independent entries over $\mathbb{Z}$ (see Lemma 2.1) and hence over $\mathbb{R}$ as $P_i(x) \in \mathbb{Z}[x]$. Now if $\theta = (\theta_1, \ldots, \theta_d) \in \mathbb{T}^d$ is irrational, then we claim that

$$q(x) = \vec{m}^t(A(x) - A(0))\theta = \sum \theta_i P_i(x)$$

is irrational, i.e., not in $\mathbb{Q}[x]$. To see this, note that otherwise we have that $q(x), P_1(x), \ldots, P_d(x)$ are linearly dependent over $\mathbb{R}$ and hence over $\mathbb{Q}$, and so as $P_1(x), \ldots, P_d(x)$ are linearly independent we must have a linear combination $q(x) = \sum \theta_i' P_i(x)$ with all $\theta_i' \in \mathbb{Q}$. But by linear independence of $P_1(x), \ldots, P_d(x)$ we have that $\theta_i = \theta_i' \in \mathbb{Q}$. So we have shown that $\vec{m}^t A(n)(x_i - x_j)$ has at least one irrational non-constant coefficient when viewed as an element of $\mathbb{R}[n]$ and hence by Weyl equidistribution we get the desired limit

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(\vec{m}^t A(n)(x_i - x_j)) = 0.$$

Now we need to focus on the case where $x_i - x_j$ is rational. Thus we may write $x_i - x_j = \frac{1}{q}\vec{a}$ where $q \in \mathbb{Z}_{>0}$ and $\vec{a} = (a_1, \ldots, a_d) \in \mathbb{Z}^d$ with $\gcd(q, a_1, \ldots, a_d) = 1$. Now by Corollary 2.4 we have that $\vec{m}^t A(x)$ has multiplicative complexity Q where

$$(1) \quad Q = \sup_{\vec{m}\in B(M)} d! \cdot (d \cdot \|A(x) - A(0)\| \|\vec{m}\|_\infty)^d \le d! d^{2d} \|A(x) - A(0)\|^d \epsilon^{-d}.$$

Thus the greatest common divisor of q and the non-constant coefficients of the polynomial $\vec{m}^t A(x)\vec{a} \in \mathbb{Z}[x]$ is at most Q. Thus if D is the maximum degree of an entry in $A(x)$, we may apply Hua's bound (Theorem 2.5) to obtain a constant $C_2 = C_2(D, \delta)$ depending only on D and any constant $0 < \delta < \frac{1}{D}$ such that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(\vec{m}^t A(n)(x_i - x_j)) = \frac{1}{q} \sum_{n=1}^{q} e\Big(\frac{1}{q}\vec{m}^t A(n)\vec{a}\Big) \le C_2 \Big(\frac{Q}{q}\Big)^{\frac{1}{D}-\delta}.$$

Now let h_q denote the number of pairs x_i, x_j such that q is the least positive integer for which $q(x_i - x_j) = 0$. We apply Proposition 2.6 to obtain that

$$\begin{aligned} k^2 &\le \frac{C_1}{\epsilon^d} \sum_{\vec{m}\in B(M)} \Big(\sum_{q=2}^{\infty} h_q C_2 \Big(\frac{Q}{q}\Big)^{\frac{1}{D}-\delta} + k \Big) \\ &\le Q^{\frac{1}{D}-\delta} C_2 (2M)^d \frac{C_1}{\epsilon^d} \sum_{q=2}^{\infty} h_q q^{\delta - \frac{1}{D}} + \frac{C_1}{\epsilon^d} (2M)^d k. \end{aligned}$$

Now apply Proposition 2.7 to get that

$$\sum_{q=2}^{\infty} h_q q^{\delta - \frac{1}{D}} \le C_3 k^{2 - (\frac{1}{D} - \delta)/(d+1)}$$

for some constant $C_3 = C_3(d, D)$ depending only on d and D. Thus we have shown that

$$k^2 \leq Q^{\frac{1}{D}-\delta} C_2 (2M)^d \frac{C_1}{\epsilon^d} C_3 k^{2-(\frac{1}{D}-\delta)/(d+1)} + \frac{C_1}{\epsilon^d} (2M)^d k.$$

Now using $M = \lfloor d/\epsilon \rfloor$ and the upper bound (1) on Q we have that

$$k \leq C_{\delta,d,D} \|A(x) - A(0)\|^{d(d+1)} \epsilon^{-2d(d+1)D-d(d+1)-\delta}$$

for some constant $C_{\delta,d,D}$ depending only on d, D and any $\delta > 0$. ∎

3. Applications to groups generated by unipotent matrices

3.1. Balls in the Cayley graph of a linear group. Let $\Gamma \subset \mathrm{SL}_d(\mathbb{Z})$ be a group generated by elements $S \subset \Gamma$ and suppose that the linear action $\Gamma \curvearrowright \mathbb{R}^d$ is irreducible. We let

$$S_r = \{s_1 \cdots s_m \mid 0 \leq m \leq r \text{ and } s_1, \ldots, s_r \in S\}$$

denote the elements of Γ that can be written as a product of at most r elements of S (including $1 \in S_r$ as it is the empty product), i.e., the ball of radius r in the Cayley graph with respect to S.

Lemma 3.1: *For each $v \in \mathbb{R}^d \setminus \{0\}$, we have that* $\mathbb{R}\text{-span}(S_{d-1}v) = \mathbb{R}^d$.

Proof. For integers $r \geq 0$ let $V_r = \mathbb{R}\text{-span}(S_r v)$. Suppose $r \geq 0$ is such that $V_r \neq \mathbb{R}^d$. Then by irreducibility of Γ and $v \neq 0$ we must have that V_r is not Γ-invariant and hence not S-invariant. Thus $SV_r \not\subset V_r$, and so $S_{r+1}v \not\subset V_r$, which means $\dim V_{r+1} \geq \dim V_r + 1$. That is, we have shown that the nested sequence of subspaces $V_0 \subset V_1 \subset V_2 \subset \cdots$ is strictly increasing in dimension until the dimension is d, with $V_0 = \mathbb{R}v$ of dimension 1, hence $V_{d-1} = \mathbb{R}^d$ as required. ∎

Lemma 3.2: *If $d > 1$ and $v \in \mathbb{R}^d \setminus \{0\}$, then $S_d v$ is hyperplane fleeing.*

Proof. Suppose not, thus there exists a proper linear subspace $W \subsetneq \mathbb{R}^d$ and $a \in \mathbb{R}^d$ such that $S_d v \subset W + a$. As $d > 1$, there exists an $s \in S$ such that $sv - v \neq 0$ (as otherwise $\mathbb{R}v$ would be a one-dimensional, hence proper, Γ invariant subspace). Now apply Lemma 3.1 to $sv - v \neq 0$ to get that $S_{d-1}(sv - v) \not\subset W$. But this contradicts $S_d v \subset W + a$ since

$$S_{d-1}(sv - v) \subset S_d v - S_d v \subset W + a - (W + a) = W. \qquad ∎$$

3.2. Constructing polynomials via unipotents. The following Proposition together with Theorem 2.8 completes the proof of Theorem 1.7.

Proposition 3.3: *Suppose that $S \subset \mathrm{SL}_d(\mathbb{Z})$ where $d > 1$ and each $s \in S$ is a unipotent element, and suppose that the action of $\Gamma = \langle S \rangle$ on $\mathbb{R}^d$ is irreducible. Then there exists a matrix with integer polynomial entries $A(x) \in M_{d\times d}(\mathbb{Z}[x])$ such that $A(n) \in \Gamma$ for all $n \in \mathbb{Z}$ and $\{A(n)w \mid n \in \mathbb{Z}\}$ is hyperplane-fleeing for all $w \in \mathbb{R}^d \setminus \{0\}$.*

Proof. Write $S = \{u_1, \ldots, u_m\}$ where each u_i is a unipotent element, and use cyclic notation so that $u_i = u_{i+jm}$ for all $i, j \in \mathbb{Z}$. Note that for each fixed i the matrix u_i^n has entries that are integer polynomials in n, hence

$$Q_N(n_1, \ldots, n_N) = \prod_{i=1}^{N} u_i^{n_i} \in M_{d\times d}(\mathbb{Z}[n_1, \ldots, n_N])$$

is a matrix with multivariate integer polynomial entries in the variables $n_1, \ldots, n_N$. Now let $N = dm$ and use Lemma 3.2 to get that

$$\{Q_N(n_1, \ldots n_N)w \mid n_1, \ldots n_N \in \mathbb{Z}\}$$

is hyperplane-fleeing for all $w \in \mathbb{R}^d \setminus \{0\}$. In other words, for each fixed $w \in \mathbb{R}^d \setminus \{0\}$, if we let $P_1, \ldots, P_d \in \mathbb{R}[n_1, \ldots, n_N]$ be the polynomials such that

$$Q(n_1, \ldots, n_N)w = (P_1(n_1, \ldots, n_N), \ldots, P_d(n_1, \ldots, n_N)),$$

then $P_1, \ldots, P_d, 1$ are linearly independent over $\mathbb{R}$. But there exists a large enough $R \in \mathbb{Z}_{>0}$ (independent of w) such that the substitutions $n_i \mapsto n_i^{R^{i-1}}$ induce a map $\mathbb{Z}[n_1, \ldots, n_N] \to \mathbb{Z}[n]$ that is injective on the monomials appearing in $Q_N(n_1, \ldots, n_N)$. Thus $P_1, \ldots, P_d, 1$ remain linearly independent over $\mathbb{R}$ after making this substitution, thus $\{Q(n, n^R, \ldots, n^{R^{N-1}})w \mid n \in \mathbb{Z}\}$ is also hyperplane-fleeing. So the proof is complete with

$$A(x) = Q(x, x^R, \ldots, x^{R^{N-1}}). \qquad \blacksquare$$

References

[1] N. Alon and Y. Peres, *Uniform dilations*, Geometric and Functional Analysis **2** (1992), 1–28.

[2] J. T. Barton, H. L. Montgomery and J. D. Vaaler, *Note on a Diophantine inequality in several variables*, Proceedings of the American Mathematical Society **129** (2001), 337–345.

[3] Y. Benoist and J.-F. Quint, *Stationary measures and invariant subsets of homogeneous spaces (III)*, Annals of Mathematics **178** (2013), 1017–1059.

[4] D. Berend and Y. Peres, *Asymptotically dense dilations of sets on the circle*, Journal of the London Mathematical Society **47** (1993), 1–17.

[5] C. Dong, *On density of infinite subsets I*, Discrete and Continuous Dynamical Systems **39** (2019), 2343–2359.

[6] C. Dong, *On density of infinite subsets II: Dynamics on homogeneous spaces*, Proceedings of the American Mathematical Society **147** (2019), 751–761.

[7] S. Glasner, *Almost periodic sets and measures on the torus*, Israel Journal of Mathematics **32** (1979), 161–172.

[8] L.-K. Hua, *On an exponential sum*, Journal of the Chinese Mathematical Society **2** (1940), 301–312.

[9] L.-K. Hua, *Additive Theory of Prime Numbers*, Translations of Mathematical Monographs, Vol. 13, American Mathematical Society, Providence, RI, 1965.

[10] M. Kelly and T. H. Lê, *Uniform dilations in higher dimensions*, Journal of the London Mathematical Society **88** (2013), 925–940.