Twisted patterns in large subsets of Zn

Comment. Math. Helv. 92 (2017), 621–640
DOI 10.4171/CMH/420

Commentarii Mathematici Helvetici

Twisted patterns in large subsets of $\mathbb{Z}^N$

Michael Björklund and Kamil Bulinski

Abstract. Let $E \subset \mathbb{Z}^N$ be a set of positive upper Banach density, and let $\Gamma < \mathrm{GL}_N(\mathbb{Z})$ be a "sufficiently large" subgroup. We show in this paper that for each positive integer m there exists a positive integer k with the following property: For every $\{a_1, \dots, a_m\} \subset k \cdot \mathbb{Z}^N$, there are $\gamma_1, \dots, \gamma_m \in \Gamma$ and $b \in E$ such that

$$\gamma_i \cdot a_i \in E - b, \quad \text{for all } i = 1, \dots, m.$$

We use this "twisted" multiple recurrence result to study images of $E - b$ under various Γ-invariant maps. For instance, if $N \geq 3$ and Q is an integer quadratic form on $\mathbb{Z}^N$ of signature (p, q) with $p, q \geq 1$ and $p + q \geq 3$, then our twisted multiple recurrence theorem applied to the group $\Gamma = \mathrm{SO}(Q)(\mathbb{Z})$ shows that

$$k^2 Q(F) \subset Q(E - b),$$

for every $F \subset k \cdot \mathbb{Z}^N$ with m elements. In the case when E is an aperiodic Bohr_o set, we can choose b to be zero and $k = 1$, and thus $Q(\mathbb{Z}^N) \subset Q(E)$. Our result is derived from a non-conventional ergodic theorem which should be of independent interest. Important ingredients in our proofs are the recent breakthroughs by Benoist–Quint and Bourgain–Furman–Lindenstrauss–Mozes on equidistribution of random walks on automorphism groups of tori.

Mathematics Subject Classification (2010). 37A45; 11P99, 37A30.

Keywords. Multiple recurrence, equidistribution, invariants.

1. Introduction

We begin by recalling the following classical result of Furstenberg and Katznelson [10]. The upper Banach density of a subset $E \subset \mathbb{Z}^N$ will be defined in Appendix A.

Theorem 1.1. *Suppose that $E \subset \mathbb{Z}^N$ has positive upper Banach density. Then, for every finite set $F \subset \mathbb{Z}^N$, there exists a positive integer k such that*

$$kF \subset E - b, \quad \textit{for some } b \in E. \tag{1.1}$$

The case $N = 1$ corresponds to Szemerédi's celebrated theorem on arithmetic progressions.

This is an archetypal result in Arithmetic Ramsey theory. We stress the order of the quantifiers; *the integer k heavily depends on the finite set F*. In this paper we shall prove a "twisted" analogue of Furstenberg–Katznelson's Theorem, for which the dependence between the integer k and the set F disappears. To motivate this line of study, we begin by giving three applications.

1.1. Quadratic forms. A very influential result in Geometric Ramsey theory by Furstenberg, Katznelson and Weiss [11] asserts that if $E \subset \mathbb{R}^N$ is a Borel set with positive density in the sense that

$$\limsup_{R\to\infty} \frac{\mathrm{Leb}(E \cap B(R))}{R^N} > 0,$$

where Leb denotes the Lebesgue measure on $\mathbb{R}^N$ and $B(R)$ denotes the Euclidean ball of radius R around the origin, then there exists $R_o > 0$ such that

$$D(E) = \{\|x-y\|^2 : x, y \in E\} \supset [R_o, \infty),$$

where $\|\cdot\|$ denotes the Euclidean norm on $\mathbb{R}^N$. In other words, all sufficiently large Euclidean distances are realized within the set E. Recently, Magyar [13] established the following discrete analogue of this phenomenon.

Theorem 1.2 ([13, Theorem 1]). *Fix an integer $N \geq 5$ and let*

$$Q(x_1, \ldots, x_N) = x_1^2 + \cdots + x_N^2.$$

Then, for every subset $E \subset \mathbb{Z}^N$ of positive upper Banach density, there exist positive integers R_o and k such that

$$k^2\mathbb{Z} \cap [R_o, \infty) \subset Q(E-E).$$

Our first application consists of an analogue of Magyar's result for *indefinite* quadratic forms. Contrary to Magyar's result, we focus here *not* on the values of Q restricted to a *difference set* of a set $E \subset \mathbb{Z}^N$ of positive upper Banach density, but rather we study the values of Q restricted to *some* translate of the set E. We stress that our techniques do not apply to the quadratic forms in Magyar's Theorem as the (real points) of the symmetry group $\mathrm{SO}(N)$ is compact. For the notion of an (aperiodic) Bohr set we refer the reader to Section 3.

Theorem 1.3. *Let $p, q \geq 1$ and $p+q \geq 3$ and $E \subset \mathbb{Z}^{p+q}$ a set of positive upper Banach density. Let Q be a quadratic form on $\mathbb{R}^{p+q}$ of signature (p,q) with integer coefficients. Let m be a positive integer. Then there exists a positive integer k with the property that for every finite subset $F \subset \mathbb{Z}^{p+q}$ with $|F| = m$, we have*

$$k^2\, Q(F) \subset Q(E-b), \quad \text{for some } b \in E.$$

If E is an aperiodic Bohr set, then k can be chosen to be 1. *In particular, if E is an aperiodic* Bohr_o*-set, then $Q(E) = Q(\mathbb{Z}^{p+q})$.*

1.2. Characteristic polynomials and their Galois groups. Our second example concerns characteristic polynomials of integer square matrices with zero trace. Let $\mathrm{Mat}_d(\mathbb{Z})$ denote the additive group of integer matrices, and define the subgroup $\Lambda_d < \mathrm{Mat}_d(\mathbb{Z})$ by

$$\Lambda_d = \big\{a \in \mathrm{Mat}_d(\mathbb{Z}) : \mathrm{tr}(a) = 0\big\}.$$

Given a matrix $a \in \Lambda_d$, we write $\mathcal{C}(a) = \det(tI - a) \in \mathbb{Z}[t]$ to denote its characteristic polynomial. We note that the map $\mathcal{C} : \Lambda_d \to \mathbb{Z}[t]$ satisfies $\mathcal{C}(\gamma a \gamma^{-1}) = \mathcal{C}(a)$ for all $a \in \Lambda_d$ and $\gamma \in \mathrm{GL}_d(\mathbb{Z})$.

The following theorem is an extension of a very recent result by the first author and A. Fish in the paper [4], to which the current paper owes the initial ideas.

Theorem 1.4. *Let $d \geq 2$ and $E \subset \Lambda_d$ a set of positive upper Banach density. Let m be a positive integer. Then there exists a positive integer k with the property that for every finite subset $F \subset \Lambda_d$ with $|F| = m$, we have*

$$\mathcal{C}(kF) \subset \mathcal{C}(E - b), \quad \textit{for some } b \in E.$$

If E is an aperiodic Bohr set, then k can be chosen to be 1. *In particular, if E is an aperiodic* Bohr_o*-set, then $\mathcal{C}(E) = \mathcal{C}(\Lambda_d)$.*

Remark 1.5. During the finalization of this paper, the authors were informed by A. Fish that he had independently proved the last assertion in Theorem 1.4 (concerning aperiodic Bohr_o sets); see [7].

Given $a \in \Lambda_d$, we denote by $\mathbb{Q}_a$ the field generated by the eigenvalues of a, or equivalently, the splitting field of the polynomial $\mathcal{C}(a)$. We note that

$$\mathbb{Q}_{ka} = \mathbb{Q}_a \quad \text{and} \quad \mathbb{Q}_{\gamma a \gamma^{-1}} = \mathbb{Q}_a, \quad \text{for all } k \in \mathbb{Q}^* \text{ and } \gamma \in \mathrm{GL}_d(\mathbb{Z}).$$

Given $P \in \mathbb{Z}[t]$, we let $\mathcal{G}(P)$ denote the Galois group (over $\mathbb{Q}$) of the splitting field of P. Thus $\mathcal{G}(\mathcal{C}(a))$ is the Galois group of the field extension $\mathbb{Q}_a/\mathbb{Q}$. Since each $\mathcal{C}(a)$ is a monic polynomial of degree d, we see that each $\mathcal{G}(\mathcal{C}(a))$ is a subgroup of the symmetric group S_d. Let $\mathcal{G}_d$ denote the set of all possible subgroups $\mathcal{G}(\mathcal{C}(a)) < S_d$ as a ranges over Λ_d. From the relations above, we see that

$$\mathcal{G}(\mathcal{C}(ka)) = \mathcal{G}(\mathcal{C}(a)) \quad \text{and} \quad \mathcal{G}(\mathcal{C}(\gamma a \gamma^{-1})) = \mathcal{G}(\mathcal{C}(a)), \quad \text{for all } k \in \mathbb{N}^* \text{ and } \gamma \in \mathrm{GL}_d(\mathbb{Z}).$$

Let $F \subset \mathbb{Z}^N$ be a finite set such that $\mathcal{G}(F) = \mathcal{G}_d$. Upon applying the map $\mathcal{G}$ to the sets $\mathcal{C}(kF)$ and $\mathcal{C}(E - b)$ in Theorem 1.4, we have established the following corollary. We stress that this result also follows from Furstenberg–Katznelson's Theorem mentioned in the beginning of the introduction.

Corollary 1.6. *Let $d \geq 2$ and suppose that $E \subset \Lambda_d$ is a set of positive upper Banach density. Then there exists $b \in E$ such that $\mathcal{G}_d \subset \mathcal{G}(\mathcal{C}(E - b))$, i.e. all possible Galois groups can be found in some translate of E.*

This result should be compared with Gallagher's Theorem [12] which asserts that "most" irreducible monic polynomials with integer coefficients have Galois group S_d.

1.3. Determinants of symmetric matrices. Our final example involves determinants of symmetric integer matrices. We let $\mathrm{Sym}_d = \{a \in \mathrm{Mat}_d(\mathbb{Z}) \mid a = a^t\}$ denote the set of all symmetric $d \times d$ integer matrices.

Theorem 1.7. *Let $d \geq 2$ and $E \subset \mathrm{Sym}_d$ a set of positive upper Banach density. Let m be a positive integer. Then there exists a positive integer k with the property that for every finite subset $F \subset \mathrm{Sym}_d$ with $|F| = m$, we have*

$$k^d \det(F) \subset \det(E - b), \quad \textit{for some } b \in E.$$

If E is an aperiodic Bohr set, then k can be chosen to be 1. *In particular, if E is an aperiodic* Bohr_o*-set, then* $\det(E) = \mathbb{Z}$.

In particular, let $E_o \subset \mathbb{Z}$ be an aperiodic Bohr_o-set, and define

$$E = \left\{\left(\begin{smallmatrix} x & z \\ z & y \end{smallmatrix}\right) : x, y, z \in E_o\right\} \subset \mathrm{Sym}_2 .$$

Then E is a Bohr_o-set in $\mathrm{Sym}_2 \cong \mathbb{Z}^3$ to which Theorem 1.7 can applied to yield the following corollary.

Corollary 1.8. *Suppose that $E_o \subset \mathbb{Z}$ is an aperiodic Bohr_o-set. Then,*

$$\{xy - z^2 : x, y, z \in E_o\} = \mathbb{Z}.$$

1.4. Invariant patterns in sets of positive upper Banach density. We now turn to generalizing the three examples above. The main idea is that the functions presented in those examples (the quadratic forms, the characteristic polynomial map and the determinant map) are all invariant under certain linear actions. More specifically, the quadratic form Q in Theorem 1.3 is preserved by $\mathrm{SO}(Q)(\mathbb{Z})$; the characteristic polynomial map $\mathcal{C}$ and the Galois group map $\mathcal{G}$ on Λ_d are both preserved by the conjugation action of $\mathrm{SL}_d(\mathbb{Z})$ on Λ_d; while the determinant map is preserved by the action of $\mathrm{SL}_d(\mathbb{Z})$ on Sym_d given by $\gamma \cdot a = \gamma a \gamma^t$. One of the main goals of this paper is to establish the following general result, to which the examples above apply (this will be verified in Appendix B).

Definition 1.9. A subgroup $\Gamma \leq \mathrm{GL}_N(\mathbb{R})$ is said to be *strongly irreducible* if for every finite index subgroup $\Gamma' \leq \Gamma$, the standard representation of Γ' on $\mathbb{R}^N$ is irreducible. We say that a Zariski connected real algebraic group G has *no compact factors* if every Zariski-continuous group homomorphism $\rho : G \to \mathrm{GL}_r(\mathbb{R})$ with bounded image is trivial (cf. Section 2 in [2]). To avoid confusion when necessary (in Appendix B), the usual Lie group theoretic compact factors will be referred to as the *compact Lie group factors*.

Theorem 1.10. *Let $\Gamma < \mathrm{GL}_N(\mathbb{Z})$ be a non-trivial finitely generated strongly irreducible subgroup whose Zariski closure in $\mathrm{GL}_N(\mathbb{R})$ is a Zariski connected semisimple group with no compact factors. Let Y be a set and suppose that $\Psi : \mathbb{Z}^N \to Y$ is a Γ-invariant function. For every $E \subset \mathbb{Z}^N$ of positive upper Banach density and $m \geq 1$, there exists a positive integer k with the property that whenever $F \subset \mathbb{Z}^N$ is a finite set of cardinality m, then*

$$\Psi(kF) \subset \Psi(E - b), \quad \text{for some } b \in E.$$

Moreover, if $E \subset \mathbb{Z}^N$ is an aperiodic Bohr*-set, then k can be chosen to be* 1*. In particular, if E is an aperiodic* Bohr$_o$*-set, then $\Psi(E) = \Psi(\mathbb{Z}^N)$.*

The following result is an immediate consequence of Theorem 1.10, and generalizes the main result in [4].

Corollary 1.11. *Let Γ and Ψ be as in Theorem 1.10 and suppose that $E \subset \mathbb{Z}^N$ has positive upper Banach density. Then there exists a positive integer k such that*

$$\Psi(k\,\mathbb{Z}^N) \subset \Psi(E - E).$$

1.5. Twisted multiple recurrence. Theorem 1.10 is derived from a "twisted" multiple recurrence result for ergodic $\mathbb{Z}^N$-actions which we shall now state. Let (X, ν) be a Borel probability measure space, i.e. X is a Borel subset of a compact and second countable space $\overline{X}$, and ν is a probability measure on the restriction of the Borel σ-algebra on $\overline{X}$ to X. Suppose that $\mathbb{Z}^N$ acts on X by Borel measurable bijections, which preserve ν. In this case we refer to (X, ν) as a $\mathbb{Z}^N$*-space*. We say that (X, ν) is *ergodic* if whenever $B \subset X$ is a Borel set which is invariant under $\mathbb{Z}^N$, then B is either a ν-null set or a ν-conull set.

We note that one can always associate to any $\mathbb{Z}^N$-space a unitary representation π_X of $\mathbb{Z}^N$ on the Hilbert space $L^2(X, \nu)$ via

$$\big(\pi_X(a)\, f\big)(x) = f((-a) \cdot x), \quad \text{for } a \in \mathbb{Z}^N \text{ and } f \in L^2(X, \nu).$$

Given a character χ on $\mathbb{Z}^N$, we write

$$L^2(X, \nu)_\chi = \big\{ f \in L^2(X, \nu) : \pi_X(a) f = \chi(a) f \big\} \subset L^2(X, \nu).$$

We say that χ is a *rational character* if there exists a positive integer m such that $\chi(ma) = 1$ for all $a \in \mathbb{Z}^N$. The set of all rational χ for which $L^2(X, \nu)_\chi$ is non-zero is called the *rational spectrum* of the $\mathbb{Z}^N$-space (X, ν). Since the constant function 1 is fixed by π_X, we note that the rational spectrum always contains the trivial character 1. If there are no other elements in the rational spectrum, we say that the rational spectrum is *trivial*.

Theorem 1.12. *Let (X, ν) be an ergodic $\mathbb{Z}^N$-space and suppose that B is a Borel set in X. Let Γ be as in Theorem 1.10. For every $\varepsilon > 0$ and integer $m \geq 1$, there*

exists a positive integer k with the property that whenever $a_1, \dots, a_m$ are elements in $k\,\mathbb{Z}^N$, then then there are $\gamma_1, \dots, \gamma_m \in \Gamma$ such that

$$\nu\Big(\bigcap_{j=1}^{m} (\gamma_j a_j) \cdot B\Big) \geq \nu(B)^m - \varepsilon.$$

If the rational spectrum of the $\mathbb{Z}^N$-space (X, ν) is trivial, then k can be chosen to be 1.

In Appendix A we outline how the following result can be deduced from Theorem 1.12. For the connection between trivial rational spectrum and aperiodic Bohr sets we refer the reader to Section 3.

Corollary 1.13. *Let $E \subset \mathbb{Z}^N$ be a set of positive upper Banach density and $m \geq 1$. Let Γ be as in Theorem 1.10. For every $\varepsilon > 0$, there exists a positive integer k with the property that whenever $a_1, \dots, a_m$ are elements in $k\,\mathbb{Z}^N$, then there are $\gamma_1, \dots, \gamma_m \in \Gamma$ such that*

$$d^*\Big(\bigcap_{j=1}^{m} (E - \gamma_j a_j)\Big) \geq d^*(E)^m - \varepsilon.$$

If E is an aperiodic Bohr set, then k can be chosen to be 1.

1.6. Proof of Theorem 1.10 using Corollary 1.13. Let Y be a set and $\Psi : \mathbb{Z}^N \to Y$ be a Γ-invariant function. Let $E \subset \mathbb{Z}^N$ be a set of positive upper Banach density and $\varepsilon > 0$ and let m be a positive integer. By Corollary 1.13 we can now find a positive integer k with the property that for all $a_1, \dots, a_m \in k\mathbb{Z}^N$, there are $\gamma_1, \dots, \gamma_m \in \Gamma$ such that

$$d^*\Big(E \cap \bigcap_{j=1}^{m} (E - \gamma_j a_j)\Big) \geq d^*(E)^{m+1} - \varepsilon,$$

If $\varepsilon < d^*(E)^{m+1}$, then the left hand side is positive, and we can find $b \in E$ such that

$$b + \gamma_j a_j \in E, \quad \text{for every } j = 1, \dots, m.$$

In particular, $\Psi(a_j) = \Psi(\gamma_j a_j) \in \Psi(E - b)$ for each j. Since $a_1, \dots, a_m \in k\mathbb{Z}^N$ are arbitrary, this finishes the first part of the proof. Finally, by the second part of Corollary 1.13, if $E \subset \mathbb{Z}^N$ is an aperiodic Bohr$_o$-set, then the integer k above can be chosen to be 1.

1.7. A non-conventional mean ergodic theorem. The proof of Theorem 1.12 will use as a black box some recent deep results by Benoist and Quint from the papers [1] and [3]. The following definition will be useful.

Definition 1.14 (BQ-pair). Let $\Gamma < \mathrm{GL}_N(\mathbb{Z})$ be a non-trivial finitely generated irreducible subgroup and let μ be a finitely supported probability measure on Γ whose support generates Γ as a semigroup. We say that (Γ, μ) is a *BQ-pair* if the Zariski closure of Γ is a Zariski-connected semisimple algebraic group with no compact factors.

Let $(\mathcal{H}, \pi)$ be a unitary $\mathbb{Z}^N$-representation on a separable Hilbert space $\mathcal{H}$. Given a character χ on $\mathbb{Z}^N$, we define

$$\mathcal{H}_\chi = \{v \in \mathcal{H} : \pi(a)v = \chi(a)v, \text{ for all } a \in \mathbb{Z}^N\}.$$

The *rational spectrum* of $(\mathcal{H}, \pi)$ is defined as the set of all rational characters on $\mathbb{Z}^N$ for which $\mathcal{H}_\chi$ is non-zero. We say that the rational spectrum is *trivial* if it is either empty or only consists of the character 1. Finally, we denote by $\mathcal{H}_{\mathrm{rat}}$ the linear span of $\mathcal{H}_\chi$, as χ ranges over the rational spectrum, and we write $\mathcal{H}^G$ for the linear subspace of $\pi(G)$-invariant vectors in $\mathcal{H}$.

Suppose that μ is a probability measure on Γ. We define

$$\mu^{*j}(\gamma) = \sum \mu(\gamma_1) \cdots \mu(\gamma_j), \quad \text{for } j \geq 1,$$

where the sum is taken over all j-tuples $(\gamma_1, \ldots, \gamma_j)$ such that $\gamma_1 \cdots \gamma_j = \gamma$.

Our main technical result in this paper can now be stated as follows.

Theorem 1.15. *Let (Γ, μ) be a BQ-pair and let $(\mathcal{H}, \pi)$ be a unitary $\mathbb{Z}^N$-representation. For every $a \in \mathbb{Z}^N$ and $v \in \mathcal{H}$, the limit*

$$Q_a v := \lim_n \frac{1}{n} \sum_{j=1}^{n} \Big(\sum_{\gamma \in \Gamma} \mu^{*j}(\gamma) \pi(\gamma a) v \Big),$$

exists in the norm topology on $\mathcal{H}$. Furthermore, for every $\varepsilon > 0$ and $v \in \mathcal{H}$, there exists a positive integer k with the property that whenever $a \in k\mathbb{Z}^N$, then

$$\| Q_a v - P_{\mathrm{rat}} v \| < \varepsilon,$$

where P_{rat} denotes the orthogonal projection onto $\mathcal{H}_{\mathrm{rat}}$. If the rational spectrum of $(\mathcal{H}, \pi)$ is trivial, then Q_a coincides with the orthogonal projection onto the space of π-invariant vectors, for all $a \in \mathbb{Z}^N \setminus \{0\}$.

1.8. Proof of Theorem 1.12 using Theorem 1.15. Let (X, ν) be an ergodic $\mathbb{Z}^N$-space and let $(L^2(X, \nu), \pi_X)$ be the associated $\mathbb{Z}^N$-representation as in Subsection 1.5. Since (X, ν) is ergodic, we see that all π_X-invariant elements are (ν-essentially) constant functions. Let $f = \mathbb{1}_B \in L^2(X, \nu)$ be the indicator function of a measurable non-null set $B \subset X$, and define

$$\big(Q_a^{(n)} f\big)(x) = \frac{1}{n} \sum_{j=1}^{n} \Big(\sum_{\gamma \in \Gamma} \mu^{*j}(\gamma) \big(\pi_X(\gamma a) f\big)(x) \Big), \quad \text{for } a \in \mathbb{Z}^N.$$

Let $f_{\mathrm{rat}} = P_{\mathrm{rat}} f$ and fix $m \in \mathbb{N}$ and $\varepsilon > 0$. By Theorem 1.15 and the fact that P_{rat} can be expressed as a conditional expectation (see §7.4 in [6]), we know that:

- There exists a positive integer k such that for all $a \in k\mathbb{Z}^N \setminus \{0\}$, and sufficiently large n, we have

$$\| Q_a^{(n)} f \|_\infty \leq 1 \quad \text{and} \quad \| Q_a^{(n)} f - f_{\mathrm{rat}} \| < \frac{\varepsilon}{m}.$$

- We have

$$0 \leq f_{\mathrm{rat}} \leq 1 \quad \text{and} \quad \int_X f_{\mathrm{rat}} \, d\nu = \int_X f \, d\nu.$$

- If the rational spectrum of (X, ν) is trivial, then $Q_a = P_{\mathrm{rat}}$ and $Q_a f = \int_X f \, d\nu$ for all non-zero $a \in \mathbb{Z}^N$. In particular, the integer k above can be chosen to be one.

Now fix $a_1, \ldots, a_m \in k\mathbb{Z}^n$. Hence, for some sufficiently large n, we have

$$\int_X Q_{a_1}^{(n)} f(x) \cdots Q_{a_m}^{(n)} f(x) \, d\nu(x) \geq \int_X f_{\mathrm{rat}}^{m-s} f^s \, d\nu - \varepsilon,$$

where s denotes the number of a_i's equal to zero (note that $Q_0 f = f$). If $s > 0$ then, since $f_{\mathrm{rat}}^{m-s} \in \mathcal{H}_{\mathrm{rat}}$ and $f^s = f$, we have

$$\int_X f_{\mathrm{rat}}^{m-s} f^s \, d\nu = \int_X f_{\mathrm{rat}}^{m-s} f \, d\nu = \int_X f_{\mathrm{rat}}^{m-s+1} \, d\nu \geq \int_X f_{\mathrm{rat}}^m \, d\nu.$$

Hence in either case we have

$$\begin{aligned} \int_X Q_{a_1}^{(n)} f(x) \cdots Q_{a_m}^{(n)} f(x) \, d\nu(x) &\geq \int_X f_{\mathrm{rat}}^m \, d\nu - \varepsilon \\ &\geq \Big(\int_X f_{\mathrm{rat}} \, d\nu \Big)^m - \varepsilon = \Big(\int_X f \, d\nu \Big)^m - \varepsilon, \end{aligned}$$

where in the second to last step we used Hölder's inequality. Upon writing out the definitions of the operators $Q_\bullet^{(n)}$, and using that f is non-negative, we see that not all terms in the expansions can be less than the right hand side, and thus, for all $a_1, \ldots, a_m \in k\mathbb{Z}^N$, we can find $\gamma_1, \ldots, \gamma_m \in \Gamma$ such that

$$\int_X f((-\gamma_1 a_1) \cdot x) \cdots f((-\gamma_m a_m) \cdot x) \, d\nu(x) \geq \Big(\int_X f \, d\nu \Big)^m - \varepsilon,$$

which gives Theorem 1.12.

2. Proof of Theorem 1.15

Let $\mathbb{T}^N$ denote the set of all homomorphisms from $\mathbb{Z}^N$ into $S^1 = \{z \in \mathbb{C}^* : |z| = 1\}$, and note that $\mathrm{GL}_N(\mathbb{Z})$ acts on $\mathbb{T}^N$ by

$$(\gamma^*\chi)(a) = \chi(\gamma^{-1}a), \quad \text{for } \chi \in \mathbb{T}^N \text{ and } \gamma \in \mathrm{GL}_N(\mathbb{Z}).$$

Given $\chi \in \mathbb{T}^N$ and $\Gamma < \mathrm{GL}_N(\mathbb{Z})$, we define

$$\Gamma_\chi = \{\gamma \in \Gamma : \gamma^*\chi = \chi\} < \Gamma.$$

We recall that an element $\chi \in \mathbb{T}^N$ is called *rational* if there exists a positive integer m such that $\chi(ma) = 1$ for all $a \in \mathbb{Z}^N$.

Lemma 2.1. *Suppose that $\Gamma < \mathrm{GL}_N(\mathbb{Z})$ is infinite[1] and strongly irreducible and $\chi \in \mathbb{T}^N$. Then the index $[\Gamma : \Gamma_\chi]$ is finite if and only if χ is rational.*

Proof. Suppose that $[\Gamma : \Gamma_\chi]$ is finite, hence Γ_χ is non-trivial as Γ is infinite. Then $\Lambda = \ker \chi < \mathbb{Z}^N$ is a non-trivial Γ_χ-invariant subgroup, and thus $V = \Lambda \otimes \mathbb{R} < \mathbb{R}^N$ is a non-trivial Γ_χ-invariant linear subspace. By strong irreducibility of Γ, we have $V = \mathbb{R}^N$, and thus Λ must have finite index in $\mathbb{Z}^N$. Let m be the order of $\mathbb{Z}^N/\Lambda$. Then we have $\chi^m = 1$, and thus χ is rational.

Suppose that χ is rational. Then $\Lambda = \ker \chi < \mathbb{Z}^N$ has finite index, and Γ acts on the finite set $\mathrm{Im}\,\chi \cong \mathbb{Z}^N/\Lambda$, which shows that $\Gamma_\chi = \mathrm{Stab}_\Gamma \Lambda$ has finite index in Γ. □

The main technical ingredient in the proof of Theorem 1.15 is the following deep result by Benoist and Quint; see Théorème 1.3 in [1] and Corollary 1.10b) in [3]. If Γ in addition contains an element with a dominant eigenvalue of multiplicity one, then this result was established earlier by Bourgain, Furman, Lindenstrauss and Mozes; see Theorem B in [5].

Theorem 2.2. *Let (Γ, μ) be a BQ-pair. For every $\chi \in \mathbb{T}^N$ and $a \in \mathbb{Z}^N \setminus \{0\}$, we have*

$$\lim_n \frac{1}{n} \sum_{j=1}^{n} \Big(\sum_{\gamma \in \Gamma} \chi(\gamma a) \mu^{*j}(\gamma) \Big) = 0,$$

if $[\Gamma : \Gamma_\chi] = \infty$, and

$$\lim_n \frac{1}{n} \sum_{j=1}^{n} \Big(\sum_{\gamma \in \Gamma} \chi(\gamma a) \mu^{*j}(\gamma) \Big) = \frac{1}{[\Gamma : \Gamma_\chi]} \sum_{\gamma \in \Gamma_\chi \backslash \Gamma} \chi(\gamma a),$$

if $[\Gamma : \Gamma_\chi] < \infty$.

[1] This is satisfied for Γ coming from a BQ pair: If Γ is non-trivial and has Zariski connected Zariski closure, then it must be infinite.

Remark 2.3. We stress that Theorem 2.2 is not explicated in neither of the papers [1] or [3]. Under the assumption that (Γ, μ) is a BQ-pair, Corollary 1.10b) in [3] asserts that for every $\chi \in \mathbb{T}^N$, there exists a Γ-invariant Borel probability measure on ν_χ on $\mathbb{T}^N$, supported on the closure of the Γ-orbit of χ, such that for every continuous function $f : \mathbb{T}^N \to \mathbb{C}$, we have

$$\frac{1}{n}\sum_{k=1}^{n}\Big(\sum_{\gamma\in\Gamma} f((\gamma^*)^{-1}\chi)\mu^{*j}(\gamma)\Big) = \int_{\mathbb{T}^N} f\, d\nu_\chi.$$

By Théorème 1.3 in [1], ν_χ is either the counting probability measure on a the (finite) Γ-orbit of χ in $\mathbb{T}^N$ (in which case the index $[\Gamma : \Gamma_\chi]$ is finite), or it is equal to the Haar probability measure on $\mathbb{T}^N$. We get Theorem 2.2 by letting $f(\chi) = \chi(a)$ for $a \in \mathbb{Z}^N$.

Let $(\mathcal{H}, \pi)$ be a unitary $\mathbb{Z}^N$-representation on a separable Hilbert space $\mathcal{H}$. Given $\chi \in \mathbb{T}^N$, we recall that we by $\mathcal{H}_\chi$ denote the Hilbert sub-spaces

$$\mathcal{H}_\chi = \big\{v \in \mathcal{H} \,:\, \pi(a)v = \chi(a)v, \ \text{ for all } a \in \mathbb{Z}^N\big\}.$$

One readily verifies that if χ_1 and χ_2 are distinct elements in $\mathbb{T}^N$, then $\mathcal{H}_{\chi_1}$ and $\mathcal{H}_{\chi_2}$ are orthogonal subspaces in $\mathcal{H}$. Since $\mathcal{H}$ is separable, we conclude that there is a possibly empty, but at most countable, set $\Omega \subset \mathbb{T}^N$ such that $\mathcal{H}_\chi$ is a non-trivial subspace for $\chi \in \Omega$. The set of rational elements in Ω will be denoted by $\mathcal{R}_N$, which we shall refer to as the *rational spectrum* of $(\mathcal{H}, \pi)$, and we write

$$\mathcal{H}_{\text{rat}} = \bigoplus_{\chi\in\mathcal{R}_N} \mathcal{H}_\chi \subset \mathcal{H},$$

where the direct sum is taken in the Hilbert space sense. The following lemma is an immediate consequence of the definitions above and the second assertion in Theorem 2.2, so we omit the proof.

Lemma 2.4. *For every $v \in \mathcal{H}_{\text{rat}}$ and $a \in \mathbb{Z}^N$, we have*

$$\lim_n \frac{1}{n}\sum_{j=1}^{n}\Big(\sum_{\gamma\in\Gamma}\mu^{*j}(\gamma)\pi(\gamma a)v\Big) = \sum_{\chi\in\mathcal{R}_N}\Big(\frac{1}{[\Gamma:\Gamma_\chi]}\sum_{\gamma\in\Gamma_\chi\backslash\Gamma}\chi(\gamma a)\Big)v_\chi$$

where $v = \sum v_\chi$ and $v_\chi \in \mathcal{H}_\chi$.

The full force of Theorem 2.2 is released in the proof of the following lemma.

Lemma 2.5. *For every $v \in \mathcal{H}_{\text{rat}}^{\perp}$ and $a \in \mathbb{Z}^N \setminus \{0\}$, we have*

$$\lim_n \frac{1}{n}\sum_{j=1}^{n}\Big(\sum_{\gamma\in\Gamma}\mu^{*j}(\gamma)\pi(\gamma a)v\Big) = 0.$$

Proof. Let $v \in \mathcal{H}_{\mathrm{rat}}^{\perp}$ with $\|v\| = 1$. By Bochner's Theorem, there exists a Borel probability measure η on $\mathbb{T}^N$ such that

$$\langle \pi(a)v, v\rangle = \int_{\mathbb{T}^N} \chi(a)\, d\eta(\chi), \quad \text{for all } a \in \mathbb{Z}^N.$$

We observe that, by an application of von-Neumann's mean ergodic theorem to the unitary $\mathbb{Z}^N$-representation $(\mathcal{H}, \pi_\chi)$ given by

$$\pi_\chi(a)v = \chi(a)^{-1}\pi(v) \quad \text{for } a \in \mathbb{Z}^N \text{ and } v \in \mathcal{H},$$

we have that $\eta(\{\chi\}) = 0$ for every *rational* $\chi \in \mathbb{T}^N$. We note that

$$\Big\| \frac{1}{n} \sum_{j=1}^{n} \Big(\sum_{\gamma\in\Gamma} \mu^{*j}(\gamma)\pi(\gamma a)v \Big) \Big\|^2 = \int_{\mathbb{T}^N} \Big| \frac{1}{n} \sum_{j=1}^{n} \Big(\sum_{\gamma\in\Gamma} \mu^{*j}(\gamma)\chi(\gamma a) \Big) \Big|^2 d\eta(\chi),$$

for all n. By Lemma 2.1, we have $[\Gamma : \Gamma_\chi] = \infty$ for every irrational χ and $[\Gamma : \Gamma_\chi] < \infty$ for every rational χ. Hence, by Theorem 2.2, we conclude that the right-hand side above converges to

$$\sum_{\chi\in\mathcal{R}_N} \Big| \frac{1}{[\Gamma : \Gamma_\chi]} \sum_{\gamma\in\Gamma_\chi\backslash\Gamma} \chi(\gamma a) \Big|^2 \eta(\{\chi\}) = 0,$$

since $\eta(\{\chi\}) = 0$ for all $\chi \in \mathcal{R}_N$, which finishes the proof. □

Upon combining Lemma 2.4 and Lemma 2.5, we conclude that the limits

$$Q_a v = \lim_n \frac{1}{n} \sum_{j=1}^{n} \Big(\sum_{\gamma} \mu^{*j}(\gamma)\, \pi(\gamma)v \Big)$$

exist for every $v \in \mathcal{H}$ and $a \in \mathbb{Z}^N \setminus \{0\}$, and

$$Q_a v = \sum_{\chi\in\mathcal{R}_N} \Big(\frac{1}{[\Gamma : \Gamma_\chi]} \sum_{\gamma\in\Gamma_\chi\backslash\Gamma} \chi(\gamma a) \Big) v_\chi,$$

where $P_{\mathrm{rat}} v = \sum v_\chi$ and $v_\chi \in \mathcal{H}_\chi$. In particular, if $\mathcal{R}_N$ is trivial, i.e. if $\mathcal{R}_N$ is either empty or consists solely of the trivial character 1, then Q_a coincides with the orthogonal projection onto the closed subspace of $\pi(G)$-invariant elements in $\mathcal{H}$.

The second assertion of Theorem 1.15 follows from the following lemma. Here, P_{rat} denotes the orthogonal projection onto $\mathcal{H}_{\mathrm{rat}}$.

Lemma 2.6. *For every $\varepsilon > 0$ and $v \in \mathcal{H}$, there exists a positive integer k such that*

$$\big\| Q_a v - P_{\mathrm{rat}} v \big\| < \varepsilon, \quad \textit{for all } a \in k\mathbb{Z}^N \setminus \{0\}.$$

Proof. Since $Q_a = 0$ on $\mathcal{H}_{\text{rat}}^{\perp}$, it suffices to prove the lemma for $v \in \mathcal{H}_{\text{rat}}$. Pick $\varepsilon > 0$ and $v \in \mathcal{H}_{\text{rat}}$ and choose a finite set $F \subset \mathbb{R}_N$ such that

$$\sum_{\chi \notin F} \|v_\chi\|^2 < \varepsilon^2.$$

Since F is a finite set, we can find at least one positive integer k such that $\chi(ka) = 1$ for all $\chi \in F$ and $a \in \mathbb{Z}^N$. We note that this implies that $Q_{ka} v_\chi = v_\chi$ for all $a \in \mathbb{Z}^N$, and thus

$$\|Q_a v - v\| = \Big\| \sum_{\chi \notin F} Q_a v_\chi \Big\| \le \Big(\sum_{\chi \notin F} \|v_\chi\|^2 \Big)^{\frac{1}{2}} < \varepsilon,$$

since $\|Q_a v\| \le \|v\|$ for all $v \in \mathcal{H}$ and $Q_a \mathcal{H}_\chi \subset \mathcal{H}_\chi$ for all $\chi \in \mathcal{R}_N$. □

3. Bohr sets and rational spectrum

We say that $E \subset \mathbb{Z}^N$ is a *Bohr set* if there exist a compact and second countable abelian group K with Haar probability measure m_K, a homomorphism $\tau : \mathbb{Z}^N \to K$ with dense image, and a non-empty open set $U \subset K$ with $m_K(\overline{U}) = m_K(U)$ such that $E = \tau^{-1}(U)$. If K is connected, we say that E is *aperiodic*, and if U contains the identity element of K, we say that B is an *aperiodic Bohr$_o$* set. We note that if $B \subset \mathbb{Z}^N$ is any aperiodic Bohr$_o$-set, then one can always find another Bohr$_o$-set C such that $C - C \subset B$.

Example 3.1. We give here an example of an aperiodic Bohr set in $\mathbb{Z}$. Let $K = \mathbb{R}/\mathbb{Z}$ and suppose that ϑ is an *irrational* number. Then $\tau(a) = a \cdot \vartheta \mod 1$ is a homomorphism from $\mathbb{Z}$ into K with dense image. Let $U \subset K$ be an open subset, e.g. an open interval. Then

$$B = \tau^{-1}(U) = \big\{ a \in \mathbb{Z} : a \cdot \vartheta \bmod 1 \in U \big\} \subset \mathbb{Z}$$

is an aperiodic Bohr set in $\mathbb{Z}$. More generally, for every integer N, we can form the homomorphism $\tau_N : \mathbb{Z}^N \to K^N$ defined by

$$\tau(a_1, \dots, a_N) = (\tau(a_1), \dots, \tau(a_N)), \quad \text{for } (a_1, \dots, a_N) \in \mathbb{Z}^N.$$

One can readily check that τ_N has dense image in K^N, and thus

$$B \times \cdots \times B = \tau_N^{-1}(U \times \cdots \times U) \subset \mathbb{Z}^N$$

is an aperiodic Bohr$_o$-set in $\mathbb{Z}^N$.

We can make (K, m_K) into a $\mathbb{Z}^N$-space with the $\mathbb{Z}^N$-action defined by

$$a \cdot x = x - \tau(a), \quad \text{for } x \in K \text{ and } a \in \mathbb{Z}^N.$$

We denote by π_K the regular representation of $\mathbb{Z}^N$ on $L^2(K, m_K)$ and given $\chi \in \mathbb{T}^N$, we define

$$L^2(K, m_K)_\chi = \{f \in L^2(K, m_K) : \pi_K(a) f = \chi(a) f\}.$$

Let $\widehat{K}$ denote the dual of K. We can view $\eta \in \widehat{K}$ as an element in $L^2(K, m_K)$ with the property that $\pi_K(a)\eta = \eta(\tau(a))\eta$ for all $a \in \mathbb{Z}^N$. Note that if $\eta_1, \eta_2 \in \widehat{K}$ satisfy $\eta_1 \circ \tau = \eta_2 \circ \tau$, then $\eta_1 = \eta_2$ since the image of τ is dense. In particular, for every $\chi \in \mathbb{T}^N$ of the form $\chi = \eta \circ \tau$, we have

$$L^2(K, m_K)_\chi = \mathbb{C} \cdot \eta.$$

Since all η are orthogonal to each other in $L^2(K, m_K)$, and together span $L^2(K, m_K)$, we conclude that

$$L^2(K, m_K) = \bigoplus_{\eta \in \widehat{K}} L^2(K, m_K)_{\eta \circ \tau},$$

where the direct sum is taken in the Hilbert space sense. Suppose that $\chi = \eta \circ \tau$ is rational, i.e. assume that there exists a positive integer m such that $\chi^m = 1$. Then,

$$\chi(a)^m = \eta(m\tau(a)) = \eta(\tau(ma)) = 1, \quad \text{for all } a \in \mathbb{Z}^N,$$

and thus $\eta(k) = 1$ for all $k \in L$, where $L := \overline{\tau(m\mathbb{Z}^N)} < K$, by continuity of η. One readily shows that L has finite index in K and thus is an open subgroup of K. In particular, if K is *connected*, then $L = K$, and $\eta = 1$, which establishes the following lemma.

Lemma 3.2. *Let K be a compact and connected abelian group and suppose that $\tau : \mathbb{Z}^N \to K$ is a homomorphism with dense image. Then the associated $\mathbb{Z}^N$-space (K, m_K) has trivial rational spectrum.*

Acknowledgements. The authors have greatly benefited from discussions with Alexander Fish, Peter Hegarty and Jean-François Quint. This work was carried out during the second author's visit to Chalmers University in September and October of 2015 funded by the University of Sydney's *Philipp Hofflin International Research Travel Scholarship*, for which he is very grateful for. He would like to also thank the Department of Mathematical Sciences at Chalmers University for their hospitality.

A. Correspondence principle

We shall now explain how one can deduce Corollary 1.13 from Theorem 1.12. The arguments in this section are nowadays rather standard, and can be traced back to the seminal paper [9] by Furstenberg.

Suppose that $E \subset \mathbb{Z}^N$. We may view E as an element in the compact and second countable space $2^{\mathbb{Z}^N}$ of all subsets of $\mathbb{Z}^N$ equipped with the product topology, on which $\mathbb{Z}^N$ acts by homeomorphisms via

$$a \cdot A = A - a, \quad \text{for } A \in 2^{\mathbb{Z}^N} \text{ and } a \in \mathbb{Z}^N.$$

Let X denote the closure of $\mathbb{Z}^N \cdot E$ in $2^{\mathbb{Z}^N}$. Then X is again a compact and second countable space, and

$$V = \{A \in X \,:\, 0 \in A\} \subset X, \tag{A.1}$$

is a clopen (closed and open) subset of X. We note that $E = \{a \in \mathbb{Z}^N \,:\, a \cdot E \in V\}$. In other words, E can be realized as the "hitting times" of the set V of the $\mathbb{Z}^N$-orbit of E in X.

More generally, let X be a compact and second space, equipped with an action of $\mathbb{Z}^N$ by homeomorphisms. Given a subset $U \subset X$ and $x \in X$, we define

$$U_x = \{a \in \mathbb{Z}^N \,:\, a \cdot x \in U\} \subset \mathbb{Z}^N.$$

For instance, if K is a compact and connected second countable group, $\tau : \mathbb{Z}^N \to K$ is a homomorphism with dense image and (K, m_K) denotes the associated $\mathbb{Z}^N$-space defined in Section 3, then for any non-empty open subset $U \subset K$, we see that

$$U_0 = \{a \in \mathbb{Z}^N \,:\, \tau(a) \in -U\} = \tau^{-1}(-U) \subset \mathbb{Z}^N \tag{A.2}$$

is an aperiodic Bohr set. Since K is connected, the $\mathbb{Z}^N$-space (K, m_K) has trivial rational spectrum by Lemma 3.2.

Let $F_n = [-n, n]^N \subset \mathbb{Z}^N$ and define the *upper Banach density* of a subset $E \subset \mathbb{Z}^N$ by

$$d^*(E) = \sup\left\{ \limsup_n \frac{|E \cap (F_n + a_n)|}{|F_n|} \,:\, (a_n) \text{ is a sequence in } \mathbb{Z}^N \right\}.$$

In particular,

$$d^*(E) \geq \limsup_n \frac{|E \cap F_n|}{|F_n|}, \quad \text{for all } E \subset \mathbb{Z}^N.$$

Let $\mathcal{P}_{\mathbb{Z}^N}(X)$ denote the (non-empty) convex set of $\mathbb{Z}^N$-invariant Borel probability measures on the compact and second countable space X. The following proposition can now be deduced from Theorem 1.1 in [9].

Proposition A.1. *Suppose that $U \subset X$ is open and $x_o \in X$ has a dense $\mathbb{Z}^N$-orbit in X. Then,*

$$d^*\Big(\bigcap_{a \in F} (U_{x_o} - a) \Big) \geq \nu\Big(\bigcap_{a \in F} a \cdot U \Big),$$

for every finite set $F \subset \mathbb{Z}^N$ *and* $\nu \in \mathcal{P}_{\mathbb{Z}^N}(X)$. *Furthermore, if* $\nu(\overline{U}) = \nu(U)$ *for all* $\nu \in \mathcal{P}_{\mathbb{Z}^N}$, *then*

$$d^*(U_{x_o}) = \nu(U), \quad \textit{for some ergodic } \nu \in \mathcal{P}_{\mathbb{Z}^N}(X).$$

A.1. Proof of Corollary 1.13. Suppose that (X, ν) is a compact and second countable $\mathbb{Z}^N$-space, and let $U \subset X$ be a non-empty open set such that $\nu(\overline{U}) = \nu(U)$ for all $\nu \in \mathcal{P}_{\mathbb{Z}^N}(X)$. For instance, we could choose:

- X to be the orbit closure of the set $E \subset \mathbb{Z}^N$ and $U = V$ as in (A.1). In this case, U is a non-empty clopen set, and there exists an ergodic $\nu \in \mathcal{P}_{\mathbb{Z}^N}(X)$ such that
$$d^*(E) = d^*(U_E) = \nu(U).$$
- K to be a compact, connected and second countable group, $\tau : \mathbb{Z}^N \to K$ a homomorphism with dense image and $(X, \nu) = (K, m_K)$ the $\mathbb{Z}^N$-space associated to (K, τ) as in Section 3. In this case, m_K is the unique $\mathbb{Z}^N$-invariant Borel probability measure on K. In particular, for any open subset such that $m_K(\overline{U}) = m_K(U)$, we have $d^*(\tau^{-1}(U)) = m_K(U)$, and $E = \tau^{-1}(U)$ is an aperiodic Bohr set.

Let $\Gamma < \mathrm{GL}_N(\mathbb{Z})$ and $a_1, \ldots, a_m \in \mathbb{Z}^N$. In the first case above, Proposition A.1 guarantees that

$$d^*(E) = \nu(V) \quad \text{and} \quad d^*\Big(\bigcap_{j=1}^{m} \big(E - \gamma_j a_j\big)\Big) \geq \nu\Big(\bigcap_{j=1}^{m} (\gamma_j a_j) \cdot V\Big),$$

for all $\gamma_1, \ldots, \gamma_m$, and in the second case above, Proposition A.1 asserts that

$$d^*(E) = m_K(U) \quad \text{and} \quad d^*\Big(\bigcap_{j=1}^{m} \big(\tau^{-1}(U) - \gamma_j a_j\big)\Big) \geq m_K\Big(\bigcap_{j=1}^{m} (\gamma_j a_j) \cdot U\Big),$$

for all $\gamma_1, \ldots, \gamma_m$.

Let Γ be as in Theorem 1.10 and suppose that (X, ν) and U are as in one of the two examples above. Let $\varepsilon > 0$ and let m be a positive integer. By Theorem 1.12, there exist a positive integer k with the property that whenever $a_1, \ldots, a_m \in k\mathbb{Z}^N$, then

$$\nu\Big(\bigcap_{j=1}^{m} (\gamma_j a_j) \cdot U\Big) \geq \nu(U)^m - \varepsilon, \quad \text{for some } \gamma_1, \ldots, \gamma_m \in \Gamma. \tag{A.3}$$

Furthermore, if (X, ν) has trivial spectrum, as in the second example above (by Lemma 3.2), then k can be chosen to be 1.

Upon combining the bounds above, we conclude that for all $a_1, \ldots, a_m \in k\mathbb{Z}^N$, we have

$$d^*\Big(\bigcap_{j=1}^{m}\big(E-\gamma_j a_j\big)\Big) \geq d^*(E)^m - \varepsilon, \quad \text{for some } \gamma_1, \ldots, \gamma_m \in \Gamma.$$

In the case when $(X, \nu) = (K, m_K)$, the integer k can be chosen to be 1.

B. Verifying the conditions for a BQ-pair

We now verify that our examples satisfy the conditions of a BQ-pair. Note that in each of our examples we have a polynomial group homomorphism $\rho : G \to \mathrm{SL}_N(\mathbb{R})$ for some Zariski closed subgroup $G \leq \mathrm{GL}_d(\mathbb{R})$, which then defines an action of G on $\mathbb{R}^N$ given by $g \cdot v = \rho(g)v$. For example, in Theorem 1.4 we consider the adjoint representation $\mathrm{Ad} : \mathrm{SL}_d(\mathbb{R})) \to GL(\mathfrak{sl}_d(\mathbb{R}))$, given by

$$\mathrm{Ad}(g)v = gvg^{-1} \quad \text{for } g \in \mathrm{SL}_d(\mathbb{R}) \text{ and } v \in \mathfrak{sl}_d(\mathbb{R}),$$

where $\mathfrak{sl}_d(\mathbb{R})$ is the real vector space of real $d \times d$ traceless matrices. In other words, Theorem 1.4 is obtained from Theorem 1.10 by setting $\Gamma = \mathrm{Ad}(\mathrm{SL}_d(\mathbb{Z}))$ (and identifying Λ_d with $\mathbb{Z}^{d^2-1}$). The following Proposition ensures that such a representation ρ preserves certain algebraic conditions in the definition of a BQ-pair.

Proposition B.1. *Let $\rho : G \to \mathrm{SL}_N(\mathbb{R})$ be a polynomial homomorphism, where $G \subset \mathrm{SL}_d(\mathbb{R})$ is a Zariski connected semisimple Lie group with no compact algebraic factors. Then for $\Gamma \leq G$ Zariski dense, we have that the Zariski closure of $\rho(\Gamma)$ is a Zariski connected semisimple Lie group with no compact algebraic factors.*

Proof. By Zariski-continuity, $\rho(G) \leq \overline{\rho(\Gamma)}^Z$ and in fact it is classical that $[\rho(G) : \overline{\rho(\Gamma)}^Z]$ is finite (see for example Corollary 4.6.5 [16]). Hence $\rho(G)$ being semisimple implies that $\overline{\rho(\Gamma)}^Z$ also is. Again by Zariski continuity of ρ, we have that $\overline{\rho(\Gamma)}^Z$ is Zariski connected. Finally, suppose that $\kappa : \overline{\rho(\Gamma)}^Z \to GL_D(\mathbb{R})$ is a bounded algebraic group homomorphism (for some D), then so is $\kappa \circ \rho$ and so $\kappa(\rho(G))$ is the trivial subgroup. Thus $\rho(G) \leq \ker\kappa \leq \overline{\rho(\Gamma)}^Z$. But since $\ker\kappa$ is Zariski closed we have that it is equal to $\overline{\rho(\Gamma)}^Z$, so there are no compact factors. □

B.1. Algebro-geometric properties. We now turn to determining the Zariski closures of $\mathrm{SL}_d(\mathbb{Z})$ and $\mathrm{SO}(Q)(\mathbb{Z})$ and verifying the required algebro-geometric properties (In this appendix, Q will always denote a quadratic form as in Theorem 1.3.). We first note the crucial fact that the groups $\mathrm{SL}_d(\mathbb{Z})$ and $\mathrm{SO}(Q)(\mathbb{Z})$ are, respectively, lattices in $\mathrm{SL}_d(\mathbb{R})$ and $\mathrm{SO}(Q)(\mathbb{R})$ (See Theorem 5.1.11 and

Example 5.1.12 in [15]). We also note that, as required by our main theorems, these lattices are finitely generated (See Theorem 4.7.10 in [15] or Chapter IX in [14]). We will demonstrate below, via Borel's density theorem, that these lattices are Zariski dense. We remark the technicality that we use the following formulation of Borel's density theorem (not explicated in [8] as it demands that G is connected), which follows immediately from a combination of (4.5.1) in [15] and (4.5.2) in [16].

Theorem B.2 (Borel's density theorem). *Let $G \leq \mathrm{SL}_N(\mathbb{R})$ be a Zariski connected semisimple Lie group (in particular, it has finitely many connected components) with no compact Lie group factors. Then any lattice in G is Zariski dense.*

Lemma B.3. *The group $\mathrm{SL}_d(\mathbb{R})$ is the Zariski closure of $\mathrm{SL}_d(\mathbb{Z})$ and is a Zariski-connected semisimple Lie group with no compact factors.*

Proof. Zariski connectedness follows from the fact that $\mathrm{SL}_d(\mathbb{R})$ is connected in the Euclidean topology. The lack of compact factors follows from the much stronger classical fact that the only proper non-trivial normal (abstract) subgroup of $\mathrm{SL}_d(\mathbb{R})$ is its center (in particular, this also shows semisimplicity). Thus Borel's density theorem may be applied. □

From now on, we identify $\mathrm{SO}(Q)(\mathbb{R})$ with $\mathrm{SO}(p,q)(\mathbb{R})$, as can be done via a linear change of coordinates.

Lemma B.4. *For $p,q \geq 1$ with $p+q \geq 3$, the group $\mathrm{SO}(p,q)(\mathbb{R})$ is a Zariski-connected semisimple Lie group with no compact factors. Moreover, the Zariski closure of $\mathrm{SO}(Q)(\mathbb{Z})$ is $\mathrm{SO}(Q)(\mathbb{R}) \cong SO(p,q)(\mathbb{R})$.*

Proof. Let $G = SO(p,q)(\mathbb{R})$ and let G^o denote the connected (in the Euclidean topology) component of $SO(p,q)$. It follows from Problems 9 and 10 of Section 3 in Chapter 1 of [17] that $[G : G^o] = 2$ and that G^o is not Zariski closed. This implies that G is the Zariski closure of G^o and thus is Zariski connected. For $(p,q) \neq (2,2)$ it is well known (see for instance Appendix A in [15]] that G^o is simple as a Lie group and hence has no compact Lie group factors, while for $(p,q) \neq (2,2)$ we have that G is a finite index quotient of $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$ (see Appendix B in [18]) and thus is semisimple with no compact Lie group factors. In either case, we have that G^o is contained in the kernel of all compact (algebraic) factors of G. Hence, since $\mathrm{SO}^o(p,q)(\mathbb{R})$ is not Zariski closed, there are no non-trivial compact (algebraic) factors. Moreover, we may apply Borel's density theorem to obtain that all lattices (and hence $\mathrm{SO}(Q)(\mathbb{Z})$) are Zariski dense in $\mathrm{SO}(Q)(\mathbb{R}) \cong G$. □

B.2. Irreducibility. It now remains to check the strong irreducibility of the subgroups in our examples. Our first lemma shows that in fact it is enough to check the irreducibility of its Zariski closure.

Lemma B.5 (Irreducibility implies strong irreducibility). *Suppose that* $\Gamma \leq \mathrm{GL}_N(\mathbb{Z})$ *is a subgroup such that its Zariski closure* $G = \overline{\Gamma}^Z \leq GL_N(\mathbb{R})$ *is Zariski connected and irreducible. Then* Γ *is a strongly irreducible subgroup of* $GL_N(\mathbb{R})$.

Proof. Let $V \leq \mathbb{R}^N$ be a non-trivial subspace invariant under a finite index subgroup $\Gamma_0 \leq \Gamma$. Then $\overline{\Gamma_0}^Z$ also preserves V and is a finite index Zariski closed subgroup of G, hence $G = \overline{\Gamma_0}^Z$ by Zariski connectedness of G. So G preserves V and so $V = \mathbb{R}^N$, as required. □

Lemma B.6. *The adjoint action (i.e. action by conjugation) of* $\mathrm{SL}_d(\mathbb{R})$ *on* $\mathfrak{sl}_d(\mathbb{R})$ *is irreducible.*

Proof. Let $W \leq \mathfrak{sl}_d(\mathbb{R})$ by a subspace that is invariant under the adjoint action. By differentiating, we see that $[\mathfrak{sl}_d(\mathbb{R}), W] = W$, i.e. W is an ideal. But it is well known that $\mathfrak{sl}_d(\mathbb{R})$ is simple. □

For a representation $G \curvearrowright V$ and $v \in V$, we let $\mathbb{R}[G]v$ denote the smallest G-invariant subspace containing v.

Lemma B.7. *The action of* $SL_d(\mathbb{R})$ *on* Sym_d *given by* $g.A = gAg^t$ *is irreducible.*

Proof. Since each non-zero element of Sym_d is in the G-orbit of some diagonal matrix, it is enough to show that $\mathbb{R}[G]A = \mathrm{Sym}_d$ for each non-zero diagonal matrix A. All positive diagonal matrices (i.e. diagonal matrices with positive diagonal entires) are in the G-orbit of some positive constant multiple of the identity matrix, but the positive diagonal matrices span the space of all diagonal matrices. Thus it remains to show that if we fix a non-zero diagonal matrix $A = \mathrm{diag}(a_1, a_2, \ldots, a_d)$, then the space $\mathbb{R}[G]A$ contains a positive diagonal matrix. Note that the G-orbit of A contains

$$\mathrm{diag}(Ka_1, K^{-1/(d-1)}a_2, \ldots, K^{-1/(d-1)}a_d) \quad \text{for all } K > 0$$

and also

$$\mathrm{diag}(a_{\sigma(1)}, \ldots, a_{\sigma(n)}) \quad \text{for all } \sigma \in S_n,$$

which can be seen from the identity

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d_2 & 0 \\ 0 & d_1 \end{pmatrix}.$$

Assuming (without loss of generality) that $a_1 > 0$, we see (by taking K large enough) that the G-orbit of A contains an element of the form $B_1 = \mathrm{diag}(b_1, \ldots, b_n)$ where $b_1 > d$ and $|b_k| < 1$ for $k = 2, \ldots, d$. The G-orbit of A also contains $B_r = (b_{\sigma(1)}, \ldots, b_{\sigma(n)})$ where σ is the transposition $(1r)$. Thus $B_1 + \cdots + B_d \in \mathbb{R}[G]A$ is a diagonal matrix with positive diagonal entries. □

Lemma B.8. *For $p, q \geq 1$ with $p + q \geq 3$, the action of $SO(p,q)$ on $\mathbb{R}^{p+q}$ is irreducible.*

This will be deduced from the following general observation.

Lemma B.9. *Let V and W be vector spaces with $\dim W > 1$ and let $H \leq GL(V)$, $K \leq GL(W)$ be subgroups acting irreducibly on V and W respectively. Now suppose that $H \times K \leq G \leq GL(V \oplus W)$ is a subgroup such that $V \times \{0\}$ and $\{0\} \times W$ are not G-invariant. Then G acts irreducibly on $V \oplus W$.*

Proof. Choose $x_0 = (v_0, w_0) \in V \oplus W \setminus \{(0,0)\}$ and let $\mathbb{R}[G]x_0$ denote the smallest G-invariant subspace containing x_0. There exists $x_1 = (v_1, w_1) \in \mathbb{R}[G]x_0$ such that $w_1 \neq 0$ (by non-invariance of $V \times \{0\}$). Now since $\dim W > 1$ and K acts irreducibly, there exists $k_1 \in K$ such that $k_1.w_1 \neq w_1$. Hence

$$x_2 := x_1 - (1, k_1).x_1 = (0, w_2) \in \mathbb{R}[G]x_0$$

with $w_2 = w_1 - k_1.w_1 \neq 0$. Since the action of K is irreducible, we have $\{0\} \times W \leq \mathbb{R}[G]x_0$. But since $\{0\} \times W$ is not G-invariant, there exists $(v_3, w_3) \in \mathbb{R}[G]x_0$ such that $v_3 \neq 0$. But $(v_3, 0) = (v_3, w_3) - (0, w_3) \in \mathbb{R}[G]x_0$. So by irreducibility of H we have that $V \times \{0\} \subset \mathbb{R}[G]x_0$. □

The lemma applies (assuming $q \geq 2$) with $V = \mathbb{R}^p$, $W = \mathbb{R}^q$, $H = SO(p)$, $K = SO(q)$ and $G = SO(p,q)$. The non-invariance of V and W follow from considering a natural embedding $SO(1,1) \hookrightarrow SO(p,q)$ and using the fact that $SO(1,1)$ acts irreducibly on $\mathbb{R}^2$ (this can be seen by considering hyperbolic rotations).

References

[1] Y. Benoist and J.-F. Quint, Mesures stationnaires et fermés invariants des espaces homogènes (French) [Stationary measures and invariant subsets of homogeneous spaces], *Ann. of Math. (2)*, **174** (2011), no. 2, 1111–1162. Zbl 1241.22007 MR 2831114

[2] Y. Benoist and J.-F. Quint, Stationary measures and invariant subsets of homogeneous spaces (II), *J. Amer. Math. Soc.*, **26** (2013), no. 3, 659–734. Zbl 1268.22011 MR 3037785

[3] Y. Benoist and J.-F. Quint, Stationary measures and invariant subsets of homogeneous spaces (III), *Ann. of Math. (2)*, **178** (2013), no. 3, 1017–1059. Zbl 1279.22013 MR 3092475

[4] M. Björklund and A. Fish, Characteristic polynomial patterns in difference sets of matrices, *Bull. Lond. Math. Soc.*, **48** (2016), no. 2, 300–308. Zbl 06571543 MR 3483067

[5] J. Bourgain, A. Furman, E. Lindenstrauss, and S. Mozes, Stationary measures and equidistribution for orbits of nonabelian semigroups on the torus, *J. Amer. Math. Soc.*, **24** (2011), no. 1, 231–280. Zbl 1239.37005 MR 2726604

[6] M. Einsiedler and T. Ward, *Ergodic theory with a view towards number theory*, Graduate Texts in Mathematics, 259, Springer-Verlag London, Ltd., London, 2011. Zbl 1206.37001 MR 2723325

[7] A. Fish, Characteristic polynomials of matrices and Bohr sets, *preprint*.

[8] H. Furstenberg, A note on Borel's density theorem, *Proc. Amer. Math. Soc.*, **55** (1976), no. 1, 209–212. Zbl 0319.22010 MR 422497

[9] H. Furstenberg, Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions, *J. Analyse Math.*, **31** (1977), 204–256. Zbl 0347.28016 MR 498471

[10] H. Furstenberg and Y. Katznelson, An ergodic Szemerédi theorem for commuting transformations, *J. Analyse Math.*, **34** (1978), 275–291 (1979). Zbl 0426.28014 MR 531279

[11] H. Furstenberg, Y. Katznelson, and B. Weiss, Ergodic theory and configurations in sets of positive density, in *Mathematics of Ramsey theory*, 184–198, Algorithms Combin., 5, Springer, Berlin, 1990. Zbl 0738.28013 MR 1083601

[12] P. Gallagher, The large sieve and probabilistic Galois theory, in *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, 91–101, Amer. Math. Soc., Providence, R.I., 1973. Zbl 0279.10036 MR 332694

[13] Á. Magyar, On distance sets of large sets of integer points, *Israel J. Math.*, **164** (2008), 251–263. Zbl 1153.11006 MR 2391148

[14] G. A. Margulis, *Discrete subgroups of semisimple Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 17, Springer-Verlag, Berlin, 1991. Zbl 0732.22008 MR 1090825

[15] D. W. Morris, *Introduction to arithmetic groups*, Deductive Press, 2015. Zbl 1319.22007 MR 3307755

[16] D. W. Morris, *Ratner's theorems on unipotent flows*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 2005. Zbl 1069.22003 MR 2158954

[17] A. L. Onishchik and E. B. Vinberg, *Lie groups and algebraic groups*, translated from the Russian and with a preface by D. A. Leites, Springer Series in Soviet Mathematics, Springer-Verlag, Berlin, 1990. Zbl 0722.22004 MR 1064110

[18] A. Zee, *Quantum field theory in a nutshell* second edition, Princeton University Press, Princeton, NJ, 2010. Zbl 1277.81001 MR 2797348

Received April 12, 2016

M. Björklund, Department of Mathematics, Chalmers University,
SE-412 96 Gothenburg, Sweden

E-mail: micbjo@chalmers.se

K. Bulinski, School of Mathematics and Statistics, University of Sydney,
Sydney, NSW 2006, Australia

E-mail: K.Bulinski@maths.usyd.edu.au