Generalizations of Furstenberg’s Diophantine result

ASAF KATZ
Einstein Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem, 91904, Israel
(e-mail: asaf.katz@mail.huji.ac.il)

(Received 31 January 2016 and accepted in revised form 22 June 2016)

Abstract. We prove two generalizations of Furstenberg’s Diophantine result regarding the density of an orbit of an irrational point in the 1-torus under the action of multiplication by a non-lacunary multiplicative semigroup of \( \mathbb{N} \). We show that for any sequences \( \{a_n\}, \{b_n\} \subset \mathbb{Z} \) for which the quotients of successive elements tend to 1 as \( n \) goes to infinity, and any infinite sequence \( \{c_n\} \), the set \( \{a_n b_m c_k x : n, m, k \in \mathbb{N} \} \) is dense modulo 1 for every irrational \( x \). Moreover, by ergodic-theoretical methods, we prove that if \( \{a_n\}, \{b_n\} \) are a sequence having smooth \( p \)-adic interpolation for some prime number \( p \), then for every irrational \( x \), the sequence \( \{p^n a_m b_k x : n, m, k \in \mathbb{N} \} \) is dense modulo 1.

1. Introduction
In his seminal paper [5], Furstenberg proved the following result.

THEOREM. (Furstenberg’s Diophantine result) Assume that \( a, b \) are two multiplicatively independent integers. Then for any irrational \( x \), the set \( \{a^n b^m x : n, m \in \mathbb{N} \} \) is dense in \( \mathbb{R}/\mathbb{Z} \).

In [2], Boshernitzan gave an elementary proof of Furstenberg’s result. Moreover, Furstenberg made the following conjecture, which is still open.

CONJECTURE. (Furstenberg’s \( \times a, \times b \) conjecture) Assume that \( a, b \) are two multiplicatively independent integers, and assume that \( \mu \) is a Borel probability measure on \( \mathbb{R}/\mathbb{Z} \), which is invariant under the maps \( T_a(x) = ax \mod 1 \), \( T_b(x) = bx \mod 1 \), and ergodic. Then \( \mu \) must be the Haar measure or atomic measure.

The strongest result to date towards Furstenberg’s conjecture is the following theorem by Rudolph and Johnson.

THEOREM. [9] In the settings of Furstenberg’s conjecture, if the measure \( \mu \) has positive entropy with respect to \( T_a \), then \( \mu \) is the Haar measure.
Rudolph and Johnson proved their measure-classification result directly by using symbolic dynamics. By different methods, Host established a related pointwise result in [7], which implies the measure-classification result.

Following Host’s ideas, Meiri defined the following class of sequences.

**Definition 1.** A sequence of integers \( \{a_n : n \in \mathbb{N}\} \) is a \( p \)-Host sequence if, for every Borel probability measure \( \mu \) on \( \mathbb{R}/\mathbb{Z} \) which is invariant under the map \( T_p(x) = p \cdot x \mod (1) \), ergodic, and has positive entropy with respect to \( T_p \), for \( \mu \)-almost every \( x \), the set \( \{a_n x : n \in \mathbb{N}\} \) is equidistributed in \( \mathbb{R}/\mathbb{Z} \).

By this definition, Host’s theorem is essentially the following statement.

**Theorem.** (Host) If \( p \) and \( q \) are co-prime integers, then the sequence \( \{q^n\} \) is a \( p \)-Host sequence.

In [13], Meiri explicitly constructed \( p \)-Host sequences by studying the \( p \)-adic distribution properties of \( p \)-adic analytic functions. As a consequence, he derived a simple way of producing \( p \)-Host sequences via \( p \)-adic interpolation.

**Definition 2.** We say that a sequence of integers \( \{a_n\} \) has \( p \)-adic interpolation if there exists a continuous function \( f(x) \) defined in the unit disc of some finite extension of \( \mathbb{Q}_p \) with \( a_n = f(n) \).

We remark that Lindenstrauss expanded Meiri’s work in [11], and Host has also used \( p \)-adic formalism in [8].

Recently in [3], Bourgain et al gave an effective proof of the Rudolph–Johnson theorem and thus Furstenberg’s Diophantine result, using inequalities regarding linear forms in logarithms to give a quantitative form of the non-lacunarity which occurs in the semigroup \( \langle p, q \rangle \subset \mathbb{N} \).

In this paper we focus on generalizing Furstenberg’s density result, by considering only one-parameter action with some extra sequence which enables us to construct some invariant sets or measures with ‘positive dimensionality’. Afterward, building upon the works by Boshernitzan and Meiri, we use the third sequence to conclude equidistribution or density.

Our first theorem is topological in nature and does not rely on measure-classification techniques.

**Theorem 1.1.** Assume that \( \{a_n\}, \{b_m\} \subset \mathbb{N} \) are increasing sequences satisfying \( \lim_{n \to \infty} a_{n+1}/a_n = 1 \) and \( \lim_{m \to \infty} b_{m+1}/b_m = 1 \), and \( \{c_k\} \) is any unbounded sequence of integers. Then for every irrational \( x \), the set \( \{a_n b_m c_k x : n, m, k \in \mathbb{N}\} \) is dense modulo 1.

The proof of this theorem follows in the spirit of Furstenberg’s own proof; the extra information needed to conclude the theorem relies on a result of Boshernitzan [1].

By combining the approach demonstrated in [3] towards the proof of Furstenberg’s result and the results by Meiri and Lindenstrauss regarding \( q \)-Host sequences, we can deduce the following theorem.

**Theorem 1.2.** Fix \( q \in \mathbb{N} \) and let \( \{a_m : m \in \mathbb{N}\}, \{b_k : k \in \mathbb{N}\} \) be two sequences of integers satisfying the following conditions:
– There exists some prime number $p$ which divides $q$ such that \( \{a_n\} \) admits a smooth $p$-adic interpolation with only finitely many critical points inside the unit disc (positive entropy).

– There exists some prime number $p$ which divides $q$ for which \( \{b_k\} \) admits a smooth $p$-adic interpolation with only finitely many critical points inside the unit disc.

For any other prime $p'$ which divides $q$, either \( \{b_k\} \) admits a smooth $p'$-adic interpolation with only finitely many critical points inside the unit disc or \( \|b_k\|_{p'} \to 0 \), where $\| \cdot \|_{p'}$ stands for the $p'$-adic norm (q-Host).

Then for any $x \in \mathbb{R} \setminus \mathbb{Q}$ the set \( \{q^n a_m b_k x : n, m, k \in \mathbb{N}\} \) is dense in $\mathbb{R}/\mathbb{Z}$.

Various other generalizations of Furstenberg’s result have previously been considered.

Call a sequence of integers \( \{a_n\} \) a universally densifying sequence if for every $\alpha \notin \mathbb{Q}$ the set \( \{a_n \cdot \alpha\} \) is dense modulo 1. A famous theorem of Hardy and Littlewood (generalizing a lemma due to Kronecker) shows that \( \{p(n)\} \) is a universally densifying sequence, where $p(n)$ is any non-constant polynomial with integer coefficients. Furstenberg’s result is equivalent to saying that a sequence of integers forming a non-lacunary multiplicative semigroup is a universally densifying sequence. In [10, Theorem 1.2], Kra proved that coupled sums of products formed from powers of multiplicatively independent integers form a universally densifying sequence, namely sets of the form \( \{\sum_{i=1}^{k} p_i^m q_i^{n_i} \cdot \alpha\} \) are dense modulo 1. Moreover, in [10, Corollary 2.2] Kra proves finer density properties of the sequence of \( \{2^n 3^m \alpha\} \) for irrational number $\alpha$, showing that adding arbitrary shifts depending on $n$ to this sequence results in a dense sequence as well.

In [6], Gorodnik and Kadyrov generalized Kra’s result to higher-dimensional settings. In [16, 17] Urban generalized Kra’s result by considering powers of multiplicatively independent algebraic integers.

Our Theorem 1.2 is used in Corollary 4.10 to provide new classes of universally densifying sequences, e.g. the sequence \( \left\{2^n 3^m : n, m, k \in \mathbb{N}\right\} \), where $p_1, p_2$ are polynomials with integer coefficients, providing examples of very sparse universally densifying sequences. This answers a question by Bugeaud.

2. Proof of Theorem 1.1

We begin the proof with the following easy lemma, essentially due to Furstenberg, which we include for the sake of completeness.

**Lemma 2.1.** Let \( \{a_n : n \in \mathbb{N}\} \subset \mathbb{N} \) be a sequence of increasing integers satisfying \( \lim_{n \to \infty} a_{n+1}/a_n = 1 \), and \( \{d_m : m \in \mathbb{N}\} \subset \mathbb{R}/\mathbb{Z} \) be a sequence such that 0 is a non-isolated point in the closure of \( \{d_m\} \). Then the set \( \{a_n d_m : n, m \in \mathbb{N}\} \) is dense modulo 1.

**Proof.** We show that the sequence is $\varepsilon$-dense, for any $\varepsilon > 0$. By the non-lacunarity of \( \{a_n\} \) there exists some $n_0$ such that for all $n > n_0$, $a_{n+1} - a_n < \varepsilon a_n$. Define $x_0$ to be a point in \( \{d_m\} \cap (0, \varepsilon/a_{n_0+1}) \). Define $S = \{a_{n_0+1}, \ldots, a_m\}$ to be all the elements which
are larger than \(a_{n_0}\) but smaller than \(1/x_0\). For all \(n_0 \leq i \leq m\) we have \(a_{i+1}x_0 - a_ix_0 \leq (a_{i+1} - a_i)x_0 \leq \epsilon a_ix_0\). Hence we deduce that the set \({Sx_0}\) is \(\epsilon\)-dense in \(\mathbb{R}/\mathbb{Z}\). By the choice of \(x_0\), we have that \(a_ix_0 \leq 1\) for any \(a_i \in S\).

**Definition 2.2.** For any sequence \({a_n : n \in \mathbb{N}} \subset \mathbb{N}\), define the exceptional set \(E_{density}(\{a_n\})\) to be all the numbers \(x \in \mathbb{R}/\mathbb{Z}\) so that \({a_n x : n \in \mathbb{N}}\) is not dense modulo 1. For an interval \(I \subset \mathbb{R}/\mathbb{Z}\) define the exceptional set \(E^I_{density}(\{a_n\})\) to be all the numbers \(x \in \mathbb{R}/\mathbb{Z}\) so that \({a_n x : n \in \mathbb{N}} \cap I = \emptyset\).

We recall the definitions of upper box dimension and upper packing dimension which will be used in the following proof.

**Definition 2.3.** (Upper box dimension) Let \(A\) be a non-empty Borel bounded subset of an Euclidean space. Denote by \(N_\delta(A)\) the smallest number of sets of diameter at most \(\delta\) which cover \(E\). We define the upper box dimension as
\[
\overline{\dim_{box}}(E) = \lim_{\delta \to 0} - \frac{\log(N_\delta(E))}{\log(\delta)}.
\]
This dimension is also known as the upper Minkowski dimension.

**Definition 2.4.** (Upper packing dimension) Let \(A\) be a Borel subset of a Euclidean space. We define the upper packing dimension of \(A\) to be
\[
\overline{\dim}_p(A) = \inf \left\{ \sup_{i} \overline{\dim_{box}}(A_i) \mid A = \bigcup_{i=1}^{\infty} A_i, A_i \text{ is bounded} \right\}.
\]

**Remark 2.5.** Obviously, \(\overline{\dim}_p(A) \leq \overline{\dim}_{box}(A)\).

The following result is due to Boshernitzan.

**Theorem 2.6.** [1, Theorem 1.3] If \({b_m : m \in \mathbb{N}}\) is a sequence satisfying \(\lim_{m \to \infty} b_{m+1}/b_m = 1\) then for any open interval \(I \subset \mathbb{R}/\mathbb{Z}\),
\[
\overline{\dim}_{box}E^I_{density}(\{b_m\}) = 0.
\]
As a result one deduces that \(\overline{\dim}_pE_{density}(\{b_m\}) = 0\). We also need the following observation.

**Observation 2.7.** Let \(A\) be a Borel set, and assume that \(\dim_H(A \times A) \geq c\) for some constant \(c\). Then \(\overline{\dim}_p(A) \geq c/2\), where \(\dim_H\) denotes the Hausdorff dimension.

This observation follows from the product properties of the Hausdorff dimension for Borel sets (cf. [12, Theorem 8.10]), namely
\[
\dim_H(A \times B) \leq \dim_H(A) + \overline{\dim}_p(B).
\]

We are now in a position to prove Theorem 1.1.

**Proof of Theorem 1.1.** Let \(x\) be an irrational number. Define the difference set \(D = \{c_k x\} - \{c_k x\}\). Because \(\{c_k : k \in \mathbb{N}\}\) is an unbounded sequence of integers, the difference set \(D\) contains zero as a non-isolated point. By Lemma 2.1, the set \({b_m D : m \in \mathbb{N}}\) is dense modulo 1. By Observation 2.7, the set \({b_m c_k x : m, k \in \mathbb{N}}\) has upper packing dimension larger than \(1/2\), and in particular \(\overline{\dim}_p(\{b_m c_k x : m, k \in \mathbb{N}\}) > 0\). By [1, Theorem 1.3], the closure of \({b_m c_k x}\) contains a point outside the exceptional set \(E_{density}(\{a_n\})\), hence the result follows. 

\[\square\]
3. Construction of a $T_q$-invariant measure with positive entropy

We start with some definitions.

**Definition 3.1.** ($T_q$ map) Given an integer $q$, the $\times q$ map on the torus is defined as

$$T_q(x) = q \cdot x \mod 1.$$ 

For a real number $x$ we denote the distance from $x$ to the nearest integer by $\|x\|$.

**Definition 3.2.** (Combinatorial entropy) Let $\{a_k : k \in \mathbb{N}\}$ be a sequence of integers. For an integer $\ell \in \mathbb{N}$, define $a_{\ell}^{(k)}$ to be $a_k \mod (\ell)$. Define the $\ell^n$ combinatorial entropy of the sequence $\{a_k : k \in \mathbb{N}\}$ by

$$h_{\text{comb}}^{\ell^n}(\{a_k\}) = \frac{\log|\{a_k^{(\ell^n)} : k \in \mathbb{N}\}|}{n}.$$ 

We define the $\ell$-adic combinatorial entropy to be

$$h_{\ell-\text{adic}}(\{a_k\}) = \lim_{n \to \infty} h_{\text{comb}}^{\ell^n}(\{a_k\}),$$

provided this limit exists. Similarly, we define the upper $\ell$-adic combinatorial entropy to be

$$\overline{h}_{\ell-\text{adic}}(\{a_k\}) = \limsup_{n \to \infty} h_{\text{comb}}^{\ell^n}(\{a_k\}).$$

**Definition 3.3.** Let $q$ be an integer. We say that a sequence $\{a_n : n \in \mathbb{N}\}$ has positive local upper $q$-adic combinatorial entropy if for some prime numbers $p$ dividing $q$, we have that $\overline{h}_{p-\text{adic}}(\{a_k\}) > 0$.

The main construction of this paper appears in the following theorem.

**Theorem 3.4.** (Existence of invariant measure) Let $q$ be an integer, $x$ an irrational number, and assume that $\{a_n : n \in \mathbb{N}\} \subset \mathbb{N}$ has positive local upper $q$-adic combinatorial entropy. Then there exists a Borel probability measure $\mu$ on $\mathbb{R}/\mathbb{Z}$ with support contained in $\{q^m a_n x : m, n \in \mathbb{N}\}$ such that $\mu$ is $T_q$-invariant, $T_q$-ergodic, and $h(\mu(T_q)) > 0$.

3.1. Difference sets of Cantor-like sets. We begin with a simple observation.

**Observation 3.5.** The dynamical system $(\mathbb{R}/\mathbb{Z}, T_q)$ is forward expansive, meaning that there exists a constant $c > 0$ so that for any two distinct points $x$, $y$, in some iteration in the future, the orbits are at least $c$ apart, namely there exists $N \geq 0$ so that $d(T^N_q x, T^N_q y) > c$. In particular, for the $T_q$ map one can choose $c = 1/(q + 1)$, as can be seen by representing $x, y \in \mathbb{R}/\mathbb{Z}$ in base $q$.

The main result of this section is the following theorem.

**Proposition 3.6.** Let $x$ be an irrational number, $q$ a fixed integer, and denote by $O$ the orbit closure $[q^m a_n x : m, n \in \mathbb{N}]$. The Minkowski difference $O - O$ contains a point of the form $\ell_n/q^n$ for every $n \in \mathbb{N}$, where $\ell_n \in \{1, \ldots, q^n - 1\}$. Moreover, we have that $\gcd(\ell_n, q)$ is the same for all $n \in \mathbb{N}$, and in particular in the case where $q$ is a prime number, we have that $\gcd(\ell_n, q) = 1$.

Those special rational points will allow us to construct measures with positive entropy. We now recall Schwartzman’s lemma.
Generalizations of Furstenberg’s Diophantine result

LEMMA. (Schwartzman [15]) Let $X$ be a compact metric space. If $T : X \to X$ is a forward-expansive homeomorphism, then $X$ is finite.

Proof of Proposition 3.6. Let $O$ denote the orbit closure of $x$ by the $T_q$ map, namely the set $O = \{T^n_q x \}$ which is infinite by irrationality of $x$, and define the attractor of $O$ to be $O' = \bigcap_{i=0}^{\infty} T_q^i O$. By definition $O'$ is $T_q$-invariant set, and by compactness it is non-empty. Moreover, all the accumulation points of $O$ are contained inside $O'$. We first show that $T_q : O \to O$ is not injective, by showing that the restriction of $T_q$ to $O'$ itself is not injective.

Assume that $T_q : O' \to O'$ is injective. Due to $T_q$-invariance, we have that the restriction of the $T_q$ map to $O'$ is surjective and hence a homeomorphism. By Schwartzman’s lemma $O'$ is a finite set, and as a result contained inside a discrete subgroup of $T$, namely there exists an integer $m$ for which $O' \subset \{ j/m \mid j = 0, \ldots, m - 1 \}$.

Define the thickening of $O'$ to be the union of the intervals $I_{j,\varepsilon}$ for $j = 0, \ldots, m - 1$, where $I_{j/m,\varepsilon} = (j/m - \varepsilon, j/m + \varepsilon)$ for some $\varepsilon < 1/2m(q + 1)$. Because $O'$ is the attractor of the system, there exists some $N_1 \gg 0$ for which $T_q^{N_1} O \subset \bigcup_{j=0}^{m-1} I_{j/m,\varepsilon}$. Fix some $x$ in one of the intervals $I_{j,\varepsilon}$. We have that

$$\text{dist}(T_q x, T_q (j/m)) \le q \text{dist}(x, j/m) \le q\varepsilon < 1/2m,$$

where dist stands for the distance function on the torus, hence we deduce that $T_q x \in I_{T_q(j/m),\varepsilon}$ as the distance from the interval $T_q(j/m)$ to any other interval of the form $I_{j'/m,\varepsilon}$ for any $j'/m \neq T_q(j/m)$ is at least $1/2m$.

Therefore, for any two points $x$, $y$ which belong to the same interval $I_{j/m,\varepsilon}$ we have that $T_q x$, $T_q y$ belong to the interval $I_{T_q(j/m),\varepsilon}$, hence their images are less than $2\varepsilon < 1/(q + 1)$ apart. By repeating the argument, the entire forward orbits of $x$ and $y$ under the $T_q$ map are close, namely $\sup_{n \in \mathbb{N}} \text{dist}(T_q^n x, T_q^n y) < 1/(q + 1)$, which contradicts forward expansiveness of the $T_q$ map on the whole torus.

Thus there exist two points $y_1, y'_1 \in O'$ with $T_q y = T_q y'$ or equivalently, by the definition of the $T_q$ map, $y - y' = \ell_1/q$, for some integer $\ell_1$ with $0 < \ell_1 < q$. Define the sequences of points $y_n = T_q^{-1} y_{n-1}$, $y'_n = T_q^{-1} y'_{n-1}$ so we have $y_n, y'_n \in O'$ for all $n \in \mathbb{N}$ and, moreover, $y_n - y'_n = \ell_n/q^n$ for some $0 < \ell_n < q^n$ as $T_q^n y_n = T_q^n y'_n$ by construction.

Moreover, $\ell_{n-1}/q^{n-1} = q \cdot \ell_n/q^n \mod (1)$ as $T_q(y_n - y'_n) = y_{n-1} - y'_{n-1}$ and by induction we get $\ell_1/q = q^{n-1} \cdot \ell_n/q^n = \ell_n/q \mod (1)$, showing that $\gcd(\ell_n, q) = \gcd(\ell_1, q)$ for all $n \in \mathbb{N}$. □

The proof of Theorem 3.4 is divided into two cases: when $q$ is a prime number, and when $q$ is composite. In §3.2 we prove the theorem for the prime case, and in §3.3 we show the modifications needed in order to handle the composite case.

3.2. Proof of Theorem 3.4: prime case. For the rest of this subsection, fix a prime number $p$ and a sequence $\{a_n : n \in \mathbb{N}\}$ which has positive $p$-adic entropy.

We now utilize the strategy proposed in [3] to produce invariant measures with positive entropy. Define $P_n$ to be the uniform partition of the unit interval into $n$ equally sized sub-intervals.
Observation. If \( p_1, p_2 \) are two atoms of \( P_n \), then \( p_1 - p_2 \) is covered by at most two atoms of \( P_n \).

Define \( \Delta \) to be the difference set \( \mathcal{O} - \mathcal{O} \) where \( \mathcal{O} = \{ T_p^n x : n \in \mathbb{N} \} \) is the forward orbit of \( x \) under \( T_p \). By Proposition 3.6 we can assume that there are sequences of points \( \{x_N\}, \{y_N\} \subseteq \Delta \) so that \( x_N - y_N = \ell_N / p^N \) for all \( n \in \mathbb{N} \). By the construction of those points, \( \gcd(\ell_N, p) = 1 \), hence \( \ell_N \) is invertible modulo \( p^N \). Assume that \( \{a_k : k \in \mathbb{N}\} \) has positive upper \( p \)-adic combinatorial entropy. Then for large enough \( N \), \( \{a_k(p^N) : k \in \mathbb{N}\} \) has more than \( p^{Nc_1} \) distinct elements, for some \( c_1 > 0 \). Hence the sequence \( \{a_k(x_N - y_N) : k \in \mathbb{N}\} \) has at least \( p^{Nc_1} \) distinct values modulo 1.

Denote by \( \Delta_N \) the set of atoms of \( P_{p^N} \) which \( \Delta \) intersects. By the above calculations, \( |\Delta_N| \geq p^{Nc_1} \), because the set \( \{a_k(x_N - y_N)\}_k \) contains at least \( p^{Nc_1} \) of the points \( \{0/p^N, 1/p^N, \ldots, (p^N - 1)/p^N\} \).

Denote by \( A_N \) the set of atoms of \( P_{p^N} \) which contain at least one point from \( \{a_kx_N : k \in \mathbb{N}\} \). Denote by \( B_N \) the set of atoms of \( P_{p^N} \) which contain at least one point from \( \{a_ky_N : k \in \mathbb{N}\} \). Define \( M_N \) to be \( A_N \) if \( |A_N| \geq |B_N| \) and \( B_N \) otherwise. By the observation, \( |M_N| \geq \frac{1}{2} |\Delta_N|^{1/2} \geq \frac{1}{2} p^{(1/2)Nc_2} \), for some \( c_2 > 0 \). Choose distinct points \( z_i \) on the orbit closure of \( \{p^N a_k x : n, k \in \mathbb{N}\} \) which lie in distinct atoms of \( M_N \).

Define the measures

\[
m_N = \frac{1}{|M_N|} \sum_{i=0}^{\lfloor |M_N| - 1 \rfloor} \delta_{z_i},
\]

where \( \delta_{z_i} \) is the unit-mass measure defined at the point \( z_i \).

**Lemma 3.7.** \( H_{m_N}(P_{p^N}) \geq c_2 N \log(p) \).

**Proof.** The proof is by computation

\[
H(m_N, P_{p^N}) = - \sum_{s \text{ is an atom of } P_{p^N}} m_N(s) \log(m_N(s)) = \log(|M_N|).
\]

By the observation from above, we can deduce the bound

\[
\log(|M_N|) \geq c_2 N \log(p).
\]

\( \square \)

Notice that the measure \( m_N \) does not need to be \( T_p \)-invariant.

We apply the following averaging procedure over \( T_p \) in order to achieve \( T_p \)-invariance of a weak-* limit of those measures. Define the \( T_p \) kth-average of \( m_N \) as

\[
m_N^k = \frac{1}{k} \sum_{i=0}^{k-1} (T_p^i) \cdot m_N.
\]

**Lemma 3.8.** For any \( 0 < k < c_2 N \), \( H_{m_N^k}(P_{p^N}) \geq c_3 N \log(p) \) for some constant \( c_3 > 0 \).

**Proof.** By convexity properties of the entropy function we have

\[
H_{m_N^k}(P_{p^N}) \geq \frac{1}{k} \sum_{i=0}^{k-1} H_{T_p^i m_N}(P_{p^N}).
\]
By construction, \( m_N \) is evenly distributed among more than \( p^{c_2 N} \) different atoms of the partition \( P_{p_N} \). Hence, in the worst case, \( T_p \cdot m_N \) is concentrated along \( p^{c_2 N - 1} \) different atoms of the partition \( P_{p_N} \), as \( T_p \) is a \( p \)-to-one map, therefore \( H_{T_p \cdot m_N}(P_{p_N}) \geq (c_2 N - 1) \log(p) \), and similarly \( H_{T_p^i \cdot m_N}(P_{p_N}) \geq (c_2 N - i) \log(p) \) for every \( i = 1, \ldots, k \). Substituting in (3.5) we get

\[
H_{m_N^k}(P_{p_N}) \geq c_2 N \log(p) - \frac{k + 1}{2} \log(p).
\]

As \( k \) was assumed to be smaller than \( c_2 N \), the claim follows.

**Proposition 3.9.** \( m_{\delta}^N \) is almost \( T_p \)-invariant, \( |T \cdot m_{\delta}^N(f) - m_{\delta}^N(f)| = O_f(N^{-\delta}) \), for any continuous function \( f \).

**Proof.** Let \( f \) be a continuous function on \( \mathbb{R}/\mathbb{Z} \). Then

\[
|m_{\delta}^N(f) - T_p \cdot m_{\delta}^N(f)| \leq \frac{1}{N^\delta} \left| \sum_{i=0}^{N^\delta - 1} (T_p^i) \cdot m_N(f) - (T_p^{i+1}) \cdot m_N(f) \right|
\]

\[
= \frac{1}{N^\delta} |m_N(f) - T_p^N \cdot m_N(f)|
\]

\[
\leq \frac{2 \| f \|_\infty}{N^\delta} \rightarrow_{N \to \infty} 0.
\]

We would like to establish a semicontinuity principle for the entropies so that a weak-\( * \) limit of those invariant measures will have positive entropy. Upper semicontinuity of the entropy is known for expansive maps (cf. [18, Theorem 8.2] and the discussion in [4, §9]), but unfortunately the arguments which are given there are applicable only if the limit is taken from a set of \( T \)-invariant measures. The \( T \)-invariance is used to establish a subadditivity argument, and more precisely, the \( T \)-invariance allows one to change the scales in the refinements of the partition in an effortless manner. We show how one can change scales in the situation we consider here.

Define \( \mu \) to be any weak-\( * \) limit of the sequence of probability measures \( \{m_{\delta}^N\} \). Because the measures \( \{m_{\delta}^N\} \) were almost \( T_p \)-invariant, \( \mu \) is \( T_p \)-invariant.

**Lemma 3.10.** (Upper semicontinuity of entropy) Under the previous assumptions, we have

\[
h_{\mu}(T_p) > 0.
\]

**Proof.** As mentioned before, we are adapting the proof given in [4, §9] to the current situation.

\( P_p \) is a generating partition for the system \( (\mathbb{R}/\mathbb{Z}, T_p) \), and its \( N \)th refinement under \( T_p \) is exactly \( P_{p_N} \). By Sinai’s theorem we can compute the entropy in the following way (cf. [4, Lemma 9.1, Proposition 9.2], for related results):

\[
h_{\mu}(T_p) = h_{\mu}(T_p, P_p) = \lim_{N \to \infty} \frac{1}{N} H_{\mu}(P_{p_N}).
\]

By the definition of the Kolmogorov–Sinai entropy, fixing \( \varepsilon > 0 \), for \( N_1 \gg 0 \) we have that

\[
\frac{1}{N_1} H_{\mu}(P_{p_{N_1}}) \leq h_{\mu}(T_p, P_p) + \varepsilon/2.
\]
One would want to compare the entropies $H_{m_N^{N_1}}(P_p^{N_1})$ and $H_{\mu}(P_p^{N_1})$ by weak-* convergence of the atoms in partition $P_p^{N_1}$. But we cannot assume that the atoms of the partition $P_p^{N_1}$ have $\mu$-null boundaries. Instead we will look in the modified partition $x + P_p^{N_1}$, where we translate every atom $p$ of $P_p^{N_1}$ by a generic number $x$ modulo 1. We argue that there exists such $x$ so that the atoms of the partition $x + P_p^{N_1}$ have $\mu$-null boundaries. Otherwise, $\mu$ will have uncountably many atoms, but as a probability measure, the set of atoms of $\mu$ is countable.

Now we claim that the entropies of the partitions $P_p^{N_1}, x + P_p^{N_1}$ are comparable; more precisely,

$$|H_{\nu}(P_p^{N_1}) - H_{\nu}(x + P_p^{N_1})| \leq O(1), \quad (3.9)$$

where $\nu$ is either $\mu$ or $m_N^{N_1}$.

Notice that if a measure $\nu$ is essentially spread uniformly over $p^{H_{\nu}(P)}$ cells in a partition $Q$, where $Q$ is a partition of $[0, 1]$ to equally sized intervals, then by translating with the number $x$ the spreading might change, but in a controllable way. In the worst case, by translating with $x$, we might have that half of the translated atoms lose their mass, and the other half have twice their original mass. Hence

$$H_{\nu}(x + Q) \geq \log(\frac{1}{2}p^{H_{\nu}(Q)}) = H_{\nu}(Q) + \log(\frac{1}{2}). \quad (3.10)$$

By symmetry, we have the inequality

$$H_{\nu}(Q) \geq H_{\nu}(x + Q) + \log(\frac{1}{2}). \quad (3.11)$$

Therefore, we have proved (3.9). By inequality (3.9) we have that

$$\frac{1}{N_1}|H_{\mu}(P_p^{N_1}) - H_{m_N^{N_1}}(P_p^{N_1})| \leq \frac{1}{N_1}|H_{\mu}(x + P_p^{N_1}) - H_{m_N^{N_1}}(x + P_p^{N_1})| + O(1/N_1). \quad (3.12)$$

By weak-* convergence we have that for every atom $p$ of $x + P_p^{N_1}$,

$m_N^{N_1}(p) \rightarrow \mu(p).$

Consequently, for large enough $N$,

$$\frac{1}{N_1}|H_{m_N^{N_1}}(x + P_p^{N_1}) - H_{\mu}(x + P_p^{N_1})| < \varepsilon/2. \quad (3.13)$$

So we have that

$$h_{\mu}(T_p, P_p) \geq \frac{1}{N_1}H_{m_N^{N_1}}(P_p^{N_1}) - \varepsilon - o(1).$$

By subadditivity of the entropy, we have that $H_{m_N^{N_1}}(P_p^{N_1}) \geq H_{m_N^{N_1}}(P_p^{N}) \geq c_3N_1 \log(p)$ for some $c_3 > 0$, as long as $N > N_1$. Hence

$$h_{\mu}(T_p, P_p) \geq c_3 - \varepsilon - o(1),$$

which we can assume is greater than zero for large enough $N$, and $\varepsilon$ small enough. \qed
Notice that this limit measure $\mu$ is not necessarily $T_p$-ergodic, but by taking the ergodic decomposition of $\mu$,

$$\mu = \int \mu^E \, d\mathcal{E},$$

we can find an ergodic component with positive entropy. This completes the proof of Theorem 3.4 in the prime case.

3.3. **Proof of Theorem 3.4: composite case.** The proof of the theorem is very similar to the proof of the prime case. Using Proposition 3.6, we construct two sequences of points \( \{x_n : n \in \mathbb{N}\}, \{y_n : n \in \mathbb{N}\} \subset \mathbb{R}/\mathbb{Z} \) for which the elements of each sequence belong to the orbit closure of $x$ under the $T_q$ map, and satisfy $x_i - y_i = \ell_i/q^i$ for each $i \in \mathbb{N}$ where $\ell_i \in \{1, \ldots, q^i - 1\}$ and $\ell_{i+1} = \ell_i \mod q^i$. By induction we deduce $\gcd(\ell_1, q) = \gcd(\ell_1, q)$; we denote $\gcd(\ell_1, q)$ as $d$. By the congruence properties of the sequence $\{\ell_n : n \in \mathbb{N}\}$, we know that $\gcd(\ell_n/d, p) = 1$ for every prime number $p$ which divides $q$, hence for every given power $p^e$ of $p$ we have $\gcd(\ell_n/d, p^e) = 1$ also. By the Chinese remainder theorem we learn that for each integer $n$, $\ell_n/d$ is an invertible element modulo $q^n$. Therefore, the linear map induced by multiplication by $\ell_n$ on $\mathbb{Z}/q^n\mathbb{Z}$ is at most a 1-to-one map.

Let $\{a_k : k \in \mathbb{N}\}$ be a sequence having $h_p$-adic($\{a_k\}) = c_1 > 0$ for some fixed prime number $p$ which divides $q$. Hence for large $N$, using the Chinese remainder theorem, the reduced sequence $\{a_k^{(q)} : k \in \mathbb{N}\} \subset \mathbb{Z}/q^{N}\mathbb{Z}$ contains at least $p^{Nc_2}$ elements, for some $c_2 > 0$ constant. Therefore, $\ell_N \cdot \{a_k^{(q)} : k \in \mathbb{N}\}$ contains at least $p^{Nc_2}/d$ elements.

Examining the Minkowski difference of the sets $\{a_kx_N : k \in \mathbb{N}\}$, $\{aky_N : k \in \mathbb{N}\}$, we deduce that at least one of those sets, say $\{akx_N : k \in \mathbb{N}\}$, intersects at least $p^{Nc_1}/2d$ atoms of the partition $P_{q^N}$. Define $\{z_n : n \in \mathbb{N}\}$ to be a set of points sampled from $\{akx_N : k \in \mathbb{N}\}$ such that each point lies in a distinct $P_{q^N}$ atom. Defining $m_N$ to be the uniform measure over the set of points $\{z_n : n \in \mathbb{N}\}$, we conclude the following analogue of Lemma 3.7.

**Lemma 3.11.** $H_{m_N}(P_{q^N}) \geq c_2N \log(p) - c_2 \log(d) \geq c_3N \log(p)$.

The rest of the proof is exactly the same as the proof of Theorem 3.4.

4. **Proof of Theorem 1.2**

In this section we will prove Theorem 1.2 by using Meiri’s characterization of $p$-Host sequences.

**Theorem 4.1.** Let $q$ be a fixed integer, $\{a_m : m \in \mathbb{N}\}$ a sequence of integers having positive upper $q$-adic entropy, and let $\{b_k : k \in \mathbb{N}\}$ be a $q$-Host sequence. Then for every $x \in \mathbb{R} \setminus \mathbb{Q}$ we have that the set $\{q^na_mb_kx : n, m \in \mathbb{N}\}$ is dense in $\mathbb{R}/\mathbb{Z}$.

**Proof.** By Theorem 3.4, there exists a Borel probability measure which is $T_q$-invariant and has $\mu$-almost every $y$, the sequence $\{b_ky : k \in \mathbb{N}\}$ is equidistributed in $\mathbb{R}/\mathbb{Z}$ with respect to the Haar measure, and in particular, dense. Approximating such a point with points from $\{q^na_mb_kx : n, m \in \mathbb{N}\}$, we deduce the theorem. \qed

In [13], Meiri proved the following theorem.
THEOREM 4.2. [13, Theorem 3.2] Assume that \( \{a_n : n \in \mathbb{N}\} \) has a smooth \( p \)-adic interpolation by a function \( f \) which has finitely many critical points inside the unit disc. Then \( \{a_n : n \in \mathbb{N}\} \) is a \( p \)-Host sequence. Moreover, assume that \( q \) is a composite integer, and for each prime number \( p \) dividing \( q \) the sequence \( \{a_n : n \in \mathbb{N}\} \) has a smooth \( p \)-adic interpolation by a function \( f \) which has finitely many critical points inside the unit disc. Then \( \{a_n : n \in \mathbb{N}\} \) is a \( q \)-Host sequence.

Lindenstrauss’s subsequent work [11, Theorem 3.2, Examples 3.2, 3.3] generalized the above-mentioned theorem, and in particular relaxed its conditions, requiring only one prime number \( p \) which divides \( q \) for which \( \{a_n\} \) has a smooth \( p \)-adic interpolation in order to conclude that \( \{a_n\} \) is a \( q \)-Host sequence, as long as for any other prime \( p' \) which divides \( q \) either \( \{a_n\} \) admits a smooth \( p' \)-adic interpolation or \( \|a_n\|_{p'} \to 0 \). A prototypical example of the above-mentioned situation is the sequence \( a_n = 2^{n^2} \) and \( q = 6 \), where the sequence is 3-Host but \( \|a_n\|_2 \to 0 \).

Moreover, during the proof of his theorem, Meiri established the following theorem.

THEOREM 4.3. [13, Theorem 3.1] Assume that \( \{a_n : n \in \mathbb{N}\} \) has a smooth \( p \)-adic interpolation by a function \( f \) which has finitely many critical points inside the unit disc. Then \( \overline{\text{radic}}(\{a_n\}) > 0 \).

Combining Meiri’s and Lindenstrauss’s theorems with Theorem 4.1, we deduce the following corollary.

COROLLARY 4.4. Let \( q \) be an integer and let \( \{a_m : m \in \mathbb{N}\}, \{b_k : k \in \mathbb{N}\} \) be two sequences of integers. If for some prime number \( p \) dividing \( q \) the sequence \( \{a_m\} \) admits a smooth \( p \)-adic interpolation with only finitely many critical points inside the unit disc, for some prime number \( p' \) which divides \( q \) the sequence \( \{b_k : k \in \mathbb{N}\} \) admits a smooth \( p' \)-adic interpolation with only finitely many critical points inside the unit disc, and for every other prime \( p' \) which divides \( q \) either \( \{b_k\} \) admits a smooth \( p' \)-adic interpolation with only finitely many critical points inside the unit disc or \( \|b_k\|_{p'} \to 0 \), then for any \( x \in \mathbb{R} \setminus \mathbb{Q} \) the set \( \{q^na_mb_kx : n, m, k \in \mathbb{N}\} \) is dense in \( \mathbb{R}/\mathbb{Z} \).

This concludes the proof of Theorem 1.2.

Definition 4.5. A locally \( p \)-adic analytic function \( f \) is a function defined by power series expansion in some open disc around the origin in a finite extension of \( \mathbb{Q}_p \).

Observation 4.6. By the formal substitution lemma for \( p \)-adic analytic functions (cf. [14, §6.1.5]), one can compose two locally \( p \)-adic analytic functions \( f(x), g(x) \) where \( g(x) \) satisfies \( g(0) = 0 \) and some moderate condition over the growth modulus, and get a locally \( p \)-adic analytic function.

Example 4.7. The sequence \( \{3^n : n \in \mathbb{N}\} \) does not admit a 2-adic interpolation, as the function \( f(x) = 3^x = \exp(x \log(3)) \), where \( \exp \) is the 2-adic exponential, is not a 2-adic analytic function defined on the whole unit disc, as the exponential has radius of convergence equal to \( 2^{-1/2} \) and the function \( \log(1 + x) \) has radius of convergence equals to 1. By examining a modified version of the function, \( f_2(x) = 3^{2-x} \), we see that the function \( f_2 \) is indeed a 2-adic analytic function defined on the whole unit disc, as
val₂(2) = 1, and therefore that \( f \) is a locally 2-adic analytic function. In general, the \( p \)-adic exponential function \( \exp_p \) only converges in the disc \( |z|_p < p^{-1/(p-1)} \); by picking a suitable integer \( k \) for which \( \text{val}_p(k) - 1/(p-1) > 0 \), we can find sub-sequences of ‘exponentially defined’ sequences which admit smooth \( p \)-adic interpolation.

In a similar fashion to the example, in view of Meiri’s and Lindenstrauss’s results, we have the following proposition.

**Proposition 4.8.** Fix an integer \( q \). Assume that a sequence of integers \( \{a_n : n \in \mathbb{N}\} \) is given by the formula \( a_n = f(n) \), where \( f \) is some locally \( p \)-adic analytic function with finitely many critical values inside some disc in \( \mathbb{Q}_p \), for some prime number \( p \) dividing \( q \). Then for a suitable sub-sequence \( \{a_{n_k} : k \in \mathbb{N}\} \subset \{a_n : n \in \mathbb{N}\} \) we have that \( \{a_{n_k} : k \in \mathbb{N}\} \) has positive upper local \( q \)-adic entropy. Moreover, if for any other prime \( p' \) which divides \( q \) either \( \{a_n\} \) admits a smooth interpolation by locally \( p' \)-adic analytic function with finitely many critical values inside some disc in \( \mathbb{Q}_p \) or \( \|a_n\|_{p'} \rightarrow 0 \), then there exists a sub-sequence \( \{a_{n_k} : k \in \mathbb{N}\} \subset \{a_n : n \in \mathbb{N}\} \) which is \( q \)-Host sequence.

**Proof.** Define \( R \) to be the minimal radius of convergence of the function \( f(x) \) from the different radii of convergence of \( f(x) \) for the various prime numbers \( p \) which divide \( q \), in case there is more than one prime \( p \) which divides \( q \) for which \( \{a_n\} \) admits a locally \( p \)-adic analytic interpolating function. Choosing some integer \( S \gg_q R \) (for example, one can take \( S \) to be the radical of \( q \) to the power of \( -\log_p(R) \) where \( p \) is the largest prime dividing \( q \)) and looking at the sub-sequence \( \{a_{S,n} : n \in \mathbb{N}\} \), we deduce that \( f(S \cdot x) \) is a smooth \( p \)-adic interpolation for this sub-sequence, having only finitely many critical points in the unit disc, and by Meiri’s theorem, the sub-sequence \( \{a_{S,n} : n \in \mathbb{N}\} \) has positive upper local \( q \)-adic entropy. Notice that for any distinct primes \( p, p' \) which divide \( q \) we have that \( \text{val}_p(p') = 1 \), therefore moving to such a sub-sequence would indeed result in a smooth \( p \)-adic analytic function with only finitely many critical points in the unit disc for any prime \( p \) for which \( \{a_n\} \) admits such interpolation. If \( \|a_n\|_p \rightarrow 0 \) then obviously \( \|a_{S_n}\|_p \rightarrow 0 \) as well, and Lindenstrauss’s characterization of \( q \)-Host sequence implies that \( \{a_{S_n}\} \) is a \( q \)-Host sequence.

Notice that by the proposition, Corollary 4.4 immediately generalizes to the case where the sequences \( \{a_m : m \in \mathbb{N}\}, \{b_k : k \in \mathbb{N}\} \) are given by interpolation by locally \( p \)-adic analytic functions, as for any \( x \in \mathbb{R} \setminus \mathbb{Q} \) one can consider the subset \( \{q^n a_{S,m} b_{S',k} x : n, m, k \in \mathbb{N}\} \subset \{q^n a_{S,m} b_k x : n, m, k \in \mathbb{N}\} \), where \( S, S' \) are the integers which have been computed in the previous proposition, which is dense by the corollary.

Combining the proposition with the observation regarding the \( p \)-adic substitution lemma, one can deduce the following generalization of Furstenberg’s density result for a sparse sequence.

**Corollary 4.9.** (Sparse density theorem) For any irrational number \( x \in \mathbb{R} \setminus \mathbb{Q} \) and two non-constant polynomials \( p_1(x), p_2(x) \) with integer coefficients, the set

\[
\left\{ 2^n 3^m 3^k \cdot 3^{p_1(m)} \cdot 3^{p_2(k)} x : n, m, k \in \mathbb{N} \right\}
\]

is dense in \( \mathbb{R} / \mathbb{Z} \).
Notice that the number of distinct elements of the sequence \( \left\{ 2^n \cdot 3^{P_1(m)} \cdot 3^{P_2(k)} : n, m, k \in \mathbb{N} \right\} \) which are contained in the interval \([1, N]\) is about the size of \( \log(N) \) multiplied by \( \log(i)(N) \) for some \( i > 1 \), hence we have shown the following result.

**COROLLARY 4.10.** Let \( r : \mathbb{N} \to \mathbb{N} \) be an increasing function, which grows at least like \( \log(i)(N) \) for some \( i > 1 \). Then there exists a sequence \( \{a_n : n \in \mathbb{N}\} \) of integers which satisfy \( |\{a_n\} \cap [1, N]| \leq r(N) \log(N) \) such that for any irrational \( x \in \mathbb{R} \setminus \mathbb{Q} \), the set \( \{a_n x : n \in \mathbb{N}\} \) is dense in \( \mathbb{R}/\mathbb{Z} \).

**Acknowledgements.** The results of this paper were obtained as part of the author’s MSc thesis at the Hebrew University of Jerusalem under the guidance of Professor Elon Lindenstrauss, to whom I am grateful for introducing me to the problem and for many helpful discussions and insights. The author also wishes to thank Uri Shapira and Peter Varju for useful comments about a preliminary version of this paper. The research was supported by ERC grant (AdG Grant 267259) and ISF grant (983/09).

**REFERENCES**

[1] M. D. Boshernitzan. Density modulo 1 of dilations of sublacunary sequences. *Adv. Math.* **108**(1) (1994), 104–117.

[2] M. D. Boshernitzan. Elementary proof of Furstenberg’s Diophantine result. *Proc. Amer. Math. Soc.* **122**(1) (1994), 67–70.

[3] J. Bourgain, E. Lindenstrauss, P. Michel and A. Venkatesh. Some effective results for \( \times a \times b \). *Ergod. Th. & Dynam. Sys.* **29**(6) (2009), 1705–1722.

[4] M. Einsiedler, A. Katok and E. Lindenstrauss. Invariant measures and the set of exceptions to Littlewood’s conjecture. *Ann. of Math.* (2) **164**(2) (2006), 513–560.

[5] H. Furstenberg. Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation. *Math. Syst. Theory* **1** (1967), 1–49.

[6] A. Gorodnik and S. Kadyrov. Algebraic numbers, hyperbolicity, and density modulo one. *J. Number Theory* **132**(11) (2012), 2499–2509.

[7] B. Host. Nombres normaux, entropie, translations. *Israel J. Math.* **91**(1–3) (1995), 419–428.

[8] B. Host. Some results of uniform distribution in the multidimensional torus. *Ergod. Th. & Dynam. Sys.* **20**(02) (2000), 439–452.

[9] A. S. A. Johnson. Measures on the circle invariant under multiplication by a nonlacunary subsemigroup of the integers. *Israel J. Math.* **77**(1–2) (1992), 211–240.

[10] B. Kra. A generalization of Furstenberg’s diophantine theorem. *Proc. Amer. Math. Soc.* **127**(7) (1999), 1951–1956.

[11] E. Lindenstrauss. p-adic foliation and equidistribution. *Israel J. Math.* **122**(1) (2001), 29–42.

[12] P. Mattila. *Geometry of Sets and Measures in Euclidean Spaces: Fractals and Rectifiability* (Cambridge Studies in Advanced Mathematics, 44). Cambridge University Press, Cambridge, 1999.

[13] D. Meiri. Entropy and uniform distribution of orbits in \( \mathbb{T}^d \). *Israel J. Math.* **105** (1998), 155–183.

[14] A. M. Robert. *A Course in p-adic Analysis* (Graduate Texts in Mathematics, 198). Springer, New York, 2000.

[15] S. Schwartzman. On transformation groups. *PhD Thesis*, Yale University, 1952.

[16] R. Urban. Algebraic numbers and density modulo 1. *J. Number Theory* **128**(3) (2008), 645–661.

[17] R. Urban. Sequences of algebraic numbers and density modulo 1. *Publ. Math. Debrecen* **72**(1) (2008), 141–154.

[18] P. Walters. *An Introduction to Ergodic Theory*. Vol. 79. Springer, New York, 2000.